Study on the Security of Payment Products and Systems in the 15 Member States

(Contract No. ETD/2002/B5-3001/C/11)

Internal Market DG

Final Report

Report date: 16th June 2003

Authors:

Tony Hegarty  PwC Luxembourg (Part 1 and Editor)
Eric Verheul  PwC Netherlands (Part 2)
Dirk Steuperaert  PwC Belgium (Part 3)
Georgia Skouma  Bogaert & Vandemeulebroeke (Part 4)

Research:

The PwC eBusiness network, PwC Research Unit (Luxembourg),
Jean Pouit, Frans van Buul, Emese Békéssy, Luc Hendrikx
Foreword

In May 2002, PricewaterhouseCoopers (PwC) was commissioned by DG Internal Market of the European Commission to undertake a “Study on the Security of Payment Products and Systems in the 15 Member States” of the European Union (EU). The PwC offices in Luxembourg, Belgium and the Netherlands collaborated in the study, together with the Belgian law firm of Bogaert and Vandemeulebroeke, and with input from the PwC offices in each member state. The result of this study, which was conducted largely in the second half of 2002, is this report.

There is a widely held perception in the EU and elsewhere that, despite strong growth in e-commerce and especially in e-banking and e-shopping, the general public lacks confidence in the security aspects of conducting transactions electronically, particularly those that involve a payment of some kind, i.e. using Electronic Payment Instruments (EPIs).

This study sets out to establish the levels of confidence that exist across the EU member states, to assess what the security situation is in practice and how such security is really implemented, and finally to what extent users of EPIs are informed and reassured about their security when using EPIs.

To achieve these aims, the PwC approach splits the survey work into four distinct parts:

- Part 1: An overview of the perception of citizens in the EU Member States of the technical security of EPIs.
- Part 2: An overview of the existing and envisaged secure payment solutions, including a technical security assessment and a comparative analysis of that security and the economic feasibility.
- Part 3: An overview on the realisation of security solutions in practice, performed on more than 500 web sites, covering all Member States in the European Union.
- Part 4: Level and quality of information provided to consumers on the technical security solutions in place.

Each part is dealt with in a separate section of this report, and draws its own conclusions from evidence presented. Overall conclusions are drawn and laid out in the section “Key Conclusions” below.

Supporting material, methodological approaches and more advanced technical analyses that lie behind the conclusions are attached to the report in a series of Appendices.

At the end of this report there is a glossary of technical terms, as well as a list of acronyms used in the report.
Key Conclusions

In a Nutshell

- European Union (EU) citizens, especially those who are regular Internet users, show a reasonably high level of Trust in electronic payments, although there still remain significant doubts about security, fraud and privacy threats. The picture is not consistent across the EU: there are significant national and regional variations.

- There exist secure, economically feasible Electronic Payment Instruments (EPIs), with more advanced underlying technology being rolled out in the near future. Electronic banking and online transfers have particularly good levels of security.

- Fraud is clearly present on the Internet, using EPIs as a means to perpetrate that fraud. However, actual fraudulent and criminal activity reported as being directly attributable to the inherent security features of EPIs has been virtually non-existent.

- Consumers are not very well informed at the point of use of the EPI, although banks and merchants generally comply with legislative requirements in this area.

There does appear to be a significant gap between the perception of the security of EPIs, with EU citizens being reasonably confident in systems that show little or no real risk in terms of crime caused by their actual use. The information communicated to users is generally not sufficient to overcome the doubts that hold some (potential) users back, and this would seem to be the easiest area to address in any initiative to improve public confidence in EPIs.
Answers to Five Key Questions

The objectives of the study can be summarised in 5 key questions, and the findings stated as the answers to those same 5 questions:

- What is consumers' real perception about the security of payment instruments?
- Which payments instruments are (or might be) more secure than others and why?
- What is the result of comparing the public perception with the real security situation?
- What security measures are actually implemented in practice (as opposed to the security which is or will shortly be available, but is not yet implemented)?
- How far are the consumers informed about the existing security measures?

What is consumers' real perception about the security of payment instruments?

The level of public confidence in Electronic Payment Instruments in the countries of the EU is generally reasonably high: an indicator devised for this study shows an overall score of 7.08 (maximum 10)\(^1\).

In order to further understand the real perceptions, two additional questions about the perceived lack of confidence and trust of the European public in Electronic Payment Instruments were posed:

To what extent does this perception actually exist in the minds of the citizens, or is it merely media “hype”?

There is indeed a significant ‘hype factor’ in the media presentation of public confidence in EPIs, as opposed to the reality as reflected in the research. This hype factor is, however, not so great that the media coverage is not fundamentally grounded in reality\(^2\).

What are the real concerns of citizens?

The principal negative factors cited by existing EPI users were: Security concerns (30%), Fraud (25%) and (lack of) Privacy (17%), respectively. Amongst non-EPI users, the concerns (negative factors) were almost identical to those amongst EPI users. One might have surmised that the non-users would have higher concern in this area, which would prevent or discourage them from becoming users. It would seem that many EPI users are aware that

---

\(^1\) However this level of confidence is not consistent across the continent: indicator values range from the highest of 8.41 (Finland) to 5.25 (Greece).

\(^2\) Indicators for the Media view, as well as for both existing and original direct research were devised (again maximum 10). For the EU, the Media indicator returns a value of 6.57, whereas the two Direct Indicators return values of 6.93 and 7.37 respectively.
there are risks, but consider that the advantages of online payments outweigh the negative factors.

**Which payments instruments are (or might be) more secure than others and why?**

Purely from a security perspective, electronic banking systems, online bank transfers, SET\(^3\) card payments and electronic payment account systems are the preferred systems. In all but the last case this is due to the usage of 2-factor authentication. The least secure system on this basis is Card Not Present payment over the Internet when no specific means of cardholder authentication are used. This is primarily due to the lack of proper authentication used, which is heavily based on credit card numbers and expiration dates that cannot be considered secrets. In addition, further elements of potential risk are the usage of weak versions of SSL\(^4\) (or no SSL at all), storage of credit card details on the merchant’s server, and inadequate protection of the merchant’s server against hacking, potentially exposing credit card information (credit card numbers and expiration dates).

**What is the result of comparing the public perception with the real security situation?**

Although the public does have reservations about the security of EPIs, the security measures actually used seem to be well established (if still not at the technological leading edge) and inherently secure.

Well established fraud schemes, however, remain in existence and can now make use of newly available communication channels such as the Internet. But even in these cases financial risk for the consumers is very low, and hardly justifies the perception that paying over the Internet is not safe.

When the current efforts of the payment industry to provide more secure cards (chip-cards), as well as some new but cost-efficient control measures (3D Secure or equivalent) are implemented, the perception of unsafe payments over the Internet will have even less justification.

---

\(^3\) Secure Electronic Transaction (see glossary at the end of this report for details)

\(^4\) Please see glossary at the end of this report for definition of terms.
What security measures are actually implemented in practice (as opposed to the security which is or will shortly be available, but is not yet implemented)?

A wide range of payment technologies exists, and more are on the brink of being introduced in the market. However, when looking at the current real world, one observes that payments over the Internet are still an almost exclusive ‘classic credit card’ business, and are almost completely dominant for cross-border payments. Although new, more secure solutions (including those that make credit card usage more secure) are available, "traditional" solutions having a relatively low degree of security are still the most used. Some of the newer solutions, whilst they are technically advanced, have nevertheless found great difficulty in achieving significant market penetration.

How far are the consumers informed about the existing security measures?

The actual levels of security of solutions in use for making payments is not presented very clearly to consumers. The majority of banks and merchants consider that they comply with the general fair trade practices and principles stipulating the timely and accurate communication of comprehensive information to consumers. They also feel that they are proactive enough to implement consumer-friendly approaches in the communication of security-related information before specific problems arise. On the other hand, consumer organisations stress that there are still many issues that remain unclear to consumers regarding e-payments (for instance, liability, role and responsibilities of all parties intervening in an e-transaction if a security threat occurs).

Generally speaking, the quality of information provided to consumers tends to be better when coming from sources such as banks and other financial institutions. Merchants often have less comprehensive information or refer customers to the site of the EPI provider.

---

5 This is far from being uniform in all EU states, e.g. Finland has a very different profile
6 Again this varies greatly from state to state: see individual country analyses in Part 4 of this report
Table of Contents

FOREWORD ................................................................. 2

KEY CONCLUSIONS ............................................................ 3

IN A NUTSHELI ........................................................................ 3

ANSWERS TO FIVE KEY QUESTIONS, ........................................ 4

What is consumers' real perception about the security of payment instruments? ................................................. 4

Which payments instruments are (or might be) more secure than others and why? ............................................. 5

What is the result of comparing the public perception with the real security situation? ....................................... 5

What security measures are actually implemented in practice (as opposed to the security which is or will shortly be available, but is not yet implemented)? ........................................................................................................... 6

How far are the consumers informed about the existing security measures? ......................................................... 6

TABLE OF CONTENTS .......................................................... 7

TABLE OF ILLUSTRATIONS .................................................... 10

1 PART 1: PUBLIC CONFIDENCE ............................................. 12

1.1 OVERVIEW OF THE PERCEPTION OF CITIZENS IN THE EU MEMBER STATES OF THE TECHNICAL SECURITY OF EPIs .................................................. 12

1.2 EXECUTIVE SUMMARY .................................................. 13

1.2.1 To what extent does this perception actually exist in the minds of the citizens, or is merely media “hype”? 14

1.2.2 What are the real concerns of citizens? ........................................................................................................... 14

1.3 BACKGROUND .................................................................. 16

1.4 METHODOLOGY OVERVIEW ......................................... 18

1.5 DETAILED ANALYSIS AT EUROPEAN UNION LEVEL ............ 21

1.5.1 The Big Picture ................................................................ 21

1.5.2 Indicator Values .......................................................... 21

1.5.3 Hype v. Reality ............................................................ 24

1.5.4 Research Indicators ...................................................... 24

1.5.5 EPI Taxonomy ............................................................. 24

1.5.6 Confidence by type of EPI ............................................ 25

1.5.7 Real Concerns ............................................................. 27

2 PART 2: OVERVIEW OF EXISTING AND ENVISAGED SECURE PAYMENT SOLUTIONS .................................................... 33

2.1 AN OVERVIEW OF THE EXISTING AND ENVISAGED SECURE PAYMENT SOLUTIONS, INCLUDING A TECHNICAL SECURITY ASSESSMENT AND A COMPARATIVE ANALYSIS OF THAT SECURITY AND THE ECONOMIC FEASIBILITY .................................. 33

2.2 EXECUTIVE SUMMARY .................................................. 34

2.2.1 Classification ................................................................ 34

2.2.2 Analysis ....................................................................... 34

2.3 INTRODUCTION ............................................................. 36

2.3.1 Objectives and scope .................................................. 36

2.3.2 Outline of this report .................................................... 36

2.4 CLASSIFICATION .......................................................... 37

2.4.1 Pay later, now or before ................................................. 37

2.4.2 Off-line payment instruments ......................................... 37

2.4.3 On-line / electronic payment instruments ........................... 38

2.4.4 Comparative analysis - methodology .............................. 41

2.5 ANALYSIS OF EPIs ....................................................... 47

2.5.1 Payment cards ............................................................ 47

2.5.2 Electronically authorised direct debit .............................. 60

2.5.3 Electronic and mobile banking, on-line bank transfers and Electronic Bill Presentation and Payment .. 67

2.5.4 Centralised account systems ........................................... 75
PART 3: OVERVIEW OF THE REALISATION OF SECURITY SOLUTIONS IN PRACTICE

3.1 AN OVERVIEW OF THE REALISATION OF SECURITY SOLUTIONS IN PRACTICE, PERFORMED ON NO LESS THAN 500 WEBSITES, COVERING ALL MEMBER STATES IN THE EUROPEAN UNION

3.2 EXECUTIVE SUMMARY

3.2.1 Introduction

3.2.2 Electronic Payment Instruments and actual security levels

3.2.3 Acceptance of payment instruments

3.2.4 The actual security solutions used for e-commerce transactions

3.2.5 The actual security solutions used for e-banking

3.2.6 Fraud Statistics

3.2.7 General Conclusion of Part 3

3.3 OBJECTIVES AND SCOPE

3.4 RESULTS OF THE WEBSITE ASSESSMENTS

3.4.1 Introduction

3.4.2 e-commerce

3.4.3 The actual security solutions used for remote e-commerce transactions

3.4.4 e-banking

3.5 FRAUD STATISTICS

3.5.1 Introduction

3.5.2 Fraud Context

3.5.3 Specific definition of “Fraud related to the use of electronic payment instruments”

3.5.4 Information Sources

3.5.5 Fraud Statistics and Other Fraud Related Information

3.5.6 Analysis and Conclusions

PART 4: LEVEL AND QUALITY OF INFORMATION PROVIDED TO CONSUMERS

4.1 LEVEL AND QUALITY OF INFORMATION PROVIDED TO CONSUMERS ON THE TECHNICAL SECURITY SOLUTIONS IN PLACE

4.2 EXECUTIVE SUMMARY

4.2.1 Key findings on the level and quality of information provided by financial institutions

4.2.2 Key findings on the level and quality of information provided by e-merchants

4.2.3 Conclusions

4.3 OBJECTIVES AND WORK SCOPE

4.3.1 Introduction

4.3.2 Objectives

4.3.3 Outline of Methodology

4.3.4 Definitions

4.3.5 Work Scope

4.4 QUANTITATIVE FINDINGS

4.4.1 Security threats subject to information requirements

4.4.2 Conclusions

4.5 QUALITATIVE FINDINGS

4.5.1 Public survey

4.5.2 Analysis of qualitative findings

4.5.3 Recommendations Reflected in Documentation Received from Respondents

4.6 COMPARATIVE ANALYSIS OF THE RESULTS IN THE LIGHT OF THE LEVELS OF PUBLIC CONFIDENCE IN EPS...
Table of Illustrations

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>The value of country confidence indicators</td>
<td>13</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Weighting of Indicators</td>
<td>19</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Interpretation of indicators</td>
<td>20</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Summary of indicator values</td>
<td>21</td>
</tr>
<tr>
<td>Figure 5</td>
<td>EU weighted indicator values</td>
<td>22</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Countries ranked by indicator</td>
<td>22</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Confidence indicators by country</td>
<td>23</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Concerns per user of EPI Class, by country</td>
<td>26</td>
</tr>
<tr>
<td>Figure 9</td>
<td>% of respondents using EPIs</td>
<td>27</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Usage of EPI types</td>
<td>28</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Positive factors of EPIs</td>
<td>29</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Negative factors of EPIs</td>
<td>30</td>
</tr>
<tr>
<td>Figure 13</td>
<td>Concerns of EPI Users and Non-Users</td>
<td>31</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Respondents’ agreement with certain statements</td>
<td>32</td>
</tr>
<tr>
<td>Figure 15</td>
<td>Classification of payment instruments</td>
<td>39</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Payment card model (credit card)</td>
<td>48</td>
</tr>
<tr>
<td>Figure 17</td>
<td>Overview of SET</td>
<td>53</td>
</tr>
<tr>
<td>Figure 18</td>
<td>Working of 3-D Secure</td>
<td>54</td>
</tr>
<tr>
<td>Figure 19</td>
<td>Security of electronic payment card transactions</td>
<td>55</td>
</tr>
<tr>
<td>Figure 20</td>
<td>Direct debit processing</td>
<td>60</td>
</tr>
<tr>
<td>Figure 21</td>
<td>Direct debit through an intermediary</td>
<td>62</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Internet transactions using PayBox</td>
<td>63</td>
</tr>
<tr>
<td>Figure 23</td>
<td>Security of direct debit intermediary systems</td>
<td>64</td>
</tr>
<tr>
<td>Figure 24</td>
<td>Security of e-banking and similar systems</td>
<td>71</td>
</tr>
<tr>
<td>Figure 25</td>
<td>Centralised account system</td>
<td>77</td>
</tr>
<tr>
<td>Figure 26</td>
<td>PayPal registration procedure</td>
<td>79</td>
</tr>
<tr>
<td>Figure 27</td>
<td>PayPal payment process</td>
<td>80</td>
</tr>
<tr>
<td>Figure 28</td>
<td>Security overview of centralised account systems</td>
<td>81</td>
</tr>
<tr>
<td>Figure 29</td>
<td>Value chain of telephony payments</td>
<td>86</td>
</tr>
<tr>
<td>Figure 30</td>
<td>Coinlet value chain</td>
<td>87</td>
</tr>
<tr>
<td>Figure 31</td>
<td>Coinlet communications flow</td>
<td>88</td>
</tr>
<tr>
<td>Figure 32</td>
<td>Security of telephony payments</td>
<td>90</td>
</tr>
<tr>
<td>Figure 33</td>
<td>Electronic payment account</td>
<td>92</td>
</tr>
<tr>
<td>Figure 34</td>
<td>Cartio flow</td>
<td>93</td>
</tr>
<tr>
<td>Figure 35</td>
<td>Security of electronic payment accounts / micro payments</td>
<td>94</td>
</tr>
<tr>
<td>Figure 36</td>
<td>Typical usage of WAP</td>
<td>114</td>
</tr>
<tr>
<td>Figure 37</td>
<td>Gateway not managed by Telco</td>
<td>114</td>
</tr>
<tr>
<td>Figure 38</td>
<td>WAP gateway operation for WTLS/SSL</td>
<td>115</td>
</tr>
<tr>
<td>Figure 39</td>
<td>WAP gateway protocols for WTLS/SSL</td>
<td>115</td>
</tr>
<tr>
<td>Figure 40</td>
<td>TLS tunnelling vs. Direct Access</td>
<td>116</td>
</tr>
<tr>
<td>Figure 41</td>
<td>Server wallet operation</td>
<td>121</td>
</tr>
<tr>
<td>Figure 42</td>
<td>Payment service provider model</td>
<td>123</td>
</tr>
<tr>
<td>Figure 43</td>
<td>PSP flow</td>
<td>124</td>
</tr>
<tr>
<td>Figure 44</td>
<td>Sample spread by country (e-commerce)</td>
<td>132</td>
</tr>
<tr>
<td>Figure 45</td>
<td>Sample spread by country (e-banking)</td>
<td>133</td>
</tr>
<tr>
<td>Figure 46</td>
<td>Sample spread by industry (e-commerce)</td>
<td>133</td>
</tr>
<tr>
<td>Figure 47</td>
<td>Breakdown of payment methods accepted</td>
<td>134</td>
</tr>
<tr>
<td>Figure 48</td>
<td>Pay before products by type</td>
<td>135</td>
</tr>
<tr>
<td>Figure 49</td>
<td>Pay now products by type</td>
<td>135</td>
</tr>
<tr>
<td>Figure 50</td>
<td>Pay later products by type</td>
<td>135</td>
</tr>
<tr>
<td>Figure 51</td>
<td>Analysis by country of payment methods offered</td>
<td>136</td>
</tr>
<tr>
<td>Figure 52</td>
<td>Analysis by country of payment methods offered</td>
<td>137</td>
</tr>
<tr>
<td>Figure 53</td>
<td>Security methods provided</td>
<td>139</td>
</tr>
<tr>
<td>Figure 54</td>
<td>Protection mechanisms by country (e-commerce sites)</td>
<td>140</td>
</tr>
<tr>
<td>Figure 55</td>
<td>Websites protected by SSL</td>
<td>141</td>
</tr>
<tr>
<td>Figure 56</td>
<td>Protection mechanisms by industry (e-commerce sites)</td>
<td>142</td>
</tr>
<tr>
<td>Figure 57</td>
<td>Customer identification on e-commerce websites</td>
<td>143</td>
</tr>
<tr>
<td>Figure 58</td>
<td>Customer identification on e-commerce websites – by country</td>
<td>144</td>
</tr>
<tr>
<td>Figure 59</td>
<td>Customer identification on e-commerce websites – by industry</td>
<td>145</td>
</tr>
</tbody>
</table>
Table of Illustrations

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>Re-establishment of Customer Identification</td>
<td>146</td>
</tr>
<tr>
<td>61</td>
<td>Use of Digital Signatures for Non-repudiation</td>
<td>147</td>
</tr>
<tr>
<td>62</td>
<td>Collectors of Payments Information</td>
<td>148</td>
</tr>
<tr>
<td>63</td>
<td>Collectors of Payments Information — by country</td>
<td>149</td>
</tr>
<tr>
<td>64</td>
<td>Collectors of Payments Information — by industry</td>
<td>150</td>
</tr>
<tr>
<td>65</td>
<td>% of websites disclosing whether information stored</td>
<td>151</td>
</tr>
<tr>
<td>66</td>
<td>% of websites disclosing location of information stored</td>
<td>152</td>
</tr>
<tr>
<td>67</td>
<td>% of e-commerce websites storing credit card numbers — by industry</td>
<td>154</td>
</tr>
<tr>
<td>68</td>
<td>% of e-commerce websites storing certain personal information</td>
<td>155</td>
</tr>
<tr>
<td>69</td>
<td>Disclosure about protection of information stored, EU-level</td>
<td>156</td>
</tr>
<tr>
<td>70</td>
<td>% of websites disclosing of information stored, by country</td>
<td>156</td>
</tr>
<tr>
<td>71</td>
<td>% of websites confirming transactions, EU-level</td>
<td>157</td>
</tr>
<tr>
<td>72</td>
<td>% of websites confirming and allowing review of transactions, EU-level</td>
<td>158</td>
</tr>
<tr>
<td>73</td>
<td>% of websites confirming and allowing review of transactions, by country</td>
<td>159</td>
</tr>
<tr>
<td>74</td>
<td>% of websites confirming and allowing review of transactions, by industry</td>
<td>160</td>
</tr>
<tr>
<td>75</td>
<td>% of e-commerce websites providing recourse assurance, by country</td>
<td>161</td>
</tr>
<tr>
<td>76</td>
<td>% of e-commerce websites providing recourse assurance, by country</td>
<td>162</td>
</tr>
<tr>
<td>77</td>
<td>% of e-commerce websites providing recourse assurance, by country</td>
<td>163</td>
</tr>
<tr>
<td>78</td>
<td>Protection mechanisms for customer information, e-banking, by country</td>
<td>164</td>
</tr>
<tr>
<td>79</td>
<td>% of e-banking websites providing detailed security information, by country</td>
<td>165</td>
</tr>
<tr>
<td>80</td>
<td>% of e-banking websites protected by SSL/TLS, by country</td>
<td>165</td>
</tr>
<tr>
<td>81</td>
<td>Analysis of e-banking websites providing customer profiles, EU-level</td>
<td>167</td>
</tr>
<tr>
<td>82</td>
<td>Processes to set up customer profiles, e-banking, by country</td>
<td>168</td>
</tr>
<tr>
<td>83</td>
<td>% re-establishment of identity, e-banking, by country</td>
<td>169</td>
</tr>
<tr>
<td>84</td>
<td>% of e-commerce websites providing recourse assurance, by country</td>
<td>170</td>
</tr>
<tr>
<td>85</td>
<td>% of e-banking websites disclosing type of information stored, by country</td>
<td>171</td>
</tr>
<tr>
<td>86</td>
<td>% of e-banking websites providing information on where customer info is stored</td>
<td>172</td>
</tr>
<tr>
<td>87</td>
<td>% of e-banking websites possibility to review transactions, EU-level</td>
<td>173</td>
</tr>
<tr>
<td>88</td>
<td>% of e-banking websites providing information on protection of customer data, by country</td>
<td>174</td>
</tr>
<tr>
<td>89</td>
<td>Methods of transaction confirmation, e-banking websites, EU-level</td>
<td>175</td>
</tr>
<tr>
<td>90</td>
<td>Methods of transaction confirmation, e-banking websites, country level</td>
<td>176</td>
</tr>
<tr>
<td>91</td>
<td>Possibility to review and modify transactions, e-banking websites, EU-level</td>
<td>177</td>
</tr>
<tr>
<td>92</td>
<td>% of e-banking websites enabling review and modification prior to authorisation</td>
<td>178</td>
</tr>
<tr>
<td>93</td>
<td>Websites offering recourse confirmation, e-banking websites, country level</td>
<td>179</td>
</tr>
<tr>
<td>94</td>
<td>Dimensions of online fraud</td>
<td>181</td>
</tr>
<tr>
<td>95</td>
<td>Where Internet fraud actually happens</td>
<td>186</td>
</tr>
<tr>
<td>96</td>
<td>Instruments involved in online fraud (%)</td>
<td>186</td>
</tr>
<tr>
<td>97</td>
<td>Credit card fraud by type (%)</td>
<td>187</td>
</tr>
<tr>
<td>98</td>
<td>E-commerce websites, security features</td>
<td>201</td>
</tr>
<tr>
<td>99</td>
<td>E-banking websites, security features</td>
<td>202</td>
</tr>
<tr>
<td>100</td>
<td>% E-commerce websites where security info is easy to find</td>
<td>204</td>
</tr>
<tr>
<td>101</td>
<td>% E-banking websites where security info is easy to find</td>
<td>205</td>
</tr>
<tr>
<td>102</td>
<td>% E-commerce websites with clear info</td>
<td>207</td>
</tr>
<tr>
<td>103</td>
<td>% E-banking websites with clear info</td>
<td>208</td>
</tr>
</tbody>
</table>
1 Part 1: Public Confidence
1.1 Overview of the Perception of Citizens in the EU Member States of the Technical Security of EPIs.
1.2 Executive Summary

Our study shows that the level of public confidence in Electronic Payment Instruments in the countries of the EU is reasonably high: an indicator devised for this study shows an overall score of 7.08 (maximum 10).

<table>
<thead>
<tr>
<th>Country</th>
<th>Overall Confidence Indicator</th>
<th>% Variance from EU average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finland</td>
<td>8.41</td>
<td>18.81</td>
</tr>
<tr>
<td>Netherlands</td>
<td>7.91</td>
<td>11.75</td>
</tr>
<tr>
<td>Sweden</td>
<td>7.79</td>
<td>10.05</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>7.58</td>
<td>7.08</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>7.50</td>
<td>5.95</td>
</tr>
<tr>
<td>Denmark</td>
<td>7.46</td>
<td>5.39</td>
</tr>
<tr>
<td>Germany</td>
<td>7.34</td>
<td>3.69</td>
</tr>
<tr>
<td>Belgium</td>
<td>7.12</td>
<td>0.58</td>
</tr>
<tr>
<td><strong>EU15</strong></td>
<td><strong>7.08</strong></td>
<td><strong>0.00</strong></td>
</tr>
<tr>
<td>France</td>
<td>6.96</td>
<td>-1.68</td>
</tr>
<tr>
<td>Ireland</td>
<td>6.91</td>
<td>-2.38</td>
</tr>
<tr>
<td>Austria</td>
<td>6.66</td>
<td>-5.91</td>
</tr>
<tr>
<td>Italy</td>
<td>6.62</td>
<td>-6.48</td>
</tr>
<tr>
<td>Spain</td>
<td>6.46</td>
<td>-8.74</td>
</tr>
<tr>
<td>Portugal</td>
<td>5.51</td>
<td>-22.16</td>
</tr>
<tr>
<td>Greece</td>
<td>5.25</td>
<td>-25.83</td>
</tr>
</tbody>
</table>

Figure 1 The value of country confidence indicators

However this level of confidence is not consistent across the EU member states: indicator values range from the highest of 8.41 (Finland) to 5.25 (Greece). Generally speaking the ‘northern’ countries show higher levels of confidence than in the south, with Nordic countries having particularly high levels.\(^7\). This is to be expected of course as electronic payments have been used in the Nordic countries for longer, and have a greater market penetration, than elsewhere.

Ten EU countries have an overall confidence indicator within 10% variance of the weighted EU average. Finland Netherlands and Sweden show variance in excess of 10% on the positive side, whilst Greece and Portugal showing variances of more than 20% on the negative side. The level of confidence in Finland, the highest, is 60% higher than in Greece, the lowest in our study.

In order to be able to analyse the levels of public confidence, a survey of media sources and existing public research, as well as significant original research were undertaken. Public research includes national research reports for a given country as well as international reports within which national data can be identified. Direct research included informal focus groups in the different member states, coupled with an online survey covering primarily the more ‘wired’ community. Separate indicators for Media, Direct

\(^7\) See detailed analysis below
Research and Indirect Research were thus devised\(^8\), and the overall confidence indicator is an amalgam of all of these. An extensive bibliography and webography is included in appendix 1.3 to this report.

Two fundamental questions about the perceived lack of trust of the European public in Electronic Payment Instruments are posed in this part of the study:

1.2.1 To what extent does this perception actually exist in the minds of the citizens, or is merely media “hype”?\(^8\)

The Media indicator developed for each country measures the degree of confidence as expressed in the public media of each country, largely derived from press and other media clippings. For the EU as a whole, the Media indicator returns a value of 6.57.

In contrast the two Direct Indicators return values of 6.93 (for the Direct Public research indicator, which measures confidence as expressed in publicly available research reports) and 7.37 (for the Direct Original research indicator, which indicates confidence expressed in original research via focus groups and an online survey).

This indicates that there is indeed a significant ‘hype factor’ in the media presentation of public confidence in EPIs, as opposed to the reality as reflected in the public and original research: the levels of confidence expressed in media sources is significantly lower than found in our research.

This hype factor is, however, not so great that the media coverage can be said to be not fundamentally grounded in reality. Additionally, the overall indicator, based on a weighted average of the individual country values, hides a number of variations in the different states.

1.2.2 What are the real concerns of citizens?\(^9\)

The real concerns of citizens have been largely measured by our online survey, and validated in our virtual focus groups. The online survey was completed by 2386 respondents from the 15 EU Member States. This may be considered as a good sample because it integrates other sources, including virtual focus groups. PwC has a designated e-business network, with a leader and team of correspondents in each of the EU member states. This network of e-business specialists are “on the ground” in each country, with the dedicated task of knowing and understanding e-business technical and social trends in their respective countries on an ongoing basis. The PwC network and its members were not merely reflecting their own personal views of confidence in EPIs, but from their own direct experience in each Member State, their feeling for the views of the general public. In this way ‘soft’ information (subjective impressions, ‘gut feelings’) not readily found in research reports, was assimilated in the study directly from each Member State.

\(^8\) For details of methodology please refer to the methodology overview below, or to Appendix 1 for full details.

\(^9\) To identify the real concerns we rely mainly on our direct research, as generally speaking the media and public research material do not provide the necessary detail. We rely especially on the web survey, which is by its nature a survey of the more ‘wired’ part of the population. For fuller analysis please see below and in Appendix 1.
These sources may be said to be biased in favour of ‘wired’ or technically aware individuals, due to the nature of the target audience. It may also be said that one needs a certain level of technical awareness to be a user of online payments. In any case, 25% of the respondents to the survey had not used EPIs, so we believe that the survey addressed a population that is completely relevant to the study.

Of those who are already users of EPIs, the greatest benefits stated were speed and convenience, as might be expected. The principal negative factors cited by EPI users were Security (30%), Fraud (25%) and (threats to) Privacy (17%), respectively. Amongst non-EPI users, the concerns (negative factors) were almost identical to those amongst EPI users. One might have surmised that the non-users would have higher concern in this area, which would prevent or discourage them from becoming users, but it would seem that many EPI users are aware that there are risks, but nevertheless consider that the advantages of online payments outweigh the negative factors.

Almost twice as many respondents agree that the EU (rather than national governments) should be responsible for building a secure framework for electronic payments (47% vs. 28%), whilst nearly a quarter thought that the law does not protect the consumer adequately.

As to who is perceived as suffering in cases of fraud or other mishaps, 25% of respondents thought that the banks suffered any losses, 10% the merchant, and a very significant 41% thought that the customer was the suffering party.

27% of respondents thought that the security risks of using EPIs were overstated, whilst another 17% said that they would ‘wait and see’ as the risks were too high at this stage, indicating that they thought things would improve.

Only 13% of respondents thought that new entrants to the EPI domain (i.e. new payment services providers or merchants with new payment models) would be more secure than existing ones, implying that there were significant barriers to new (presumably technically advanced) instruments gaining acceptance.
1.3 Background

There is a widely held perception in the EU and elsewhere that the general public lacks confidence in the security aspects of conducting transactions electronically, particularly those that involve a payment of some kind, i.e. using Electronic Payment Instruments (EPIs).

This general perception, often perpetuated in media sensationalism, and sometimes merely anecdotal, needs to be clarified and measured, both on a European level and in each Member State, to determine:

- To what extent this perception actually exists in the minds of the citizens, or is merely media “hype”?
- What are the real concerns of citizens?

In undertaking this study, we have endeavoured to derive a measurement of confidence in EPIs at individual state level, allowing comparison and contrasting between states, as well as allowing the derivation of an overall Euro-indicator of public confidence in EPIs.

The perceptions that people have are not readily measurable or tabulated, unless one understands the language and the cultural milieu in which those people exist. To take this into account we utilised the PwC e-business network to obtain focus-group style input from people on the ground in each member state. The national perceptions are partly reflected in the media of each country, so a media review is a good starting point.

Additionally, previous studies may have been carried out (on a European, national or regional basis) that may shed light on these perceptions, and these need to be taken into account.

The perceptions identified from these two methods can be further refined and more clearly stated by taking input from people directly involved in electronic business in each country, who will have been aware of people’s perceptions over an extended period of time, effectively providing input from virtual “focus groups” that contain representative samples of that state’s population. PwC has a designated e-business leader in each of the EU member states, usually a partner of the firm. This network of e-business specialists are “on the ground” in each country, with the dedicated task of knowing and understanding e-business technical and social trends in their respective countries. The study team took advantage of this ready-made network of correspondents during the course of the study. Each was contacted individually, and asked to take sounding amongst clients and colleagues, effectively forming virtual focus groups, to take the pulse of national attitudes to confidence in EPIs. The input that they thus provided was also fed into the study results.
PwC dedicated research resources have been mobilised to undertake the desk-based and direct research necessary to make the analysis of consumer attitudes to payments systems.

Specific activities undertaken were:

- **Desk-based research of:**
  - Existing surveys (national and international)
  - Press clippings libraries
  - Research from professional research organisations e.g. Datamonitor
  - Websites of e.g. consumer organisations, central banks, pressure groups

- **Direct research:**
  - Scanning PwC knowledge bases
  - Direct–contact survey of consumer organisations
  - Web survey on all PwC member state websites, and Eurochambres site
  - Utilising the PwC network for evidence gathering from small representative samples of people, using e-business leaders in each territory

The results of the two strands of research have been taken into account in compiling national and EU-wide indicators.
1.4 Methodology Overview

The methodology used in this part of the study is detailed in Appendix 1.1: however, a brief overview here is appropriate. Measuring such an intangible thing as “confidence” in any directly comparable way, e.g. the comparison of confidence in EPIs between the citizens of 2 member states is not a straightforward task.

There are a number of disparate information sources to take into account: these information sources can be classified into three groups:

1. **Media Sources**
   - Press Clippings
   - Media Features

2. **Direct Sources (Public)**
   - Research Reports
   - Consumer Organisations

3. **Direct Sources (Original)**
   - Web Survey
   - Focus Groups

The three sets of information, about Europe as a whole can be used to derive three **Indicators of Public Confidence in Electronic Payment Instruments**:

- Media Sources
- Direct Sources (Public)
- Direct Sources (Original)

---

10 A large amount of data for each country has been utilised in compiling these indicators, held in a number of extensive spreadsheets. Some data from Press and Public Sources do not refer directly to the topic of public confidence in EPIs, but rather refer to it in an oblique way whilst addressing other issues. For example, the Bank for International Settlements (BIS) in its “Survey of Electronic Money Developments” makes certain inferred assumptions about public confidence levels in participating countries.
Within each indicator are two weighted components. Each indicator is given a value of between 1 (confidence is extremely low) and 10 (confidence is extremely high). An overall Public Confidence Indicator is derived from the three separate indicators, with weighted values for the three components. The relative weighting of the different components can be seen in the table below:

<table>
<thead>
<tr>
<th>Weighting</th>
<th>Indicator</th>
<th>Media Sources</th>
<th>Direct Sources (Public)</th>
<th>Direct Sources (Original)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Press Clippings</td>
<td></td>
<td>Research Reports</td>
<td>Web Survey</td>
</tr>
<tr>
<td>2</td>
<td>Media Features</td>
<td></td>
<td>Consumer Organisations</td>
<td>Virtual Focus Groups</td>
</tr>
<tr>
<td>2[weight]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3[weight]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5[weight]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2 Weighting of Indicators

Media Sources were given an overall weighting in the overall indicator of 2 (out of 10). Within the Media Sources, Press Clippings and Media Features (e.g. news reports) were balanced 8/2 respectively. Although press clippings services were used in the research, as well as direct reference to national and international publications, we feel that, overall, the direct question of public confidence in the security of EPIs is not really asked in the media. This media evidence is somewhat tangential therefore, and we feel that this justifies the relatively low weighting of 2/10.

Public Direct Sources were given an overall weighting in the overall indicator of 3 (out of 10). Within the Public Direct Sources, Research Reports and Consumer Organisations were balanced 7/3 respectively. The direct relevance of much of this source material suffers from the same lack of focus as the media coverage (although there are exceptions), and this justifies the weighting of 3/10.

Original Direct Sources were given an overall weighting in the overall indicator of 5 (out of 10). Within the Original Direct Sources, the Web Survey and Virtual Focus Groups were balanced 5/5 respectively. These original research findings thus account for 50% of
the weighting of the overall confidence indicator. We feel that this large weighting is justified because these sources are much more targeted on the particular questions to be asked than are the existing research data.

As this part of the study aims to give an “Overview of the Perception of Citizens in the EU Member States of the Technical Security of EPIs” it seems justified to give due importance to the direct voice of the citizen.

The significance of the value of the indicators can be seen in the table below:

<table>
<thead>
<tr>
<th>Confidence Indicator Value</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Perfect public confidence in EPIs of all types, no reservations about their use</td>
</tr>
<tr>
<td>9</td>
<td>Extremely high level of public confidence in EPIs of all types, few reservations about their use</td>
</tr>
<tr>
<td>8</td>
<td>Very high level of public confidence in EPIs of most types, few reservations about their use</td>
</tr>
<tr>
<td>7</td>
<td>High level of public confidence in EPIs of most types, but significant reservations about their use</td>
</tr>
<tr>
<td>6</td>
<td>Reasonable level of public confidence in EPIs, but very significant reservations about their use</td>
</tr>
<tr>
<td>5</td>
<td>Mediocre level of public confidence in EPIs, serious reservations about their use</td>
</tr>
<tr>
<td>&gt;=4</td>
<td>Very poor level of public confidence in EPIs, major reservations about their use</td>
</tr>
</tbody>
</table>

Figure 3 Interpretation of Indicators

The Media Indicator can be compared with the two Direct indicators to answer the first of the fundamental questions posed in the study:

• To what extent does the perception actually exists in the minds of the citizens, or is merely media “hype”?

Of the two Direct indicators, the one from Public sources tends to measure the confidence levels of the general population, whilst the indicator from Original sources targets a more ‘wired’ audience, more likely to have been in a position to use EPIs.

Deeper analysis of the two Direct (Research) indicators can thus be used to answer the second of the fundamental questions posed in the study:

• What are the real concerns of citizens?
1.5 Detailed Analysis at European Union Level

1.5.1 The Big Picture

This section analyses the survey results at EU level, highlighting the similarities and differences on a regional and country-wise basis. For a detailed analysis of each individual member state please refer to Appendix 1.2.

1.5.2 Indicator Values

The table below shows the value of the various confidence indicators, and of all of their component parts described above for each of the EU Member States.

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Austria</th>
<th>Belgium</th>
<th>Denmark</th>
<th>Finland</th>
<th>France</th>
<th>Germany</th>
<th>Greece</th>
<th>Ireland</th>
<th>Italy</th>
<th>Luxembourg</th>
<th>Netherlands</th>
<th>Portugal</th>
<th>Spain</th>
<th>Sweden</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Sources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Press Clippings</td>
<td>7</td>
<td>7</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>8</td>
<td>7</td>
<td>8</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>Media Features</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>6</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>6.80</td>
<td>7.60</td>
<td>8.80</td>
<td>6.00</td>
<td>6.20</td>
<td>5.80</td>
<td>6.80</td>
<td>6.80</td>
<td>8.00</td>
<td>4.80</td>
<td>5.80</td>
<td>8.20</td>
<td>7.20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct Sources (Public)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research Reports</td>
<td>7</td>
<td>8</td>
<td>8</td>
<td>7</td>
<td>7</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>8</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Consumer Organisations</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>8</td>
<td>6</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>6.00</td>
<td>7.00</td>
<td>7.70</td>
<td>8.00</td>
<td>6.70</td>
<td>5.30</td>
<td>6.00</td>
<td>6.70</td>
<td>7.70</td>
<td>7.70</td>
<td>6.00</td>
<td>6.00</td>
<td>8.00</td>
<td>7.70</td>
<td>7.70</td>
</tr>
<tr>
<td>Direct Sources (Original)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Survey</td>
<td>7</td>
<td>7</td>
<td>8</td>
<td>8</td>
<td>7</td>
<td>8</td>
<td>5</td>
<td>8</td>
<td>8</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>8</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>Virtual Focus Groups</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>8</td>
<td>7</td>
<td>8</td>
<td>5</td>
<td>7</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>5</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>7.00</td>
<td>7.00</td>
<td>7.50</td>
<td>8.50</td>
<td>7.50</td>
<td>8.00</td>
<td>5.00</td>
<td>7.50</td>
<td>7.50</td>
<td>8.00</td>
<td>5.50</td>
<td>7.00</td>
<td>7.50</td>
<td>7.50</td>
<td>7.50</td>
</tr>
<tr>
<td>Overall Confidence Indicator</td>
<td>6.66</td>
<td>7.12</td>
<td>7.46</td>
<td>8.41</td>
<td>6.96</td>
<td>7.34</td>
<td>5.25</td>
<td>6.91</td>
<td>6.62</td>
<td>7.58</td>
<td>7.91</td>
<td>5.51</td>
<td>6.46</td>
<td>7.79</td>
<td>7.50</td>
</tr>
</tbody>
</table>

Figure 4 Summary of Indicator Values

From all of these indicators, an EU-level set of indicators is generated. In order to give accurate and relevant indicators, it is necessary to use a weighting factor for each country to reflect the relevant importance of each in the EU context.\(^{11}\)

---

\(^{11}\) The weighting method chosen is based on the methodology employed by the European Commission Directorate General for Economic and Financial Affairs, in particular the Methodology of the Country Weights for Aggregation Purposes. As the use of EPIs indicates making purchases, the “Private Final Consumption Expenditure” weightings are used. Standard weightings are produced for each year, and the 2002 weighting is used here.
The weightings are applied to each of the three sub-indicators as well as to the Overall Confidence Indicator. This gives the following harmonised values (figure 5):

![Figure 5 EU weighted indicator values](image)

Having established values for the indicators at EU level, we can then look at the rankings of the individual member states compared to the overall values (the table in figure 6 is ranked in descending order of Overall Confidence Indicator):

<table>
<thead>
<tr>
<th>Country</th>
<th>Media Sources Indicator</th>
<th>Direct (Public) Indicator</th>
<th>Overall Public Sources Indicator</th>
<th>Direct (Original) Indicator</th>
<th>Overall Confidence Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU15</td>
<td>6.57</td>
<td>6.93</td>
<td>6.78</td>
<td>7.37</td>
<td>7.08</td>
</tr>
</tbody>
</table>

![Figure 6 Countries ranked by indicator.](image)

Within the Overall Confidence Indicator, sub-indicators for Public Sources and Direct Original have been derived, each of which contribute 50% weighting to the Overall Confidence Indicator.
Figure 7 (above) gives a graphical representation of the different indicators by country (with EU-level figures for reference).
1.5.3 **Hype v. Reality**

For the EU, the media indicator returns a value of 6.57, whereas the two Direct Indicators return values of 6.93 and 7.37 respectively. This significantly lower value of the indicator derived from media coverage, especially when compared with the value derived from the original research (7.37) strongly indicates that there is a significant ‘hype factor’ in the media presentation of public confidence in EPIs, as opposed to the reality as reflected in the research, and especially in the direct research undertaken in this study.

The media indicator indicates a confidence level nearly 11% lower than that expressed by the direct research indicator. This “hype factor” is, significant as it is, not so great that the media coverage is not totally disparate from the reality.

Additionally, this average hides a number of variations in the different states, which can be noted in the above tables, and which are examined further in the country analyses in Appendix 1.2 to this report.

1.5.4 **Research Indicators**

For the EU, the Public and Original Research Indicators have values of 6.93 and 7.37 respectively. The Public value of 6.93 would seem to indicate a greater level of confidence than reflected in the media, but the Original figure of 7.37 rates the level of confidence amongst the relatively ‘wired’ part of the population even higher.

Again, this average hides a number of variations in the different states, which can be noted in the above tables, and which are examined further in the country analyses, which can be found in Appendix 1.2.

1.5.5 **EPI Taxonomy**

For the purposes of analysing public confidence in electronic payments, the only payment types specified were “pay before” “pay now” and “pay later”. This simple taxonomy was used in the survey, because it was felt that respondents would be confused by any finer granularity of characterisation. More detailed analysis and taxonomies of different types of EPI may be found in Parts 2 and 3 of this report. Basically, the three categories include the following sub-categories:

- “Pay before” products
  - Wallets (Proton, …)
  - e-wallets
  - Voucher

- “Pay now” products
  - e-banking (funds transfer)
  - direct debit transactions
  - mobile payments
  - micropayments

- “Pay later” products
  - ‘Classic’ Credit card payments
  - ‘Secured’ Credit Card payments (SET and derivatives)
  - Electronic cheque
1.5.6 Confidence by type of EPI

In the analysis of 613 websites in part 3 of this report, and as depicted in figure 47, the most frequently proposed EPIs on European e-commerce websites were “Pay later” products. Indeed, 73% of the whole sample proposed payment with credit cards and/or electronic cheques. “Pay now” products took second place with 55% of the visited European websites allowing e-banking, direct debit transactions and mobile payments. Finally, “Pay before” products were less successful as only 3% of the assessed websites used them.

Amongst the “Pay later” products, classic credit cards were clearly predominant (98%). Direct debit was the first “Pay now” method proposed (82%) followed by e-banking (14%). The most frequent “Pay before” options were the wallets with 50% and e-wallets with 42%.

The levels of acceptance of these classes of EPIs indicated by the above results clearly implies a positive perception of their security (by the very fact of their usage) and it is reasonable to extrapolate that the positive perception of the security correlates with the degree of usage.

This analysis is broadly supported by our survey results, which show actual usage patterns (EU level) of 48% for “Pay Later” products, 40% for “Pay now” products and under 10% for “Pay before” products (see Figure 10 below).

In order to further analyse the levels of confidence expressed in different types of EPI, we have used the ratio between the number of specific concerns cited in our survey for each class of EPI and the number of professed users of that class of EPI as the key indicator\(^{12}\).

Respondents were invited to express specific concerns about usage in practice of classes of EPI: they could state that they had used more than one class of EPI, and could also express multiple concerns.

By dividing the numbers of actual concerns expressed, by the number of actual users of that EPI class as stated in the survey, we arrive at the following ratios:

- Pay before \(\rightarrow\) 2.45
- Pay now \(\rightarrow\) 2.18
- Pay Later \(\rightarrow\) 2.23

This analysis indicates a very similar level of concern (and its corollary, confidence) for each class of EPI. Respondents were slightly more concerned about “Pay before” instruments, and least concerned about “Pay now” instruments. This result supports the view that “Pay before” instruments implicitly reflect a need for greater trust in the EPI than for “Pay now” and “Pay later” instruments.

\(^{12}\) The relevant survey questions were 2a and 2b – please refer to Appendix 1, section 1.1.5.
As with all of the EU-average indicators devised in this study, analysis at national level shows significant differences. Figure 8 (below) tabulates the ratios for each EU state.

<table>
<thead>
<tr>
<th>Country (overall confidence indicator)</th>
<th>Pay Before Products</th>
<th>Pay Now Products</th>
<th>Pay Later Products</th>
<th>Average (weighted by number of users)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Wallets, e-wallets, vouchers ...</td>
<td>e-banking (funds xfer) direct debit transactions mobile payments micro payments ...</td>
<td>‘Classic’ Credit card ‘Secured’ Credit Card (SET and derivatives) Electronic cheque ...</td>
<td></td>
</tr>
<tr>
<td>Netherlands (7.91)</td>
<td>1.87</td>
<td>1.98</td>
<td>0.99</td>
<td>1.46</td>
</tr>
<tr>
<td>Finland (8.41)</td>
<td>1.14</td>
<td>1.43</td>
<td>1.75</td>
<td>1.47</td>
</tr>
<tr>
<td>Austria (6.66)</td>
<td>2.00</td>
<td>1.81</td>
<td>1.78</td>
<td>1.80</td>
</tr>
<tr>
<td>Denmark (7.46)</td>
<td>2.33</td>
<td>2.05</td>
<td>1.68</td>
<td>1.94</td>
</tr>
<tr>
<td>Sweden (7.79)</td>
<td>2.88</td>
<td>2.05</td>
<td>2.14</td>
<td>2.17</td>
</tr>
<tr>
<td>Greece (5.25)</td>
<td>2.00</td>
<td>2.27</td>
<td>2.17</td>
<td>2.20</td>
</tr>
<tr>
<td>Portugal (5.51)</td>
<td>3.00</td>
<td>2.50</td>
<td>1.50</td>
<td>2.20</td>
</tr>
<tr>
<td>Belgium (7.12)</td>
<td>2.37</td>
<td>2.15</td>
<td>2.23</td>
<td>2.22</td>
</tr>
<tr>
<td>EU (7.08)</td>
<td>2.45</td>
<td>2.18</td>
<td>2.23</td>
<td>2.23</td>
</tr>
<tr>
<td>France (6.96)</td>
<td>2.75</td>
<td>2.26</td>
<td>2.26</td>
<td>2.31</td>
</tr>
<tr>
<td>UK (7.50)</td>
<td>2.80</td>
<td>2.32</td>
<td>2.34</td>
<td>2.46</td>
</tr>
<tr>
<td>Spain (6.46)</td>
<td>0.00</td>
<td>2.67</td>
<td>2.33</td>
<td>2.50</td>
</tr>
<tr>
<td>Ireland (6.91)</td>
<td>2.39</td>
<td>2.31</td>
<td>2.82</td>
<td>2.58</td>
</tr>
<tr>
<td>Luxembourg (7.58)</td>
<td>3.08</td>
<td>2.53</td>
<td>2.58</td>
<td>2.64</td>
</tr>
<tr>
<td>Italy (6.62)</td>
<td>2.50</td>
<td>2.75</td>
<td>2.67</td>
<td>2.67</td>
</tr>
<tr>
<td>Germany (7.34)</td>
<td>2.67</td>
<td>3.00</td>
<td>2.73</td>
<td>2.81</td>
</tr>
</tbody>
</table>

Figure 8 Concerns per user of EPI Class, by Country

It can be seen that there is a reasonable inverse correlation\textsuperscript{13} between the overall confidence indicator and the weighted average of concerns per user of EPI class. However, certain countries that have a high value for the overall confidence indicator also exhibit a high level of concern (most notably Germany, Luxembourg, and UK). Clearly the concerns expressed by EPI users shows a high degree of awareness of the (potential) insecurities of EPIs, but are not sufficient to affect the overall confidence level to a high degree in these countries.

Conversely, some countries that have a low value for the overall confidence indicator also show low levels of concern (most notably Greece and Portugal). This perhaps indicates a lack of “informedness” in these countries about the potential insecurities.

\textsuperscript{13} i.e. fewer concerns expressed, on average, the higher the value of the overall confidence indicator.
1.5.7 Real Concerns

1.5.7.1 Research Basis

In assessing the real concerns of citizens it is necessary to look particularly at the original research done for the study, as little previous research has addressed the specific concerns of citizens at national level. Thus the data presented here comes largely from the Direct Sources (Original) Research undertaken in the course of the study, particularly the web survey. We must therefore put a ‘health warning’ on these statistics, as they have been derived primarily from surveying the more ‘wired’ segment of the population.

1.5.7.2 EPI users and non-users

At EU-level, 75% of respondents had used EPIs previously. This division between EPI-users and non EPI-users is used in subsequent analysis.
1.5.7.3 Usage by Class of EPI

As can be seen above in section 1.5.5, for the purposes of analysing public confidence in the security of electronic payments, the only payment types specified were “pay before” “pay now” and “pay later”.

At EU-level, 48% of EPI usage reported was of the “Pay Later” variety, with 40% “Pay Now.” Only 10% of usage was “Pay Before”.

![Usage of EPI Types](image-url)
1.5.7.4 Positive Factors

Figure 11 Positive factors of EPIs

Amongst EPI users, the main positive factors cited were Convenience (46%) and Speed (43%), with Confidence as an explicit factor cited at 11%. These results are hardly surprising as the whole ethos of electronic payments is bound up with speed and convenience.
1.5.7.5 Negative Factors

Principal negative factors cited by EPI users were Security (30%), Fraud (25%) and (threat to) Privacy (17%), respectively. The general security fears and the threat of fraud are not surprising as major negative factors. However the fear of threat to privacy is a more significant factor than might have been anticipated, perhaps indicating a growing awareness of Privacy issues online.

Interestingly, 15% of EPI users cite refund worries as a negative factor, with 5% also aware that the Merchant involved may not be who he appears to be.

Only 4% of EPI users gave “Insufficient Information” as a negative factor, which would seem to support the conclusions of Part 4 of this report.
1.5.7.6 Positive and Negative Factors for non-EPI Users

Amongst non-EPI users, the concerns (negative factors) were almost identical to those amongst EPI users. This comparison can be seen in more detail below (figure 13). This result seems somewhat surprising, as one might expect the non-users to have significantly greater levels of concern than habitual users. It would seem however that EPI users are generally aware of concerns over security, but for them the positive factors outweigh the negative.

Figure 13 Concerns of EPI Users and Non-Users
1.5.7.7 What’s on the Citizens’ Minds?

All respondents were asked to indicate whether they agreed with certain statements related to public confidence in EPIs. The graphic above (figure 14) indicates the percentage of all correspondents agreeing with each statement.

Almost twice as many respondents agree that the EU (rather than national governments) should be responsible for building a secure framework for electronic payments (47% vs. 28%). Nearly a quarter thought that the law does not protect the consumer. As to who suffers in cases of fraud or other mishaps, 25% thought that the banks suffered any consequent losses, 10% the merchant, and a very significant 41% the customer.

27% of respondents thought that the security risks were overstated, whilst another 17% said that they would ‘wait and see’ as the risks were too high at this stage. Only 13% thought that new entrants to the EPI domain would be more secure, implying significant barriers to new (presumably technically advanced) instruments gaining acceptance.
2 Part 2: Overview of Existing and Envisaged Secure Payment Solutions

2.1 An overview of the existing and envisaged secure payment solutions, including a technical security assessment and a comparative analysis of that security and the economic feasibility.
2.2 Executive Summary

2.2.1 Classification

In this part of the study we have developed a taxonomy for Electronic Payment Instruments and Integrated Payment Solutions, which is a refinement of the classical taxonomy consisting of Pay Before, Pay Now and Pay Later systems. This taxonomy is closely related to concepts of existing, off-line payment systems and results in the following seven main Payment Instrument classes:

1. Systems based on payment cards, e.g. usage of a credit card for direct payment to an on-line merchant (known as Card Not Present payment over the Internet) and variants thereof.
2. Systems based on Electronically authorised direct debit, the on-line analogue of an authorisation form signed by a payer, mandating a party to draw money from its account.
3. Electronic and mobile banking, on-line transfers and Electronic Bill Presentment and Payment (EBPP) systems.
4. Centralised account systems, systems that amongst other things feature Person-to-Person payments and that avoid the financial clearing process.
5. Telephony account systems, closely related to (GSM) telephony subscription accounts that enable payment to merchants.
6. Systems based on Electronic payment accounts, micropayments and “cheques”, enabling the payment of small amounts of money, like a few Euro cents, from a consumer to a merchant.
7. Electronic cash and cheques, payments that are not based on an “account” but on digital data with nominal and transferable value.

In our study these classes are further divided into subclasses, which can be seen as abstractions of payment systems actually occurring in practice. We have examined the security properties of each of these seven classes and their subclasses and have also illustrated this with concrete product examples. In addition to the taxonomy, we have examined generic security building blocks that are used within Payment Instruments. An example of such a building block is the Secure Sockets Layer (SSL), the standard web browsing encryption method. For both the seven main Payment Instrument (sub-) classes and the building blocks we have formulated good security practices and some of the shortcomings in implementing those in current practice.

2.2.2 Analysis

We have finally performed a high-level comparative analysis of the security and economic feasibility of the seven main Payment Instrument classes and their subclasses. For this we have first developed a comparison model based on four indicators: “Security risk”, “Usefulness”, “Ease of Obtaining” and “Critical mass”. These assessments deal with what can be accomplished in principle. Consequently, it is not implied that any actual instance of a payment system will automatically have the same assessment as its abstraction.

From this analysis it appears that purely from a security perspective, electronic banking systems, on-line bank transfers, SET card payments and electronic payment account
systems are the preferred systems. In all but the last case this is due to the usage of 2-factor authentication. The least secure system on this basis is Card Not Present payment over the Internet when no specific means of cardholder authentication are used. This is primarily due to the lack of proper authentication used, which is heavily based on credit card numbers and expiration dates that cannot be considered secrets. In addition, further elements of potential risk are the usage of weak versions of SSL (or no SSL at all), storage of credit card details on the merchant’s server, and inadequate protection of the merchant’s server against hacking, potentially exposing credit card information (credit card numbers and expiration dates).

Centralised account systems can in principle support only limited technical security. The reason for this is that the very advantages of these systems (such as easy registration procedures) would be gone if better security measures (such as strong authentication) would be implemented. We remark that of some current implementations of centralised account systems it is debatable if they provide even this limited level of security. Examples of such payment systems are Paypal, Anypay, Billpoint, Moneyzap, C2it, Monneta, e-monee, Web Dollar, Fire Pay, NetTeller, YourTeller. The vast majority of centralised account systems are US-based and only a few, like anypay.com, are European\textsuperscript{14}.

On the analysis of Usefulness, telephony account systems are the highest ranked, although all of the first four categories are rated “good”. On the analysis for Ease of Obtaining, there is a very mixed set of results, with Card Not Present systems scoring highest. On the analysis of critical mass, there is no clear leader: Card Not Present, Once-off cards, e-banking and centralised account systems rank as ‘good’. Our overall economic feasibility analysis shows that one system stands out as the most feasible payment instrument from a combined security and economic perspective: Electronic/mobile banking systems, with a cluster of 7 different (sub) systems close behind.

Please refer to the tables in 2.5.8 for details.

\textsuperscript{14} At the finalisation stages of this report ING bank introduced a new European centralised account system called way2pay (www.way2pay.com).
2.3 Introduction

2.3.1 Objectives and scope
The objectives of this part of the study are to provide an overview of the existing and envisaged secure payment solutions, including a technical security assessment and a comparative analysis of that security and the economic feasibility.

Our scope consisted of:
- Electronic payments systems that are used on the Internet.
- Mobile payment systems.

The following has not been examined in detail or left out of scope at all:
- Traditional electronic payment systems that are used in the real world (debit card transactions, e-purse transactions) have not been examined in detail.
- Non-electronic payment methods that are used for paying on the Internet (e.g. cash-on-delivery, postal order).
- Payment systems used between merchants (accepting payments from consumers) and financial institutions. Of course such systems are a significant chain in Internet payment process but have been left out of scope for three reasons:
  - Such systems are very diverse as they are quite often tailor-made. They consequently also have a proprietary nature quite often.
  - Such systems are generally not considered to be part of Electronic Payment systems on the Internet.
  - Such systems are generally not considered to be the weak link in Internet payment processes.

2.3.2 Outline of this report
Below, we will:
- present our classification of Electronic Payment Instruments (EPIs) and Integrated Payment Solutions and our framework for the comparative analysis which results in seven EPI classes, abstractions of payment systems occurring in practice,
- make a detailed examination of the EPIs, in 7 sections, one for each group of EPIs identified.
- elaborate on our comparative analysis of security and economic feasibility.

In addition, we will distinguish and describe what we term “building blocks”. These are shared notions among the different EPIs. Building blocks are both technologies that are used for a variety of payment systems (SSL, WAP/WLTS, I-mode) or concepts that can be used in the implementation of various payment systems (Wallets and Payment Service Providers). The methodology and literature we used in this part of the study is described in the Appendix of this reported related to part 2 of the study (Appendix 2).
2.4 Classification

2.4.1 Pay later, now or before
A commonly used taxonomy for payment systems consists of

- **Pay later** systems, in which actual payment by the consumer takes place after the transaction, such as credit cards.
- **Pay now** systems, in which payment is immediate, during the transaction. Examples include debit cards.
- **Pay before** systems, in which payment takes place before the transaction, such as prepaid cards.

It turns out that modern developments have created a situation in which this taxonomy needs to be extended to classify all types of electronic payment. One of the main reasons for this is the emergence of Integrated Solutions that often use more basic EPIs as part of their service. Payment is often “chained”, and doesn’t have a clear classification in terms of *later, now, before*.

As an example: GSM phones can be used for electronic payment using premium SMS. How should we classify this? The payment is immediate and irreversible, like a *pay now* system. But the owner may pay phone bills monthly, in which case it seems like a *pay later* system, or have a prepaid phone, in which case it seems like a *pay before* system.

For these reasons, we have adopted for this part a more refined taxonomy, trying to connect concepts of Electronic Payment Instruments with concepts of existing, off-line payment instruments.

2.4.2 Off-line payment instruments
In figure 15 we show both off-line and on-line payment instruments. In this paragraph, we will describe the classification of the off-line instruments, in order to make the connection to on-line instruments in the next paragraph.

The most basic off-line payment instrument is simply cash (bottom left of the diagram). Cash payments may be made by handing over cash to the payee. They can also be made indirectly, in case of a cash-on-delivery payment or a postal money order.

Cashless payments usually involve bank accounts (top left of the diagram). Payments can be made using a payment card (debit or credit). An account holder may write cheques that give the payee permission to draw the specified amount from his account at a later time. Furthermore, an account holder may sign a mandate for direct debit, after which the payee can initiate the transaction. Another possibility is that the account holder orders the bank to transfer money to another account.

Of lesser importance are the non-cash, but also non-banking account payments. In this category falls the electronic purse (the only method that is used *identically* on the Internet and in real life). Gift certificates, vouchers etc. fall under the category of non-banking
prepaid cheques. Money surrogates consist of Airmiles and similar, that are usually obtained in a loyalty program but can be used to (partially) pay goods and services.

2.4.3 On-line / electronic payment instruments

Electronic payment instruments can be divided into two major groups: they may be **account based**, i.e. there is some personal account on which credit is stored and that is accessible only by the owner (like a bank account). Alternatively, the payment instrument may be **payable-to-bearer** in which case ownership is not registered, but is simply defined by being in possession (like in the case of cash or a gift voucher).

Account-based systems can be further divided into systems where a traditional account system is extended to be used on-line (for instance, e-banking with an ordinary bank account), and systems that are dedicated for electronic payment (such as centralised payment systems). These “extended” systems consist of the payment card systems and access based systems. Payment card systems mimic the use of payment cards in an off-line situation. This may be by handling Internet payment like mail- or telephone orders, or by using specific secure protocols. These systems are the examined later in the study.

Access systems let the customer do things that would formerly require sending paper forms to the bank, such as authorising direct debit (see below) and making transfers (see below).

The systems that have non-traditional or dedicated accounts for electronic payment include centralised account systems, telephony based systems (in which the telephony account is used for non-telephony payments) and purely electronic credit accounts. Payable-to-bearer systems are the electronic equivalent of off-line money or cheques. Each of these is examined in detail below.
Figure 15 (above) presents a classification of electronic payment instrument, ordered in two separate ways. In the left hand side of the figure, real-world payment instruments are classified. On the far left, the broad categories are mentioned (bank account based, non-bank account based and cash) and these are connected to specific payment instruments (payment cards, cheques etc.) These real-world payment instruments are connected to similar electronic payment instrument.

Although the comparison of real-world payment instruments with similar electronic payment instruments helps to understand the concept behind these systems, for a detailed analysis another classification is useful. This is a classification based on the principle characteristics of the payment instrument. It starts from the basic distinction between “payable to bearer” and “account-based” systems, and is then refined going to the left until a connection with each of the electronic payment instrument can be made. This classification has also been used to group the electronic payment instruments into sections for this report. The various distinctions that have been made are discussed in detail below.
Furthermore, the figure includes the pay now / later / before classification of the various systems which is still widely in use and has been included in the classification as a reference.

The various payment methods that will be discussed in this report have been summarised in the table below. We have mentioned several examples of brands, and the examples that have been studies in most detail as a representative example for the system.

<table>
<thead>
<tr>
<th>Section</th>
<th>Payment method</th>
<th>Examples of brands</th>
<th>Example studied in detail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 1: Payment cards</strong></td>
<td>MOTO(-like) transactions</td>
<td>Visa, Mastercard, American Express</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Secure card protocols (SET)</td>
<td>Visa, Mastercard</td>
<td>SET, 3-D Secure</td>
</tr>
<tr>
<td></td>
<td>Secure card protocols (3-D Secure, SecureCode UCAF)</td>
<td>American Express, ABN-AMRO</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Once-off cards</td>
<td>American Express</td>
<td>-</td>
</tr>
<tr>
<td><strong>Section 2: Electronically authorised direct debit</strong></td>
<td>Electronically authorised direct debit</td>
<td>Paybox</td>
<td>Paybox</td>
</tr>
<tr>
<td><strong>Section 3: Electronic/mobile banking, on-line bank transfer and EBPP</strong></td>
<td>Electronic/mobile banking</td>
<td>BNP Paribas, Deutsche Bank, Nordea</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>On-line bank transfer</td>
<td>Rabobank, Nordea</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Electronic bill presentment and payment</td>
<td>Nordea, Telefact</td>
<td>-</td>
</tr>
<tr>
<td><strong>Section 4: Centralised account systems</strong></td>
<td>Centralised account systems</td>
<td>Paypal.com, Anypay.com, Billpoint.com</td>
<td>Paypal</td>
</tr>
<tr>
<td><strong>Section 5: Telephony account systems</strong></td>
<td>Telephony account systems</td>
<td>Cointel, Mobile2Meter, Postbank/O2</td>
<td>Cointel, Postbank/O2</td>
</tr>
<tr>
<td><strong>Section 6: Electronic payment account systems</strong></td>
<td>Electronic payment account systems</td>
<td>Cartio, Clickshare</td>
<td>Cartio</td>
</tr>
<tr>
<td><strong>Section 7: Electronic cash and cheques</strong></td>
<td>Electronic prepaid cheques</td>
<td>wwwbon</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Electronic cash</td>
<td>DigiCash, MicroMint, PayWord</td>
<td>-</td>
</tr>
</tbody>
</table>

In this report we will describe the EPIs mentioned above in further detail. Many such EPIs are based on certain building blocks that are non-specific for EPIs. A separate section of this report describes those building block in further detail. For convenience we have briefly summarised the building blocks and some other terms in the table below.
2.4.4 Comparative analysis - methodology

As we have seen, we have developed a taxonomy for Electronic Payment Instruments and Integrated Payment Solutions, which is a refinement of the classical taxonomy consisting of Pay Before, Pay Now and Pay Later systems. This taxonomy is closely related to concepts of existing, off-line payment systems and results in the following seven main Payment Instrument classes:

1. Systems based on payment cards, e.g. usage of a credit card for direct payment to an on-line merchant (known as Card Not Present payment over the Internet) and variants thereof.
2. Systems based on Electronically authorised direct debit, the on-line analogue of a authorisation form signed by a payer, mandating a party to draw money from its account.
3. Electronic and mobile banking, on-line transfers and Electronic Bill Presentment and Payment (EBPP) systems.
4. Centralised account systems, systems that amongst other things feature Person-to-Person payments and that avoid the financial clearing process.
5. Telephony account systems, closely related to (GSM) telephony subscription accounts that enable payment to merchants.
6. Systems based on Electronic payment accounts, micropayments and “cheques”, enabling the payment of small amounts of money, like a few Euro cents, from a consumer to a merchant.
7. Electronic cash and cheques, payments that are not based on an “account” but on digital data with nominal and transferable value.

In order to evaluate these payment systems in a comparative analysis, we have identified four indicators (see definitions below):

- Security risk
- Usefulness
- Ease of Obtaining
- Critical mass.

N.B. The assessment deals with what can be accomplished in principle. Consequently, this does not imply that any actual instance of such a payment system will automatically have the same assessment as it abstraction.

Each of these indicators are evaluated as ++, +, +/-, - or --. The definitions of each of the indicators and the meaning of particular valuations with regard to each indicator are given below. Based on the 4 indicators we calculate an overall score for each payment system, where ++ provides +2 points descending to -- providing –2 points. The evaluation of the indicators will be presented in the “security” “economic feasibility” analysis below.

The results of the overall comparative analysis are presented after the analysis of individual EPIs, in section 2.5.8 of this report.
2.4.4.1 Security Risk

N.B. In all of the subsequent analyses, the use of passwords is recognised as being inherently prone to lax security in actual usage. However, we have not used the use of passwords as a negative security feature as this is not a technical insecurity.

The security risk takes into account both the possibility that a system gets compromised (which is related to technical security) and the amount of money that could be at stake (based on the ranges of use of a payment system). The technical security is determined for a type of payment system as it can be reasonably implemented in principle. Individual implementations may have a higher or lower risk depending on security measures actually in effect. For technical security, we use the following definitions:

<table>
<thead>
<tr>
<th>Technical Security</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>++</td>
<td>Excellent security capable of meeting all security objectives. Will also protect privacy as appropriate.</td>
</tr>
<tr>
<td>+</td>
<td>Good security, for instance protecting against unauthorised transactions with 2 factor authentication.</td>
</tr>
<tr>
<td>+/-</td>
<td>Limited security measures, for instance based on password security.</td>
</tr>
<tr>
<td>-</td>
<td>Technically insufficient security, but with limited possibilities for exploitation of the flaws.</td>
</tr>
<tr>
<td>--</td>
<td>Security is critically flawed.</td>
</tr>
</tbody>
</table>

The typical transaction ranges in electronic payments are defined in the table below:

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micropayments</td>
<td>Less than €2</td>
</tr>
<tr>
<td>Standard payments</td>
<td>Between €2 and €500</td>
</tr>
<tr>
<td>Large payments</td>
<td>More than €500</td>
</tr>
</tbody>
</table>

N.B. The assessment deals with what can be accomplished in principle. Consequently, this does not imply that any actual instance of such a payment system will automatically have the same assessment as it abstraction.
Technical security of a system and its transaction range together determine the security risk, according to the following table. This table relates a given technical security and a certain transaction rate to a **balanced score**. For instance, a system with technically insufficient security (i.e., rated -) that is used for micropayments has a balanced security that is limited (i.e., +/-). Compare the sixth row in the table below.

<table>
<thead>
<tr>
<th>Technical Security</th>
<th>Transaction range</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Micro</td>
</tr>
<tr>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>+/-</td>
<td>+</td>
</tr>
<tr>
<td>-</td>
<td>+/-</td>
</tr>
<tr>
<td>--</td>
<td>-</td>
</tr>
</tbody>
</table>
2.4.4.2 Usefulness

Our definition of usefulness is primarily based on the transaction ranges that are supported by a payment system. Transaction amounts for electronic payments by consumers range from less than a Eurocent to thousands of Euros. Individual payment systems are usually suitable only for parts of this range. The extent of this part is clearly a major factor in determining a system’s usefulness. However, if a payment system is specifically designed for only a limited transaction range, then this is also taken into account.

In addition to the transaction range factor, we have recognised two other usefulness factors. The first of these is whether or not the system supports one consumer paying another (rather than a merchant). This is called Person-to-Person transfer (P2P), and may increase the usefulness of a system. The second additional factor is the ability of the system to handle transactions in real-time, in such a way that payment can be fully integrated with electronic shopping. Most electronic payment systems can do this. If they cannot, this tends to decrease the usefulness of the system.

In order to determine usefulness based on supported transaction ranges, it is necessary to define the various transaction ranges that could be supported by a payment system and to define how supporting each transaction range would contribute to the usefulness of the system. The transaction ranges we use for this analysis are the same that have been defined for the security analysis. The contribution to usefulness of each transaction range should be based on market need for that range. Actual figures on the distribution of electronic transactions would not provide accurate input for a usefulness study, as some of the payments systems are envisioned to open entire new markets (such as micropayments). Therefore, we have determined the following table for usefulness based on the following assumptions:

- There is some need for micropayments in general (e.g. for buying newspaper / magazine articles, downloading logos, ring tones etc.). Although the total volume of payments is not nearly as large as for standard range payments, it is important in niche markets, and opens new markets.
- There is no foreseeable market yet for very small micropayments so far, e.g. less than one Eurocent.

This is further defined in the table below in which ‘X’ means that a payment system supports the specific range. When determining the usefulness of a particular system the score from the table below is either increased or decreased according to the two factors mentioned above, as well as taking into account what transactions the system is aimed at.

<table>
<thead>
<tr>
<th>Applicable Transaction ranges</th>
<th>Usefulness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro Std. Large</td>
<td></td>
</tr>
<tr>
<td>X X X</td>
<td>++</td>
</tr>
<tr>
<td>X X X</td>
<td>+</td>
</tr>
<tr>
<td>X X</td>
<td>+</td>
</tr>
<tr>
<td>X</td>
<td>+/-</td>
</tr>
</tbody>
</table>
2.4.4.3 Ease of obtaining

Ease of obtaining is a measure for the amount of trouble a consumer has to go through before she can start using the product. In assessing this, we assume that the consumer already has the following: a bank account, a cellular phone capable of sending SMS message, the ability to access the Internet and a regular credit card. Using these assumptions, we define the following levels of ease of obtaining:

<table>
<thead>
<tr>
<th>Ease of obtaining</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>++</td>
<td>No trouble at all. This instrument is directly available for the consumer.</td>
</tr>
<tr>
<td>+</td>
<td>Easily obtainable, immediately available after entering some information on a website.</td>
</tr>
<tr>
<td>+/-</td>
<td>Requires the exchange of some paper documents before payments can be made.</td>
</tr>
<tr>
<td>-</td>
<td>Rather difficult to obtain. May require the installation of some specific software. Some consumers won’t succeed.</td>
</tr>
<tr>
<td>--</td>
<td>Very difficult to obtain, infeasible for the regular consumer.</td>
</tr>
</tbody>
</table>
2.4.4.4 Critical mass

Payment systems that are popular with consumers, will become popular with merchants, and payments systems that are used by merchants, attract consumers. In this way, an upward spiral is created. Of course, the reverse is also true. Therefore, the presence of a “critical mass” (the point above which the spiral will be upward) is a factor in determining the feasibility of a payment system. Critical mass is determined by not only by amount of consumer and merchant users, but also by the importance of critical mass to the system, and the compatibility of various implementations of the system. We determine critical mass according to the following definitions:

<table>
<thead>
<tr>
<th>Critical mass</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>++</td>
<td>The majority of consumers and merchants use / accept this system.</td>
</tr>
<tr>
<td>+</td>
<td>A large body of consumers already uses this system, or system is rather insensitive to critical mass considerations.</td>
</tr>
<tr>
<td>+/-</td>
<td>Obtaining critical mass will be one of the major challenges for this system in order to achieve long-term success.</td>
</tr>
<tr>
<td>-</td>
<td>System has entered a downward spiral and obtaining critical mass in the future seems unlikely, or previous attempts to launch the system have failed.</td>
</tr>
<tr>
<td>--</td>
<td>System is no longer in use due to lack of interest.</td>
</tr>
</tbody>
</table>
2.5 Analysis of EPIs

2.5.1 Payment cards

2.5.1.1 Introduction and examples

Payment cards are divided into credit and debit cards. Credit cards are in use since the 1960’s. They offer a cashless payment method that is accepted by a wide range of merchants all over the world. Well-known brands include Visa, MasterCard and American Express. Below, we will describe the traditional mode of operation of credit cards, and new developments relating to Internet.

Credit cards do not draw directly from a bank account, but from an intermediary payment account (this is the source of the credit). In contrast, debit cards draw directly from a bank account. Debit cards are not widely used on the Internet, but are widely used in Europe to pay in stores. There are some initiatives for making debit cards available for use on the Internet.

When used on the Internet, there may be some debate whether debit cards are a payment card EPI or an e-banking EPI. This is caused by the fact that many e-banking systems use the possession of a debit card as an authentication mechanism. When the e-banking system is modified such that the user interface enables “individual transactions” in contrast to a complete login to this system, payment will look and feel like payment card payment, but will technically be an e-banking payment. Examples of such systems are Nordea Solo and Rabobank Direct Betalen. We will discuss these systems below in the section on e-banking, and we will make the distinction between both types more clear.

In this chapter we will only consider those debit card systems that are more or less similar to credit card systems. An example of a debit card system that works like a credit card system is Switch. Like a credit card, Switch allows for payment with card present by using the magnetic stripe, but also allows transaction using a telephone or the Internet. The only difference of the system with respect to credit cards is that the payment is drawn immediately from a payment account. Because of this similarity, we will mainly consider credit card systems in our discussion below.

An example which differs from credit cards to a greater extent is SET Debit. We will discuss this system in the section on SET below.

---

15 Systems based on payment cards, e.g. usage of a credit card for direct payment to an on-line merchant (known as Card Not Present payment over the Internet) and variants thereof.
16 http://www.nordea.fi
17 http://www.rabobank.nl
18 http://www.switch.co.uk
2.5.1.2 Traditional use of credit cards

The credit card system distinguishes between several actors in a credit card transaction:

- The **cardholder** is the person who pays using the credit card.
- The **merchant** is the organisation that accepts the credit card payment.
- The **issuer** is the credit card organisation that has a contract with the cardholder.
- The **acquirer** is the credit card organisation that has a contract with the merchant.
- The **credit card association** licences issuers and acquirers, organises settlement between them. Some credit limit is set (e.g., a monthly threshold) by the issuer or by the acquirer.

The issuer and the acquirer are typically banks. The issuer is the bank providing the credit card to the consumer. In many cases, one bank can act both as an issuer and an acquirer. However, to analyse the payment system, both functions should be distinguished, as they may be different banks.

The relationships between these parties are depicted in Figure 16. For debit cards, the system is similar, but the clearing system is different, and the payment will always need to be authorised by the issuer.

In order to make a payment, the cardholder shows the credit card to the merchant. The merchant will then request authorisation for this transaction from the acquirer. The acquirer will ask the issuer for authorisation, or provide authorisation himself in case of a small amount. If authorisation is granted, the cardholder signs a credit card authorisation receipt. The merchant verifies the signature with the signature on the credit card, and keeps the authorisation receipt. The merchant claims the payment from the acquirer. The acquirer
pays the merchant, and claims from the issuer. The issuer will then charge the cardholder’s account.

In case of a credit card, the account that is charged is not a direct checking or savings account. This implies that some line of credit is involved. This may be either implicit (in case the cardholder should settle his account monthly, and implicit credit is present due to delayed payments) or explicitly (in case the credit card account offers credit to a certain drawing limit).

Principally, this system does not require on-line verification of the cardholder’s balance. However, in order to prevent abuse, some limit is set by the acquiring bank on transactions that may take place without verification. For transactions exceeding this balance, on-line verification will take place over telephone or using an electronic system.

2.5.1.3 Security methods

One of the principle security objectives for a credit card system is to prevent payments with a particular card being made by someone else than the cardholder. This may be especially in the interest of the cardholder, when he is liable for any payment made. In that case, the objective is cardholder authentication. It may also be in the interest of the issuer, acquirer or merchant, when they are liable, in which case there is also an element of non-repudiation, the cardholder being unable to deny that he has authorised a transaction.

In the traditional use of credit cards, both are accomplished by the combination of credit card presence and the signature. Both the presence of the card itself and the verification of the signature provide authentication of the cardholder. The fact that the merchant keeps the signed authorisation provides for non-repudiation.

**MOTO transactions**

Long before the rise of the Internet, there was a need to conduct transactions without the cardholder and the merchant being on the same location. Examples of such transactions are hotel reservations and orders for delivery of goods. Such transactions are called mail order/telephone order, or MOTO transactions. MOTO transactions are examples of a broader class of transactions called Card Not Present (CNP) transactions which we will discuss later. In the case of MOTO transactions, the security methods used in the traditional use of credit cards are of no use, as both the verification of the presence of the card and the verification of the signature require physical presence of the cardholder at the merchant.

- Without any additional security measures, the cardholder is only authenticated by knowledge of the credit card number and expiration date. In order to compensate this lack of authentication additional information is verified such as for example:
  - Name
  - Address
  - Date of birth
  - Possible additional information available on the credit card next to credit card number and expiration date.
These measures on their own do not provide for adequate security and are therefore supplemented with rigorous fraud detection systems. In case the additional information is intercepted, disclosed by the merchant or retrieved from other sources, an attacker may use this information to make payments.

**Card Not Present transactions over the Internet**

When credit cards need to be used on the Internet, the most obvious choice is to simply use the mechanism employed in MOTO transactions leading to the concept of Card Not Present (CNP) transactions over the Internet. In order to prevent interception of the information, the channel between the browser and the web server needs to be secured against two main threats. The first threat is eavesdropping on the connection between the browser and the web server. The second threat is that an attacker tries to mimic a site from a legitimate organisation, enticing users to hand over confidential information. A web server can be protected against these threats using SSL. The cardholder can then verify the identity of the merchant by inspecting (see building blocks):

- the SSL server certificate that is used to establish the secure connection,
- the Certificate Authority that issued this certificate.

Still, this system is not completely secure. The fraud rate for Internet transactions far exceeds that for ordinary credit card transactions. One of the fundamental reasons for this is that one cannot easily stay anonymous in case of a fraudulent ordinary credit card transaction or MOTO transaction. For an ordinary credit card transaction the fraudster needs to be physically present in a store and in a ordinary MOTO transaction the fraudster needs to provide an address to ship goods to. The Internet has changed this situation. Sites that charge for on-line retrievable content, such as software, video, music and graphics are an attractive location to commit fraud, as anonymity can be maintained. It is especially in this sector that fraud rates are soaring. Besides the possibility of fraud, another disadvantage of the system is the need for cardholders to share a lot of information with the merchant, which is both personal and is sufficient to make credit card transactions on behalf of the cardholder on the Internet. In other words, the cardholder needs to trust the merchant for a transaction to correctly happen, which is something that is not always the case.

The disadvantages of CNP/SSL transactions described above have led to the development of several types of secure alternatives providing better cardholder authentication. These include:

- Once-off credit card numbers,
- Secure card protocols, such as
  - Secure Electronic Transactions (SET)
  - 3-D Secure / Verified by Visa
  - MasterCard SecureCode / UCAF

---

19 about.ccbill.com, quoting Meridien Research, Inc., states that of Internet credit card transactions, 10% is fraudulent, whereas real world credit card transactions only have a 1% fraud rate.
Once-off credit card numbers
The idea behind this system is that the credit card issuer provides the cardholder with a new credit card number for each transaction. After one transaction, the issuer marks the number invalid. As additional security measures, the credit card may have an expiry date in the near future, and a particular transaction limit may be set on the once-off credit card. The major advantage of this system is that it does not require any changes at the merchant site, since from a merchant’s perspective, this is a normal credit card transaction. Examples of such systems used in Europe are ABN-AMRO e-wallet and American Express Private Payments / Blue. The ABN-AMRO e-wallet is a generator of once-off credit card numbers in the form of a wallet. (See building blocks.) American Express Private Payments generates once-off credit-card numbers using a chip on the credit card and a PC-based chipcard reader.

Secure Electronic Transaction (SET)
The SET protocol is a strong secure payment protocol developed by Visa and MasterCard. It makes extensive use of public key cryptography to authenticate both cardholders and merchants and to maintain confidentiality of the cardholders’ personal information.

Although its security-technical merits are widely recognised, it has failed to become accepted on a wide scale and is now something of the past. Since the cardholder is identified using a certificate, the cardholder needs some kind of wallet (see building blocks) to store his certificate and the corresponding private key. Originally, this wallet was envisioned to be located on the client’s browser (a client wallet). As implementation of SET in this form proved difficult, attempts have been made to implement it using a server wallet, in which case the cardholder authenticates himself to the wallet server using some other means than public key cryptography.

3-D Secure / Verified by Visa
3-D Secure, or “Verified by Visa”, is a new payment model regulated by Visa International. The 3-D Secure payment model does, contrary to SET, not use public key cryptography for authentication the cardholder. The essence of the system is that the cardholder is authenticated by the issuer before a transaction can take place.

In the 3-D Secure system, a user enters a credit card number if he wants to make a transaction. After entering the number, a pop-up window will be presented that requires authentication. The method of authentication can be chosen by the issuer, and may be a simple password or a stronger method. After successful authentication, the transaction takes place.

---

20 www.abnamro.nl
21 www.americanexpress.com/privatepayments
22 www.setco.org
23 http://www.usa.visa.com/microsites/verified
MasterCard SecureCode / UCAF

MasterCard SecureCode is a payment model designed to use Cardholder authentication data within the credit card payment process, comparable to 3-D Secure. It uses the Universal Cardholder Authentication Field (UCAF) to communicate this information between various parties.

Similarly to 3-D Secure, SecureCode leaves the choice of authentication mechanism open to the Issuer. It may be username / password, but it can also be a challenge / response system using a chip on the credit card.

2.5.1.4 Technical Overview

SET

An outline of the working of SET is shown in Figure 17. SET is a highly complex protocol, and many of the complexities have been left out. The general idea is that the Cardholder digitally signs a request containing both financial information (‘credit card number’) and order information to pay the Merchant. This signed request is sent to the Merchant that transfers it to its (acquiring) Bank and this bank sends it through to the Cardholder’s bank (issuing bank). This bank validates this request by – amongst other things – verifying the digital signature. The issuing bank informs the acquiring bank about the result of this validation and the acquiring banks transfers this result to the merchant. Characteristic of SET is that the merchant cannot read financial info (only the issuing bank can) and that the banks cannot see order information. Furthermore, the following variations are possible:

- The client certificate and cryptographic keys may be located on a separate server (see building blocks – wallets)
- The authorisation process (i.e., ‘can the transaction take place?’) and caption process (execute the transaction) may be split in two rather than having them as a single step.

Although the SET standards describe it as a generic payment card protocol, it is widely considered as a credit card protocol. There are also extensions of SET that allow it to function for debit transactions (SET-debit).

---

24 Dutch payment processor Interpay (http://www.interpay.nl ) has used these extensions to allow SET debit transactions to be cleared through Interpay. To this end, users are required to provide Message Authentication Codes on their payment instructions for which they use the chip on their debit card and a separate, small device with a number Pad that enables communication with that chip. Alternatively, the users can employ a separate challenge-response token issued by the bank. From July 1, 2002 Interpay has stopped the provisioning of SET, and this example is merely meant to illustrate how a SET debit transaction differs from a SET credit transaction.
The Cardholder initiates a transaction, and the Merchant responds with a signed message and certificate. Cardholder authenticates Merchant.

Cardholder sends Payment Instructions (PI) and Order information (OI). Both are signed by Cardholder. PI (containing cc#, exp date) can only be read by the Acquirer, OI can be read by the Merchant.

Merchant sends an authorisation and caption request, containing the PI (which can be decrypted by the acquirer) and a representation of a signature of the OI by both Cardholder and Merchant, which shows agreement but doesn’t disclose the information to the acquirer.

The acquirer responds to the authorisation request (after consulting the issuer) and, because a caption request was included, sends the amount transferred. This message is signed by the acquirer.

**3-D Secure**

The main point of the system is that the issuer (the bank who has provided the consumer with the card in the first place) authenticates the cardholder and then informs the merchant about the result. The issuer can do this, because it has provided the cardholder with means of authentication together with the credit card. This can either be a password, or a hardware token. To summarise, the following steps are taken:

- Consumer initiates transaction with merchant.
- Consumer authenticates to issuer, who informs merchant.
- Merchant then completes transaction with the acquiring bank.

This is described in detail in Figure 18. In this model, we assume that the merchant site will handle the entire process himself. This is not necessarily the case, as payment may take place through a payment proxy or a payment service provider.

Under 3D Secure based systems there exists a liability shift for the consumer (once authenticated, the cardholder is no longer liable for unauthorised transactions) as well as for the merchant (once the cardholder is authenticated, the merchant no longer bears the possible costs of fraud). Whilst these are legal, and not technical issues, they may have a relevant impact on customer confidence and on the economic feasibility (as a driver to reach critical mass).

The SecureCode system will not be discussed in detail here as it is quite similar to 3-D Secure. The most important difference with 3-D Secure is that no direct communication...
between the Cardholder and the Issuer takes place; the Cardholder sends encrypted authentication data to the Merchant that sends through to the Issuing Bank for validation.

![Diagram of 3-D Secure process]

**Figure 18** Working of 3-D Secure
2.5.1.5 Security objectives

Bearing in mind the security objectives model presented above, and the limitations of our scope stated, we can look at the payment card model as shown in Figure 19. The relevant type of information that should be protected is transactional. The information must be protected in transit, and while stored on the merchant’s computer.

![Security of electronic payment card transactions](image)

Based on this analysis, we have the following security objectives:

1. Confidentiality of information in transit.
2. Confidentiality of transaction information while stored on the merchant’s server.
3. Qualified confidentiality of the transaction: ideally, the merchant knows all about the good or service ordered, and is not aware of the payment details (except that payment has been made), and the acquirer only knows about the payment details, but isn’t aware of other transaction details.
4. Cardholder authorisation of the transaction. This includes making sure the cardholder knows the identity of the merchant.
5. Non-repudiation by the cardholder that he ordered the transaction.
2.5.1.6 Best practices

In the best practices section, we describe measures that are generally taken or should be taken in order to meet the security objectives specified above.

CNP transactions over the Internet

A. Adequate use of SSL (see building blocks), in order to protect the confidentiality of information in transit (objective 1), and to enable the cardholder to verify the merchant’s identity by inspecting the merchant identity in the SSL server certificate used and the Certificate Authority that issued the certificate (objective 4).

B. Requesting a lot of additional information apart of card number and expiry date, such as name and address as specified on card and the card verification value (objectives 4, 5).

C. Not storing credit card information on the web/application server, or storing it only for a short while (objective 2).

D. Protecting the web/application server against hacking by firewalls, adequate patching, system hardening (objectives 2, 4).

E. Limiting the maximum transaction amount for Internet transactions (objective 4, mitigating).

F. Not using these transactions for content delivery over Internet, as fraud is more difficult to manage (objective 4, mitigating).

Meeting objective 3 is hard using CNP transactions. In order to accomplish it, merchants could use a payment service provider (PSP) (see the Chapter on PSPs). It may be easier for a consumer to trust a large well-known PSP than some individual web merchant, especially if the PSP has been audited for security and privacy practices. This could be communicated to the consumers using the PSP with a third party statement or seal. Therefore, we also recommend the following best practice:

Merchants should employ well-known PSPs that have been audited for security and privacy practices by an independent third party auditor.

Once-off credit card numbers

Once-off numbers are more secure than ordinary credit card transactions. The best practices for CNP transactions still hold (as merchants aren’t even aware that it’s a once-off number), but the impact of not implementing them fully is reduced (a stolen once-off credit card number is worthless).

In addition to the best practices for CNP transactions mentioned above, the following holds: Using a strong level of authentication (including a “something you own” part like a challenge-response token) for access to the application, which provides new once-off numbers.

SET

A. SET is a protocol which is designed to meet all the security objectives by making extensive use of cryptography. Simply using a correct implementation is therefore the basis of best practice. In addition:
B. Protecting the web/application server against hacking by firewalls, adequate patching, system hardening (objectives 2, 4).
C. Providing strong access control to the SET private keys (objectives 4, 5)

3-D Secure / Verified by Visa / SecureCode
A. Adequate use of SSL (see building blocks), in order to protect the confidentiality of information in transit (objective 1), and to enable the cardholder to verify the merchant’s identity (objective 4).
B. Use of a strong method of authentication by the Issuer (objectives 4, 5).
C. Not storing credit card information on the web/application server, or storing it only for a short while (objective 2).
D. Protecting the web/application server against hacking by firewalls, adequate patching, system hardening (objectives 2, 4).
E. Protecting the authentication server against hacking by firewalls, adequate patching, system hardening (objectives 2, 4).

2.5.1.7 Findings
The extent to which these best practices are in use is highly variable. The most important non-conformities are:
- CNP transactions over the Internet / once-off numbers
  - In some cases, lack of proper authentication
  - Weak versions of SSL in use, or no SSL at all
  - Storage of credit card details on the merchant’s server
  - Inadequate protection of the merchant’s server against hacking whereby retrieving credit card information (credit card numbers and expiration dates)

The last two issues have led to several incidents in which credit card numbers and personal details became available to the intruder.

- SET / 3-D Secure / SecureCode
  - Authentication systems used (username/password) for authorising a transaction (3-D Secure) or obtaining access to private keys (SET) may have inherent weaknesses such as bad choice of password.

2.5.1.8 Analysis of security
All card payment methods support a range of transactions from a few Euros to very large amounts, for which there is a clear need in e-commerce. Payments below a few Euros are not feasible for payment cards, as transaction costs will be too high compared to the transaction amount. As transactions can easily amount to several thousands of Euros, security is obviously important to keep the payment method economically feasible.

2.5.1.8.1 Card Not Present (CNP)
We rate the technical security of Card Not Present payment over the Internet as insufficient as no specific means of cardholder authentication are used. This is primarily due to the lack of proper authentication used heavily based on credit card numbers and expiration dates that cannot be considered secrets. In addition, further elements of potential risk are the
usage of weak versions of SSL (or no SSL at all), storage of credit card details on the merchant’s server, and inadequate protection of the merchant’s server against hacking, potentially exposing credit card information (credit card numbers and expiration dates). The technical security evaluation is therefore (-).

2.5.1.8.2 Secure Electronic Transactions (SET)  
SET has been shown to be technically very secure (see above). The technical security evaluation is therefore (++).

2.5.1.8.3 Once-off Cards  
Once-off cards offer a good level of security. They prevent theft of a credit card number, but they do not provide the same level of privacy protection and non-repudiation as SET does. Therefore, technical security evaluation is (+).

2.5.1.8.4 3-D Secure and SecureCode  
3-D Secure and SecureCode type of systems offer a level of security that is strongly dependent upon the type of authentication chosen by the issuer. For now, it seems that issuers are choosing username / password. In this case, security is improved to a limited extent only. In principle, however, 3-D Secure and SecureCode type of systems can provide good technical security. Therefore technical security evaluation is (+).

2.5.1.9 Analysis of economic feasibility  
Such instruments are useful for both standard and large payments, so for all the usability evaluation is (+).

2.5.1.9.1 Card Not Present (CNP)  
In most areas, CNP payments are acceptable. The critical mass evaluation is therefore (+).

One of the big advantages of CNP payments is that customers don’t need anything new to start paying on the Internet – the same credit card they used in the “real” world is sufficient. The ease of obtaining evaluation is therefore (++).

2.5.1.9.2 Secure Electronic Transactions (SET)  
SET is difficult for cardholders to obtain and use, one reason being the need for specific software. The ease of obtaining evaluation is therefore (-).

SET has not obtained critical mass, as merchants have not adopted it and it is now something of the past. The critical mass evaluation is therefore (+)

2.5.1.9.3 Once-off Cards  
These are relatively easy to obtain. In some cases, the once-off functionality comes with the card (American Express Blue) but in general some exchange of paper documents is required. Therefore the ease of obtaining evaluation is (+/-)
Critical mass is not that important for this system, as merchants don’t need to adopt it. From their perspective, everything seems like an ordinary CNP transaction. Therefore the critical mass evaluation is (+).

2.5.1.9.4 3-D Secure and SecureCode

The registration process can be performed entirely online or it can be a combination of a physical mail out of the password and online registration. In the United States the registration process is often entirely online and involves the cardholder answering a series of security question posed by the card issuer. For this concept to work it is required that the card issuer has access to these security questions / answers. It appears that obtaining such security questions / answers in the United States can be done by the use of so called credit check agencies, companies that are less common in Europe. However, in principle the registration in Europe of 3-D Secure and SecureCode type of systems can be done entirely on-line too, e.g., by the use of information on previous account statements. The ease of obtaining evaluation is (+)

Critical mass is important to these systems, as merchants need to implement it as well. As these systems are rather new, it is at this point unclear whether critical mass will be reached. The critical mass evaluation is (+/-).

The score on combined security and economic feasibility is determined in Section 2.5.8.

2.5.2 Electronically authorised direct debit

2.5.2.1 Introduction and examples

Traditional use of direct debit

Direct debit transfers are very popular in Europe: they made up 25.8% (respectively 27.3%) of all non-cash Euro area payments in 1999 (respectively 2000). Typical areas of application include subscriptions and utility bills. In a direct debit transfer, the payer authorises the payee to draw money from his account, usually by putting a signature on an authorisation form (the mandate). The payee itself initiates the transfer by sending a request to the bank. The bank itself usually does not check the authorisation, but simply executes the order. The direct debit mechanism is illustrated in Figure 20.

Direct debit mandates are available in two forms: the single mandate and the permanent mandate. The single mandate authorises the payee to once draw a specific amount of money from the bank account. The permanent mandate is used for recurring costs such as subscriptions, utility and telephony bills, and authorises the payee to continuously draw “the amount due” from the account.

---

26 Systems based on Electronically authorised direct debit, the on-line analogue of a authorisation form signed by a payer, mandating a party to draw money from its account.

27 See table 13, ECB Blue Book 2002
Depending on local regulation, the payer may be protected in this scheme by being entitled to reverse the transaction after receiving his bank statement within a certain amount of time.\textsuperscript{28}

\textit{Direct debit on Internet}

The popularity of direct debit transfers has led to this method being applied on the Internet. To do this, a few different models have been designed:

- Accepting a single mandate for direct debit through the Internet
- Accepting a permanent mandate (with a real signature) off-line, and giving the customer a username/password to pay on-line
- Direct debit by a third party

The first method is tricky on the Internet, as no real signature is placed. In order to do it properly, electronic signatures are needed. However, the infrastructure to put electronic signatures is not available yet.

The second method is more secure, because a real signature is used and the method isn’t entirely Internet-based. The customer will give a permanent mandate for direct debit to the merchant. The customer then gets an electronic account (username and password) as the merchant’s site. The customer can buy goods using this username and password. The merchant receives payment for the goods by sending a payment requests to the bank.

The third method is more interesting than the first two. The first two methods are not “essentially” electronic: they are simply copies of the existing way direct debits are used, but then using the Internet as a communication medium. On the other hand, the third method is new in the sense that an additional party (the \textit{intermediary}) is introduced. Rather than authorising each merchant for direct debit, only the intermediary is authorised. Merchants receive payments through this intermediary. This is illustrated in Figure 21.

This model has two major advantages over the other ways of using direct debit on the Internet:

- Only one (permanent) mandate is necessary for all payments. This makes it less inconvenient to get an off-line signature for the mandate.
- The model can easily include payments to private persons in addition to payments to Internet merchants. (Person-to-Person payment.)

\textsuperscript{28} For example, in the Netherlands single mandates cannot be reversed, and permanent mandates may be reversed within a period of 35 days.
The most important representative of this model is Paybox\textsuperscript{29}. We will look into the working of Paybox in somewhat more detail in the next section.

2.5.2.2 Technical Overview

Sign-up for Paybox takes place on the website. After signing up, a low payment limit will be assigned, and the customer may choose a 4-digit personal identification number (PIN). Paybox will send an mandate for direct debit form using ordinary mail. The customer must return this form. After verifying the mandate, Paybox will increase the customer’s payment limit. The customer will receive a new PIN to be used in further transactions.

Paybox payment takes place using a GSM phone. Paybox supports two different types of payment:
\begin{itemize}
  \item Internet transactions
  \item “Send money” transactions to other GSM phones.
\end{itemize}

The flow of Internet transactions is illustrated in Figure 22. Essentially, it amounts to the following:
\begin{itemize}
  \item The consumer initiates the transaction with the merchant.
  \item The merchant “redirects” the consumer to Paybox, who authenticates the user.
  \item Paybox then completes the transaction with the bank.
\end{itemize}

One of the most important aspects of the protocol is that confirmation of the transaction takes place using the GSM protocol. Since GSM has a relatively strong authentication using the Secure Identity Module (SIM), and encryption of the data, the resulting level of authentication of the payer is rather strong. We remark that the authentication keys stored in the SIM can be cloned relatively easily, if an attacker has access of the enabled SIM for some time. We also remark that GSM encryption does not specifically protect the integrity

\textsuperscript{29} http://www.paybox.net
of information sent over the radio link. We refer to the building block section on GSM security.

![Diagram of Internet transactions using Paybox]

Transactions to other GSMs rather than merchants follow a similar pattern. The transaction is initiated by the payer calling Paybox over GSM. The payer will then enter the GSM number of the person it wants to transfer money to, and enter the amount. The payer enters its PIN code for authentication. Paybox will send the request to the bank, and confirm the payer and the merchant by SMS or email.

If the payer pays money through Paybox to a person who hasn’t signed up for Paybox yet, this person will still receive an SMS, but the transfer itself will be postponed until this person has signed up.

### 2.5.2.3 Security objectives

We will concentrate our discussion of the security objectives of direct debit systems on systems using an intermediary. This is illustrated in Figure 23. Importantly, there is no real transactional information between the merchant and the intermediary. The actual transaction information is sent between the payer and the intermediary.
In this system, we have the following security objectives:

1. Confidentiality of information in transit between the payer and the intermediary.
2. Confidentiality of transaction information while stored on the intermediary’s server.
3. Confidentiality of information in transit between the intermediary and the merchant.
4. Confidentiality of information stored on the merchant’s server.
5. Account holder authorisation of the transaction. This includes making sure the account holder knows the identity of the merchant and the intermediary.
6. Non-repudiation by the account holder that he ordered the transaction.
7. Integrity of the information transmitted between the intermediary and the merchant.
8. Availability of the intermediary’s site.
9. Qualified confidentiality of the transaction: ideally, the merchant knows all about the good or service ordered, and is not aware of the payment details (except that payment has been made), and the acquirer only knows about the payment details, but isn’t aware of the goods and services ordered.

2.5.2.4 Best practices

In order to meet the security objectives, the following best practices should be followed:

A. Using a secure protocol for the payer/intermediary communication in order to protect the confidentiality of information in transit (objective 1), and to enable the payer to verify the merchant’s and intermediary’s identity (objective 5).
B. Protecting the intermediary’s system against hacking by firewalls, adequate patching, system hardening (objectives 2, 7, 8).
C. Protecting the merchant’s web/application server against hacking (objective 4).
D. Using a strong authentication method to authorise individual transactions (objectives 5, 6). If passwords are used, controls should exist to ensure that these passwords are sufficiently strong.
E. The intermediary obtaining a legally binding signature for the permanent mandate (objectives 5, 6).
F. Using a secure protocol between the intermediary and the merchant, authenticating both parties, preventing eavesdropping and guaranteeing integrity (objectives 1, 3, 7).
G. Having a privacy policy that limits the information shared between the merchant and the intermediary (objective 9).

2.5.2.5 Findings

Looking at Paybox, we see that the fourth best practice mentioned above, strong authentication, is met in an unconventional way: it is realised by the combination of using a GSM phone in combination with a PIN code. The GSM protocol makes it hard to intercept calls or to impersonate another secure identity module (SIM). Additionally, if one loses a GSM, it is possible to have it blocked.

The apparent security flaw of using a weak type of password (a PIN code) is therefore sufficiently compensated by the fact that one also needs to physically possess something (a SIM module), making the overall authentication mechanism strong.

The GSM protocol also assists in implementing objective A. Merchant identity can be verified by Paybox mentioning the merchant’s identity to the user.

A weak point in the Paybox security is the confidentiality of transaction information (best practices A, F) after the transaction has been made. Paybox confirms the transaction using SMS (as secure as GSM voice calls), email (not so secure) or through a specific API (security unknown).

The implementation of many others of the best practices is not easy to verify, especially relating to the API communication between the merchants and Paybox.
2.5.2.6 Analysis of security

There is little to say about the inherent security of a electronically authorised direct debit system, as the way users will perform the authorisation may vary. However, in principle a dual-channel approach consisting of https and GSM can be used (as in Paybox), which makes for a rather secure system. The technical security evaluation is (+).

2.5.2.7 Analysis of economic feasibility

Building on the extensive use of direct debit in Europe, there seems to be a clear case for electronically authorised variants. The transaction range for which people will use the system is probably somewhat smaller than that of credit cards, limited to a few hundred Euros. On the other hand, direct debit is also used for transactions amounting to a few Euros, a range for which payment cards are not very well suited. Electronically authorised direct debit can also be used for Person-to-Person transfers, increasing the usefulness of these systems. The usefulness evaluation is (++).

Ease of obtaining an account is reasonable, although a paper signed mandate should be sent. The ease of obtaining evaluation is (+/-).

Critical mass has not been reached yet, and it is not certain whether it will be. The critical mass evaluation (+/-).\(^{30}\)

The score on combined security and economic feasibility is determined in Section 2.5.8.

---

\(^{30}\) At the finalisation of this report, a Paybox press release states that Paybox discontinues its mobile payment service in the UK, Sweden and Germany; it will only be continued in Austria. See http://www.paybox.net/public_relations_pressrelease_686.html
Electronic and mobile banking, on-line bank transfers and Electronic Bill Presentation and Payment

2.5.2.8 Introduction and examples

On-line alternatives
Bank transfers account for 35.7% (respectively 36.2%) of all non-cash Euro area payments in 1999 (respectively 2000), making it the most popular non-cash payment instrument available. Off-line bank transfers are also used a lot on the Internet, but have some drawbacks. One of which is the long time (a few days up to a week) that bank transfers need to be credited to the beneficiary’s account.

The popularity of bank transfers in combination with problems with using off-line transfers on the Internet, makes it a logical candidate for creating an on-line version. Several models have been developed, including
- Electronic and mobile banking
- Electronic Bill Presentment and Payment (EBPP)
- On-line bank-transfers

Electronic and mobile banking systems offer the possibility of performing banking actions that traditionally require receiving or sending in paper documents, such as receiving a bank statement or sending in a payment order. Additionally, electronic banking systems may offer advanced features, such as scheduled payments, opening up additional (savings) accounts, buying stocks etc. Currently most major banks in Europe offer e-banking systems, such as BNP Paribas in France, Deutsche Bank in Germany, ABN-AMRO in the Netherlands and Nordea in the Nordic countries.

A specific service similar to or part of electronic banking is electronic bill presentment and payment (EBPP). In standard e-banking systems, the payer must enter all the transaction details manually. With EBPP, the transaction details are automatically entered from the electronic bill, and the payer only has to authorise the payment. EBPP is not widely used yet. Some examples include Telecast and Nordea Solo.

Very similar to e-banking is the on-line bank transfer. In an on-line bank transfer, the account holder will be redirected to the bank’s application by the merchant’s site. In this case, the payer instructs the bank to transfer money using the Internet, which is processed immediately (contrary to the off-line bank transfer). A big advantage of this system is that the payee immediately receives the money on his account. However, this is usually only

---

31 Electronic and mobile banking, on-line transfers and Electronic Bill Presentment and Payment (EBPP) systems
32 See table 13, ECB Blue Book 2002
33 www.bnpparibas.com
34 www.deutschebank.de
35 www.abnamro.nl
36 www.nordea.com
37 www.telefact.fr
38 www.nordea.fi
possible if both the payer and the payee have an account at the same bank. Examples of such systems are Rabo Direct Betalen\textsuperscript{39} and, again, Nordea Solo.

As electronic banking, EBPP and on-line bank transfers use common technology, we discuss them together in this chapter. In this section, we will identify the various channels through which these payment instruments operate. In the next section, we will have a more detailed look on the authentication methods used for these systems.

Channels
Electronic banking and on-line transfers may take place over a number of different access channels. These include:

Voice-telephony
This is the oldest method, but still in use. Account holders have an ordinary telephone call with either the bank’s computer, entering data using the telephone keypad, or with an operator.

Direct dial up by modem
As PC’s gained popularity and modems were commonly held by consumers in order to access the Internet, banks wrote e-banking applications that ran on the account holders computer and contacted the bank by making a modem call. At the time, it was considered more secure and cheaper than having such a system over the Internet, but currently, these systems are losing ground.

Internet
The modem system had a number of disadvantages: client software is required, and therefore access can only take place from a single PC and a modem is required whereas consumers are migrating to a variety broadband systems for accessing the Internet rather than using traditional modems. As a result, banks developed Internet sites for e-banking to replace the client-side e-banking applications.

GSM/SMS
The advent of GSM phones made it inevitable for banks to develop mobile banking systems (M-banking). Although the voice-telephony technique can be used on a GSM, there are some additional possibilities: the security features of the SIM can be used to perform authentication, and SMS may be used to transfer information between the account holder and the bank.

I-mode and WAP
I-mode and WAP are emerging mobile techniques that provide Internet-like functionality on an advanced cellular phone. Banks are starting to develop e-banking applications for these channels, but such applications aren’t commonplace yet.

\textsuperscript{39} www.rabobank.nl
2.5.2.9  Technical Overview

Electronic Banking Systems
The single most interesting aspect of the working of electronic banking systems is the way authentication of the account holder is performed. Apart from this, they are computer applications directly linked to the bank’s central computers. Other account systems (like the centralised account systems and telephony account systems that will be discussed later) are typically not directly linked to a bank’s central computer, implying that payment from financial institutions to these systems can only be done in an indirect manner.

Therefore, after discussing EBPP and on-line transfers, we will focus on authentication methods in our discussion of the working of these systems.

EBPP
In our discussion of the working of EBPP systems we can be brief. The provider of the EBPP system may either be a bank or a third party. In both cases, the EBPP provider will have contracts with the organisations whose bills it can present electronically. Typically, these include telecommunications and utility companies. The organisations will send in the bills, and the payer only has to authorise the payment. In case the EBPP provider is a bank, the provider can process the payment itself (such as with Nordea Solo). In other cases, the EBPP provider will execute bill payment by using a direct debit transfer.

On-line bank transfers
On-line bank transfers work fundamentally the same as e-banking systems. The main difference is in the initiation of the application: in an e-banking system, the account holder will see some kind of menu, and makes choices to perform particular actions. In an on-line bank transfer, the account holder will be redirected to the bank’s application by the merchant’s site. In this process, transaction details will also be communicated. Then, the bank’s application immediately presents the transaction screen to the account holder. Therefore, the e-banking and on-line bank transfer systems may very well be one and the same application (such as with Nordea Solo).

Authentication
The simplest way to protect e-banking and similar applications is by using a password or PIN in combination with the account number. However, this is considered to be too insecure to use as authentication for e-banking, one of the main reasons being interception of the password. Therefore, stronger alternatives have been developed. One line of thought is to use password-like authentication, but making sure that intercepting these passwords would do no harm, as they can only be used once (‘once-off’). If an attacker would somehow be able to intercept an once-off pass code, the attacker would not be able to use it in a new transaction. Examples of this idea are:

- Once-off pass codes that are sent by the bank using paper mail. Although old-fashioned, this is a reasonably effective system that can be used for each e-banking channel, including voice telephony.
- Hardware tokens using a challenge response protocol (calculators). When the account holder tries to log in, a number is presented that he must enter in the
calculator. The calculator then produces a new number, based on the number entered and a cryptographic secret contained in the calculator. The bank’s computer can verify that the user possesses this cryptographic secret.

- Hardware tokens using a time-dependent code. The hardware token produces a number using a hash function that has as input either the time or previous numbers, and a cryptographic secret. The user enters the number produced by the token, and the bank’s computer can, by doing the same calculation, verify that the user is in possession of the secret.

- Smart cards. Which can either be used as a hardware token based on a challenge response protocol using a separate smart card reader (as discussed above) or can be used in combination with a smart card reader connected to a computer. In the last setting, the smart card is used to perform a challenge response protocol which is based on either:
  - secret key cryptography, in which the user shares a secret, a cryptographic key, with the bank, knowledge of which can be shown by encrypting messages randomly generated by the bank.
  - public key cryptography in which the bank possesses the user’s public key (incorporated in a digital certificate) and in which the user can prove knowledge of the accompanying private key by digitally signing messages randomly generated by the bank.

In many cases the hardware tokens and smart card mentioned above are protected with a PIN code that needs to be typed in to enable it; if the PIN code is typed in incorrectly a fixed number of times, e.g., three, the token or smart card will be blocked. We remark that once-off pass codes themselves do not provide protection against attacks whereby the attacker takes over a session as soon as the user has authenticated itself. This in fact is a general problem in all authentication protocols including those based on digital certificates. This problem is usually addressed by first establishing a secure channel between the user and the organisation authenticating the user with the following properties:

- The user can validate that the channel is established with the correct organisation.
- The channel, or the information that is sent over it, cannot be manipulated by other parties.

In practice such channels are often based on SSL.

Another idea is to verify possession of the (debit) card that belongs to account to which the user wants electronic access. This can be done by:

- Electronic card readers directly connected to the workstation. This is not a very popular method, because it requires connecting hardware to the computer and installing some software. The account holder therefore cannot use this on arbitrary computers.

- Electronic card readers that function as a challenge response hardware token after inserting the card (and possibility entering a PIN). This is becoming increasingly popular. As prices for card readers declined, these have become more economic than ordinary hardware tokens, as card readers are identical for all account holders and easily be distributed, whereas ordinary hardware contains contain a secret and are personal.
2.5.2.10 Security objectives

From a viewpoint of information exchange, e-banking and similar application are rather simple. A diagram is presented in Figure 24. Some complexity arises due to the fact that a lot of different channels may be used between the account holder and the bank.

![Figure 24 Security of e-banking and similar systems](image)

Security objectives for e-banking and similar are:
1. Confidentiality of information in transit (both transactions and statements).
2. Confidentiality of information stored at the banking system.
3. User authorisation of transactions.
4. Non-repudiation by the user that he approved the transaction.
5. Integrity of the information disclosed by the bank.
6. Availability of the banking system.

2.5.2.11 Best practices

Best practices include:

- Using a secure protocol for the account holder / bank communication in order to protect the confidentiality of information in transit, and for the account holder to be able to identify the bank (objectives 1, 5). The actual technology to realise this is strongly dependent on the channel used:

  Voice telephony
  Inherently less secure. As a result, information presented over the telephone should be limited, and all authentication secrets should be once-off.

  Direct dial up by modem
  The developers of e-banking applications will have to implement a secure protocol themselves. Generally speaking, employing an existing protocol in a new way (like SSL) is preferable over designing it from the ground up. Security should never be “security by obscurity”, i.e. complete knowledge on the working of the application should not enable an attacker to gain access. As the client software should be trusted in this case, a secure distribution channel of this software must be set up, and users must be aware that they should not obtain software from any other channel. Additionally, the software may need to be signed (e.g. in case of an applet).
Internet
Adequately using SSL, see building blocks.

GSM/SMS
GSM/SMS messages are not very secure in terms of confidentiality, similar to voice telephony.

I-mode, WAP
- Using the security features available for these systems, see building blocks.
- Protecting the banking system against hacking by firewalls, adequate patching, system hardening (objectives 2, 5, 6).
- Using a strong authentication method to authenticate users for access (objective 2) and to authorise individual transactions (objectives 3,4). A simple password should never be used. Stronger alternatives have been discussed above under authentication.

2.5.2.12 Findings
E-banking applications are usually well-secured, as trust of account holders in the system is essential. Several banks apply an authentication method that is based on challenge-response in combination with something you have. This may be either a specific hardware token, or a chip that is on the same card used for off-line banking. If simple password authentication were used for e-banking, this would severely compromise security, but we have seen no such systems in use.

There have been some problems regarding the security of modem e-banking applications. The attack pattern is that someone pretends to be the bank while distributing a modified version of the software. However, this will be obsolete in the near future, as banks are changing from client/server software to Internet/browser based software.
2.5.2.13 Analysis of security

Regarding security, electronic banking, on-line transfers and EBPP are rather similar. Security of e-banking systems is often based on once-off pass codes, e.g., using a hardware device combined with a PIN, as authentication based on fixed passwords is too weak for direct access to a banking account. The 2-factor authentication enables very secure systems. Therefore the technical security evaluation is (++). The same holds for on-line transfers.

EBPP seems to be somewhat riskier, as more parties are involved that need to be able to trust each other. The technical security evaluation for this is (+).

2.5.2.14 Analysis of economic feasibility

Standard and large transaction amounts can be handled with all of these systems, but micropayments are not generally appropriate. For all these systems, this leads to a basic usefulness evaluation of (+).

For electronic banking, the following adjustments have to be made to the usefulness evaluation:

- Electronic banking can be used to transfer money to merchants as well as other consumers with a bank account. This way, it allows for Person-to-Person payment which increases the usefulness of the system.
- Electronic banking has one significant drawback as a payment system: in contrast to many other systems, it cannot usually be used to complete a transaction on-line, in real time. For an electronic payment system, it is a desirable property that it can be integrated with electronic shopping systems. This means that, after a consumer has chosen to buy goods, the consumer is automatically redirected to a system where he can authorise his payment. After authorisation has taken place, the merchant should be informed of the payment, in order to be able to report this to the consumer and start the delivery of goods or services. Electronic banking is not designed to be integrated with an electronic shop in this way (on-line bank transfer systems are designed for this purpose). Additionally, electronic bank transfers are usually not processed in real time, unless in some cases where the participants of the transaction both have accounts with the same bank.

The positive outweighs the negative contribution to the usefulness perception. The usefulness evaluation of electronic banking is therefore (++).

There is a clear economic feasibility for electronic banking. Most European banks are offering this to their clients and even encouraging it, as it enables them to save on costs of running bank offices for clients. Some are even focused entirely on their Internet presence and do not have ordinary offices. Electronic banking is already widely in use. As payment is really the same as in the case of an “ordinary” bank transfer, critical mass is not very important to these systems. The critical mass evaluation is (+). Due to the way the banking system operates, on-line bank transfers can normally only occur within the same bank. Inter-bank transfers will be processed overnight during batch processing. As a result,
merchants will need to have a contract with each individual bank through which they would like to accept on-line transfers. This is only interesting if many users will use on-line transfers, so critical mass becomes an important matter. The critical mass evaluation is (+/-). EBPP may in principle be very convenient for the end user, but is also dependent on critical mass. For the user, EBPP is most interesting if many different bills are electronically presented. It provides little added value if there are only one or two companies doing it. The critical mass evaluation is therefore (+/-). As a result, adoption of EBPP will probably be slow in the near future.

Regarding ease of obtaining, electronic banking, on-line transfers and EBPP are rather similar; for all three of them the exchange of some paper documents is required before payment can be made: the ease of obtaining evaluation is (+/-).

The score on combined security and economic feasibility is determined in Section 2.5.8.
2.5.3 Centralised account systems

2.5.3.1 Introduction and examples

Background
All electronic payment systems involve transferring money to/from money accounts. Accounts are traditionally issued by banks and similar financial institutions, such as credit card issuers. However, they may in principle be issued by any other organisation, as an “account” is nothing but a representation of a financial claim that one party has to another.

Transferring money from one account to another one is easy if both accounts have been issued by the same party. The reason is that in that case, money transfer is just an administrative procedure, without any “real” money changing place. If the accounts have been issued by two separate issuers, the situation becomes more complex.

Suppose the payer holds an account issued by issuer A, and the payee holds an account issued by issuer B. Then for the payer to transfer money from her account to the payee’s, issuer A must debit the payer’s account and issuer B must credit the payee’s account to the same amount. Furthermore, this amount must be transferred from issuer A to issuer B in “real” money. This process is called clearing.

Money transfers in a centralised account system
Centralised account systems try to offer a cost-effective and convenient way of paying electronically by avoiding the clearing process. To do this, they make it very easy to open up an account at the system. If someone wants to transfer money to an account on the system, or receive money from an account on the system, he should open up his own account on the system. In this way, all transfers remain within the system itself and clearing is avoided. This property makes Person-to-Person (P2P) payment possible in an easy and cost-effective fashion and it is this characteristic property of centralised account systems that distinguishes it from telephony account and electronic payment account systems.

Besides being cost-effective and convenient, these systems in principle also offer a security and trust advantage over credit card payments. Indeed, with Internet credit card payments, the customer must have sufficient trust in the merchant and his website to offer his credit card details to the website. Centralised account systems, on the other hand, do not require the customer to provide any confidential information to the merchant: in such a system, the customer only needs to trust the centralised account system itself.

Finally, an advantage that should be mentioned about these systems is that they offer a way to make electronic payments to individual persons. This creates a sharp distinction with most other systems, that only are feasible to pay companies, since individuals cannot or will not afford the infrastructure required to accept payments from these EPIs. This

40 Centralised account systems, systems that amongst other things feature Person-to-Person payments and that avoid the financial clearing process.
property makes centralised account systems popular to pay for goods bought at electronic auction sites.

**Deposits and withdrawals**

The idea of centralised account systems has a catch: the system as described above is completely “closed” and doesn’t allow for “real” money to be transferred from and to the centralised account system. Without this functionality, the system is almost useless.

As for transferring money to the system, centralised account systems allow deposits by account holders to their own account. These deposits may be made by any other payment instrument, credit cards being commonly used for this purpose.

As for transferring money from the system, the centralised account system may allow this only for “merchant” accounts. In that case, from a consumer perspective, all money needs to be spent “within” the system. This is most commonly the case in systems designed for micropayments. Alternatively, the centralised account system may allow account holders to withdraw money from their own account. This may be done by a “traditional” payment system such as a bank transfer, a cheque etc. In some cases, the centralised account system acts as a credit card issuer. Account holders use a credit card issued by the system to pay an accepting merchant, or to collect money from an ATM.

**Examples**

The market for centralised account systems is highly volatile and we will not try to provide a list of all systems. However, some examples are presented below.

One of the most famous and successful of centralised account systems is [www.paypal.com](http://www.paypal.com). It currently has approximately 16 million registered users (July 2002), and is available in 38 countries, including all 15 EU member states.

Other systems available within the EU are Germany-based [www.anypay.com](http://www.anypay.com) (not fully operational yet) and eBay’s [www.billpoint.com](http://www.billpoint.com). The latter represents a general trend in which on-line auctions also deploy centralised account systems, as a means to settle payment for transactions committed at their auction site.

In the United States, traditional banks are also entering this market. An advantage for these players is that the “virtual” account can be linked to a “real” account, facilitating deposits and withdrawals. Examples are Western Union’s [www.moneyzap.com](http://www.moneyzap.com) (planning to expand internationally) and Citibank’s [www.c2it.com](http://www.c2it.com). Also credit card issuers are entering the market enabling payments between (existing) cardholders. Credit card issuers are also entering the market with systems resembling centralised account systems that enable payments between (existing) cardholders. To this end, Visa offers its Visa Direct service and MasterCard has formed an alliance with CertaPay to offer P2P services. P2P services will provide enhanced security via 3D-Secure or e-banking authentication.

---

41 [www.visaeu.com](http://www.visaeu.com)
Some other systems not mentioned above are: Monneta, e-Monee, Web Dollar, Fire Pay, NetTeller and YourTeller. The vast majority of centralised account systems are US based and only a few, like anypay.com, are European. We remark that at the finalisation of this report ING bank introduced a new European centralised account system called way2pay (www.way2pay.com).

2.5.3.2 Technical Overview

In this section, we will describe the working of a centralised account system in more detail. We will first describe it in a generic way. Then, we will examine the main representative of these systems, Paypal.com, in more detail.

Setting the stage

An overview of the working of a centralised account system is presented in Figure 25.

![Figure 25 Centralised Account System](image)

Our discussion is based on the following assumptions:

- There have been accounts issued to both the payer and the payee. In case the payer would transfer money to the payee, but the payee wouldn’t have an account, systems like Paypal would automatically create an account for the payee.
- The payer has sufficient credit on her account to make a transfer to the payee. We won’t discuss deposits/withdrawals in this section, as these are done using other payment instruments.
- The payee may be either a natural person (in case of a “Person-to-Person” transfer) or an artificial person (such as a web merchant).
Money transfer procedure
When the payer wants to transfer money to the payee, the following will take place:

- The payer instructs the centralised account system to transfer money from her account to the payee’s.
- The system validates the transaction and if everything is ok, performs it.
- The system notifies the payee (and the payer) about the transaction that took place

In practice, a combination of web and email traffic is used to perform these steps. The payer will usually authorise the payment on a (secure) website owned by the centralised account system. The system will send out a payment notification to the payee (and the payer) using email. However, email being insecure, the payee cannot rely on this, and will therefore verify the payment on the system’s secure website.

In case the payee is a web merchant, the payer is probably visiting the payee’s website prior to visiting the system’s site. The payee’s web shop would usually offer the payer a number of payment methods, and if the payer chooses the centralised account system, redirect the payer to the system’s site, automatically filling out the transaction details.

Paypal registration
In our description of the Paypal system, we will start by outlining the Paypal registration procedure. Paypal has two levels of registration: non-verified users and verified users. The registration steps can be found in Figure 26.
In order to become an ordinary, non-verified member, only the email address is confirmed. By sending an email to the address mentioned in the registration, and requesting a number sent in this email to complete the registration, Paypal verifies that the person registering on the website in fact has access to the email address. The payer may send money as a non-verified member, however, the payer would still have to fund its account in some way to do this. In order to become a verified member, the payer must add a credit card or bank account to its Paypal account (henceforth, we will assume it is a credit card). Paypal will charge the credit card with a membership fee, and state a 4-digit member number in the transaction details. The payer will note the number on its credit card statement. By requesting this number when the payer wants to become a verified member, Paypal verifies that the payer is the actual owner of the credit card.

**Paypal payment**

The Paypal payment process is outlined in Figure 27. After logging in, the payer can order a payment to the payee. In order to do this, the payer will enter the payee’s email address along with the transaction amount, a note, shipping details if necessary, and the source of funding for this order. Then, Paypal will send an email to the payer as a confirmation, and an email to the payee as a notification. The payee can then log in to Paypal to accept the
payment. The payer may transfer money to the payee even if he doesn’t have a Paypal account yet; in that case, the payee needs to register before claiming the money. In order to be able to claim the money, the payee also has to add a credit card or bank account to his Paypal account. With the payee’s acceptance of the payment, the transaction is finalised.

![Paypal payment process diagram]

A payment has now been made, but is has status "unclaimed" and may be cancelled by either party.

- Payer logs in to Paypal.com using a username and password
- Payer orders money to be sent
- Paypal confirms payment to Payer, and notifies Payee
- Payee logs in to Paypal.com using a username and password
- Paypal present account details to Payee, and requests acceptance
- Payee accepts the payment

The payment is now "claimed" and is final.

Figure 27  Paypal payment process
2.5.3.3 Security objectives

A simple diagram showing the centralised account system from a perspective of setting security objectives is presented in Figure 28.

From this, we can deduce the following security objectives:

1. Confidentiality of information in transit between the Payer and the Centralised Account System (CAS) (both transactions and statements).
2. Confidentiality of information stored at the CAS.
3. Confidentiality of information in transit between the CAS and the Payee.
4. Account holder authorisation of transactions. Transactions may include payment, deposit and withdrawal. In case of payment, authorisation should include proper merchant authentication.
5. Non-repudiation by the account-holder that he ordered the transaction.
6. Non-repudiation by the payee that he received payment.
7. Integrity of the information sent by the CAS to the Payee.
8. Availability of the CAS.
9. Availability of payment information stored in the CAS.
2.5.3.4 Best practices

In order to meet the security objectives, a set of best practices should be used. They are rather similar to those used for e-banking, as a CAS acts a lot like a bank.

A. Using a secure protocol for the account holder / CAS communication in order to protect the confidentiality of information in transit, and for the account holder to be able to identify the CAS (objective 1). The actual technology to realise this is strongly dependent on the channel used. Please refer to the section on e-banking for more details.

B. Using a secure protocol for the CAS / merchant communication in order to protect the confidentiality of information in transit, and for the merchant to be able to identify the CAS (objectives 1, 7).

C. Protecting the CAS against hacking by firewalls, adequate patching, system hardening (objectives 2, 4, 7, 8, 9).

D. Availability of transaction records should be protected by back-ups etc. (objectives 5, 6, 9).

E. Transaction records should remain accessible to account holders and merchant for a defined period of time (objectives 5, 6, 9).

F. Using a strong authentication method to authenticate users for access (objective 2) and to authorise individual transactions (objectives 4, 5). A simple password should never be used. Stronger alternatives have been discussed above in the e-banking section.

G. The account holder should have a means to be sure about the identity of the payee (objectives 4, 5).

H. There must be a legally signed agreement between the account holder and the CAS stating that the CAS is authorised to process these payments, defining liability for disputed transactions etc. (objectives 5, 6).

I. There must be a legal agreement between the account holder and the CAS that includes a privacy section, stating at least

J. That the CAS will not disclose personally identifiable information (PII) from the account holder to the merchant or a fourth party, and

K. Which PII relating to the account holder will be available to the merchant upon payment to the merchant. (objective 2).

L. As CASs are integrated systems requiring other EPIs for deposits and withdrawals, the implementation of these EPIs should follow best practice as well.

2.5.3.5 Findings

CASs generally do not implement all of the best practices mentioned above. As CASs are a lot like e-banking applications, this would be technically possible. But the business model of CASs depends on cheap, easy subscription and international access. This makes it economically infeasible to use a strong means of authentication. Password authentication is generally considered not very secure, as users have a tendency to choose weak passwords and to write them down.
Paypal has shortcomings at the following best practices:

A, B: secure communication channels
Paypal communication takes place over http using SSL, which is secure, but also using electronic mail (SMTP). This is an insecure protocol as it sends messages in clear text. Message integrity / authentication can be implemented using electronic signatures, but Paypal doesn’t use these.

F: user authentication
Paypal uses ownership of an email address to authenticate users on first registration. In order to make withdrawals or make larger payments, ownership of a credit card or bank account is required to complete the transaction. These methods are reasonably secure. However, for individual payment actions, Paypal uses a simple username / password authentication, which is highly insecure.

G: verification of payee identity
Payees are identified by their email address, which is a weak method. This can go wrong by making a typo, or by attackers obtaining an address which suggests they are from a certain organisation. In case of ordinary bank transfers this is much stronger: an account number should often have specific properties (such as divisibility by 11) in order to prevent typographical errors, and the name and city of the payee are matched with the account number.

The verified member / non-verified member scheme adopted by Paypal doesn’t fully address any of these problems. It protects Paypal against credit card charge backs, as it verifies that the Paypal account holder is the owner of the credit card of which he entered the details, but is does not protect the Paypal transactions themselves.
2.5.3.6 Analysis of security

The technical security of centralised account systems strongly depends on the way they are implemented. By creatively applying multiple channels for communication (such as SMS combined with Internet, or access codes on credit card transcripts combined with Internet) some level of security can be obtained. However, this will probably always be only a limited level of security. The reason for this is that the very advantages of these systems (such as easy registration procedures) would be gone if better security measures (such as strong authentication) would be implemented. The technical security evaluation is therefore (+/-). We remark that of some current implementations of centralised account systems it is debatable if they provide even this limited level of security, whereas the emerging P2P services will provide enhanced security (Visa Direct and the Mastercard/Certapay offering will use 3D-Secure or e-banking authentication).

2.5.3.7 Analysis of economic feasibility

As Paypal and similar systems appear to be booming and many financial institutions are developing similar systems, there can be little debate about the economic feasibility of these systems. The critical mass evaluation is therefore (+).

This increasing popularity is due to several reasons:

• They enable Person-to-Person transfers, in contrast to most other payment systems. This factor confirms the usefulness evaluation of (+).
• Creating an account is very easy - ease of obtaining evaluation (+).

Still, the market for these systems is highly volatile with mergers and acquisitions taking place, and is it not sure yet what the final landscape will look like.

The score on combined security and economic feasibility is determined in Section 2.5.8.

---

42 In 2002 the number of Paypal users doubled to 20 million members worldwide and in July 2003, Paypal had over 25 million members worldwide. Ebay acquired Paypal in October 2002 and for the full year 2003 Ebay expects that net revenues for the Payments segment will be approximately $300 to $310 million which includes net revenues from Billpoint. Since October 2002 Paypal also supports Euros and Pounds Sterling.
2.5.4 Telephony account systems

2.5.4.1 Introduction and examples
Telephony in general and GSM telephony in particular can be used as a means for electronic payment both for Internet-related and other payments. GSM telephony has a number of interesting properties for electronic payment:

- It can feasibly be used for small payments, whereas other payment types are generally too expensive to use for transfer of less than €2.
- It is widely available among consumers.
- It’s considered to be far more secure than Internet payments.

A telephone can be used for payment in a variety of ways, some of which have been discussed in other chapters (direct debit, m-banking, centralised accounts). However, in the usage of telephony previously discussed, the telephone was merely a medium. The same holds for integrated solutions in which a (WAP) telephone can be used to make various types of electronic payments: this will be discussed in the chapter on Payment Service Providers (PSPs).

In this chapter, we consider models in which telephony is the payment instrument as such and the telephony account is related to the payment. There are various models for this listed below. These can be grouped into two major classes: the “premium rate” models and the “direct transfer” models. All of these models share the value chain illustrated in Figure 29. Although there typically is a central party managing the payments (typically the operator) in telephony account systems, there exist significant distinctions with the notion of centralised account systems, such as the relation with the telephone infrastructure and the fact that Person-to-Person (P2P) transactions are usually not possible.

Premium-rate models
Perhaps the most important model employed for using telephony as a payment instrument, is the premium-rate model. In this case, the merchant has a contract with a telephony operator. The telephony operator provides the merchant with a phone number. Whenever a consumer accesses the number, the consumer’s account will be charged at a much higher rate than when dialling ordinary numbers. This “premium” is shared between the mobile operator and the merchant. This basic model can be used in various ways:

Premium-rate SMS: In order to obtain access, the user has to send an SMS message to a premium-rate number. These numbers cost a fixed amount per message. Typically, the user gets a code on the website, and has to SMS this code to the premium rate number. The website will either detect this directly, or a response is sent to the user by SMS, which he then has to enter on the website.

---

43 Telephony account systems, closely related to (GSM) telephony subscription accounts that enable payment to merchants.
**Premium-rate voice:** This is a model similar to premium-rate SMS, but using an ordinary voice telephone call. The major disadvantage of this model is that premium-rate numbers are charged by the minute. Therefore, in order to pay a particular amount, the user has to stay on the phone for a while. He will then hear a message similar to “You have now paid 2 Euros and can access the site”. The advantage of this system is that it is available on all telephones, whereas SMS is currently only available on GSM phones.

**Premium-rate dialup:** This model is widely in use in Rather those cases where consumers need to pay to gain access to a website. Rather than having the paid content on the Internet, the content is available only on a private computer accessible by modem. The modem is connected to a premium-rate phone number. The user is then charged by the minute for using the site. Disadvantages of this system include the need for a modem and the installation of some software.

**Direct-transfer models**
A newer model, different from the premium model, consists of directly charging the telephony account when a payment has been made. In this cases, the telephony account, ordinarily only used for accounting charges for telephone usage, now starts to act as a general-purpose payment account. To do this, payment software installed by the operator may be used to make payments directly from the account rather than through a premium service. For instance, the mobile user’s GSM might contain an additional menu with which one perform payment debited from the user’s pre-paid credit with the operator. Applications can be integrated in a GSM phone by using the SIM toolkit (see the section on GSM security), which can also support the use of specifically encrypted SMS messages.
Some examples of telephony payment systems are:

- The Coinlet system by Portalify\(^{44}\). This system can use both premium-rate SMS, premium-rate voice, or alternatively a 3\(^{rd}\) party payment system. We will examine the working of the Coinlet system in more detail in the next section.
- Mobile2Meter\(^{45}\). This is a GSM/WAP payment system designed specifically to replace parking meters.
- Postbank/O2 mobile banking. This is a prepaid system using the GSM toolkit. We will also describe this in some more detail below.
- Vodafone/T-Mobile m-Pay Bill\(^{46}\). This is a telephony account system intended for small transfers that either charged to the telephony bill (post-paid) or debited from the telephony credit (pre-paid). This model will also be described in more detail below.

2.5.4.2 Technical Overview

**Coinlet**

In the Coinlet model, a 4\(^{th}\) party is introduced in addition to the payer, merchant and telephony operator. This is the Coinlet server. The merchant is not connected directly to the telephony operator, but through the Coinlet server. Coinlet is in effect a Payment Service Provider model. This is illustrated in Figure 30. The steps that are followed are illustrated in Figure 31.

Figure 30 Coinlet value chain

44 http://www.portalify.fi
45 http://www.mobile2meter.com
46 http://mpay-bill.vodafone.co.uk/home.html
Postbank-O2 mobile banking

Clients of the Postbank are provided with WAP telephones supported by the O2 network based on a pre-paid subscription. With these WAP telephones Postbank clients can access an M-banking application. In addition to this WAP functionality, the issued phones have a SIM Toolkit application stored on the SIM during personalisation at the manufacturer. With this application the client can use applications using special menus in the telephone. One such application is a revalue application, with which clients can increase the pre-paid credit of their phone at O2, by transferring money from their Postbank debit account to the pre-paid credit system of O2.

The communication between this application and the Postbank employs a special type of Short Messages Service (SMS) and is in fact completely independent of the WAP functionality of the phone. In more detail a revalue operation by the clients looks as follows:

The client initiates the revalue function using a special menu on its phone and types in the amount to be debited to the O2 pre-paid credit. The maximum amount is currently Euro 700.

On basis on this amount and other information, the application forms an encrypted SMS and sends this over the air to O2. This encryption is uniquely based on special cryptographic keys on the user’s SIM card. O2 sends this message to the Postbank, which decrypts and verifies this message and parses the actual message. If this parsing is successful then a revalue message is sent O2. The client will be sent an SMS notification by the Postbank.
Vodafone/T-Mobile m-Pay Bill
The m-pay bill system is intended to pay small amounts of money by having these charged to the mobile telephone bill (postpaid) or deducted from airtime credit (prepaid). Primary examples for which this system is useful is to buy cellphone logos, ringtones, games, e-cards etc.

The m-pay system can be used in two ways:
1. To buy items on web sites. The merchant’s web site will have an option to choose payment through m-pay. After selecting this payment option, the consumer will be redirected to the m-pay site. The consumer is authenticated using a username and password. After the consumer has authorised the payment, m-pay will inform the merchant that payment has been received.
2. To buy items on WAP sites. This works in a similar manner to buying on web sites, but rather than by entering a username and password, the consumer is authenticated by his cell phone number and a PIN code.

2.5.4.3 Security objectives

Premium-rate models
In order to determine the security objectives, we start from the more general model, in which the telephony payment provider is not the same as the telephony operator. This is depicted in Figure 32.

The figure looks more complicated than the same figure for other payment instruments, but a some of the potential security issues are solved immediately by the nature of the payment method. For instance, the actual transaction is committed by making the telephone call or sending the SMS. As this is the transaction, there is no transactional information as such that can be intercepted or spoofed. The security of the telephony payment system is accepted, apart from its new use as an EPI. All amounts are relatively small, and the costs of hacking the system would exceed the profit. Additionally, there is the possibility of blocking a phone in case of loss.

In order to link an Internet-session to a telephonic payment, statements needs to be transmitted between the payer, the merchant and the telephony service provider. This is usually based on codes (the merchant sends the code to the payer, the payer sends the code using the telephone, the telephony service provider informs the merchant that a payment has been made for this code). Therefore, no personally identifiable transactional information is needs to be stored on the merchant’s site.

In this system, we identify no new security objectives compared to those already in place for ordinary use of a telephone.

For premium-rate dialup, the most important security risk is that the merchant uses malicious software will cause the browser to always dial the premium-rate number while the user thinks the premium-rate number will on be dialled for accessing the specific site. Although the software is usually signed, this doesn’t help as it only proves the authenticity
of the software but not that the company that signed it is trustworthy. There is no clear best practice that will help overcome this problem.

**Figure 32** Security of telephony payments

**Direct-transfer models**
In case of the direct-transfer model, telephone calls are used to make a payment from your payment account. Payment amounts may exceed those used in premium based systems. In this case we have the following security objectives:

1. The payer and the telephony operator should have strong mutual authentication.
2. There should be non-repudiation of transactions.
3. Transactions information should remain confidential.

**2.5.4.4 Best practices**
For direct-transfer models, we recommend the following best practices to meet the security objectives:

A. Use a SIM toolkit to communicate using encrypted SMSs. The SMS channel is considered to be too insecure to initiate and authorise the transactions of the amounts allowed in prepaid systems.

B. Use cryptographic keys on the SIM to have the telco authenticate the user and provide non-repudiation.

C. Make sure the SIM toolkit application authenticates the bank using public key cryptography.

**2.5.4.5 Findings**
The Postbank/O2 banking application implements best practice A. Best practices B and C are also implemented by the cryptographic scheme, as impersonating parties will not be able to decode the SMS messages.
Because in the case of direct-transfer models the basic means of authentication is possession of the SIM, passwords (in this case, PIN codes) only provide an additional level of security and the inherent weaknesses of password security are in principle not relevant here. An exception to this is the m-pay system when in it used to pay on web sites. Because the telephone itself is not used for authentication, the possession of the SIM is not required to make payments. Having strong passwords is essential in this case.

2.5.4.6 Analysis of security
As the telephony infrastructure is highly regulated and only a limited number of parties have access to the underlying switching infrastructure it is generally considered to be more secure than the Internet without any further security measure like SSL/TLS. More concretely, the intrinsic protection of confidentiality, integrity and authenticity (e.g., caller line ID) against criminal attack is considered good. The technical security evaluation is (++).

2.5.4.7 Analysis of economic feasibility
Telephony account systems have a strong point in offering a large range of transactions, including small transactions (an example that is often used is buying a can of soda from a vending machine) and larger transactions (e.g. paying an electricity bill). The usefulness evaluation is therefore (+).

In order to get ready to receive telephony payments, merchants will need to take the required services from telecommunication operators. In order to allow as large a population of potential consumers as possible to pay this way, merchants will need to set this up for all major telecommunication operators in their service area. As merchants need to put an effort in getting ready to receive telephony payments, critical mass is an important issue. This has not been reached yet, but with the popularity of GSM and the increasing popularity of systems like iMode, these systems have much potential. The critical mass evaluation is (+/-).

The ease of obtaining this payment system depends on whether the consumer’s current telephony provider and device support it. If so, it will be rather easy to start using the service. The ease of obtaining evaluation is (+/-).

The score on combined security and economic feasibility is determined in Section 2.5.8.
2.5.5 Electronic payment accounts, micropayments and “cheques”

2.5.5.1 Introduction and examples

Electronic payment accounts and micropayments

Electronic payment accounts are most commonly used to solve the problem of paying small amounts on the Internet typically from a consumer to a merchant. This distinguishes such systems from centralised account systems where Person-to-Person (P2P) payments are typically possible. The strategy followed in one of aggregation: rather than paying for each transaction using the expensive “real money” payment infrastructure, a larger sum of money is paid once, which is then used the create credit on a dedicated electronic account for micropayments. The conceptual model is illustrated in Figure 33.

![Figure 33: Electronic payment account](image)

Of course, this scheme may be used by a single merchant (e.g. an online casino), in which case it doesn’t really act as a separate electronic payment instrument. But it can also be offered by a micropayment organisation that tries to connect to as many merchants as possible, in which case it is a payment instrument in its own right. Examples of such providers of micropayments are Cartio Micropayments and Clickshare.

---

47 Systems based on Electronic payment accounts, micropayments and “cheques”, enabling the payment of small amounts of money, like a few Euro cents, from a consumer to a merchant.
48 www.cartio.com
49 www.clickshare.com
Systems that are suitable for micropayments but that are based on telephony (charging micropayments to the telephone bill or deducting it from a prepaid account) have been discussed in the section on telephony account systems above.

**Electronic prepaid cheques**

A similar system may also be used for paying non-micro amounts of money. The most important reason for employing such a system in that case is offering the possibility of prepaid payments on the Internet. An example of this usage is wwwbon\(^{50}\). This is a scheme in which a user buys a “cheque” in a retail store. This cheque contains a secret number, much like a prepaid GSM card. By entering the cheque number on the Internet site of the issuing organisation, one obtains credit that can be spent in a number of Internet stores. Although this system is presented to the consumer as a cheque/coupon system, it is conceptually more similar to electronic payment account type systems, with a particular manner of transferring money to the account.

### 2.5.5.2 Technical Overview

An overview of the working of the Cartio system is presented in Figure 34. Cartio can operate with or without a client-wallet (see building blocks). The flow shown is without a wallet. Notable about this protocol is that it is rather weak: knowledge of the payer’s password will enable anybody to make payments using the payer’s account. This is a typical feature of micropayment systems: because payment amounts are rather limited, security does not have to be as tight as with credit cards or bank transfers.

![Cartio flow](image)

---

\(^{50}\) [www.wwwwbon.nl](http://www.wwwwbon.nl)
2.5.5.3 Security objectives

From a security point of view, electronic payment account systems are similar to centralised account systems. The flow and storage of information is almost identical (see Figure 35). Security objectives are similar, but differences arise due to the fact that these systems are mainly used for small amounts. For example, non-repudiation becomes irrelevant. In order to prevent security problems, amounts should be kept small: this is a new security objective.

1. Confidentiality of information in transit between the Payer and the Electronic Payment Account System (EPAS) (both transactions and statements).
2. Confidentiality of information stored at the EPAS.
3. Confidentiality of information in transit between the EPAS and the Payee.
4. Account holder authorisation of transactions. Transactions may include payment and deposit.
5. Integrity of the information sent by the EPAS to the Payee.
6. Availability of the EPAS.

![Figure 35: Security of electronic payment accounts / micro payments](image)

2.5.5.4 Best practices

In order to meet the security objectives, the following best practices should be followed:

A. Using a secure protocol for the account holder / EPAS communication in order to protect the confidentiality of information in transit, and for the account holder to be able to identify the EPAS (objective 1). The actual technology to realise this is strongly dependent on the channel used. Please refer to the section on e-banking for more details.
B. Using a secure protocol for the EPAS / merchant communication in order to protect the confidentiality of information in transit, and for the merchant to be able to identify the EPAS (objectives 1, 5).
C. Protecting the EPAS against hacking by firewalls, adequate patching, system hardening (objectives 2, 5, 6).
D. Using an authentication method to authenticate users for access (objective 2) and to authorise individual transactions (objectives 4). As long as payments are small, a simple password may suffice. However, as bad choice passwords is a risk, the system should enforce passwords policies such as minimum length, use of digits etc.
E. As the inherently weak security of such a system is made acceptable by keeping payments small, limits should be set on the maximum balance on an electronic payment account, and the maximum amount of a single transaction. The balance should not be able to become negative.
F. As EPASs are integrated systems requiring other EPIs for deposits, the implementation of these EPIs should follow best practice as well.

2.5.5.5 Findings

- Cartio seems to implement most of the best practices, although for some it is not possible to verify this without examining the system in detail.
- Cartio limits the account balance to USD 50. As payments cannot be made in excess of the account balance, this also limits individual transactions to USD 50.
- Cartio uses username/password authentication. The user identity is stored on the computer using a cookie. Cartio also offers the possibility of using a client wallet. In this case, no user authentication takes place at all. Cartio recommends this option only for use on a computer that is at home or otherwise in private possession. Still, this seems a debatable technology from a security point of view.

Clickshare, like Cartio, uses username/password authentication. Although there are some controls on password security (minimum length of 6, case sensitivity), this still allows for very weak passwords.
Analysis of security

From a security point of view, electronic payment account systems are similar to centralised account systems. The economic rationale for these types of system is that they are able to process small transaction amounts at a low price. As the payments are meant from consumers to merchants, and transaction amounts are small, security requirements are less strict than for other payment methods. The technical security evaluation is (+), but the security risk evaluation is (++).

2.5.5.6 Analysis of economic feasibility

It is very easy for a user to sign up for any of these accounts: the ease of obtaining evaluation is (+). They can simply use another electronic payment instrument to transfer money to the account. However, the economic feasibility is based on the idea that there is a large potential market for small transactions (under € 5). Although it was believed some time that there was a market for such transactions, for instance in downloading magazine articles and other content, this never really took off, and neither have the electronic payment accounts. Therefore, the usefulness evaluation is (+/-), and the critical mass evaluation is (+/-).

The score on combined security and economic feasibility is determined in Section 2.5.8.
2.5.6 Electronic cash and cheques\textsuperscript{51}

2.5.6.1 Introduction and examples

Transferring the idea of “money” to the Internet

All systems described in previous chapters have in common that they work by providing access to some kind of account. This may be a credit card or bank account, a telephony account or a micropayment account. In that sense, they can be called Remote Access Payment instruments.

Contrasted to this idea, one could try to recreate the notion of nominal value on the Internet. In the real world, banknotes, coins and cheques written to the bearer have a particular nominal value. They can be used for payment by handing them over physically to the payee. By making an electronic equivalent of these instruments, an Electronic Money Instrument could be developed.

One of the principal problems in real-world cash and cheque payments is forgery. This means creation of cash or cheques by someone else than the legitimate issuer. This problem is solved in the real world by making forgery economically unfeasible (coins) or technically unfeasible (banknotes, cheques).

In an Electronic Money Instrument, physical money must be replaced by some kind of data. The problem of forgery splits in two sub problems:

- How to prevent the issuing of new but forged money?
- How to prevent copying/double spending of money?

The first problem may be solved by either using a digital signature or similar (the equivalent of bank notes and cheques) or by making it computationally extremely expensive to create money (the equivalent of coins).

The second problem may be solved by:

- Maintaining a list of money exchanged for real money or new electronic money. This automatically forces an “expiry date” on money, as without such a date, this list must be kept and will grow indefinitely.
- Exchanging electronic money for new money after a payment has been received. By doing this, the payee can be sure that the money was still good, and that the new money can only be spent by him.

In addition to the problems of forgery and double spending, most electronic money schemes have the objective to protect the privacy of the users by ensuring that its usage cannot be traced back.

\textsuperscript{51} Electronic cash and cheques, payments that are not based on an “account” but on digital data with nominal and transferable value.
2.5.6.2 Technical Overview

Electronic Money Instruments can be divided into smart card based systems and software only systems:

- **Smart card based systems:** Smart card based systems, or ë-purses, have gained some ground in the off-line world. They are commonly used to pay small amounts within organisations (such as vending or copying machines), and are increasingly applied for parking meters etc. They can also be used for on-line payment, but this does require specific hardware on the client side. One of the examples is the Finnish Avant card. The existing card based electronic money instruments have not developed into real "bearer instruments" in the sense that the e-money issued would circulate as surrogates for coins and notes.

- **Electronic banknotes, or signed money:** Software-only Electronic Money Instruments based on “signed” money seemed to be the future in the mid 1990’s. Important brands included DigiCash, Cybercash and Netcash. However, they never really took off due to complexity and perceived insecurity, and are not in use anymore.

- **Electronic coins, or minted money:** The idea of making it computationally infeasible to forge money has been developed most clearly in the MicroMint model. This model, developed by famous cryptographers Rivest and Shamir uses hash-function collisions to mint coins. This is a condition in which a set of random numbers yield the same result under some complicated, not-invertible function. Because the function is not invertible, the only way to obtain these numbers is by trying. This requires dedicated hardware, time, and is on a per-coin basis easier to do if you make a lot of coins. Despite its theoretical merits, though, it has never become popular.

- **Hash Chains:** Another mathematical way of creating an Electronic Money Instrument is using hash chains. This is a model that could be used for micropayments. The basic mathematical idea is that it is easy to calculate and verify a chain of hash values, but difficult to calculate the reverse chain. Therefore, in reverse order, hash values could be used as electronic coins. One could calculate a chain of say, 101 values, and then sent the last one to the issuer requesting to attach a value of € 10 to a chain of 101 values. The other 100 values could then be used as coins worth € 0.10 each. Examples of such systems are PayWord and PayTree, but neither system has gained much ground.

- **Electronic cheques:** A money instrument based on secrets that has gained some ground is the idea of the prepaid card. An issuer creates a lot of cards which contain a secret. The cards are made such that the secret must be “opened” to get to the secret, i.e., one can distinguish between cards that have been used and cards that have not. By entering the secret on a cell phone or on the issuers website, the credit is added to some kind of electronic account. From that point on, payment can take place as described in the previous chapter. An example of such a system is PaySafecard.

---

52 www.avant.fi
53 www.paysafecard.at
2.5.6.3 Analysis of security

The security concept of these systems is often very good throughout and based on complex cryptographic protocols. The technical security evaluation is (+).

2.5.6.4 Analysis of economic feasibility

2.5.6.4.1 Electronic Cash

Purely electronic money instruments seem to have failed - critical mass evaluation: (-). The economic feasibility of these systems is lacking, as there is little need for such small transactions and the systems would probably be difficult to understand and operate for an ordinary user. Usefulness evaluation: (+/-), ease of obtaining evaluation: (+/-). Smart-card based systems gained some ground in the off-line world, but they are not very popular on the Internet. Prepaid cards are used a lot for cellular phones, but not for paying on the Internet - critical mass evaluation: (-). There may be a niche market however, for instance for juveniles who want to shop on the Internet, but cannot have a credit card, or as gift vouchers. It should be noted that at the finalisation of this report the European Central Bank published a report on the security objectives of electronic cash according to the Common Criteria.\(^54\)

2.5.6.4.2 Cheques

Obtaining this payment system amounts to obtaining the prepaid cheque itself and registering this on the Internet. (Usefulness evaluation: (+), ease of obtaining evaluation: (+/-)). As we expect none of these systems to play a major role any time soon, we will not go into more detail for these systems.

The score on combined security and economic feasibility is determined in Section 2.5.8.

2.5.7 Summary of Analyses

A summary of the analyses of the various payment methods with relation to the criteria identified in 2.4.4 above, is shown in the tables below. A comparative analysis of the various payment methods identified above is shown at the end of the chapter.

For each payment type on our list of 7, and for each of these indicators, we have derived an evaluation ranging from – to ++\textsuperscript{55}.

\textsuperscript{55} Please refer to section 2.4.4 for details
2.5.7.1 Security Risk,

<table>
<thead>
<tr>
<th>Report Section</th>
<th>Payment method</th>
<th>Security risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.1 Payment Cards</td>
<td>CNP over the Internet transactions</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Secure card protocols (SET)</td>
<td>++</td>
</tr>
<tr>
<td></td>
<td>Secure card protocols (3-D Secure, SecureCode UCAF)</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>Once-off cards</td>
<td>+</td>
</tr>
<tr>
<td>2.5.2 Electronically authorised direct debit</td>
<td>Electronically authorised direct debit</td>
<td>+</td>
</tr>
<tr>
<td>2.5.3 Electronic/Mobile Banking, online transfer &amp; EBPP</td>
<td>Electronic/mobile banking</td>
<td>++</td>
</tr>
<tr>
<td></td>
<td>On-line bank transfer</td>
<td>++</td>
</tr>
<tr>
<td></td>
<td>Electronic bill presentment and payment</td>
<td>+</td>
</tr>
<tr>
<td>2.5.4 Centralised Account System</td>
<td>Centralised account systems</td>
<td>+/-</td>
</tr>
<tr>
<td>2.5.5 Telephony account systems</td>
<td>Telephony account systems</td>
<td>+</td>
</tr>
<tr>
<td>2.5.6 Electronic payment account systems</td>
<td>Electronic payment account systems</td>
<td>++</td>
</tr>
<tr>
<td>2.5.7 Electronic Cash and Cheques</td>
<td>Electronic prepaid cheques</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>Electronic cash</td>
<td>+</td>
</tr>
</tbody>
</table>

From this analysis it appears that purely from a security perspective, electronic banking systems, on-line bank transfers, SET card payments and electronic payment account systems are the preferred systems. In all but the last case this is due to the usage of 2-factor authentication. The least secure system on this basis is Card Not Present payment over the Internet when no specific means of cardholder authentication are used. This is primarily due to the lack of proper authentication used, which is heavily based on credit card numbers and expiration dates that cannot be considered secrets. In addition, further elements of potential risk are the usage of weak versions of SSL (or no SSL at all), storage of credit card details on the merchant’s server, and inadequate protection of the merchant’s server against hacking, potentially exposing credit card information (credit card numbers and expiration dates).

Centralised account systems can in principle support only limited technical security. The reason for this is that the very advantages of these systems (such as easy registration procedures) would be gone if better security measures (such as strong authentication) would be implemented. We remark that of some current implementations of centralised account systems it is debatable if they provide even this limited level of security. Examples
of such payment systems are Paypal, Anypay, Billpoint, Moneyzap, C2it, Monneta, e-monee, Web Dollar, Fire Pay, NetTeller, YourTeller. The vast majority of centralised account systems are US-based and only a few, like anypay.com, are European\textsuperscript{56}.

\textsuperscript{56} At the finalisation stages of this report ING bank introduced a new European centralised account system called way2pay (www.way2pay.com).
### 2.5.7.2 Usefulness

<table>
<thead>
<tr>
<th>Report Section</th>
<th>Payment Method</th>
<th>Usefulness</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.1 Payment Cards</td>
<td>CNP over the Internet transactions</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>Secure card protocols (SET)</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>Secure card protocols (3-D Secure, SecureCode UCAF)</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>Once-off cards</td>
<td>+</td>
</tr>
<tr>
<td>2.5.2 Electronically authorised direct debit</td>
<td>Electronically authorised direct debit</td>
<td>+</td>
</tr>
<tr>
<td>2.5.3 Electronic/Mobile Banking, online transfer &amp; EBPP</td>
<td>Electronic/mobile banking</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>On-line bank transfer</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>Electronic bill presentment and payment</td>
<td>+</td>
</tr>
<tr>
<td>2.5.4 Centralised Account System</td>
<td>Centralised account systems</td>
<td>+</td>
</tr>
<tr>
<td>2.5.5 Telephony account systems</td>
<td>Telephony account systems</td>
<td>++</td>
</tr>
<tr>
<td>2.5.6 Electronic payment account systems</td>
<td>Electronic payment account systems</td>
<td>+/-</td>
</tr>
<tr>
<td>2.5.7 Electronic Cash and Cheques</td>
<td>Electronic prepaid cheques</td>
<td>+/-</td>
</tr>
<tr>
<td></td>
<td>Electronic cash</td>
<td>+/-</td>
</tr>
</tbody>
</table>

On this analysis of usefulness, telephony account systems are the highest ranked, although all of the first four categories are rated “good”.
### 2.5.7.3 Ease of Obtaining

<table>
<thead>
<tr>
<th>Report Section</th>
<th>Payment method</th>
<th>Ease of obtaining</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.5.1 Payment Cards</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNP over the Internet transactions</td>
<td>++</td>
<td></td>
</tr>
<tr>
<td>Secure card protocols (SET)</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Secure card protocols (3-D Secure, SecureCode UCAF)</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Once-off cards</td>
<td>+/-</td>
<td></td>
</tr>
<tr>
<td><strong>2.5.2 Electronically authorised direct debit</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronically authorised direct debit</td>
<td>+/-</td>
<td></td>
</tr>
<tr>
<td><strong>2.5.3 Electronic/Mobile Banking, online transfer &amp; EBPP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic/mobile banking</td>
<td>+/-</td>
<td></td>
</tr>
<tr>
<td>On-line bank transfer</td>
<td>+/-</td>
<td></td>
</tr>
<tr>
<td>Electronic bill presentment and payment</td>
<td>+/-</td>
<td></td>
</tr>
<tr>
<td><strong>2.5.4 Centralised Account System</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Centralised account systems</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td><strong>2.5.5 Telephony account systems</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephony account systems</td>
<td>+/-</td>
<td></td>
</tr>
<tr>
<td><strong>2.5.6 Electronic payment account systems</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic payment account systems</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td><strong>2.5.7 Electronic Cash and Cheques</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic prepaid cheques</td>
<td>+/-</td>
<td></td>
</tr>
<tr>
<td>Electronic cash</td>
<td>+/-</td>
<td></td>
</tr>
</tbody>
</table>

On this analysis for Ease of Obtaining, there is a very mixed set of results, with Card Not Present systems scoring highest.
### 2.5.7.4 Critical Mass

<table>
<thead>
<tr>
<th>Report Section</th>
<th>Payment method</th>
<th>Critical mass</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.1 Payment Cards</td>
<td>CNP over the Internet transactions</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>Secure card protocols (SET)</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Secure card protocols (3-D Secure, SecureCode UCAF)</td>
<td>+/-</td>
</tr>
<tr>
<td></td>
<td>Once-off cards</td>
<td>+</td>
</tr>
<tr>
<td>2.5.2 Electronically authorised direct debit</td>
<td>Electronically authorised direct debit</td>
<td>+/-</td>
</tr>
<tr>
<td>2.5.3 Electronic/Mobile Banking, online transfer &amp; EBPP</td>
<td>Electronic/mobile banking</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>On-line bank transfer</td>
<td>+/-</td>
</tr>
<tr>
<td></td>
<td>Electronic bill presentment and payment</td>
<td>+/-</td>
</tr>
<tr>
<td>2.5.4 Centralised Account System</td>
<td>Centralised account systems</td>
<td>+</td>
</tr>
<tr>
<td>2.5.5 Telephony account systems</td>
<td>Telephony account systems</td>
<td>+/-</td>
</tr>
<tr>
<td>2.5.6 Electronic payment account systems</td>
<td>Electronic payment account systems</td>
<td>+/-</td>
</tr>
<tr>
<td>2.5.7 Electronic Cash and Cheques</td>
<td>Electronic prepaid cheques</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Electronic cash</td>
<td>-</td>
</tr>
</tbody>
</table>

On this analysis of critical mass, there is no clear leader: CNP, Once-off cards, e-banking and centralised account systems rank as ‘good’.
2.5.7.5 Overall

In order to arrive at an overall ranking for combined security and economic feasibility, we assign “++” 2 points descending to “—“ being assigned –2 points. The analytical basis of the ratings for each indicator in this table can be found in the respective sections above, as referenced in column 1 of the table.

<table>
<thead>
<tr>
<th>Report Section</th>
<th>Payment method</th>
<th>Combined security and economic feasibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.1 Payment Cards</td>
<td>CNP over the Internet transactions</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Secure card protocols (SET)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Secure card protocols (3-D Secure, SecureCode UCAF)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Once-off cards</td>
<td>3</td>
</tr>
<tr>
<td>2.5.2 Electronically authorised direct debit</td>
<td>Electr. authorised direct debit</td>
<td>2</td>
</tr>
<tr>
<td>2.5.3 Electronic/Mobile Banking, online transfer &amp; EBPP</td>
<td>Electronic/mobile banking</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>On-line bank transfer</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Electronic bill presentment and payment</td>
<td>2</td>
</tr>
<tr>
<td>2.5.4 Centralised Account System</td>
<td>Centralised account systems</td>
<td>3</td>
</tr>
<tr>
<td>2.5.5 Telephony account systems</td>
<td>Telephony account systems</td>
<td>3</td>
</tr>
<tr>
<td>2.5.6 Electronic payment account systems</td>
<td>Electronic payment account systems</td>
<td>3</td>
</tr>
<tr>
<td>2.5.7 Electronic Cash and Cheques</td>
<td>Electronic prepaid cheques</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Electronic cash</td>
<td>0</td>
</tr>
</tbody>
</table>

Our feasibility analysis shows that one system stands out as the most feasible payment instrument from a combined security and economic perspective: Electronic/mobile banking systems, with 4 points. A cluster of 7 different systems each score 3 points.


2.6 Building Blocks

2.6.1 Communications security of Internet applications (HTTP/SSL)

2.6.1.1 Introduction

The Secure Sockets Layer (SSL) is one of the most widely used encryption techniques on the Internet to secure the communication between web browsers (‘the Client’) and web servers (‘the Server’). In this case the SSL protocol is set between the reliable transport protocol TCP/IP and the HTTP protocol on which the World Wide Web is based. This is why the resulting protocol is known as HTTPS (HTTP over SSL). One should not confuse HTTPS with SHTTP (Secure HTTP) that is a different and now obsolete protocol that was exclusively designed to provide encryption capabilities to HTTP. This is contrary to the SSL protocol that can be used between any reliable transport protocol and an application based thereon like FTP (file transfer), POP3/SMTP (mail).

SSL was developed by Netscape in the early 1990s, and the latest version of SSL (version 3.0) was published by Netscape in 1996 to fix the many security weaknesses in SSL 2.0. SSL was adopted, although in a slightly modified form, by the Internet Engineering Taskforce (IETF) under the name Transport Layer Security (TLS 1.0) in RFC 2246. Although the differences between TLS 1.0 and SSL 3.0 are not very big, they are significant enough that TLS 1.0 and SSL 3.0 do not interoperate. As the same holds for SSL 2.0 and SSL 3.0 there are in fact three ‘SSLs’ in use on the Internet: SSL 2.0, SSL 3.0 and its most general form TLS 1.0. Due to its many security weaknesses, one should not use SSL 2.0. From this point forward we will focus on TLS 1.0. For simplicity we will use the term SSL to indicate the use of either SSL2, SSL3 or TLS over the Internet.

In its general setting, TLS defines a Client (typically a browser in the case of HTTPS) and a Server (typically a web server in the case of HTTPS). TLS is based on public key encryption and the Server is always issued a certificate whereas this is an option for the Client. TLS can provide a secured connection between the Client and the Server that has any or all of the following security properties:

- **Confidentiality**: The communication between the Client and the Server is not accessible by other parties while in transit.
- **Integrity**: The communication Client and the Server cannot be changed unnoticed by other parties while in transit.
- **Server Authenticity**: The Client is ensured that it is communicating with the Server whose identity is based upon the common name in a X.509 certificate issued by a Trusted Third Party.
- **Client Authenticity**: The Server is ensured that it is communicating with the Client whose identity is based upon the common name in a X.509 certificate issued by a Trusted Third Party.

To provide Server Authenticity, the Server needs to be issued with a X.509 certificate, the associated private key is usually stored in software on the Server’s file system but can also
be stored in hardware in a Host Security Module (HSM). We note that the use of so-called hardware ‘SSL accelerators’ do not influence secure storage of the private key but only reduce the encryption load of the servers. Although its use common, the use of X.509 server certificates is not strictly necessary; the Server can also use a so-called anonymous certificate in which case TLS will not provide Server Authenticity. To provide Client Authenticity, the Client needs to be issued an X.509 certificate, the associate private key of which can be stored in software on the Client’s file system or in hardware in a smart card or a USB token. The use of Client certificates – even in software – is not cost effective for many applications. This is why the first three security properties mentioned above are most common for TLS connections. In some implementations of TLS, most notably WTLS (see the next section), three security classes are explicitly distinguished:

- Class 1 TLS: certificate based authentication of server or client is not required.
- Class 2 TLS: certificate based authentication of server is mandatory, certificate based client authentication is optional.
- Class 3 TLS: certificate based authentication of both server and client is mandatory.

We remark that this terminology is somewhat confusing as some Cryptographic Service Providers use the term ‘class’ to distinguish different levels of certificate quality. TLS consists of two important parts, both to be described in the following sections:

- **TLS-handshake** In this part of TLS a key-exchange protocol is performed between the Client and Server resulting in the exchange of a cryptographic key called *master secret*. This key-exchange protocol is primarily based on public key encryption.
- **TLS session**: In this part the master secret is used to set up a secure session involving conventional secret key encryption techniques.

### 2.6.1.2 TLS-handshake

In outline, the TLS handshake is as follows:

- The client initiates the handshake (and indeed the TLS session) by sending the Server its TLS version number, cipher settings, randomly generated data, and other information the server needs to communicate with the client using TLS.
- On reply the server sends the client the server’s TLS version number, cipher settings, randomly generated data, and other information the client needs to communicate with the server using TLS. The server also sends its own certificate and, if the client is requesting a server resource that requires client authentication, requests the client’s certificate.
- The client uses some of the information sent by the server to authenticate the server:
  - Has the certificate expired?
  - Is the certificate issued by a trusted party, i.e., a party whose verification public key is in the client’s certificate store?
  - Is the certificate signed by the trusted party?
  - Is the certificate not revoked by the trusted party, i.e., is it on the Certificate Revocation List (CRL) of the trusted party?
o Does the Domain Name mentioned in the certificate match the Domain Name of the Server. In the case of a Browser this means: does the Domain Name in the URL match that in the certificate?

• If the server cannot be authenticated, the user is usually warned of the problem and depending what the problem is, and the TLS implementation in force, informed that:
  o the connection can be established but that there are risks related to this connection.
  o an authenticated connection cannot be established and the TLS handshake is aborted.

• If the connection can be established, the client goes on to the next step.

• Using all data generated in the handshake so far, the client (with the cooperation of the server, depending on the cipher being used) creates the pre-master secret for the session, encrypts it with the server’s public key (obtained from the server’s certificate, sent in Step 2), and sends the encrypted pre-master secret to the server.

• If the server has requested client authentication (an optional step in the handshake), the client also signs another piece of data that is unique to this handshake and known by both the client and server. In this case the client sends both the signed data and the client’s own certificate to the server along with the encrypted pre-master secret.

• If the server has requested client authentication, the server attempts to authenticate the client:
  o Has the certificate expired?
  o Is the certificate issued by a trusted party, i.e., a party whose verification public key is in the Server’s certificate store?
  o Is the certificate signed by the trusted party?
  o Is the certificate not revoked by the trusted party, i.e., is it on the Certificate Revocation List (CRL) of the trusted party?

If the client cannot be authenticated, the session is terminated. If the client can be successfully authenticated, the server uses its private key to decrypt the pre-master secret, then performs a series of steps (which the client also performs, starting from the same pre-master secret) to generate the master secret. This concludes the TLS handshake.

2.6.1.3 Notes:

• A widely used, but insecure use of TLS on the Internet is to first send the Client a web-form collecting sensitive information (e.g. a password) over HTTP (i.e. unprotected) and placing a GET or POST command in the web-form using HTTPS. That is, in this situation the Client types in the sensitive information, clicks the ‘post-it’ button after which a TLS session is set-up and the information is sent to the Server. The problem with this use of TLS is that the web-form itself is not protected so that an attacker could for instance change the HTTPS call to a HTTP call, or could change the return IP address to one under the attacker’s control. To address this problem, it is best if Server first establishes a TLS-session (noticeable by the lock on the bottom of the screen in a Browser environment) and then requests the Client to type in sensitive information.
• One of the security flaws in SSL 2.0 is that it allows an active attacker to change the cipher lists sent by Client and Server in steps 1 and 2, allowing him to remove all high encryption capabilities from the cipher list. This may result in a weak TLS-session (e.g., 40 bits).

• The Server cert revocation check (step 3d) is not often used within Browser Clients. Technically it is possible, by incorporating a so-called CRL distribution point extension field in the Server certificate, pointing the Client to the location (e.g., ftp, HTTP, LDAP) of the CRL.

• In a typical browser environment, the manufacturer of the browser provides a default ‘trusted’ certificate store, which does not necessarily coincide with the Client’s choice.

• When Client certificates are used, TLS enforces that the Server is issued a Server certificate (e.g., does not use an anonymous certificate). The reason for this is rather subtle but is related to the prevention of a specific ‘man-in-the-middle’ attack: the Client thinks that he authenticates itself to Server A, while Server B just passes the authentication information onto Server A, whereby Server B is actually logging onto Server A. TLS prevents this attack by incorporating the Server’s public key in the piece of data signed by the Client in step 5.

• Depending on the TLS implementation/configuration, the Client certificate is either sent to the Server unencrypted or first an TLS-session is formed (without Client authentication) over which the Client certificate and signed data is sent and after which the TLS-session is ‘upgraded’ to two-side authenticated TLS-session. The reason for sending the Client certificate over a premature TLS-session is not to protect its authenticity or integrity as those are protected by the certificate itself as it is signed by a Trusted Party. This reason might be the protection of the confidentiality of the Client certificate and thereby the identity of the Client might be the reason. To indicate, suppose that the fact that a person uses the application is privacy sensitive (e.g., applying for a job) then sending the person’s (Client) certificate in plain will reveal the person’s use of the application. The TLS specification does not specify which of the two modes should be used.

• The private key of the Server can either be stored in software or in hardware (in a Host Security Module). In either case, the private key can usually be protected by a password, which is advisable. Also, in some implementations the private key can be marked as ‘non-extractable’ meaning that it cannot be exported from the system. This setting is also advisable. We remark that in general the assurance level that private keys cannot be extracted or passwords can be guessed is higher when using (certified) hardware.

• In case of the use of a Client certificate, the associated private key can usually be protected by a password, which is advisable. Also, in some Client implementations, the private key can be marked by the user as ‘non-extractable’, meaning that it cannot be exported from the Client. This setting is also advisable. We remark that both settings apply to both private keys protected by software and hardware; in general the assurance level that private keys cannot be extracted or passwords can be guessed is higher when using (certified) hardware.
2.6.1.4 TLS-session

After the TLS handshake both the Client and Server posses the master secret, which is used to generate the *session keys*, which are symmetric keys used:

- to encrypt and decrypt information exchanged during the SSL session, and
- to calculate Message Authentication Codes (MACs) to protect its integrity, i.e., to detect any changes in the data between the time it was sent and the time it is received over the SSL connection.

The choice of the encryption and MAC method is based on the first two steps of the TLS-handshake.

2.6.1.5 TLS Security Settings

Below we list the most relevant security settings of TLS, its ‘good practice’ setting and the possible methods for the Client to notice the setting in a typical browser environment.

<table>
<thead>
<tr>
<th>Type</th>
<th>Good Practice Setting</th>
<th>Browser Inspection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of TLS</td>
<td>First establish a TLS-session before requesting Clients to enter sensitive information.</td>
<td>Properties of the connection in File menu, or clicking the lock at the bottom of the browser screen.</td>
</tr>
<tr>
<td>Support of SSL 2.0, SSL 3.0, TLS 1.0</td>
<td>SSL 3.0, TLS 1.0</td>
<td>Properties of the connection in File menu or in the advanced settings (to disable SSL 2.0).</td>
</tr>
<tr>
<td>Use of trusted party issuing the Server certificate.</td>
<td>Use of appropriate trusted party issuing the Server certificate. Do not use anonymous certificates.</td>
<td>Properties of the connection in File menu, or clicking the lock at the bottom of the browser screen.</td>
</tr>
<tr>
<td>Use of non-revoked Server Certificate</td>
<td>Automatic server certificate revocation check. Requires CDP in server certificate. Although this would be a good practice setting, it is not commonly used.</td>
<td></td>
</tr>
<tr>
<td>Encryption of Client certificate.</td>
<td>The Client certificate should be sent over a premature TLS connection.</td>
<td></td>
</tr>
<tr>
<td>Public key size of Server (in Server certificate)</td>
<td>≥ 1024 bits</td>
<td>Properties of the connection in File menu.</td>
</tr>
<tr>
<td>Encryption Settings of Server</td>
<td>Only support High Encryption (128 bits).</td>
<td>This is not directly observable from a browser, but is observable with the openssl tool. The Client can determine the encryption setting of an established session via the Properties of the connection in File menu, or clicking the lock at the bottom of the browser screen.</td>
</tr>
<tr>
<td>MAC Settings of Server</td>
<td>Support HMAC based on full MD5 or SHA-1.</td>
<td>This is not directly observable from a browser.</td>
</tr>
<tr>
<td>Protection of Server private key</td>
<td>Usage of good password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prevention of export of private key</td>
<td></td>
</tr>
</tbody>
</table>
2.6.2 Communications security of GSM, SMS, WAP applications

2.6.2.1 Introduction

Standard GSM

The standards for the Global System for Mobile communication (GSM) are developed and maintained by the European Telecommunication Standards Institute (ETSI). Within a GSM communication there is typically a radio link to a GSM base station (owned by the user’s telco, or one of its roaming partners), that links the user’s GSM device either to another GSM device, through another GSM base station or to a conventional phone, through the Public Telephone Switched Network (PTST). Both variants are depicted below.

The wireless, circuit based, communication between the GSM device and the Base Station can be protected using standard GSM encryption:

- The A5-1 or A5-2 encryption algorithm protects the confidentiality of the communication.
- Authentication of the communication (referred to as A3/A8) can be provided by an ETSI standardised encryption method (COMP128) or can be a Telco proprietary method. The authentication keys used are stored in the Subscriber Identification Module (SIM), which is implemented as an integrated circuit card (smart card).

With respect to these encryption methods, we note:

- Integrity of the wireless communication is not protected by encryption.
- The A5-2 encryption algorithm is a weakened version of the A5-1 encryption algorithm and is meant as an ‘exportable’ version of A5-1. Although the specifications of the A5 encryption algorithm are not public, they seem to be leaked and placed on the Internet. In a 1999 paper, A. Birykov, A. Shamir and D. Wagner have shown attacks on the (alleged) A5-1 encryption algorithm that can be carried out in real time on a single PC.
- We note that the end user has typically no way to verify which of the two encryption algorithms is used or that in fact encryption is used at all, which is actually sometimes the case.
- GSM networks can be configured such that they do not perform authentication based on the SIM authentication keys, but perform identification based on a specific identifies supplied by the GSM device.
- Although SIM cards are specifically designed not to retrieve cryptographic keys residing on them, many SIM cards are not adequately protected against ‘side channels’ attacks, such as power consumption analysis, electromagnetic emanations. It was shown by IBM in 2002 (http://www-1.ibm.com/industries/financialservices/ibmpress/index_3.html#9) that the authentication key in a SIM card can be retrieved by these kinds of analysis. Also in 1998, it was shown that COMP128 allowed for retrieving the authentication key by probing the SIM card with specific challenges. This attack has resulted in a new specification of COMP128 (called COMP128-2). It is unclear if all telcos have
switched to this new standard. All and all, these results indicate that the authentication keys stored in the SIM can be cloned relatively easily, if an attacker has access to the enabled SIM for some time.

GSM networks also support packet based communication, which is called GPRS, enabling mobile connection of devices such as computers using the Internet Protocol. Compared with conventional Internet Protocol connections, e.g. a leased lines, an important security issue is the radio link. GPRS uses the same encryption protocols for protection of the radio link as used in GSM telephone (circuit) communication, but the encrypted tunnel encompasses a longer route. Where GSM circuit encryption terminates at the GSM base station, GPRS encryption terminates at a GPRS Support Node (GSN) which is typically located at a central telco computer centre.

As with conventional phones, applications for GSM phones can be based on Interactive Voice Response systems (IVRs) making use of the GSM’s simple keyboard. Specific for GSM is the Short Message Service (SMS). SMS messages are sent over the so-called signalling channel that this shared by GSM users using the same base station. As a consequence, there is no guarantee that SMS messages are not delayed or actually received. This is something that (sensitive) SMS based applications should properly address.

**SMS Messages**

SMS messages can be encrypted in similar fashion as GSM circuit based information. See above. SMS has given rise to new types of applications. For instance the downloading of content like images or ringing sounds and the initiation of financial transactions which are discussed elsewhere in this report. ETSI has developed a standard for SMS based applications called the **SIM Application Toolkit** that “provides mechanisms which allow applications, existing in the SIM, to interact and operate with any Mobile Equipment which supports the specific mechanism(s) required by the application”. The SIM toolkit enables the usage of cryptographic keys that are placed on the SIM card by the telco in the personalisation phase. By using these keys to additionally protect SMS messages (e.g., their authenticity using a Message Authentication Code or MAC) an additional layer of security is placed on SMS that is highly independent of the wireless network security implemented by the telco.

**WAP over GSM**

The Wireless Application Protocol (WAP) is an open specification (see [www.wapforum.org](http://www.wapforum.org) for details) that allows mobile users with wireless devices to access parts of the Internet. In essence, WAP can be seen as a combination of the HTTP, TCP and IP protocols for wireless devices. Like HTTP, WAP can be based on several underlying data communication protocols, e.g., GSM, GPRS and even Bluetooth. In this section we focus on the most common use of WAP based on ‘circuit based’ GSM networks.

WAP is optimised to address that wireless devices have small screens and low computational capabilities, which is one of the reasons that WAP devices usually do not
communicate with WAP servers on the Internet directly but make use of a WAP proxy, commonly known as a WAP Gateway. Between the WAP device and the WAP Gateway all communication is condensed by the WAP protocol stack to meet the low capabilities of the WAP device. WAP also defines the Wireless Mark-up Language (WML) which can be seen as a condensed form of the Hypertext Mark-up Language (HTML) commonly used in Internet browsers. WAP devices typically cannot handle HTML contents. We remark that in many implementations of WAP, the IP protocol is actually used within the WAP protocol stack, i.e., the WAP device is issued an IP address.

The communication between the WAP Gateway and WAP server is based on standard HTTP over TCP/IP, although the WAP Gateway typically expects Wireless Mark-up Language (WML) contents instead of Hypertext Mark-up Language (HTML) contents. Most WAP Gateways will convert HTML content into WML content, which is then readable by WAP devices. The WAP Gateway is usually operated by the mobile operator of the subscriber. An overview of the typical usage of WAP is depicted in Figure 36.

![Figure 36](Typical usage of WAP)

The communication between the WAP Gateway and the WAP Server over the Internet usually travels over physical cables (fibre, trunked telephone cable, bulked microwave radio links) with its known security problems, most notably eavesdropping. In the setting of WAP over GSM, the communication between the WAP device and WAP Gateway travels through a wireless GSM connection between the WAP device and a GSM Base Station, the communication between this base station and the WAP Gateway travels through the Telco’s Wide Area Networks and/or the Internet if the WAP Gateway is managed by an other party then the Telco. This is depicted in Figure 37.

![Figure 37](Gateway not managed by Telco)
The wireless communication between the WAP device and the Base Station can be protected using standard GSM encryption technology. The general considerations on GSM security described above imply that without further protection the communication between the WAP device and WAP Gateway is not properly protected. This was addressed by the Wapforum and has resulted in the Wireless Transport Layer Security (WTLS) protocol which is an adaptation of the earlier discussed TLS protocol taking into account the low capabilities of WAP devices. WTLS is not an mandatory layer in the WAP stack, so WAP devices do not necessarily implement it.

A common usage of WTLS is to protect the communication between the WAP device and the WAP Gateway; the communication between the WAP Gateway and the WAP server is separately protected using SSL. This is depicted in Figure 38.

![Figure 38: WAP Gateway operation for WTLS/SSL](image)

Figure 39 describes this setting from a protocol perspective.

![Figure 39: WAP Gateway protocols for WTLS/SSL](image)

It follows that in this set-up, the WAP Gateway needs to perform a security-sensitive decrypt-encrypt operation for information coming out of one encrypted tunnel and going in the next. This means that in this set-up there is no end-to-end security between the WAP
device and the WAP server. Moreover, as the end-user can typically not verify that the communication between his WAP device and the WAP gateway is WTLS protected (as is typically the case with an Internet browser with its ‘lock’) he has to trust on the security of the WAP Gateway. The end-user also has to trust that the WAP Gateway establishes a suitable SSL connection with the WAP Server. Typically the WAP gateway will inform the WAP server about the security properties of the WTLS connection with the client and as the WAP server can determine (and in fact influence) the security properties of the SSL connection between the WAP gateway and the WAP server, the WAP server can have an overview of the security properties between WAP device and WAP server. Preferably, the trust of the end-user should be enforced by a statement of a third party auditor on the security management of the WAP Gateway and on the appropriate contractual obligations made by the party responsible for the WAP server to verify the adequacy of the WTLS/SSL security settings.

As a result on criticism on this lack of end-to-end security of WTLS, the WAP industry has produced different implementations of WTLS as well that can provide more end-to-end security:

- Gateway switching, here the gateway of the client’s gateway (typically handled by the clients Telco) is switched to the gateway in the proximity of the WAP server. This switching can for example be done by SMS (Short Message Service).
- TLS tunnelling, here conversion between the wireless environment and the Internet environment takes places on the transport (TCP) level. The TLS protocol is placed on top of that.
- Direct Access, here a direct transport (TCP) connection between the WAP device and the WAP Server is used. The TLS protocol that is place on top of that.

The last two designs, which are illustrated in Figure 40, provide the best forms of end-to-end security.

![Figure 40 TLS Tunnelling vs. Direct Access](image)

For the adequate security settings of WTLS and SSL we refer to the previous section. With respect to client authentication, the WAP standards define a hardware security module (Wireless Identification Module, or WIM) for the storage of the client’s private keys. The WIM of a WAP device can be combined with its Subscriber Identification Module (SIM)
card which is then typically called a SWIM card. In addition to this, as part of WAPs WMLscript specification, which is comparable with JavaScript for web browsers, a signText function is defined that can be used to digitally sign messages in the WAP browser using a private key in the client’s (S)WIM. In this respect, WAP browsers can be more advanced than typical WEB browsers.

Unlike the situation with Internet WEB servers, WAP gateways often use anonymous server certificates (or Class I level WTLS in the WAP terminology). As the use of anonymous server certificates is susceptible to man-in-the-middle attacks these implementations employ long-life pre-master secrets (see previous section) that are exchanged at the first communication between WAP device and gateway that typically never expire.

### 2.6.2.2 Security Settings

Below we list the most relevant security settings specifically relating to GSM, SMS and WAP applications and its ‘good practice’ setting.

<table>
<thead>
<tr>
<th>Type</th>
<th>Good Practice Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of Radio communication between GSM device and base station.</td>
<td>Use of A5-1.</td>
</tr>
<tr>
<td></td>
<td>Use of network authentication.</td>
</tr>
<tr>
<td>SMS messages</td>
<td>Adequate address of possible SMS message delays.</td>
</tr>
<tr>
<td></td>
<td>Use of SIM Toolkit for high financial transactions.</td>
</tr>
<tr>
<td>Use of WTLS</td>
<td>Usage of a WAP device that implements WTLS, preferably supporting certificate based authentication of servers (Class 2 or higher).</td>
</tr>
<tr>
<td></td>
<td>Do not use anonymous certificates for the WAP gateway. If anonymous certificates are used, then refreshing of pre-master secrets should either not be possible or should be closely monitored, this to prevent man-in-the-middle-attacks.</td>
</tr>
<tr>
<td></td>
<td>End-to-end Security (preferably) or Gateway switching, or third party audit statement on security of the (external) Gateway and on the WAP server to verify the adequacy of the WTLS/SSL security settings.</td>
</tr>
<tr>
<td></td>
<td>For general TLS settings we refer to the previous section.</td>
</tr>
</tbody>
</table>

### 2.6.3 Communications security of I-mode applications

#### 2.6.3.1 Introduction

The I-mode services are based on proprietary protocols of NTT DoCoMo a large Japanese Telco. As such, the details of the protocols and specification are not publicly available and our descriptions are primarily based on information found on the Internet, e.g., on the site of NTT DoCoMo. Unlike a typical implementation of WAP, I-mode is not based on a circuit switched network but on a packet switched network (GPRS). This means that users are always connected to the network and do not have to ‘dial in’ to it (like in typical WAP implementations). We note that one can also implement WAP on top of GPRS so that WAP can also be ‘always on’, but this is not yet commonly done. As GPRS is based on the GSM network, its communication also travels through the GSM radio network and its security is based on the same encryption techniques.
In general one can say that the I-mode protocols resemble the Internet protocols and concepts more than WAP protocols. To illustrate, like WAP, I-mode also defines its own Mark-up Language, which is called cHTML for Compact HTML. However, cHTML is a superset of HTML which means that an I-mode device can actually read HTML contents although cHTML will typically look better. This is in contrast to WAP, where HTML pages must be translated to WML first. I-mode devices are standard IP enabled and many of the protocols based on IP are supported by the I-mode protocols, most notably TLS. However, like WTLS, TLS is not an mandatory layer in I-mode, i.e. not all I-mode devices implement it.

In effect, I-mode browsers can be very similar to standard Internet browsers including their capabilities of setting up an end-to-end secured, TLS based connections with Web servers. This means that the discussion of communication security of I-mode applications is very similar to that of Internet applications.

### 2.6.3.2 I-mode Security Settings

Below we list the most relevant security settings specifically relating to I-mode applications and its ‘good practice’ setting.

<table>
<thead>
<tr>
<th>Type</th>
<th>Good Practice Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of Radio communication</td>
<td>Use of A5-1.</td>
</tr>
<tr>
<td>between I-mode device and base station</td>
<td>Use of authentication.</td>
</tr>
<tr>
<td>Usage of TLS.</td>
<td>Usage of an I-mode device that implements TLS, preferably supporting certificate based authentication of server (Class 2 or higher).</td>
</tr>
<tr>
<td>Network protection of I-mode device</td>
<td>The I-mode device’s IP address should be adequately protected from the Internet (e.g., by a packet filter installed by the Telco or Internet Service Provider).</td>
</tr>
</tbody>
</table>
2.6.4 Wallets

2.6.4.1 Introduction and examples

Definition
Electronic wallets are an important trend in e-commerce and electronic payment instruments. The concept of electronic wallet (henceforth “wallet”) can be applied to many of the electronic payment instruments described above. Therefore, we will describe it here as a building block rather than describing it separately for each EPI.

A wallet may be defined as:

“An encrypted storage medium holding credit card and other financial information that can be used to complete electronic transactions without re-entering the stored data at the time of the transaction.”

The aspect of encryption in this definition is important: a wallet generally contains confidential information, that should normally only be accessible by the owner. The owner may authorise transactions in which the information in the wallet is used and/or disclosed to another party.

Another important element in this definition is the phrase without re-entering the stored data. This is the primary rationale of using wallets: wallets prevent the need of re-entering data over and over both in cases where this is tedious (e.g. credit card detail) or even infeasible (e.g. entire certificates).

2.6.4.1.1 Client versus server wallets
Wallets may be distinguished depending on the location where they are stored.

• A client wallet is stored on the workstation that is used by the wallet owner to access the Internet. Typically, this means that the wallet owner has the use a workstation that is his private property, contrary to those in Internet cafés, libraries etc.

• A server wallet is stored on a third party server. This implies a high level of trust between the wallet owner and the party that controls the server. Some means of authentication is required to provide the owner access to his wallet.

• Sometimes, a chip card containing similar data is also called a wallet. However, in this report we will stick to the more commonly used terminology, and not include chip cards in our discussion of wallets. Chip cards are most commonly used to store electronic cash equivalents, and are called e-purses in that context.

2.6.4.1.2 Use of electronic wallets and examples
Electronic wallets may be used to store a variety of information:

• Credit card information (card number, expiry date, verification value)
• Personal / address information (name, billing address, shipping address)
• Authentication information (passwords, certificates)
• Electronic credit card certificates (SET)

57 Definition from www.investorwords.com
• Transaction logs
• Electronic equivalents of cash

Some examples of client wallets are:
• **ABN-AMRO e-wallet**\(^{58}\): This is a wallet that contains credit-card details (only for cards issued by ABN-AMRO) and address information. As an extra functionality, it offers secure payment by generating one-time restricted credit card numbers (described in more detail in the chapter about credit cards.) It is protected by a card reader based token.
• Gator eWallet\(^{59}\): This is a general purpose wallet that can be used to store all HTML form-type data, including personal information, credit-card details and passwords. It is protected by a “master password”. A limited amount of information is also sent to the Gator server.
• **SET Wallet Plug-in**\(^{60}\): This is the original wallet developed for the SET protocol. It contains a SET certificate, the electronic equivalent of a physical credit card.

Some examples of server wallets are:
• Yahoo! Wallet\(^{61}\): This wallet stores credit-card details and address information. With this wallet, users can shop at a number of Yahoo! Stores. It is protected by the password used for non-secure Yahoo! Services combined with a security key (similar to a PIN code).
• Microsoft .NET Passport\(^{62}\): .NET Passport is primarily designed as a single-sign on type service. Access through various websites (e.g. Hotmail) can be obtained using Passport authentication (password). Contrary to the Gator architecture (storing passwords that are entered on forms), the .NET Passport architecture uses a central server that is known by the protected sites.
• **Element ServerWallet**\(^{63}\): This is an implementation of the SET protocol, where the SET wallet is located on a server rather than at the client. The wallet also stores transaction information. The method of authentication may be customised for particular brands, ranging from very weak (password) to strong (chip card readers) authentication.

Credit card details appear to be the most commonly used content in wallets. Additional security functionality is promised.

On the other hand, wallets containing electronic equivalents of cash generally appear to be in a theoretical or design stage.

### 2.6.4.2 Overview of working

**Client wallets**

58 www.abnamro.nl
59 www.gator.com
60 www.mastercardintl.com/newtechnology/set
61 wallet.yahoo.com
62 www.passport.com
63 www.element.be
Client wallets are relatively simple in operation and generally work as a browser *plug-in*. A plug-in is a piece of software that communicates with the browser through the browser’s application programming interface (API). In this way, it can modify and extend the browser’s capabilities.

The wallet plug-ins are designed such that they can recognise when they need to activate themselves. This is generally the case when a user sees a particular HTML form, or clicks on a link for secure payment through the wallet. In that case, the plug-in usually opens a separate window through which the user can control the wallet. If a user authorises a transaction using the wallet, the wallet will either set up communication with the merchant website, or fill in HTML forms for the user.

**Server wallets**

Server wallets conceptually operate as is shown in Figure 41. There is someone who owns a server wallet, the user. There is a server that contains the wallets (the Wallet Server). There is a webserver that needs some information from the user. The user is capable of managing the information in her wallet, adding or changing personal information, credit card information, certificates etc. In order to do this, she needs to authenticate herself to the Wallet Server.

![Server wallet operation](image-url)

*Figure 41* Server wallet operation
When the user connects to the webserver which requests information from her wallet, somehow, the user's browser is instructed to contact the Wallet Server. This can be done through:

- Redirection (in the case of .NET Passport)
- A small plug-in (thin client, in the case of Element Server Wallet).

Typically, the Wallet Server will request authentication. After successful authentication, the Wallet Server will present the transaction details as proposed by the webserver to the user. The user needs to authorise this transaction. After authorisation, the Wallet Server will retrieve the information needed by the webserver from the user’s wallet and send it to the webserver. This may either be done directly in server-to-server communication (as is done by Element Server Wallet) or by using cookies and redirects (as is done by .NET Passport).

2.6.4.3 Security objectives

From a security perspective, both client and server wallets are nothing but storage systems of information. It is essential that a user can trust the wallet: it must remain available and under total control of its owner. The following objectives apply:

- Confidentiality of information stored in the wallet. This is very important, since wallets are often used to store private keys and other authentication data.
- Integrity of information stored in the wallet.
- Availability of the wallet and the information stored within.

2.6.4.4 Best practices

From the security objectives, the following best practices may be derived:

- Software must be adequately protected against hacking (objectives 1, 2, 3).
- Software must be trustworthy, e.g. not contain trojans. In order to do this, the software must be audited and a third party statement must be present.
- The information stored in a wallet must be encrypted, in such a way that access to the storage medium by itself will not disclose the information. The encryption key may be a password- or phrase.
- Strong authentication is required to access the wallet.
- The organisation providing the client wallet or the organisation

2.6.4.5 Findings

Our findings indicate major shortcomings with respect to the best practices. These include:

- Lack of trust. It is not widely believed that the owners of wallet are by definition trustworthy. (e.g. .NET passport)
- Authentication is generally very weak, using only a password.
- TPMs for wallet software are rare.

We conclude that wallets often leave an impression of security at a naive user that is not realistic. In addition, an insecure wallet becomes a single-point-of-failure for personal security, similar to loosing a physical wallet.
### 2.6.5 Payment Service Providers

#### 2.6.5.1 Introduction and examples

Payment service providers (PSPs) offer the service of handling payments to Internet merchants. By using a PSP, a merchant need not worry about the difficult task of connecting to each different payment method. For example, rather than having the infrastructure to accept Visa, MasterCard and off-line bank transfers, the merchant will have an account with a PSP, and the PSP will have the infrastructure to accept payments. PSPs combine various types of payments instruments and can be considered an Integrated Solution. An overview of the concept is shown in Figure 42.

![Payment Service Provider model](image)

Figure 42  Payment Service Provider model

PSPs have a diverse background. Most started from a single type of payment (e.g. credit cards or bank transfers) and started offering other payment types later on. Others concentrate on a specific channel (e.g. payment through mobile phone). Most PSPs are non-banks, but banks are showing interest in this market as well. PSP offering is expanding from mere payment to related services such as payment collection, credit checks, currency pooling etc. One of the largest PSPs in Europe is Bibit. Bibit offers a large range of payment instruments for Internet transaction. Cell phone producer Nokia is also a PSP, but specifically offering GSM/WAP based payment instruments, including telephony payment, but also credit card payment.

---

64 [http://www.bibit.nl](http://www.bibit.nl)
65 [http://www.nokia.com](http://www.nokia.com)
2.6.5.2 Overview of working

When a user wants to “check out” at an on-line store, the store uses a PSP to process payment. The actual point at which control is handed over to the PSP is variable, but usually, the store is responsible for collecting transaction details, and then hands over control to the PSP for collecting payment details, including the choice of payment method. Alternatively, the store may be responsible for having the payer select a payment method. An overview of the process is presented in Figure 43. This diagram is based on an Internet PSP. In case of a telephony PSP, the flow is slightly different: there may be no “redirects” from the merchant’s site to the PSP, in this case the payer must enter transaction details manually.

2.6.5.3 Security objectives and best practices

A payment service provider should follow best practice for each EPI that is offered. Additional security objectives are:

- Confidentiality of information sent between the PSP and the merchant.
- Integrity of information sent between the PSP and the merchant, especially the authenticity of a payment confirmation by the PSP.
- Availability of the PSP system is of paramount importance, as a Internet store using this system will not be able to process any payments if the PSP goes off-line.

These security objectives should be met by best practices including

- Using a secure protocol between the PSP and the merchant. Usually, this will be custom made software rather than a standard protocol like https.
- Protecting the PSP server against hacking, having multiple servers running on different platforms, etc.

![Diagram of PSP flow](image-url)

Figure 43  PSP flow
3 Part 3: Overview of the Realisation of Security Solutions in Practice

3.1 An overview of the realisation of security solutions in practice, performed on no less than 500 websites, covering all Member States in the European Union.
3.2 Executive Summary

3.2.1 Introduction

We have reviewed a sample of 613 websites throughout Europe. The sample included both e-commerce sites (454 sites) and e-banking sites (159 sites). The main purpose of our review was to assess which electronic payment instruments are actually implemented in real world, and more important, which of the available security measures are implemented to protect customers.

It is important to understand that we have, as most (potential) customers of these websites would do, limited our assessment to information that was freely available on the site, i.e. we have not attempted to register or to perform an actual transaction.

A major difference between this part of the report and part 2 is that:

- Part 2 focused on the inherent security features of single payment products, i.e. took the ‘inside’-focus;
- Part 3 focuses on what can be observed with regard to payment possibilities and visible security measures, i.e. the ‘outside’-focus.

3.2.2 Electronic Payment Instruments and actual security levels

In order to better understand the remainder of this section of the report, it is important to recognise that secure payment solutions depend on a number of factors, i.e.

- Inherent security features of the payment products used
- Site security, i.e. how well secured is the site infrastructure
- The way security features of payment products are implemented
- Non-technical security measures (procedures, policies…)

From the bullet list above it is obvious that the three latter are site-related and not payment product related. In addition, many sites will offer multiple payment options using different payment products. We have therefore not attempted to structure this report on actual security per different payment product used, but rather reviewed and reported on a site-basis.

The reason for that is, as we have explained above, total security of the electronic payment depends much more on site-wide security than on then inherent security features of payment product.

In order to facilitate the review, we have defined a number of generic security requirements that most consumers would find acceptable, and reviewed to which degree these requirements are currently met. The requirements and methodology is described in Appendix 3.1.
3.2.3 Acceptance of payment instruments

Classic credit cards, direct debit cards and e-banking are clearly the most commonly accepted EPI’s. 78% of the European websites accept classic credit cards, 51% direct debit cards and 9% e-banking. The use of other EPI’s such as Wallets, e-Wallets, mobile payments and electronic checks remains rather exceptional on European e-commerce sites. Important regional differences exist however. Besides electronic payments, 9% of the European e-commerce websites still accepts cash on delivery.

As part of our assessment of e-banking, we found that banks are mainly promoting e-banking and direct debit as instruments for online payments. Despite this focus, pay now products continue to be less popular than classic credit cards in this market segment. The success of e-banking for online payments in Finland shows that standardisation stimulates the penetration rate because it lowers the implementation effort for the merchants. However, no similar Europe wide standardisation initiative for pay now or pay before products seems to have been successful so far. For the pay later products on the other hand, the large multination payment processing organisations do have such standards in place (e.g. the EMV standard).

3.2.4 The actual security solutions used for e-commerce transactions

A high percentage (40%) of the reviewed websites does not explain the security features in use to the consumers. In more than half of these cases, our consultants could derive part of this information from technical details. In 19% of the selected websites, our consultant had no indication whatsoever on the security mechanisms in use. Companies that do disclose this type of information in general use a clear and concise language.

On 68% of all websites analysed, we found that SSL/TLS was used to provide server authentication and confidentiality of the data during transfer. If we split the websites for which no security information is available proportionally over the different security mechanisms, we can conclude that 84% of all e-commerce sites probably uses SSL/TLS. Hence it is the de facto standard mechanism.

Authentication is a necessity that allows merchants to link orders and payment instruments to customers. This can be done on a per transaction basis (10%) or based on a working email address (14%). Most merchants however allocate customer accounts (76%)

The last two techniques also allow them to create a customer profile for each of their customers. This profile can contain both payment information and other personal information. 23% of the websites do not indicate whether they collect payment information themselves or a third party does that this. However based on the data from the other websites, we found a correlation with the EPI used. Credit card numbers are mostly stored by the merchants themselves. The majority of the e-commerce websites do not disclose how they protect the customer information they store.
Furthermore, the customer needs assurance that the merchant has received his payment. He also wants comfort on transaction integrity and confidentiality and the fact that only duly authorised transactions will be executed. He also wants to know what his possible methods of recourse are e.g. in case of non-delivery of goods, duplicate processing or incorrect payments. Most websites do not provide any information with regard to these aspects.

Non-repudiation controls are not very common on e-commerce sites. This is probably related to the relatively low average transaction value. Based on the responses to the self-assessments, we conclude that this mostly varies between 6 and 600 EUR and that most transactions are under 60 EUR. Merchants therefore probably assume that most consumers are not too concerned about this.

We experienced that the e-commerce universe is undergoing constant and rapid change. Between the time that the sample of websites was selected and the end of the study, a substantial portion of these sites:

- Went out of business;
- Were bought by non-European legal entities;
- Changed the security information or set-up; or
- Their policy regarding electronic payment instruments or the information disclosed on this subject.

### 3.2.5 The actual security solutions used for e-banking

For online banking SSL/TLS is also the prevailing security technique to provide server authentication and confidentiality of the data during transfer (78% used SSL/TLS with server certificate only and an additional 8% with server and client certificate).

In order to identify their customers, e-banking websites use customer accounts. The two most secure methods for setting up such customer account, i.e. the offline-process and the online-process combined with an out of band verification, were the most popular with respectively 70% and 46% of the e-banking websites proposing them. This process is regulated in most countries and consequently regional differences exist. In Austria, Portugal, France, Denmark and Italy a one step online registration process was possible at some banks.

With the exception of the Danish banks, the majority of European banks provide limited or no information on:

- The type of customer information stored;
- Where it is stored; and
- The security measures taken to protect stored customer information

Only half the sites visited provided information about:

- The confirmation process for transactions received; and
- The possibility for customers to review and modify transaction before authorisation and execution.

Also on the subjects of non-repudiation controls and the recourse options of the customer in case of problems with a transaction, very limited information is provided.
3.2.6 Fraud Statistics

Many definitions of fraud with electronic payment instruments are currently in use. There are links and overlaps with classic card fraud schemes and Internet frauds. The amount of fraud taking place on the Internet and with Payment Instruments (especially cards) is impressive and amounts to billions USD (US). Some activities are particularly vulnerable to fraud, e.g. auction sites, gambling sites, adult sites. However, in the majority of cases, financial damage is incurred by merchants and financial institutions, not by the consumers.

When taking a more narrow view on fraud, fraud with electronic payment instruments could be defined and limited to the following:

- Counterfeit and copying of debit/credit cards, only in case data needed to successfully copy cards has been obtained through interception of electronic payments message or electronically stored data.
- Counterfeit of electronic money, e.g. unauthorised re-loading of e-wallet
- Interception or unauthorised modification of electronic payment messages, e.g. money transfer through an Internet banking application.

It has become apparent that there are no freely available statistics on fraud as we have described it. In order to draw at least some conclusions, we have therefore used a number of related and freely available statistics on card and Internet fraud, and we have talked to a number of payment industry and banking professionals.

The conclusion from these sources is that, as far as the reduced definition of electronic payment instrument fraud used in this report is concerned, no documented fraud cases exist. There are however a lot of Internet frauds (especially in adult and gambling sites, as well as some auction frauds) and there is a lot of card fraud, but these are more or less independent of the ‘electronic’ nature of the payment method. In either case, the consumer is not suffering great financial losses. One could therefore conclude that the bad reputation or perception of insecurity related to electronic transmission/interception from ‘payments over the Internet’ or other electronic instruments is not substantiated by hard facts. The perception that fraud is taking place with payments over the Internet in general, thus using other mechanisms, is of course fully justified.

3.2.7 General Conclusion of Part 3

As we saw in part two of this study, an impressive amount of payment technologies exist or is on the brink of becoming available. However, when looking at the current real world, one observes that payments over the Internet are still an almost exclusive ‘classic credit card’ business, and that new solutions, how technically advanced they may be, are hardly used.

The security in use for making payments is not presented very clearly to consumers, and the most frequent scheme is the well-established SSL scheme. Again, almost no other more technically advanced schemes are used.

---

66 This includes e.g. abuse of card data obtained through a hacked merchant database containing customer payment data, but this excludes e.g. physical card copying at shops.
Although security practices are presented rather poorly and security measures taken seem to be of the traditional variety, actual fraud, which is caused by the electronic nature of the payment, is virtually absent. Well established fraud schemes, if this term may be used, however remain to exist and now also use the newly available communication channels such as the Internet. But even in these cases financial risk for the consumers is very low, and hardly justifies the perception that paying over the Internet is not safe. When the current efforts of the payment industry to provide more secure cards (chip-cards), as well as some new but cost-efficient control measures (3D-Secure or equivalent) are implemented, the perception of unsafe payments over the Internet will have even less ground.
3.3 Objectives and Scope

The objectives of this part of the study are the assessment of the actual security solutions used for remote transactions with the different Electronic Payment Instruments (EPIs). The following taxonomy of EPIs, as elaborated and described in part 2 of the study, will be included in the review:

- “Pay before” products
  - Wallets (Proton, …)
  - e-wallets
  - Voucher
- “Pay now” products
  - e-banking (funds transfer)
  - direct debit transactions
  - mobile payments
  - micropayments
- “Pay later” products
  - ‘Classic’ Credit card payments
  - ‘Secured’ Credit Card payments (SET and derivatives)
  - Electronic cheque

Since the focus of the EPIs was mainly on those that are used on the Internet, the scope of this part of the study was set to gather information on the security requirements related to any electronic payment instrument that is used on the Internet. Moreover, the analysis and the indication of the security-related features of each EPI were already described in the second part of the study on the Security of Payment Products. Therefore we will try to provide insight on the realisation of security solutions in practice.
3.4 Results of the Website Assessments

3.4.1 Introduction

The results of the survey are structured as follows:

- They are split between e-commerce websites and banking websites, given the quite different nature of both types of sites.
- In each of both sections, we use generic security requirements (see the introduction to “The actual security solutions used for remote e-commerce transactions”) as the basic structure for our report.
- In the e-commerce section this is preceded by an introduction on which Electronic Payment Instruments the merchants accept.
- Subpopulations where profiled and benchmarked against the complete set of results. In both the e-commerce and the e-banking section, we report the difference identified per country. In the e-commerce section we also explored differences by Industry. Where significant differences were identified this is highlighted.

The following graphics show how the websites analysed are broken down by country, and in the case of e-commerce sites, by industry (i.e. what type of merchant).

![Sample spread per country - E-commerce](image)

Figure 44 Sample spread by country (e-commerce)
Sample spread per country - E-banking

Austria 4%
Belgium 15%
Denmark 4%
Finland 4%
France 9%
Germany 18%
Greece 1%
Ireland 2%
Italy 9%
Luxembourg 2%
Netherlands 4%
Portugal 6%
Sweden 2%
Spain 3%
United Kingdom 17%

Sample spread per country - E-commerce

Shopping 37%
Books, Music, DVD and Video 26%
Online Services 1%
Media and entertainment 6%
Travel 10%
Hardware/electronics/computer/office supplies 15%
Software 5%
3.4.2 e-commerce

3.4.2.1 Payment methods accepted – Overall picture

As depicted in the graph below, the most frequently proposed Electronic Payment Instruments (EPIs) on European e-commerce websites were the “Pay later” products. Indeed, 73% of the whole sample proposed to pay with credit cards and/or electronic cheques.

The “Pay now” products took second place with 55% of the visited European websites allowing e-banking, direct debit transactions and mobile payments. Finally, the “Pay before” products were less successful as only 3% of the assessed websites used them.

3.4.2.2 Distribution between various EPIs inside the three categories “Pay later”, “Pay now” and “Pay before”.

Amongst the “Pay later” products, classic credit cards were clearly predominant (98%). Direct debit was the first “Pay now” method proposed (82%) followed by e-banking (14%). The most frequent “Pay before” options were the wallets with 50% and e-wallets with 42%. These results are depicted in the following graphics:

![Breakdown of payment methods accepted](image-url)
"Pay before" products
Results for Europe

Vouchers 8%
E-wallets 42%
Wallets 50%

"Pay now products"
Results for Europe

Direct debit transaction 82%
Mobile payments 4%
E-banking 14%

"Pay later" products
Results for Europe

Electronic cheque 2%
Classic credit card payments 98%

Figure 48 Pay Before products by type

Figure 49 Pay Now products by type

Figure 50 Pay Later products by type
3.4.2.3 Payment methods proposed - Analysis by Country

Across payment categories (later, now, before) the four most frequently proposed EPIs on the 15 Member States’ websites were the classic credit cards (71% of all the European websites visited indicated that they accept this instrument), the direct debit cards (45%) and e-banking (8%). Other payment methods such as e-banking, wallets, mobile payments and electronic cheque were also present but in some countries only as displayed in next graphic. When we extrapolate these findings for the “unknown” part, this results in 78% of all sites that accept credit card, 51% direct debit cards and 9% e-banking.

Classic credit cards were the leading EPI on the e-commerce websites of Spain, The Netherlands, Belgium, Italy, Greece, France, Luxembourg, Ireland and the United Kingdom. Direct debit transactions were preferred in Sweden, Denmark, Finland, Germany, Portugal and Austria.

e-banking was very common in Finland (71%) and quite often used in Portugal (38%) and The Netherlands (24%). e-banking is probably so widely used in Finland because the consortium of the Finnish banks provides a unified interface to nearly all Finnish e-banking solutions. This significantly reduces the implementation effort of this EPI for merchants. In Finland mobile payments (20%) and electronic cheques (16%) were also quite often proposed to the customers. In other Member States the mobile payments were rarely used. The share of electronic cheques was significant in Ireland also (11%). Finally, the wallet was used but quite rarely in Greece (9%), Finland (7%), Belgium (6%), Italy (4%) and Spain (3%).
3.4.2.4 Payment methods proposed - Detail per industry

The classic credit card was predominant on the websites devoted to books, CDs and DVDs (79%), shopping (76%), travel (73%), media & entertainment (62%), and hardware and electronics (62%).

Online service and software providers preferred the direct debit transactions (67% and 54% respectively). e-banking was mainly used by on online services (17%), software vendors (13%) and providers of hardware & electronics (12%).
3.4.3 The actual security solutions used for remote e-commerce transactions

In this section, we will cover the security solutions that were implemented on the e-commerce websites to address the following seven generic security requirements:

<table>
<thead>
<tr>
<th>Ref</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The customer (= originator of the payment instruction) needs assurance that his payment transaction is made to the correct counter party (= receiver of the payment instruction)</td>
</tr>
<tr>
<td>2</td>
<td>The customer wants assurance that the counter party can link the payment instruction to him, and that this link cannot be denied.</td>
</tr>
<tr>
<td>3</td>
<td>The customer wants assurance that the information given to the counter party in a payment instruction cannot be (re-)used by another party to generate another, fraudulent, transaction.</td>
</tr>
<tr>
<td>4</td>
<td>The customer needs assurance that the counter party has received his payment transaction.</td>
</tr>
<tr>
<td>5</td>
<td>The customer needs assurance that the transaction integrity is maintained, i.e. that the transaction will be completed, that the amount and other parameters remain unchanged and that the transaction will be executed only once.</td>
</tr>
<tr>
<td>6</td>
<td>The customer needs assurance that only duly authorised payment transactions are executed.</td>
</tr>
<tr>
<td>7</td>
<td>The customer needs assurance that he has recourse in case of problems with payment instructions, e.g. in case on non-delivery of goods, duplicate processing, incorrect amounts, ….</td>
</tr>
</tbody>
</table>

We noted that the percentage of e-commerce websites for which the security features in use could not be identified was significant (19%).

This ‘unknown’ part should normally be split between the others, although no absolute guarantee can be given. The results must consequently be considered carefully and one should bear this limitation in mind for the rest of the report.
3.4.3.1 Security Requirement 1

The customer (= originator of the payment instruction) needs assurance that his payment transaction is made to the correct counterpart (= receiver of the payment instruction)

A customer wants to be sure that he is communicating with the correct counter party when he provides payment information. Cryptographic techniques are mostly used to achieve this. Often these techniques also provide assurance on confidentiality and integrity of transactions while being transmitted over the Internet (related to the security requirements 3 and 5).

3.4.3.1.1 Overall Situation

SSL/TLS, with a server certificate only, is a commonly used cryptographic technique to encrypt the information transferred across the Internet. However, it also allows the end-user to easily verify whether the webserver actually belongs to the merchant (if he has trust in the issuer of the server certificate). This study proved it to be by far the most popular security mechanism with 68% of all the European e-commerce websites using it.

A very small percentage (2%) of European e-commerce websites used SSL with both a server and a client certificate allowing the identification of both the vendor and the customer. Besides, only 1% of the sample used other encryption mechanisms.

The percentage of e-commerce websites without protection mechanism for the transmission of information was significant (10%). Those sites did not provide their
customers with protection systems aimed at guaranteeing that the receiver was the correct one and the transaction confidentiality and integrity were preserved.

Based on this, SSL/TLS can be considered the de facto standard. However, very few e-commerce websites explained how to verify if the site was secure and to whom the digital certificates were issued (only 19% for the whole Europe with little variation across countries).

3.4.3.1.2 Detail per country

![Protection Mechanisms by Country (e-commerce sites)](image)

Figure 54 Protection Mechanisms by Country (e-commerce sites)
Two of the fifteen Member states counted more than 80% of their e-commerce websites securing the information transfers: the United Kingdom with 89% of the considered websites using SSL combined with a server certificate and Spain with 84% of the e-commerce websites using the same mechanism.

SSL combined with server and client certificates was used in two countries only, namely Austria (6%) and Germany (1%). Other encryption mechanisms were noted in Sweden (10%) and Italy (4%) exclusively.

It is in Sweden, Luxemburg, Belgium Portugal and Ireland that the highest percentages were noted of e-commerce websites explicitly showing that no security feature was in use for information transfers (Relatively 35%, 33%, 24%, 24% and 22%).

It appeared that except in Austria (6%), Sweden (5%) and the UK (3%), no e-commerce vendors provided a protection of their complete site. Actually, in most of the cases, only the transactional part of the e-commerce websites was protected.
3.4.3.1.3 Detail per industry

The online services displayed quite a different profile from other industries. Indeed, Only 33% of the concerned websites used SSL/TLS with a server certificate and 50% clearly did not provide protection mechanism for the information transfer.
3.4.3.2 Security Requirement 2

The customer wants assurance that the counterpart can link the payment instruction to him, and that this link cannot be denied.

![Customer identification on E-commerce websites](image)

This security requirement satisfies the concern for any customer of e-commerce website to guarantee that the vendor could unambiguously identify and link him with the transaction he has originated.

To that purpose, the websites could use customer accounts that are set up when first becoming a customer (and then re-used) with the definition of credentials or simply a personal e-mail address.

We noted that a majority (76%) of the visited European e-commerce websites requested the set-up of a customer account before processing any transaction while 14% of the e-vendors required a working e-mail address only. For the rest of the sample, no information was available.
In Luxemburg and Austria the requirement to set up a customer account was generalised (100%). In Germany, France, Belgium and Spain, it concerned more than 80% of the e-commerce websites. In Ireland, contrary to the other countries, the identification method most frequently used was the working e-mail address (56%). Denmark also presented a particular profile, as none of the Danish e-commerce websites required to their customers the set-up of an account and only 38% of them asked for a working e-mail address.
3.4.3.2.2 Detail per industry

The highest proportions of websites, which did not require the set-up of a customer account before processing a transaction, were noted on the websites selling software and online services. They amounted to 17% of the respective samples. For the websites proposing the set up of a customer account, different processes were possible.

The one step online process was by far (90%) the most popular way of creating a customer account or customer profile. There was little deviation from this European average on the country level. However, one can notice that three countries offered alternatives. In Portugal and Sweden, 10% of the e-commerce websites proposed a two-step online set up and 10% of Belgian websites combined an online process with an out of band verification.
In case of problems with his credentials the customer should have the possibility to re-establish his identity. In Europe, 49% of the visited websites did not clearly explain the possibilities provided to solve the problems customers could have with their credentials. This percentage rose up to 73% in Greece, 78% in Ireland, 79% in Finland and 83% in Luxemburg.

The most frequent way of re-establishing customers’ identity offered by European e-commerce websites was to request a new password, which would then be sent by email. Except from Denmark, the websites of all the Member States proposed this service. The Danish websites suggested to contact the helpdesk (15%) or requested a new registration to their customers (54%). This latter option was also frequent in Sweden (30%). The use of emergency questions was not very common as seven countries only offered this option. The least frequently-used system was to send an URL.
Finally, different systems could be provided by the e-commerce websites to guarantee that the link between the customers and their transactions could not be denied (non-repudiation of the transactions).

![Digital signatures on E-commerce websites for non-repudiation](image)

Figure 61 Use of Digital signatures for non-repudiation

93% of the European e-commerce websites either did not have or did not explain the mechanisms they used to prevent repudiation of the transactions. Only seven European e-commerce websites explicitly mentioned the mechanism they used to guarantee non-repudiation and only two protection systems appeared as significant.

The digital signature was used by 29% of the German e-commerce websites and 10% of the Belgian ones. Less than 10% of the websites in Greece, The Netherlands, Austria, Portugal and the United Kingdom used this system. Digital signature also guarantee transaction integrity (cfr security requirement 5) Trusted Third Party tokens do not seem to be used on e-commerce websites. From a sector perspective, on the one side we noted that the digital signature was mainly used by software vendors (17%). Less than 8% of the other sectors’ samples disclosed to use such a protection. On the other side, the Trusted Third Party Token was exclusively used by shopping websites.
3.4.3.3 Security Requirement 3

The customer wants assurance that the information given to the counterpart in a payment instruction cannot be (re-)used by another party to generate another, fraudulent transaction.

![Collector of the payment information for E-commerce websites - results for Europe](image-url)

The customer wants assurance about the collector of his payment information: is it the vendor himself or a third party? He also wants to know

- That the data is secure during transit over the Internet;
- Who collects (payment) information and where it is stored.
- Which part of his personal information is stored after the transaction;
- if the storage is secure.

Security during transit has been discussed as part of the first security requirement.

The customers should be informed about the collector of their payment information (e.g. credit card information)

- Considering the global results for Europe, 57% of the visited websites collected the payment information themselves while 20% worked with a third party.
3.4.3.3.1 Detail per country

In Austria and Belgium, all the visited websites provided information about the collector of the payment information. While in the first country the collector was the vendor exclusively, a repartition was noted in the second with 43% of vendors and 57% of third party announced as payment information collectors.

In Finland and Denmark, a significant proportion of the e-commerce websites delegated the collection of payment information to a third party (71% and 62% respectively). As indicated in the overview of payment instruments per country, many Finnish e-commerce sites make use of the unified interface to the online banking solutions. In this case, it are the banks who collect the payment information for the merchants.

In Denmark it was even the sole collector explicitly mentioned.

On Luxemburg’s e-commerce websites, the collector of payment information was never disclosed. Obviously the small sample size for this country should be taken into account.

Figure 63 Collectors of Payments Information – by country
3.4.3.2 Detail per industry

The online service providers were the most transparent with respect to their collector of the payment information: 67% of them collected the payment information directly while the other 33% let a third party do it.

On the other hand, the websites selling travels were a little less transparent with only 64% of them disclosing the name of the information collector (53% themselves and 11% a third party).
The type of customer information stored and the place where this information is stored should also be communicated.

### Figure 65

**Percentage of E-commerce websites providing disclosure about the type of information they store**

- **United Kingdom**: 65%
- **Sweden**: 50%
- **Denmark**: 38%
- **Finland**: 36%
- **Spain**: 23%
- **Average Europe**: 22%
- **Ireland**: 22%
- **Belgium**: 19%
- **Greece**: 18%
- **Italy**: 16%
- **Portugal**: 10%
- **France**: 7%
- **Austria**: 6%
- **Germany**: 1%
- **The Netherlands**: 0%
- **Luxembourg**: 0%

- Considering the European average, it appeared that only 22% of the visited e-commerce websites provided disclosure about the type of customer information they stored.
- Apart from the United Kingdom (65%) and Sweden (50%), e-commerce websites announcing the information they stored were in a minority (less than 50% of the respective countries’ samples).
However, the absence of such a disclosure did not mean that the vendors did not store any information.

- 23% of the European websites provided disclosure about the place where customer information was stored.
- For Luxemburg, The Netherlands, Finland, Greek and Austria, the type of information stored was not disclosed. For Finnish, Greeks and Austrian e-commerce websites while respectively 36%, 18% and 6% of them declared to store customer information none of them explained where this information was stored.
- In the opposite, the majority of ecommerce websites in the United Kingdom (72%) referred explicitly to the storing place. Italy, Denmark and Spain followed with 40%, 31% and 26% of their visited websites being transparent about the place where customer information is stored.

**Figure 66 % of websites disclosing location of information stored**

- Germany: 1%
- France: 8%
- Sweden: 10%
- Portugal: 14%
- Belgium: 19%
- Ireland: 22%
- Average Europe: 23%
- Denmark: 31%
- Spain: 26%
- Italy: 40%
- United Kingdom: 72%
- Germany: 1%
Different types of information can be stored. A distinction is to be made between the information on credit card number and the other personal information.

Amongst the 22% of European e-commerce websites storing customer information, only 11% stored the credit card number. On a country level, the highest percentages were noted in the United Kingdom (36%), Ireland (33%) and Belgium (29%).
3.4.3.3.3 Detail per industry

![Diagram showing percentage of e-commerce websites storing credit card numbers by industry](image)

Important differences were noted between sectors. The online service and software vendors never stored the credit card numbers while on the contrary, more than 10% of the travel vendors (22%) and the books, CDs & DVDs’ sellers (14%) stored this information.
Apart from the credit card number, some e-commerce websites collected and stored other personal information. E-commerce websites most often stored information related to the name and address of their customers. Information about the customers’ age and profession were less frequently stored as displayed in the graph above.
Finally, the customer should be informed about the mechanisms used to protect the information stored.

64% of all the European e-commerce websites did not provide disclosure about the protection mechanisms they used. The other 36% where equally sub-divided into detailed disclosure (18%) and simple declaration that efforts had been made to protect the customer information stored on the site (18%). The most transparent websites regarding the protection of customer information were those of the UK, Italy, Portugal, Belgium and Spain.
3.4.3.4 Security Requirement 4

The customer needs assurance that the counterpart has received his payment transaction

To assure the customer that the counterpart has received his payment transaction, a confirmation should be sent to him. Various methods (online, email,...) are possible. The originator of the confirmation can also be different, depending on the collector of the payment.

- On 79% of the European e-commerce websites, there was no explicit reference to any confirmation method.
- Considering the other websites, the majority of confirmations originated from the online merchant himself (15%) and the rest (6%) from a third party.
3.4.3.5 Security Requirement 5
The customer needs assurance that the transaction integrity is maintained, i.e. that the transaction will be completed, that the amount and other parameters remain unchanged and that the transaction will be executed only once.

3.4.3.6 Security Requirement 6
The customer needs assurance that only duly authorised payment transactions are executed.

![E-commerce website provide their customer with the possibility to review and modify transaction prior to authorisation](image)

Results for Europe

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>25%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 72  % of websites confirming and allowing review of transactions, EU-level

To assure that only duly authorised payment transactions are executed the way payment information is collected is critical. This issue was discussed previously. Secondly, the customer should have the possibility to perform a final check before authorising the transaction. This allows him verify the integrity of the transaction.

Other more technical controls that guarantee transaction integrity such as digital signatures have been discussed previously.

The European e-commerce websites visited only rarely provided information about a possible final check option.

- Considering the global results for Europe, no information related to the possibility for the customer to check his order before execution could be found on 69% of the visited websites. This however does not necessarily mean that the option did not exist.
- 6% of the e-commerce website clearly did not offer to their customers the possibility to check their order while 25% explicitly included a final check before execution.
3.4.3.6.1 Detail per country

A majority of the Danish (62%), Swedish (60%), English (53%) and Portuguese (52%) e-commerce websites provided a final check possibility to their customers. The same option was provided in 48% of the Belgian websites.

Regarding Greece and Austria no clear information about the option of final check before execution was available on their e-commerce websites.

Finally, a significant percentage of websites, which clearly did not offer the final check possibility, could be found in Portugal (24% of the visited Portuguese websites), Finland (21% of the Finnish ones), Sweden (20%), Luxembourg (17%), Belgium (14%) and Ireland (11%).
3.4.3.6.2 Detail per industry

The option to review and modify transactions before authorisation was given in six of the seven sectors examined. Online services never disclosed to offer such a possibility.

Figure 74  % of websites confirming and allowing review of transactions, by industry
3.4.3.7 Security Requirement 7
The customer needs assurance that he has recourse in case of problems with payment instructions, e.g. in case of non-delivery of goods, duplicate processing, incorrect amounts, etc.

![Recourse assurance provided to the customer by E-commerce websites](image)

Figure 75  % of e-commerce websites providing recourse assurance, by country

The customers as with other channels should have with e-commerce a recourse option in case of problems with his payment instructions.

- The majority of e-commerce websites visited across Europe (58%) did not provide any information related to the recourses in case of problems with payment instructions.
- The three countries where the e-commerce websites were the most precise about customer recourses were Belgium, the United Kingdom and Denmark. In the opposite, none of the websites visited in Luxembourg and The Netherlands provided any information related to the recourse issue.
- The most frequent recourse offered to customers by European e-commerce websites was linked to the payment method.
• In the United Kingdom, Denmark and Italy the percentage of websites providing the recourse assurance to their customers standard to the payment method was of 84%, 77% and 71% respectively.
• In a few countries, e-vendors proposed site-specific recourses also (Austria, Belgium, Denmark, France, Germany, Portugal and Sweden).
• Belgian e-commerce websites displayed an atypical profile as the major recourse option they offered was site related (67%). Moreover Belgian websites were the only ones to propose a combination of site-specific and payment method-specific recourse options (14%).

3.4.3.7.1 Detail per industry

![Figure 76](image_url)

% of e-commerce websites providing recourse assurance, by industry

Around half of the e-commerce websites selling books (52%), hardware (45%) and travels (44%) offered a recourse possibility to their customers. On the contrary no recourse was possible with online services.
3.4.4 e-banking

Introductory remark: this section reports on the same 7 generic security requirements as defined in the methodology. However, for a more logical flow they have been put in a different order.

3.4.4.1 Security requirement 1

The customer (= originator of the instruction) needs assurance that his transaction is made to the correct counterpart (= receiver of the instruction)

Almost all the European e-banking websites (92%) explicitly proposed mechanisms to protect the customer information transmitted over the web. SSL/TLS combined with a server certificate was the most popular protection mechanism (78%). This also allows the end-user to easily verify whether the webserver actually belongs to the merchant.

SSL/TLS combined with a server and a client certificate was used by 8% of the visited websites; and 6% of them provided other encryption mechanisms.
3.4.4.2 Detail per country

SSL/TLS with server certificate only was the most frequent system in all countries but one, namely Denmark. In Denmark, SSL/TLS with client and server certificate is the prevailing security technique observed. The answer ‘Other techniques’, as observed in some countries, has been selected when no exact reference to the technique used is given, but when it is still mentioned that public/private key cryptography is used.

On average, only 30% of the visited websites clearly explained how a customer could verify the site’s certificate (and hence authenticity).
Figure 79  % of e-banking websites providing detailed security information, by country

Figure 80  % of e-banking websites protected by SSL/TLS, by country
• The majority of the European e-banking websites using SSL/TLS security techniques, protected the transactional part (73%) of the site, as opposed to the complete site. Italy seems to be an exception to this rule.
• As for the remainder of the answers, it was not possible to find out without registering or conducting a transaction which part of the site was protected – however, since the use of SSL/TLS was announced at the website, one could conclude that in these cases the transactional part of the site as a minimum will also be protected.
3.4.4.3 Security requirement 4

The customer wants assurance that the counterpart can link his instruction to him, and that this link cannot be denied.

Figure 81 analysis of e-banking websites providing customer profiles, EU-level

In order to identify their customers, e-banking websites use customer accounts, with customer identification and authentication credentials, i.e. means by which the customer can prove that he/she is who he claims to be. The customer accounts have to be created or initiated in some way – the registration process.

- Some European e-banking websites propose several options to their customers for the set up of their account.
- The two most secure methods for setting up a customer account, i.e. the offline-process and the online-process combined with an out of band verification, were the most popular with respectively 70% and 46% of the e-banking websites proposing them.
- The two-step online process was used by 22% of the European e-banking websites and finally only 4% of the sample proposed the one step online process.
3.4.4.3.1 Details per country

![Figure 82 processes to set up customer profiles, e-banking, by country](image)

- Except for those of Greece and Sweden the e-banking websites proposed several alternatives.
- In The Netherlands all the visited websites used both the “offline” and the “online + out of band verification” processes.
- The two-step online process is used in Denmark and Italy only;
- We observed a one step online registrations process was used Austria, Portugal, France, Denmark and Italy.
In case of problems with his authentication credentials the customer should have the possibility to re-establish his identity.

![Re-establishment of the customer identity with the E-banking websites in case of problem](image)

- The majority of European e-banking websites provided the support of a helpdesk to customers who had problems with their credentials.
- Swedish websites were the only to propose a new registration as unique solution.
- The Finnish websites were not clear about how to re-establish user credentials.

Different systems can be provided by the e-banking websites to guarantee that the link between the customers and their transactions could not be denied (non-repudiation of the transactions)

However, 60% of our sample of the European e-banking websites did not contain any explicit reference to a mechanism guaranteeing non-repudiation. This does not mean that these mechanism does not exist, but simply that it was not possible to know without entering into a relationship with the bank.
In some countries however, numerous websites provided digital signatures and/or a Trusted Third Party token. A combination of both systems was noted in Sweden. This was actually the sole country where Trusted Party token was used (by 20% of the websites). The websites of all the other countries used only digital signatures. In The Netherlands, all the e-banking websites used the digital signature. High percentages were noted in Spain (80%) and Denmark (67%) also.
3.4.4.4 Security requirement 5

The customer wants assurance that the information given to the counterpart in an instruction cannot be (re-)used by another party to generate another, fraudulent, transaction.

![Bar chart showing percentage of E-banking websites providing disclosure about the type of information they store, by country.]

- Greece: 50%
- Italy: 36%
- The Netherlands: 25%
- Finland: 7%
- Germany: 18%
- Average Europe: 9%
- United Kingdom: 7%
- Belgium: 4%

**Figure 85** % of e-banking websites disclosing type of information stored, by country

The customer wants to know which personal information is stored and where this information is stored. He also wants to know if the storage is secure.

- Only 9% of our sample of European banking websites contain information as to which personal information is stored.
- The e-banking websites of seven Member States only were clear about the type of customer information they store.
- The number of 50% of Greece has limited value given the small sample size (2).
As for the question where personal customer information is stored, once again
• only a minority of e-banking websites (15% of the global sample) informed the customer about the storage place.
• In Denmark, however, 67% (4 out of 6) of the visited websites were transparent on that issue.
With regard to the security measures taken to protect stored customer information, only 8% of the European e-banking websites explained these in more or less detail. Another 38% declared that security efforts were made, and the remainder (54%) did not make any statement.
3.4.4.1 Detail per country

![Disclosure about protection of customer information stored by E-banking websites](image)

Figure 88 % of e-banking websites providing information on protection of customer data, by country

All the Danish e-banking websites provided a detailed explanation. High percentages were noted in The Netherlands (75%) and the UK (63%) also. Half of Italian websites and 20% of the Swedish ones simply declared to provide security efforts. No information was available on the e-banking websites of Greece and Austria.
3.4.4.5 Security requirement 3

The customer needs assurance that the counterpart has received his payment transaction

51% of the European e-banking websites did not explicitly inform their customers about the confirmation process for transactions processed. The online confirmation was the preferred system (45%) while only a minority (2%) of the visited websites proposed confirmation through e-mail. Actually, the latter system was proposed in Austria (17%), Portugal (14%) and Germany (3%).

Only the Portuguese websites offered confirmation through classical mail (14%). Some banks offered multiple confirmation mechanisms, hence totals of 100% and more in the table below. The amount of ‘unknown’ answers indicates that it is not clear how transactions are confirmed without entering into relationship with the bank.
Transaction confirmation by E-banking websites

![Figure 90: Methods of transaction confirmation, e-banking websites, country level](image-url)

Security of Payment Products and Systems in the 15 Member States
Part 3: Overview of the Realisation of Security Solutions in Practice
3.4.4.6 Security requirement 2

The customer needs assurance that the transaction integrity is maintained, i.e. that the transaction will be completed, that the amount and other parameters remain unchanged and that the transaction will be executed only once.

3.4.4.7 Security requirement 6

The customer needs assurance that only duly authorised payment transactions are executed.

In Europe, more than half of the visited e-banking websites (51%) did not provide information about the possibility for customers to review and modify transactions before authorisation and execution.
E-banking websites provide their customer with the possibility to review and modify transaction prior to authorisation

The most transparent e-banking websites were found in Ireland and The Netherlands (100%). A review option was also announced on 80% of the Spanish and Swedish e-banking websites.

Finally, no clear review option was provided on significant numbers of websites in France (14%), Belgium (8%) and the UK (4%).
3.4.4.8 Security requirement 7
The customer needs assurance that he has recourse in case of problems with payment instructions, e.g. in case of non-delivery of goods, duplicate processing, incorrect amounts, etc.

A very large proportion of the European e-banking websites (75%) did not explain the recourse options in case of problems with the transactions. The Italian websites were the most explicit with 71% of the assessed websites assuring the same recourses for e-banking as for the traditional banking services. Denmark was not far behind with half of the Danish sites providing the ‘traditional’ recourse assurance. In Portugal and the Netherlands, respectively 57% and 25% of the websites offered recourse assurance specific for online banking.
3.5 Fraud Statistics

3.5.1 Introduction

The scope and objective of this section of the report is as follows:

We have endeavoured, to the extent possible, to collect and present statistics on fraud with EPI’s, with relation to the type of service, type of EPI and turnover. We have consulted a number of sources of information to that purpose, including:

- Press reports
- Banks reports
- Regulator reports
- Payment organisations
- Our own network

The ultimate objective of this part of the study is to provide some insight:

- On the context and extent of actual fraud
- As to what exactly could be considered specific fraud related to electronic payment instruments – one could distinguish e.g. between fraud attempted or committed via new (electronic) channels (e.g. Internet), and fraud actually linked to the abuse of electronic payment instruments. The latter is the real subject of this study;
- Whether a trend is visible for such fraud cases;
- Whether security measures have (or could have) an influence on fraud numbers;
- Whether consumers are impacted and if so, to which extent.

The remainder of this section of the report contains the following sub-sections:

- Defining the context of fraud and indicating qualitatively the extent
- Definition of ‘fraud related to electronic payment instruments’
- Overview of information sources consulted with regard to fraud with electronic payment instruments;
- Overview of the statistics and related information obtained;
- Analysis and conclusions if possible.
3.5.2 Fraud Context

Fraud is a very broad concept, and no unique or unambiguous definition exists today. Fraud in the context of electronic payments is an important topic for consumers and is a very popular subject in the press. It is furthermore not easy to define fraud with electronic payment instruments, nor is it easy to find exact statistics on it. However, information and studies exist on:

- Internet fraud, not necessarily limited to payment fraud, but also including general scams e.g. inducing people to make transactions or to give away their payment credentials
- Payment card fraud, not necessarily limited to electronic payment fraud, but also including theft, counterfeit etc.

When looking at fraud and at the data currently available from mainly payment processing organisations, law enforcement and government organisations, we feel that these data could or should be presented along three dimensions, taking into account

- the type of service/activity
- the channel over which payments are made
- the mechanism by which fraudsters obtain payment credentials

The following diagram illustrates this:

![Diagram showing three dimensions of online fraud](image-url)
From the study we performed it became clear that statistics on fraud are currently not available in this format, but that some ‘qualitative’ conclusions can be drawn from the statistics and other data available:

- actual fraud on the Internet is real and exists, most particularly in some areas such as auctions, gambling and adult sites;
- the Internet seems, depending on the source of the information, to be more vulnerable to fraudulent transactions then the channels previously used; estimates vary around 5 to 30 timers higher rates.
- Financial damages are substantial; global bank card fraud for 2002 amounts to 3.8 billion USD\(^\text{67}\) according to Nilsson
- With regard to credit card fraud\(^\text{68}\), total amount of fraud for 2002 in the US amounts to 1.8 billion USD, of which 860 million USD is on-line fraud (fraud rate on-line 2.1%, or 30 times higher then off-line fraud rate of 0.07%)
- One of the most successful attacks on payment credentials is the theft (or hacking) of large databases of payment card data at merchant or payment processing sites;
- In most cases, financial damage is NOT with the consumer but  with merchants and financial institutions – most ratios indicate between 2% and 10% of damage to be taken by consumers. It is obvious that even if consumers are relatively safe for the consequences of fraud, the total amount of damage still remains.
- Actual fraud damage is, in 68% of the fraud cases lower then USD 250, and only higher then USD 1000 in 12% of fraud cases.\(^\text{69}\)

This concludes our statement on general fraud statistics. In the following section of the report, we have narrowed down the definition of fraud (see below) for the following reasons:

1. we have focused on what we believe is still a major concern with many consumers, i.e. the uncertainty on electronic transactions and what can happen with payments data sent electronically;
2. we believe that the way in which we define this sub-set of fraud has some value, in the way it demonstrates where risks are not so important.

\(^{67}\) The Nilsson Report, June 2003
\(^{68}\) http://www.epaynews.com/statistics/fraud.html#26
\(^{69}\) http://www.epaynews.com/statistics/fraud.html#26
The reader is asked to read the following section of the report with care, because the conclusions may at first sight be somewhat surprising, but the very narrow sub-set of fraud reviewed must obviously be taken into account.

3.5.3 Specific definition of "Fraud related to the use of electronic payment instruments”

3.5.3.1 Specific Definition

Given the fact that Fraud related to electronic payment instruments includes numerous aspects (see figure above)– we have narrowed down the most common definitions of fraud and selected the following to be within the scope of this part of our study:

- Counterfeit and copying of debit/credit cards, only in case data needed to successfully copy cards has been obtained through interception of electronic payments message or electronically stored data\(^\text{70}\)
- Counterfeit of electronic money, e.g. unauthorised re-loading of e-wallet
- Interception or unauthorised modification of electronic payment messages, e.g. money transfer through an Internet banking application.

Other fraud cases, e.g. card copying at shops, fraud at processing firms or mail firms, merchant fraud, family fraud etc., are not considered for this particular sub-set of fraud.

We have concentrated our review in this section of our report therefore around the following five questions:

1. Are there any reported cases of successful abuse of counterfeit or copied debit/credit cards based on interception or theft of electronic transaction data?
2. If so, what is the estimated amount of fraud compared to total volume of payment transactions.
3. Are there any reported cases of successful counterfeit electronic money (e-wallets, micropayments etc.)?
4. If so, what is the estimated amount?
5. Are there any reported cases of unauthorised modifications of Internet banking transactions?

\(^{70}\) This includes e.g. abuse of card data obtained through a hacked merchant database containing customer payment data, but this excludes e.g. physical card copying at shops.
3.5.4 Information Sources

Our research, including desk research of publicly available resources and interviews with payment and banking professionals has shown that:71

1. there are no statistics purely on fraud with electronic payment instruments
2. there are numerous statistics on card fraud (mainly ‘classic’ fraud, e.g. copying, theft)
3. there are statistics on Internet related fraud, including some payment fraud (which is also ‘classic’ in the sense that it is similar to e.g. credit card fraud with stolen card data or fraudulent merchants/buyers)
4. the only organisations that have a good view on the actual extent of electronic payment instrument fraud are the payment processors (credit card processors such as MasterCard, Visa or domestic debit processors such as Interpay, Banksys, …) - those organisations however do not publish fraud data and are very reluctant to disclose actual fraud cases or figures
5. the statistics available reflect the use of electronic payments instruments today – e.g. there are virtually no data available regarding fraud with pay-before products.
6. research results or statistics are often generic, and are rarely focused on specific countries

With respect to the five questions asked, the answers we would suggest are perhaps surprising:

1. Are there any reported cases of successful abuse of counterfeit or copied debit/credit cards based on interception or theft of electronic transaction data? 
   No reported cases found, a few suspected cases of successful interception/counterfeit. In contrast, there are multiple reported cases of theft of card/payment databases at merchant sites or payment processors, which confirms that payment security is much more dependent on overall site security than on inherent security of the payment instrument.
2. If so, what is the estimated amount of fraud compared to total volume of payment transactions? 
   The actual amount, limited to our definition, is not known. It should be very small given the almost non-existent occurrence. Actual financial damage for genuine consumers is non-existent.
3. Are there any reported cases of successful counterfeit electronic money (e-wallets, micropayments etc.)? 
   No cases found.
4. If so, what is the estimated amount? 
   None.
5. Are there any reported cases of unauthorised modifications of Internet banking transactions? 
   No reported cases of deliberate unauthorised access. There are a number of known cases where poor application and site security compromised confidentiality of Internet bank accounts. Theoretical review and intrusion tests show that some Internet bank solutions and implementations could be vulnerable.

71 Some of the bullet points below are already listed in the previous section of the report, but are included again for completeness purposes.
Since there are no statistics readily available specifically on the fraud cases as defined in the scope of our study, we have taken statistics as close as possible to draw some possible conclusions. These mainly include statistics on card fraud and Internet fraud.

The following sources were consulted:

- Source 1 – www.fraud.org
- Source 2 – about.ccbil.com
- Source 3 – www.cardwatch.org.uk
- Source 4 – our own network
- Source 5 – interview with Corporate Security and Fraud manager of large payment processor.
- Source 6 – Interviews with banking officials
- Source 7 – Our own survey and experience in this matter; we have both used our own previous assignments in this matter, as well as the self-assessment questionnaires sent to the webmasters of all reviewed sites.
3.5.5 Fraud Statistics and Other Fraud Related Information

3.5.5.1 Source 1 – www.fraud.org

Payments made on the Internet are not always payments by EPIs (and vice-versa), but could involve the more classical ways of payments too, e.g. ‘online auctions’ where the buyer pays the money in advance to the seller bank account or pays cash, etc.

Nonetheless it is interesting to see where Internet fraud actually happens:

The top Internet fraud “scams” numbers, from 1999 to 2001, indicate that online-actions still account for the majority of the scams (87% to 70%), and that “general merchandise scams” are second with 7% to 9%. When looking at how payments were made in cases of Internet fraud, the ratio of credit card payments has increased and now stands almost at the same level as money orders.
3.5.5.2 Source 2 – about.ccbill.com
This source groups different sources on online fraud in business. Amongst its findings and trends:

- 1% of all credit card transactions in brick and mortar stores today are fraudulent, but nearly 10% of all Internet transactions are fraudulent (Source: Meridien Research, Inc)
- Online credit card fraud rates are three of four times of retail-related fraud in general. Consumers believe that their credit card is 12 times more likely to be defrauded online than offline (Source Jupiter Media Matrix)
- The average credit card fraud rate is 7 cents per 100$, compared with the online rate of between 25 & 28 cents per 100$ charged online.
- In most cases of online fraud, the merchants have to bear the damage (88%). In 10% of the cases the merchant banks bears the losses, and only in 2% consumers are ultimately liable.

3.5.5.3 Source 3: www.cardwatch.org.uk
The information published by cardwatch allows users to estimate the relative importance of Internet related card fraud compared to overall card fraud numbers.

![Credit card fraud by type (%)](image)

“Most Internet fraud involves criminals using card details fraudulently obtained in the real world to make card-not-present transactions in the virtual world. Currently such fraud on Internet transactions is low - estimated losses remain modest at around £12 million,(UK only) around three per cent of total card fraud losses.”

The diagram above shows the different kinds of credit card frauds. Internet credit card fraud, which is part of CNP or Card Not Present fraud, is only a part of one of the three main categories of credit card fraud.
3.5.5.4 Source 4 – Our own network

PricewaterhouseCoopers conducted a study in business week with dealt with the issue of online credit card fraud in the USA, which we believe is also relevant to Europe.

Two comments made by PwC are relevant for this study:

1. e-Business Risk: Lessons from the past, by John Musgraeve (comments on an article in Business week).

2. Dispelling the myth on Internet Security Issues by Rosie Lombardi

This study shows on-line credit card fraud amounts to a minuscule 0.05 per cent of all cheque and credit card fraud. In reality, consumers today are much more likely to be victimised by lower-tech fraudulent means such as telephone scams or a waiter stealing a credit card number.

Once again this study confirms that not customers, but merchants are bearing most of the risk. An individual's liability is generally limited to $50 for lost or stolen credit cards. The study further comments that general security levels are low, resulting in other then payment security problems (e.g. denial of service attacks), which cause substantial more damage then payment fraud.

3.5.5.5 Source 5: Interview with Payment Processing Firm

We interviewed an official at a major credit (and debit) processing firm. According to this official, the rate of fraud on the Internet (with credit cards) is no higher then fraud that is committed offline. However some specific sites are more vulnerable to fraud (online gambling sites, adult sites). Huge penalties are imposed to these websites in case of fraudulent transactions in order to solve this issue, with relative success.

Other points from the interview include:

- Fraud numbers differ between US and Europe because of the fact that telecom costs in US are lower. In the US 100% of all traffic goes online, in Europe this is only 65%. This results in different fraud types between US and Europe.
- In more than 90 % of online frauds the financial damage is taken by the merchants, not by the consumers;
- New technologies are being put in place (with the support of the EU commission) to combat the fraud risk in card not present transactions. (E.g. verified by VISA, authentication of cardholder by chip card, adding of a parameter to the card e.g. the validation date)
- The EU is also putting in place the necessary legal framework to combat plastic card fraud. There is an ongoing collaboration between the payment industry and the Commission on this subject.
3.5.5.6 Source 6- Interview with Banking and Payment Industry officials

We have inquired with a number of banking officials and payment industry officials. As far as the scope of our review concerns (see the questions in the introduction section), no incidents or fraud cases as determined in our scope have occurred over the last year. The countries covered in this exercise were Belgium, The Netherlands, the UK and Greece. In total, 8 Officials were contacted and we received 6 replies.

3.5.5.7 Source 9- PricewaterhouseCoopers’ experience and survey

When reviewing our own experience and contacting our own network, we have noted only one instance where card data and PIN-code data were successfully intercepted and probably decrypted, resulting in a large number of counterfeit cards. There was no financial loss involved for the cardholders. The actual fraud took place outside the EU, but the counterfeit cards were used within EU territories.

In the self-assessment questionnaire sent to the webmasters of the sites reviewed, we have asked the question whether the site had suffered from fraud, and if so, what the extent of the damage was. We have received no positive answers to these questions, i.e. no fraud was mentioned.
3.5.6 Analysis and Conclusions.

Based on the very limited statistical data available, and based upon our experience and interviews, our conclusions for the reduced definition of fraud with payment instruments are as follows:

- Classic credit cards and the way they are used make them vulnerable to fraud, and their use over the Internet has increased this risk. However, most fraud observed is not linked to the ‘electronic’ nature of the transaction (see our restricted definition of fraud) but is an extended form of the classic and known fraud schemes.
- Older card technology (magstripe instead of chip-cards) is inherently more vulnerable to fraud – counterfeit cards, intercepted transaction data etc.
- New technology (chipcards) is available, and there are no documented cases of successful fraud when these technologies’ security features (card authentication mainly) are fully utilised.
- We have not found any documented cases of successful fraud of pay-before products or internet-banking fraud.
- In the majority of fraud cases, there was no financial loss for the consumer and the risk was at the merchant.
- There are no statistics or facts that can substantiate the public perception that ‘paying with a credit card over the Internet’ is substantially more unsafe than paying with the same card at a restaurant or that this brings a financial risk to the consumer. It is important to realise that only a few of the perceived threats are substantiated by the facts, i.e.
  - Poor security at merchants or processing companies, allowing fraudsters to steal large amounts of card data, allowing them to abuse these cards -> **Real and Important Risk** – not specific to ‘electronic payment’
  - Unreliable merchants (or co-consumers in the case of auction sites e.g.) resulting in goods not delivered to expectations -> **Real and Important Risk**, – not specific to ‘electronic payment’
  - Actual financial loss for the consumer is virtually non-existent, since the risk for most Internet (credit-card) payments is with the merchant -> No real risk for consumers
  - Successful interception and abuse of card data has virtually not been reported yet – and even in case this would happen, the risk is again most probably with the merchant -> No real risk for the consumer
  - For other electronic payments, e.g. pay-before cards, debit cards, electronic banking, the opinions are much more favourable, which is also substantiated by very limited or absent reports of fraud.
4 Part 4: Level and Quality of Information Provided to Consumers

4.1 Level and quality of information provided to consumers on the technical security solutions in place
4.2 Executive Summary

The easy accessibility offered by the Internet today enables the average consumer to become a more systematic user of the network and to approach in an easy way a wide range of new products and services. e-payment systems are simultaneously a new area of services but also a means to acquire them.

In principle, anyone can now execute by himself complicated and risky transactions. The typical thing with e-payment services is that, since less personal contact is involved in the e-payment transaction, consumers have, to an ever-increasing degree, to interpret by themselves information provided at a distance about the use, functionality and security of EPIs.

This part of the study primarily concentrates on the level and quality of information provided to consumers in relation to the technical features of the e-payment solutions in place. In particular, we looked into

• whether any information at all supports the use of a given EPI and the carrying-out of an e-transaction in general;

• the nature and quality of the information communicated to consumers about the security aspect of e-payment methods and products in use; and

• whether the security-related information is brought to the knowledge of consumers in such a way (appearance and form of information) as to raise their confidence in the quality and efficiency of the technical means implemented in or supporting e-payments.

There is no uniform approach at the EU level about which informative elements should be drawn to the consumers’ attention in relation to the security of e-payments and in which form.

The results of our findings vary when making a distinction between two market categories:

(1) the financial institutions and banks who integrate EPIs and e-payment solutions in their business in a professional way and as a kind of “buy-in” product, and

(2) e-merchants using EPIs as a means of obtaining payment from their clients.

4.2.1 Key findings on the level and quality of information provided by financial institutions

This market category is more attentive in making the public aware about the security features of the e-payment solutions they put forward. On an average basis, banks and Payment Service Providers communicate such information in a standardised and proactive way and in a sufficiently clear and consumer-friendly language. Nevertheless, despite these overall positive results, there is still a need for more transparent availability of information with regard to a number of security aspects, which continue to be of concern to consumers.

It is noteworthy, for instance, that only a few e-banking websites provide explanations about

• the kind of customer information they store;

• the rules and processes of data storage;
• the confirmation process for transactions processed;
• the assurance that the given EPIs offer to counter-parties against the risk of non-repudiation;
• the problem-solving mechanisms that the financial institution in question has put in place to encounter failures or deficiencies of the applications system used.

4.2.2 Key findings on the level and quality of information provided by e-merchants

Our findings are less encouraging with regard to the efforts displayed by e-merchants to provide full and clear information about the security of the payment systems they propose on-line.

Information that is often missing from the e-commerce websites is for example:
• how e-merchants verify their customers’ credentials;
• whether buyers have the possibility to check the details of the payment ordered before execution;
• whether and how payment has indeed been performed; and
• how the e-payment system may prevent repudiation.

However, it is difficult to make an overall general estimation for this market category, since:
1. more strict regulatory approaches may be followed in some countries compared to others, given the lack of any EU-wide formal legislative approach on the informative elements that should be communicated to consumers with regard the security of e-payment systems, and
2. e-merchants are not themselves providers of e-payment solutions, as is often the case of financial institutions and banks, so communication of important payment-related information is sometimes provided “by reference” to the websites of the service provider(s) offering the EPI in question.

4.2.3 Conclusions

As for the quality of information provided to consumers about the security of EPIs, a distinction should be drawn on the basis of the market category supplying such information. It is noteworthy that explanations about the given EPI or EPS are more explicit and consumer-friendly on the side of market segments that offer EPIs or EPSs as a professional service. This is generally the case of financial institutions and banks that put on the market such payment solutions as a new business product.

On the contrary, categories that will use the given EPI in the framework of their e-commerce operations as a pure means of payment, exclusive or not, are less concerned about making their customers fully confident in the security features and mechanisms supporting the e-payment solution they put forward. In the last case, important security aspects are often not clearly addressed by e-merchants, or reference is made to the websites or other information sources of the payment service providers.
However, it should be stressed that, although this observation reflects the average picture at the EU level, it would be risky to make generalisations, since national legislation, (sector-specific or general fair trade practices rules of the given country) or even self-regulatory initiatives, may impose stricter rules on the kind of information that should be communicated to the public and on the way that this needs to be done.

As for the consumers’ approach, it has been identified that in some countries, consumers seek by themselves security-related information on many occasions in a proactive manner. The incentive of this appears to be mandatory legislation in a few cases or, simply, in most cases the consumers’ better awareness of the security risks involved in e-payment operations. If the adoption of mandatory legislation cannot be regarded as a solution reaching market consensus (consumer organisation being for the adoption of a harmonised legislative framework whilst EPIs’ operators and banks are not), it is clear that common self-regulatory approaches and encouragement of consumers’ education on an EU scale is generally considered as an appropriate means to streamline the existing diverging approaches on the nature and quality level of security-related information that need to be communicated to consumers.

As for the form, content and availability of the security-related information, best practices are developed, sometimes boosted by national legislation. The majority of banks consider that they comply with the general fair trade practices principles stipulating the in-time and accurate communication of comprehensive information to consumers, moreover they also feel that they are proactive enough to implement consumer-friendly approaches in the communication of security-related information before specific problems arise. On the contrary, consumer organisations stress that there are still a lot of issues that remain unclear to consumers regarding e-payments (for instance, liability, role and responsibilities of all parties intervening in an e-transaction if a security threat occurs). A legislative solution with a view to streamlining the quality and appearance of security-related information furnished to consumers across the European Union may be a possible remedy according to the majority of consumer protection bodies. However, a legislative approach is welcome on the side of bank institutions and Payment Service Providers only in isolated cases. On the contrary, these market categories believe that the level and quality of security-related information can be enhanced effectively, only through self-regulatory initiatives and consumers’ better education.
4.3 Objectives and Work Scope

4.3.1 Introduction

This part primarily concentrates on the level and quality of information provided to consumers in relation to the technical features of the e-payment solutions in place.

Our findings are eloquent about the fact that, in connection to e-payments, consumers are invited to use new state-of-the-art technology in a constantly changing applications environment. We saw that e-payment systems change the traditional communications and operational interfaces consumers have been used to until nowadays: payments can now be made at a distance and in the absence of any face-to-face contact. However, the fundamental consumers’ requirements for easily-obtainable, accurate, useful and objective information have not changed, despite of the fact that technology offers now alternative ways of making payments by virtual means.

The lack of personal contact and of the “hand-to-hand” execution of a payment undoubtedly makes consumers feel insecure about their payments. A first concern is whether the e-transaction has indeed been performed. Other questions arise after that, for instance, whether the payment was made in the way in which it was intended to. Applying the general rule of fair trade practices in the e-payment case as well, one should admit that, at least from a consumer’s perspective, the feeling of uncertainty about the efficacy of a product or service can be lowered if consumers are in a position to make informed choices about the different kind of services and equipment available to them.

Having this in mind, it is believed that consumers are hesitant to use Electronic Payment Instruments (EPIs) and Systems (EPSs) because, among other reasons, they are not sufficiently aware of how securely their transactions are carried out through these means of payment. The first part of the study discussed, inter alia, this hypothesis. In parallel to the findings of part I, we attempt in the following chapters to evaluate the quality, comprehensibility and accessibility of information available to consumers about the technical assurance of e-payment products and applications that are currently used.

4.3.2 Objectives

We have discussed so far the security of EPIs and EPSs from a technical and comparative point of view, as well as the implementation of the given security solutions in practice.

The goal of this part is threefold: first of all, to find out whether any information at all supports the use of a given EPI and the carrying-out of e-transactions in general. Presuming that the answer to the first question is yes, the task then is to look into the nature and quality of the information communicated to consumers about the security aspect of e-payment methods and products in use. The third concern is to investigate whether the security-related information is brought to the knowledge of consumers in such a way (appearance and form of information) as to raise their confidence in the quality and efficiency of the technical means implemented in or supporting e-payments.

72 In this sense, see also publication of the National Consumer Council, UK, Communications Reform, Submission to the Department of Trade and Industry and the Department for Culture, Media and Sport, June 2000, p. 3, available at: http://www.ncc.org.uk.
In this respect, the emphasis in the chapters below is put on highlighting what kind of information is made available to consumers before, at the time or after they have made an e-transaction. Concurrently, the analysis will examine how this information is communicated to consumers either individually or in public.

### 4.3.3 Outline of Methodology

The one facet of our analysis (indicating the consumers’ trust in e-payments) is covered through input received by different categories of market players on the basis of a public survey that we undertook in Part 3 of this study. These results were compared to the findings on the consumers’ general perception of the security of EPIs that has been discussed in previous parts of this study (especially, Part 1).

The fact-finding relating to the second objective (research and assessment of the information supplied to consumers relating to the security of EPIs) were gathered on the basis of a selective screening of websites providing this kind of information. Basic guide to the carrying-out of this assessment was the statistical information provided in the previous part (Part 3) through the individual examination of a representative sample of websites. In addition, valuable data in this respect have been collected through the public survey that we undertook.

The detailed methodology used to carry out the public survey and of the overall work done is discussed in detail in Appendix 4.

### 4.3.4 Definitions

Since the reflections that follow address one particular market category, being the consumers as actual or potential users of EPIs, it is deemed worthwhile to clarify the meaning of consumer. In the view of the consolidated community legislation[^73] and most member-states’ laws on consumer protection, consumers are:

> Private individuals acting with a private purpose without any commercial intention and outside their trade, business or profession.

On the other hand, we found it essential to choose for the purposes of the public survey a rather “objective” terminology addressing the e-payments area. To this end, we referred to the definition of EPIs as being led down in the Recommendation of the European Commission concerning transactions by EPIs and in particular the relationship between issuer and holder (97/489/EC)^[74]. This act defines an Electronic Payment Instrument as:

> A remote access payment instrument, being an instrument that enables a holder to access funds held on his/her account at an institution, whereby payment is allowed to be made to a payee and usually requiring a personal identification code and/or other similar proof of identity. This includes in particular payment cards (credit, debit, deferred debit or charge cards) and phone- and home-banking applications.


or

An electronic money instrument, being a reloadable payment instrument other than a remote access payment instrument, whether a stored-value or a computer memory, on which value units are stored electronically, enabling its holder to effect transactions that are defined below (see, Work Scope).

4.3.5 Work Scope

It should be stressed that the scope of the findings highlighted below relate only to the use of EPIs in an electronic environment, meaning primarily:

- Paying on an e-commerce website (e.g., with a credit card)
- Transferring money through an e-banking application.

Thus, electronic transactions used in traditional stores were not investigated, since the emphasis was placed on those payments in which an electronic medium, e.g., Internet, telephone, mobile phone, plays a role in order to carry out the payment at a distance. The different kinds of payment cards (e.g., credit, debit etc.) are therefore covered only insofar as they are associated with the use of an electronic communications environment or system to carry out a payment operation online:

- Internet/web-site payment associated with any kind of payment cards (including smart cards and stored value cards)
- Digital cash
- Electronic wallets
- Home and phone-banking
- Payment through (mobile) telephony bill
- m-commerce (paying using a mobile phone)
- t-commerce (as seen on TV using technology embedded in the set top box).

On the other hand, it was not our intention to look into the general feeling of security consumers have when carrying out e-transactions. Issues addressing the protection of consumers in general when using EPIs, which are mostly related to traditional banking business and not technical security as such, are not discussed under Part 4 either. Consequently, questions addressing cool off period, privacy protection in general, refund or compensation mechanisms, information available to consumers about costs and charges when using an EPI, are excluded from the scope of this part.
4.4 Quantitative Findings

4.4.1 Security threats subject to information requirements

We identified in Part 3 seven key areas considered to be sensitive enough to be a potential source of concern for consumers in relation to the security assured in an EPI prior to, during or after making an e-payment. Those issues are most of the times preceded by a more generic one concerning the usability, functionality and added value of a given EPI or electronic payment application.

To put it simply, a consumer willing to perform or having already performed an electronic payment operation may be required to have adequate information on the following:

1. **The customer (= originator of the payment instruction) needs assurance that his payment transaction is made to the correct counterpart (= receiver of the payment instruction)**
   - How the sender (originator) is identified during and after an e-transaction;
   - How the recipient is identified during and after an e-transaction;
   - How to ensure that the e-transaction took place as due.

2. **The customer wants assurance that the counterpart can link the payment instruction to him, and that this link cannot be denied**

3. **The customer wants assurance that the information given to the counterpart in a payment instruction cannot be (re-)used by another party e.g. to generate another, fraudulent, transaction**
   - Protection of financial and personal data in case of fraudulent use of a given EPI;
   - Protection of financial and personal data in case of theft, loss or accidental misuse of a given EPI;
   - Protection of financial and personal data against intrusions and/or fraudulent use of the e-payment system used;
   - Description of processes and mechanisms, including description of appropriate technical safeguards, to fully protect the information transmitted all through the e-payment process against unauthorised disclosures;
   - Description of security features embedded into the given EPI or EPS to detect, prevent and counter third-party intrusions or other abuses. Description of security features (e.g., special security tokens) embedded into the given EPI or EPS to alert the user in time in case of technical shortcomings or failures of the operating system.

4. **The customer needs assurance that the counterpart has received his payment transaction**
   - Explanation on the confirmation procedure following an e-payment transaction.

5. **The customer needs assurance that the transaction integrity is maintained, i.e. that the transaction will be completed, that the amount and other parameters remain unchanged and that the transaction will be executed only once**
   - Description of security features (e.g., special security tokens) embedded into the given EPI or EPS to stop the e-transaction in case of accidental misuse, technical shortcomings or failures of the operating system;
   - Possibility for the customer to perform a final check before authorising the transaction;
• Explanations provided after a technical shortcoming or failure has been occurred.

(6) The customer needs assurance that only duly authorised payment transactions are executed

(7) The customer needs assurance that he has recourse in case of problems with payment instructions

• Availability of information on the mutual responsibilities of the parties involved in an e-payment transaction (system operator / payment service provider / consumer);
• Information about limitations of liability;
• How to rectify the operational/system fault;
• How to react in case of operational failures;
• How to minimise the direct and consequential damages.

The results of the website assessment in relation to information provided in each of the security areas highlighted above have already been analysed and measured under Part 3 of this study. Those results contribute to the assessment of what kind of informative elements are communicated to consumers relating to e-payments and illustrate by figures whether or not such information is indeed communicated and how the security-related information is provided.

Further to the review of what kind of informative elements are communicated to consumers relating to e-payments and how often information relating to the seven security objectives outlined above can actually be found on websites, this section attempts to demonstrate “how” this information is communicated on currently operational e-commerce and e-banking websites. The quantitative figures that are shown in this section result from the survey of the sample of e-banking and e-commerce websites that we discussed above.

It is an established principle of the consumer protection law that information communicated to consumers should in general be widely available, easily accessible and comprehensible.

Accordingly, the sections below present the results that come out of the websites’ assessment at the application of these three criteria:

• Availability
• Accessibility
• Comprehensibility

4.4.1.1.1 Availability of security-related information

The first basic need of the average consumer at the supply of any products or services is to learn what the offered product or service is and how it actually works. The law on fair trade practices in all EU member states stipulates expressly the service provider’s obligation to disclose certain information relevant to the product or service.
Therefore, the starting point of our website assessment was to examine whether or not the websites surveyed provided any general information on the meaning, technical description and functionality of EPIs, namely on

- The technical features of an EPI, usability, purpose and added-value of their implementation;
- Instructions about how to use an EPI;
- Instructions about how to prevent physical, functional or other defaults of an EPI and/or flaws of the e-payment system in question.

Our findings are summarised as follows:

- On average, 60% of the e-commerce websites visited contained explanations about how the website secured e-payment transactions. The overall results, however, show significant disparities in the availability of this type of information across the European Union.

4.4.1.2 e-commerce websites

- Security-related information was found on over 75% of the e-commerce websites scanned in France, Spain and the UK.
- In nine (9) countries\(^{75}\) the ratio was below the EU average, the lowest being 28% (nearly the one-third of the e-commerce websites of the sample) in the Netherlands.

4.4.1.3 e-banking websites

- With respect to the e-banking websites surveyed, the results of the survey are even more encouraging. The overwhelming majority of the websites surveyed (on average, 86%) contained an explanation of the website’s security features.
- In eight (8) member states\(^{76}\), all the financial institutions surveyed supplied security related information on their websites. This figure fell below 70% only in one country (Portugal).

The Charts below illustrate these findings:

\(^{75}\) These countries are: Germany, Italy, Portugal, Sweden, Finland, Ireland, Luxembourg, Austria and the Netherlands.

\(^{76}\) These countries are: Denmark, Finland, Greece, Ireland, Luxembourg, Spain, Sweden and the Netherlands.
Figure 98 e-commerce websites, security features
4.4.1.4 Accessibility of security-related information

The information provided to consumers should be made available in such a way that it is not difficult for an average consumer to find.

In Part 1 above, we saw that a small, though not negligible percentage (10.42%) of the responses to the public survey confirmed that insufficient information about the security of EPIs is a barrier to the wider use thereof. In the light of this finding, it seems that informative elements, which, in the view of the average consumer, can significantly influence the final decision to use or not an e-payment application, should be within an easy reach to him/her. Accordingly, consumers should not need to make any special or extraordinary effort to find the information.
The findings of our survey regarding the level of accessibility of the security-related information on the websites scanned are resumed as follows:

- On average, explanations on the security features were easy to find on 58% of the e-banking websites and on 26% of e-commerce websites visited.
- Where security-related information was easy to find, it was made available either in the general frame or as a link on each web page.
- In many cases, the security-related information was part of the Frequently Asked Questions (FAQ) section of the website, often only as part of other general issues relating to the use of e-commerce functions.

4.4.1.5 e-commerce websites

- While the large majority of the visited e-commerce websites in the United Kingdom contained explanations about the security feature in use (77%), in only 12% of the cases could consumers find such information easily.
- During the survey, difficulties were experienced to find security-related information on Austrian e-commerce websites: While 31% of all the sites surveyed did contain such information, in only 6% of the cases was it easy to find.

4.4.1.6 e-banking websites

- Financial service providers take care in making security-related information easily accessible on their websites, in the majority of the cases (average 57%) by providing a permanently visible link in the general frame.

The charts below illustrate these findings:
Percentage of E-commerce websites where the security information is easy to find

- France: 47%
- Spain: 45%
- Denmark: 38%
- Greece: 36%
- Italy: 35%
- Belgium: 33%
- Average EU: 26%
- Germany: 26%
- Portugal: 24%
- Luxemburg: 17%
- Finland: 14%
- Ireland: 11%
- United Kingdom: 11%
- Sweden: 10%
- The Netherlands: 8%
- Austria: 6%

Figure 100  % e-commerce websites where security info is easy to find
Figure 101  Percentage of e-banking websites where security info is easy to find
4.4.1.7 Comprehensibility of security-related information

Making security-related information comprehensible means that, it should appear in a clear and explicit manner, drafted in a wording that attracts consumers’ attention and makes it understandable to an average consumer.

Accordingly, the explanations shall be given in a plain and not technically heavy language. Technical information shall also be provided in a way that reflects layman thinking without supposing or requiring specific IT knowledge (e.g., in relation to encryption etc.).

With reference to our previous findings regarding the accessibility of information, we would also point out that complicated or too technical wording can practically make the information “inaccessible” to an average consumer.

In this respect, our survey illustrated the following:

- Where information is available on the website, it is drafted in an easily understandable way in 83% of the e-banking websites surveyed and on 55% of the visited e-commerce websites.
- In some cases the aspiration to avoid difficult language results in explanations that are too brief or too general to inspire consumer confidence.
- It is noteworthy that, in certain countries, whereas e-merchant websites failed to provide clear security-related explanations on their websites, the e-banking websites of the same country showed a high level of user-friendly wording (e.g., Sweden, the Netherlands and Luxembourg).

4.4.1.7.1 e-commerce websites

- Clear, comprehensible explanations were available on a large number of e-commerce websites surveyed. We only found sporadic examples of confusing or overly technology-heavy wording.

4.4.1.7.2 e-banking websites

- In eight (8) countries77, all the websites surveyed demonstrated full (100%) compliance with the comprehensibility requirement.
- The level of compliance in the other member states can also be considered high, with only four countries78 falling below the high EU average of 83%.

The charts below illustrate these findings:

---

77 These countries are: Denmark, Finland, Greece, Ireland, Luxembourg, Spain, Sweden and the Netherlands.
78 These countries are: France, Belgium, Italy and Portugal.
Percentage of e-commerce websites where the security information is elaborated in a clear comprehensive language

- France: 77%
- United Kingdom: 76%
- Spain: 71%
- Germany: 57%
- Average Europe: 55%
- Italy: 55%
- Greece: 55%
- Belgium: 52%
- Denmark: 46%
- Portugal: 43%
- Finland: 36%
- Ireland: 33%
- Austria: 25%
- Luxemburg: 17%
- The Netherlands: 16%
- Sweden: 15%

Figure 102: % e-commerce websites with clear info
Percentage of e-banking websites where the security information is elaborated in a clear comprehensive language

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Netherlands</td>
<td>93%</td>
</tr>
<tr>
<td>Sweden</td>
<td>87%</td>
</tr>
<tr>
<td>Spain</td>
<td>83%</td>
</tr>
<tr>
<td>Luxemburg</td>
<td>83%</td>
</tr>
<tr>
<td>Ireland</td>
<td>83%</td>
</tr>
<tr>
<td>Greece</td>
<td>83%</td>
</tr>
<tr>
<td>Finland</td>
<td>83%</td>
</tr>
<tr>
<td>Denmark</td>
<td>83%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>83%</td>
</tr>
<tr>
<td>Germany</td>
<td>83%</td>
</tr>
<tr>
<td>Austria</td>
<td>83%</td>
</tr>
<tr>
<td>Average EU</td>
<td>83%</td>
</tr>
<tr>
<td>France</td>
<td>71%</td>
</tr>
<tr>
<td>Belgium</td>
<td>67%</td>
</tr>
<tr>
<td>Italy</td>
<td>64%</td>
</tr>
<tr>
<td>Portugal</td>
<td>43%</td>
</tr>
</tbody>
</table>

Figure 103: % e-banking websites with clear info
4.4.2 Conclusions

Our concluding remarks concerning the measuring of the websites assessed against the availability, accessibility and comprehensibility criteria are the following:

• The e-banking websites across the European Union already meet these criteria at a satisfactory level (as shown in the above figures)

• The majority of e-commerce websites provide security-related information, drafted in most of the times in a clear and comprehensible language. However, it is often difficult to find this information.

• On average within the European Union, e-commerce websites still show a lower level of prudence in explaining their security features to users, but the differences between countries, as well as among individual e-mERCHANTS within the same EU member state, are significant.
4.5 Qualitative Findings

4.5.1 Public survey

4.5.1.1 Objectives

In the previous chapter, we furnished some quantitative data indicating the responsiveness of e-banking and e-commerce websites to the need of informing consumers vis-à-vis a number of security threats. We also attempted to assess security-related information provided on the websites screened against three quality criteria: the availability, accessibility and comprehensibility of informative data addressed to consumers on these websites.

In this chapter, we first attempt to identify the nature of informative data that consumers feel concerned to be aware of in order to make e-payments. The data have been collected through a market survey inviting a number of market players to respond to a questionnaire tackling the core issues of our subject matter. The market categories that have been selected to co-operate for the purposes of our investigation were:

- Financial institutions (banks, credit institutions, bank associations at member state level);
- Consumer protection organisations and other bodies representing consumers’ interests;
- Other authorities at the member state level, notably bank and consumer Ombudsmen, more rarely public authorities as such;
- Providers of different services (such as payment or insurance service suppliers etc.).

A sample of the questionnaire(s) sent (both ordinary form and simplified version), as well as a summary of the methodology used to approach these organisations and the difficulties encountered, can be found in the Appendix 4.

Second, on the basis of the responses received through the survey, we provide indications on how the market categories surveyed assess themselves the quality and level of security-related information provided to consumers. The criteria used for this assessment are highlighted in the section that follows. They tackle in substance the same issues that were identified as potential security threats or risks in Part 2 of this report.

Third, in the light of comments and other remarks that we received through the survey, we discuss in a separate section the recommendations of the market players on how making the security-related information more accurate, transparent and reliable to the eyes of the average consumer.

We shall stress however that, given the fact that feedback was sought directly from the market players concerned with the subject matter, some of whom are engaged in e-payment operations and, as normal, defend their own professional interests and practices, the results of the survey shall be regarded with a certain caution. On the other hand, and despite our systematic efforts to receive as much feedback as possible, not all market
players contacted in the EU member states were always either willing or in a position to help with this exercise.

The total number of contributions that we received until the day of the drafting of the present document amounts to approximately 60, varying between complete responses to questionnaires, partial answers, excuses for inability to reply or forwards to more appropriate representative bodies. 150 organisations were approached either by writing through telephone interviews or, most of the times, by both ways.

Nevertheless, the findings that we present below, being the results of a careful comparative evaluation of all answers received, reflect common concerns and, therefore, shall be treated as a relatively reliable indication. Whenever we present a finding deviating from the general view expressed in the rest of responses received, we make explicit reference thereof.

4.5.1.2 Assessment criteria
Basic indicators of our structuring the questionnaire of the public survey were:

➢ Measuring consumers’ need(s) in terms of security-related information
The organisations/bodies contacted were asked to report the consumers’ queries or complaints that they may have received about the lack or insufficiency of information received regarding the security of EPIs.

As indicative cases, we highlighted:
- Queries or concerns about how to use an EPI or EPS
- Identification concerns
- Concerns of evidence
- Data Protection concerns
- Security against fraudulent use of EPI or hacking of EPS
- Integrity concerns (payment made to the right counter-party, in-time, with the right amount, with adequate proof of payment).
- Questions of functional security (system failures, other technical operational problems).

➢ Criteria of self-assessment of the quality and level of information provided
As mentioned above, the criteria that we used in order to evaluate the quality and level of information supplied to consumers express basically the potential security threats being the subject of the quantitative findings.

The issues below try to identify the nature and kind of security-related information sought by consumers.\(^{79}\)

In the public survey, we put forward these criteria in the form of questions. These questions try to identify the manner in which the information is provided (the ‘how’). Accordingly, the entities approached were asked to report\(^{80}\):

---

\(^{79}\) The full content of questions asked can be found in Appendix 4.
• **In what circumstances** the information is provided. The possible answers could be:
  - Standard, in a proactive manner without the consumer having expressed a prior request.
  - After the consumer’s explicit request (orally or in writing)
  - In other ways [to specify].

• **Where** the information is provided. The possible answers could be:
  - On the website (of the e-merchant or Payment Service Provider)
  - In a hard document (user’s guide, promotional leaflet, brochure, other documentation provided in hard copy etc.)
  - By contract (and if yes, where in the contract: separate annex, body text, general terms and conditions etc.)
  - Only orally
  - Indirectly (by indicating, for instance, the website of other party - Payment Service Provider etc.)
  - Other location(s) [to specify].

• **When** the information is provided. The possible answers could be:
  - Before signing the services agreement or engaging in the e-payment operation
  - Upon performing the e-payment operation
  - After signing the services agreement or performing the e-payment service.

• **How** the information is worded. The possible answers could be:
  - In a clear, comprehensible, user-friendly wording and layman’s language
  - In a confusing, complicated wording in a technology-heavy language
  - In another way [to specify].

• **How** the information appears. The possible answers could be:
  - In big, clear letters, in a visible location/link on the website
  - In small, fade letters, information scattered in different locations on the website, through hidden links;
  - In another appearance [to specify].

At the end of these questions, the respondents were asked to give their own opinion about the level and quality of security-related information provided. The quality levels indicated in the questionnaire were the following four:

- A very poor and inadequate level to inspire consumers’ confidence
- An adequate level
- A satisfactory level
- A very good level.

---

80 The full content of questions asked can be found in Appendix 4.
Three tables enclosed in the appendices\textsuperscript{81} guide the reader in assessing the qualitative findings. These are:

- A first table ("General Overview of Responses") illustrates the number of responses received, if any, as per country and market category.
- A second table ("Summary of Qualitative Findings") presents in the form of columns the input to each question of the questionnaire. We distinguish between three market categories:
  - Financial institutions (being primarily responses received by banks and bank associations);
  - Providers of services and other authorities (notably, Payment Service Providers -PSP-, Ombudsmen and providers of other services (e.g., insurance);
  - Bodies, at the European or national level, representing consumer interests.
- A third table ("Detailed Overview of Responses") indicates the responses received as per country and market category, as well as of the reference source (answer by questionnaire, documentation or other).

The qualitative results are analysed in the following section.

They are completed with additional comments drawn up on the basis of documentation that some organisations sent to us in support of their responses.

\textsuperscript{81} See Appendix 4
4.5.2 Analysis of qualitative findings

4.5.2.1 Preliminary Research

As shown in the tables enclosed in Appendix 4, a lot of the organisations contacted through the survey confirmed that they were not in a position to provide full or sometimes even partial answers to the questionnaire for the following reasons:

- They had received no complaints addressing specifically the lack of information available to consumers in relation to the security of e-payments. On the other hand, some bank institutions\(^\text{82}\) reported that the majority of complaints they receive are related to traditional banking business when using EPIs, not to the technical security \textit{per se} thereof.
- There is no information available (statistical or service reports) to document their answers.
- Although such queries or complaints may have been addressed at member-state level, there is no efficient communication thereof between the authorities in charge of these matters (bank institutions, ombudsmen or consumer organisations and Payment Service Providers).

Some respondents stressed, however, that the lack of incoming data about how consumer perceive the security standards of the e-payment environment does not mean that consumers are confident in carrying out transactions on-line. One reason of this hesitance is that consumers still believe that EPIs and EPSs involve high security risks\(^\text{83}\).

4.5.2.2 Responses to SECTION I of the questionnaire\(^\text{84}\)

4.5.2.3 Nature of consumer complaints reported

4.5.2.3.1 Security against fraudulent/unauthorised use of EPIs

Comparing the negative to the positive replies under this question\(^\text{85}\), it appears that a frequent case of worry from a consumer’s viewpoint in relation to e-payments is fraud. In consumers’ mind, the fraud is perceived as:

- Fraudulent use of the EPI or EPS itself by third unauthorised parties;
- Unauthorised access or interference with the applications system supporting the e-payment application (i.e., “hacking”).

The overwhelming majority of organisations replying positively to this question indicated that they had indeed witnessed, if not actual bad incidents experienced by consumers\(^\text{86}\).

\(^{82}\) Being the Austrian and Finnish Bankers’ associations.

\(^{83}\) Being the Ombudsman of the Belgian Association of Banks, comment received by \textit{Konsument Europa}, Sweden.

\(^{84}\) We refer to the structure of questions as outlined in the Questionnaire of Phase II (see Appendix 4).

\(^{85}\) As illustrated in the table “Detailed Overview of Responses” in Appendix 4, although 19 organisations reported no complaints in relation to fraudulent use of EPIs, 14 of them seemed to consider this issue as a probable security risk.

\(^{86}\) Certain respondents denied explicitly that customers’ complaints of that kind have ever been reported to them, e.g., SEB Merchant Banking Sweden. A public consultation that the Commission of Health and Consumer Protection of Austria (VKI) has carried out recently revealed that misuse of credit cards while
themselves, at least a lot of queries for clarification about the existence and quality of security features (e.g., security tokens, encryption etc.) that ensure the safety of EPI or EPS against threats of fraud. The consumer’s concerns are mostly associated with fraudulent use of credit cards, that seem to represent today the most widely-used means of e-payment, and the risk of having card details intercepted through unauthorised system penetration in order to make fraudulent transactions.

However, the constant concern that consumers have in this context refers primarily to the result of the fraudulent use of EPI, not to the security means of preventing it. Consumers need basically to know how the liability question is solved in case of fraud. A real question that a consumer asked in this sense was, for instance, who should be held liable if the account access security was undermined, enabling an unauthorised person to get access to an account because of a failure of the security system.

It is not unusual that customers turn to the bank to get a detailed technological analysis of the security systems and protocols used in order to evaluate by themselves the transaction risk involved in case of fraudulent use of EPI/EPS. It appears from the cases reported that consumers can have severe hesitations to make an e-payment if no information is communicated to them about the security features protecting such payment. Other credit institutions reckoned that the security-related information concerning the fraudulent use of EPI is indeed insufficient to inspire consumer confidence and efforts have been made to clarify this dark point in the Q&A part of the bank’s website.

Other questions referred to what constitutes case(s) of fraud, which are irrelevant to our subject matter and, therefore, not quoted.

---

87 In this sense, the queries received by the BBL Bank in Belgium. The Bank is asked notably to clarify questions of liability if a third party fraudulently intrudes into the payment system (“by breaking” a code or discovering a flaw in the system infrastructure/operation) supported by the e-payment system of the bank (Home’Bank). According to the Bank, such queries are clarified through detailed information given to customers on the security features protecting integrity and confidentiality of the e-payment system and statement of the reason(s) demonstrating why the fraudulent risk shall be regarded as very remote to worry consumers.

88 Certain banks confirmed such concern on the basis of the questionnaire, e.g. The Royal Bank of Scotland, UK, and so did FIA-NET France.

89 As reported by Piraeus Bank, Greece.

90 The case reported by the European Consumer Centre of Italy referred to a client criticising the lack of information about the security protocol supporting the e-payment, although the e-merchant’s website gave the option of buying on-line. In this sense, also the response received by the National Consumer Council, UK.

91 Explicitly stated by Nordea Bank of Sweden and the Commercial Bank of Greece.

92 Cases reported by the National Bank of Greece.
4.5.2.3.2 Integrity concerns

On the basis of the responses to the questionnaire received, 34 organisations confirmed that consumers come often with questions regarding the overall security surrounding an electronic transaction. A frequent consumer’s query in this context is to what extent the information about an e-payment application confirms explicitly that the payment was made in time and towards the right counter-party. Also, that the due amount is charged and that the e-payment application used provides adequate proof of the payment.

The organisations contacted had the option to report consumers’ concerns with regard to one, more than one or all of the above-mentioned elements. In the majority of responses, all elements addressing the integrity of a transaction are of concern to consumers. In the cases in which only two elements were selected, these were notably about the in-time execution of the e-payment order and the evidence of payment.

To a certain extent, we agree with the response given by a few organisations that these problems are not typical to on-line transactions but refer to traditional security risks inherent to both off-line and e-payments. Accordingly, the ultimate concern of a consumer, even in the case of an e-payment operation, is to assure that the transaction will be accepted by the counter-party and the ordered goods will be received.

However, as stressed in our introduction, given that nowadays less personal contact is involved in the performance of e-transactions, customers have, to an ever increasing degree, to seek by themselves for the information that companies make available on their website or through another means “at a distance” when clarifying the “due execution” of an e-payment order. If the information is not sufficiently clear, consumers shall interpret it on the basis of their own knowledge and experiences. Along these lines, consumers regard e-transactions as particularly risky if things “go wrong” once the user loses control over the payment order. However, the cases reported (particularly the risk of unjustified payments) relate to the classical problems of the banking business (especially, arising from the use of payment cards) and do not address a specific security problem or consumer’s worry on the matter.

Another credit institution pointed out that problems relating to the performance of the transaction as such occur occasionally with respect to third (non-EU) countries. In these cases, consumers confuse sometimes the acceptance of an order by a foreign bank with the confirmation that the transaction has indeed been carried out. Another problem relating to the cross-border e-payment operations are delays in the execution of payment orders, that

---

93 e.g., FIA-NET France.
94 In this sense, the Royal Bank of Scotland, UK.
95 In this sense, several opinions expressed by consumer protection organisations, such as the National Consumer Council of UK. This organisation reported that five customers complained about having wrong amounts being charged during e-payment operations. In addition, in the first release of the White Paper published by the FIA-NET network (12 April 2001), it was reported that 12% of the 716 queries that the network received since its setting-up in 2000 addressed e-payment issues. The majority of these questions referred to the technical implementation of e-payments solutions but also to the absence of any close control felt by the users at the moment of the on-line purchase.
96 Being the BBL, Belgium.
97 As reported by Nordea Bank, Sweden.
the bank in question tried to clarify in the section of “Q&A” on its website. These situations reflect probably a need for better clarification of the trans-border payment procedure to consumers but, as we mentioned above, do not address a specific security-related problem or worry in this respect.

On the contrary, a problem relating specifically to the transactional security ensured by an EPI or EPS is the confirmation of the execution of the payment order by the operating system\(^{98}\). This problem is also highlighted in the documentation\(^{99}\) received through the questionnaires and is discussed in the recommendations chapter below.

This issue is intrinsically related to consumers’ worries about how to receive proof of an e-transaction. Most of the times, this information is not explicitly explained in the description of the security measures supporting an e-payment application, as deployed on the websites or other communication means of PSP or e-merchants. However, this concern does not address a particular security threat typical to e-payments.

4.5.2.3.3 Concerns about how to use EPIs

A third series of complaints communicated by consumers relate to the functionality and usability of EPIs – EPS. In other words, to what extent consumers know how to use an EPI to perform an e-payment.

Most of the complaints reported here\(^{100}\) addressed problems regarding using passwords, handling of the applications menu on-line or even generation of other identification features (e.g., virtual PAN generation). Another category of queries refers to data that customers shall introduce on their own, e.g., by typing before a PC screen\(^{101}\). Consumers’ requests for clarifications or help in this respect are encountered through help-desk solutions maintained by banks on a round-the-clock weekly basis (24 hours/7 days per week), call centres and via explanations given in the Q&A section on the website.

It was also pointed out that, though consumers are quite familiar with the use of payment cards (credit/debit), they are still less aware of how using other EPIs\(^{102}\). Consumers’ ignorance about new e-payment applications (e.g., mobile or phone banking) explains, according to some opinions\(^{103}\), why the number of transactions involving such instruments remains still nowadays very low.

\(^{98}\) In this sense, the European Consumer Centre of Italy reported that consumers have been complaining about not receiving any confirmation of the execution of the payment order when they buy on-line. Although in some cases, short messages on the computer screen follow the sending of the payment order, these messages cannot be printed on paper. Nor, even at a later stage, do consumer receive any such confirmation from the PSP or e-merchant by e-mail, so the only possibility to verify whether the payment has indeed been made is through recourse to the monthly payment extracts sent by the PSP.


\(^{100}\) Commercial Bank of Greece, SEB Merchant Banking Sweden and the Association of Italian Banks, Bank Ombudsman of the Netherlands and the National Consumer Agency of Denmark.

\(^{101}\) As reported by the SEB Merchant Banking of Sweden.

\(^{102}\) National Consumer Council of UK.

\(^{103}\) According to the Ombudsman of the Belgian Association of Banks.
4.5.2.3.4 Questions on functional and operational security

Nine (9) of the organisations contacted reported having received a few queries about the security of EPIs against technical shortcomings or failures of the operating system.

As a starting point we should stress that, financial companies are relatively optimistic of being able to control security risks relating to unauthorised trespass, sabotage and other intentional or accidental operational risks. On the other hand, consumer organisations claim that security deficiencies are seldom brought to consumers’ attention. It is a fact that there are no definitive security solutions available, so Payment Service Providers and financial institutions should communicate transparent information about how users of EPIs or EPSs should act in order to minimise the consequences of such failures or pinpointing alternative solutions.

The responses received through the questionnaire confirm that certain consumers wonder whether the e-transaction can still be performed in case of sudden interruption of the operating system. Technical failures, however, do not only affect the operating system alone. Sometimes they are attributed to technical failures of the user’s own device (e.g., a payment card) or they are aggravated because of the consumer’s ignorance to use an EPI or to identify in-time a technical problem.

Nevertheless, in the light of the responses received, it is noteworthy that financial institutions or Payment Service Providers in general seem to be in a position to cope with the problem, on condition that the promised permanent technical assistance is provided on a real non-stop basis and it is as efficient as it is claimed to be.

To avoid such risks, it is clear that consumers need to be well informed about how they should use an EPI and what their own responsibilities are in case of failures attributed to their own wrong usage. In particular, consumers need to know the liability risk(s) they may encounter in case of technical flaws and failures of EPIs/EPSs. It was stressed that the risks involved in the use of technology must not be put on the consumer but should be borne by the party offering services by means of technology, who is in principle better equipped to deal with these risks.

---

104 Finnish and Swedish banks, for instance, underlined that their operational systems are really secure against operational technical flows or failures.
105 BEUC.
107 In this sense, cases reported by the National Bank of Greece. Explanations to consumers were given through the bank’s help desk.
108 According to the opinion expressed by the Ombudsman of the Belgian Association of Banks.
Financial institutions assured that such clarifications are normally provided through the help-desks of financial institutions or within the Q&A section on the banks’ websites. The possibility to have specific clauses on this issue, set out in the services agreement signed with customers, is not excluded either\textsuperscript{110}. On the basis of claims reported by consumer organisations\textsuperscript{111}, it seems that, in some cases, e-merchants deny any liability if technical failures occur with the operating system or if customers experience any problems with regard to the operation of an e-payment application.

4.5.2.3.5 Identification concerns
Surprisingly, only seven (7) of the organisations reported that consumers had from time to time expressed worries about the identification of the counter-parties in an e-transaction.

In most of the queries reported, consumers needed to know how the EPI or e-payment application ensured that they were properly identified as payers; also, whether the EPS in question furnished adequate proof of the payer’s identity, so that it can be demonstrated, if contested at a later stage, that the payer had indeed paid\textsuperscript{112}. In some other cases, consumers asked explanations about the function and usability of identification mechanisms used by financial institutions on-line\textsuperscript{113}.

A more worrying element arising from the reported cases is that it still remains unclear to many consumers and e-merchants how the liability question is settled in case of unauthorised use of the identification mechanisms or devices used for e-payments. Consumer organisations confirmed through the survey that e-merchants often report that it is entirely the responsibility of the consumer to protect his identification data in order to avoid fraudulent use thereof.\textsuperscript{114}. On the basis of the responses collected, it seems that providers of other on-line services share this opinion. However, it was also pointed out that those who should be most worried about the authentication security of an EPI are not consumers but e-merchants who need to know whether their counter-party is the real holder of the EPI (being, for instance, a payment card)\textsuperscript{115}.

Other questions about identification risks when using EPIs are closely related to the issues discussed above (risks of fraud). In particular, some concerns were expressed with respect to the encryption and processing of information in SSL payments\textsuperscript{116}. In some other cases,

\textsuperscript{110} As reported by Nordea Bank of Sweden.
\textsuperscript{111} The European Consumer Centre, Italy.
\textsuperscript{112} In this sense, the European Consumer Centre of Italy received a few queries: Consumers asked how their identity could be ensured and proved to e-merchants at the on-line payment by credit cards. Consumers complained that this kind of information was not easy to be found on the web sites of e-merchants.
\textsuperscript{113} The National Bank of Greece reported that some users did not understand the purpose of the TAN (Transaction Authentication Number) list, that the bank is using as alternative to electronic signatures, so it had to provide more to-the-point explanations about the added-value of the TAN mechanism.
\textsuperscript{114} The European Consumer Centre of Italy.
\textsuperscript{115} This argument was put forward by FIA-NET, France.
\textsuperscript{116} In this sense, FIA-NET, France.
consumers complained to their bank institutions because e-merchants refused to use the identification means put in place to make e-payments\textsuperscript{117}.

4.5.2.3.6 Data Protection concerns

It is also astonishing that only eight (8) respondents reported that they received queries about how consumers’ personal data are protected throughout an e-payment operation.

However, consumer organisations appear to be more sceptical than financial institutions about whether consumers receive appropriate information about the way(s) Payment Service Providers and e-merchants process personal data. They report that there is still a lack of awareness, understanding and clarity about what measures are put forward in practice to protect data transmitted through e-payment operations\textsuperscript{118}. Some consumers are concerned whether encryption mechanisms can fully ensure appropriate protection of the financial and personal data when buying on-line\textsuperscript{119}.

It was also reported that\textsuperscript{120}, in some cases e-merchants’ websites provide adequate information about how the customers’ personal data are processed and state explicitly the use thereof for the purposes of unsolicited commercial communications. However, these websites do not provide actually any means to consumers to refuse the processing of their data for this purpose.

The respondents to our survey noted no other specific complaints or consumers’ worries in relation to personal data processing. We consider that the lack of reactions in this direction should not be interpreted as a sign of the high quality of information supplied to consumers in this respect. In our view, it is due to the fact that data protection concerns are probably reflected in the responses to the integrity of e-transactions (discussed above) and other questions (fraudulent use of EPI, security of the e-transaction, authentication).

\textsuperscript{117} In a case reported by Nordea Bank Finland, merchants refused to use hash digit that the bank had put in place as means of identifying the identity of the seller (This hash was calculated from the message sent to the bank within the transaction).

\textsuperscript{118} As reported by the National Consumer Council, UK.

\textsuperscript{119} In this sense, remark by FIA-NET, France.

\textsuperscript{120} By the European Consumer Centre of Italy.
4.5.2.4 Responses to Section II of the questionnaire

4.5.2.5 Modes and timing of the information provided

In the sections below, we discuss the input received through our survey indicating the manner(s) in which security-related information is provided to consumers. We analyse the responses received in relation to the following questions:

- In what circumstances the security-related information is provided
- Where it can be found
- When it is supplied
- How it is worded, and
- In which form it appears

4.5.2.5.1 In what circumstances the security-related information is provided

The indicative alternatives given through the questionnaire were:

- Standard, in a proactive manner without the consumer having expressed a prior request.
- After the consumer’s explicit request (orally or in writing)
- Other (to be specified)

The majority of responses indicated that security-related information is provided as standard information (presumably by posting a “standard” text on the website of the PSP/e-merchant/bank etc.), without consumers’ prior explicit concern. A few of the organisations indicated both ways (standard and upon explicit request), but in no case was it claimed that information was communicated only whenever there was an explicit request. Nor did the respondents mention expressly that such information is never provided to consumers.

However, consumer organisations contest that the existence of such “standard” information on the websites is always complete or easy to find. In a few cases, it was doubted whether security-related information could be found at all.

4.5.2.5.2 Where the security-related information is provided

In this question, the organisations were asked to indicate the means through which security-related information is most usually provided. The indicative solutions highlighted in the questionnaire were:

- On the website [notably of the Payment Service Provider (or e-merchant)].
- On the standard contract (or services agreement) concluded between the PSP and the consumer.
- In a hard document [could be, a separate annex to the written contract, a separate section of the body of the contract, amongst other contractual clauses.
- In the terms and conditions (T&C) accompanying the standard contract (services agreement) concluded between the PSP and the consumer.

---

121 In this sense, the UK National Consumer Council.
122 Statement of the Lisbon Arbitration Centre for Consumer Conflicts, Portugal.
• In another hard document [could be, a separate user’s guide, brochure, promotional leaflet, etc. issued by the PSP].
• By reference to a security solution or product without specifying details.
• By reference to the security solution with further details.
• By providing indirect links [e.g., inviting the user to look for information elsewhere, in the website of the manufacturer/provider of the security solution].
• Information provided only orally [there is no “location” of the information at all]
• Other

In the light of the responses provided to this question, it seems that the website of the Payment Service Providers, and less often of the e-merchant, is the most usual way of informing consumers about the security assured by the given EPI/EPS. Beside general descriptive texts of the security solutions implemented in an e-payment system, a lot of points are clarified through the “Q&A” (Questions and Answers) section of websites. The experience has shown that consumers sometimes go directly to this section to find user-friendly explanations on real or fictitious queries reflecting the thinking and experience of the average consumer.

Most of the websites of banking institutions are interactive, meaning that consumers can ask their questions on-line and answers are provided by e-mail.

Other popular ways, at least on the side of financial institutions, are the standard services agreements signed with their customers and, to a lesser extent, the Terms and Conditions (T&C) accompanying these contracts. In a few cases only, respondents indicated explicitly the location of the security-related information in contract, being a separate annex\(^{123}\). On some occasions, financial institutions indicated in addition that information upon explicit concern is provided through call-centres\(^ {124}\) or help-lines that serve sometimes exclusively e-banking or similar operations.

Another alternative is to supply security-related information in other hard documents (i.e., promotional leaflets of a new banking service, user guides etc.), especially technical parts thereof\(^ {125}\).

4.5.2.5.3 When the security-related information is provided

Respondents were asked to indicate the stage at which, on an average basis, security-related information was made available to consumers. The alternatives put forward in the questionnaire were:

• Before the signing of the general services agreement (or, in general, before entering into an e-contract with the Payment Service Provider, bank or e-merchant).
• At the moment of signing the general services agreement (or, in general, upon entering an e-contract with the Payment Service Provider, bank or e-merchant).
• After the signing of the general services agreement (or, in general, after entering into an e-contract with the Payment Service Provider, bank or e-merchant).

---
\(^{123}\) Nordea Bank in Finland, Association of Italian Banks, SEB Merchant Banking Sweden.
\(^{124}\) Association of Italian Banks.
\(^{125}\) As specified by BBL Belgium, Piraeus Bank Greece, Nordea Bank Finland etc.
• Never.
• Other.

The majority of the responses received by the financial institutions indicated that information was supplied before the consumer performs the service in offer, being the e-payment operation as such or another service, which integrates or relates to an e-payment application. This is probably due to the fact that most of the times, as we described above, security-related information is provided on the website of a PSP or financial institution, that customers may visit without any obligation to engage in a concrete e-payment act.

In some cases, respondents selected the three solutions (before, upon, after) but without giving any explanations why they made this distinction. In our view, the marking of all three options could mean that some information is provided before entering the service, whilst other elements are disclosed at the time the service is performed (i.e., e-payment operation is in course). However, the organisations concerned did not clarify what kind of information is provided before/at or after entering the contract or performing the service respectively.

On the other hand, the consumer organisations seem to recognise that security-related information is provided at all the above-mentioned stages. As in the case of financial institutions, consumer bodies did not specify either what kind of security-related information is disclosed at each stage. Neither was any comment received criticising that partial disclosure of some information before the entering of the contract should be regarded as detrimental to consumers’ interests.

It was however rightly emphasised\textsuperscript{126} that, regardless of whether or not security-related information is theoretically accessible prior to performing a service (e.g., making an e-payment), there is no obligation for a consumer to consult it before making an e-payment.

4.5.2.5.4 How the security-related information is worded

As we discussed in the previous chapter, a criterion to evaluate the “accessibility” of information to an average consumer is by assessing the wording in which the information is formulated.

In our questionnaire, the organisations contacted were asked to indicate whether on an average basis security-related information was worded:

• In a clear, comprehensible, user-friendly language; in clear-cut sentences reflecting laymen thinking.
• In a confusing language, with reference to many technical terms and using complicated phrases.
• In another way.

\textsuperscript{126}Federation of the Consumer Organisations, Germany.
With very few exceptions, all financial institutions reported that security-related information is communicated in a user-friendly language. Sometimes, the language used is formal but without making reference to complicated legal terms and worded in clear sentences. A more neutral approach is reflected in the view of other authorities saying that the quality of the language used is variable and, in some cases, confusing and technology-heavy. Some of the consumer organisations indicated that the language used was comprehensible but without excluding variations in certain cases. In one occasion, it was reported that the language was confusing and technology-heavy. However, no further explanations were made in this respect.

4.5.2.5.5 In which form the security-related information appears

“Accessible” information means also that information is made attractive and visible to consumers. Easy accessibility to security-related information entails that consumers will not have to spend a lot of time or to make excessive efforts to find where the information is located. Also, that information is quite striking, thus appearing in a form and characters that draw consumers’ attention and incite them to read it. Accordingly, we asked the organisations contacted to indicate whether on an average basis the security-related information is provided:

- In big, clear letter characters and in a very visible place (e.g., of the website, contract etc.).
- In small letter characters and in fade fonts difficult to read, scattered in different places on the website/contract, accessible through a “hidden” web link or written only on the back side of a contract.
- Other

In their large majority, financial institutions reported that the information appears in a user-friendly way (as per first bullet point). Third parties were more neutral in their assessment, mentioning that situations may vary. The consumer organisations, with one exception, did not express any particular view in this respect, assessing the appearance of security-related information as satisfactory in general.

4.5.2.6 Responses to Section III of the questionnaire

4.5.2.6.1 Overall evaluation

We also invited the organisations contacted to give us their own mark on whether the overall level of the security-related information provided to consumers should be regarded as:

- A very poor and inadequate level to inspire consumers’ confidence.
- An adequate level.

---

127 SEB Merchant Banking, Sweden.
128 As indicated by Commercial Bank, Greece.
129 Notably, Ombudsman of the Belgian Association of Banks and Geschillencommissie Bankzaken.
130 According to the Lisbon Arbitration Centre for Consumer Conflicts, Portugal.
131 The only exception is reported by the SEB Merchant Banking, Sweden.
132 The Ombudsman of the Belgian Association of Banks was sceptical as to whether information appears always in a “user-friendly” appearance.
133 Being the Lisbon European Arbitration Centre for Consumer Conflicts stating that the security-related information does not appear in a “consumer friendly” form.
• A satisfactory level.
• A very good level.

The mark that prevails in the answers of financial institutions is “satisfactory”. There is a
general belief among the credit institutions that security systems have evolved over the
years and the quality of information provided to consumers has been adjusted accordingly
to the requirements of the contemporary users. In addition, it is claimed that the quality and
level of the security-related information provided depends sometimes on the category and
personal knowledge of the customer that financial institutions and Payment Service
Providers can discover only through their personal dealings with customers. A few
banks were more reticent in their evaluation, assessing that the information provided is
adequate. Only one bank found that the level of information supplied is indeed very
good. However, it would be too risky to generalise such a positive assessment, given that
more neutral organisations, like Bank Ombudsmen, were more reluctant to confirm so
encouraging evaluations.

On the contrary, consumer organisations provide variable answers: A few of them were
negative in their evaluation; two others found that the information provided was
satisfactory, whilst one assessed that the overall level was adequate. Only one national
consumer body evaluated the level as very good.

As a concluding remark, we can assume on the basis of the responses received that
financial institutions are in principle satisfied with the security-related information they
communicate to their customers. However, more neutral institutions and consumer
organisations appear to be more sceptical in this regard. We did not receive explicit
comments justifying the marks awarded through the questionnaires. However, we consider
that the respondents’ suggestions as formulated below are explicit of the fact that many
improvements still need to be made in order to attain a satisfactory level of communication
with consumers in the e-payments area.

4.5.2.7 Responses to Section IV of the questionnaire

4.5.2.7.1 Recommendations

The last question addressed in the questionnaire was whether the market categories
approached could come up with some suggestions on how improving the level and quality
of security-related information.

The indicative solutions that we put forward were:
• Legislation addressing standard elements of information, as well as the means of
  communication thereof.
• Soft law (codes of conduct, standard contracts, dissemination of best practices).
• Consumers’ education through appropriate means and action taking.

Respondents were also invited to explain their position or provide other comments.

---

134 The Ombudsman of the Belgian Association of Banks shared this view.
135 Being the Nordea Bank of Finland.
136 Being the Consumer Protection Board in Finland
The findings of our survey under this question are summarised below.

4.5.2.7.2 Consumer organisations
The majority of the answers received clearly favour the adoption of legislative solutions.

Some of the respondents reported their national experience to justify this view. An illustrative example in this sense is the comment received by the National Consumer Agency in Denmark.

It seems that Denmark has adopted specific legislation to regulate the time, form and quality of information that should be provided to consumers when using certain payment instruments (notably e-payment cards). The beneficial result for consumers is that all financial institutions and service providers in Denmark are now used to communicating information regarding the security of EPIs in a routine way, while consumers have ample possibilities to find information about the security of EPIs if they wish so (e.g., on the websites of card issuers).

Similar statements by other consumer protection bodies show that the Danish view supporting subject-specific legislation should not be regarded as an isolated case. Binding legislation should also clarify the legal obligations and responsibilities of all parties involved in e-payments (being notably, e-commerces, Payment Service Providers and customers).

Moreover, a few organisations expressed doubts about whether soft-law solutions are really so efficient in practice as it was initially thought.

A few answers underlined the importance to act simultaneously at all the proposed levels (binding regulation, soft law and consumer education), since efficient solutions could not be elaborated through unilateral approaches. Regarding soft legislation, it was emphasised that soft law instruments tackling the area of payments should be reviewed in order to better reflect the consumers’ concerns. The legal enforceability of soft-law instruments should also be enhanced. On the other hand, consumers should have easy access to the support and enquiry services maintained by financial institutions and Payment Service Providers and should be better informed about the availability and efficacy of redress procedures.

---

137 Along these lines, the Federation of German Consumer Organisations stressed that Payment Service Providers and e-commerces shall be bound by law to inform consumers in a clear manner before making an e-transaction. Similarly, the Lisbon Administration Centre for Consumer Conflicts of Portugal emphasised the importance of the adoption of a legislative act that will address standard elements of information and, as a complement, the working up of codes of conduct, standard contracts and dissemination of best practices.

138 According to documentation received from BEUC.

139 Being primarily the Federation of German Consumer Organisations and the Finnish Consumer Association. The latter expressed the view that private organisations and entities subscribing to soft-law instruments (e.g., codes of conduct) are those who, surprisingly enough, adopt “consumer-friendly” business practices anyhow.

140 The National Consumer Council, UK.
4.5.2.7.3 Financial Institutions

Unlike consumer organisations, the bankers’ view is that soft law solutions should prevail over stringent regulatory approaches. It is believed that legislation on the subject matter already exists, but it is not well known to consumers. What consumers need at this stage is not more legislation but better knowledge on the security aspects of using the Internet in general[^141]. On the contrary, new law-making efforts in the area would worsen consumers’ confusion vis-à-vis the already fragmented picture that the banking systems present today around Europe[^142].

The sources of information about the security of EPIs should become more transparent. Certain respondents claimed that, although the information that consumers receive about security is ample, there are no clear criteria on how the average consumer should distinguish the good and reliable information source from the bad one[^143].

A good number of respondents emphasised the need to enhance consumers’ education on the security of e-payment systems. These educational activities should be taken jointly by public authorities, consumer associations and financial institutions, with the focus on prevention and not only rectification[^144].

Better education should help consumers adopt a more proactive and responsible role vis-à-vis the handling and performance of state-of-the-art payment technologies. Customers should learn how to look after their security and responsibilities must not be sought only on the side of the Payment Service Providers. The development of technology today has opened new opportunities for consumers to find information on products and services by themselves instead of passively waiting for the information to come to them.

Not merely soft law, but self-regulation in general seem to be better viewed in the banking environment, since such solutions are based on the companies’ own acceptance of responsibility and participation. Providers of Internet services, including e-merchants, seem to share this view: Self-regulatory instruments reflecting the concerns of all market categories and striking the right balance of responsibilities is preferential to strictly political, administrative or technocratic approaches[^145].

However, even self-regulation should avoid standardised approaches, since standardised contracts would proliferate standardised services, which would restrict competition in an open market[^146].

4.5.2.7.4 Bank Ombudsmen

The Ombudsman of the Association of Belgian Banks, as well as the Dutch Banking Commission for the Prevention of Conflicts, stressed the importance to have the security

[^141]: SEB Merchant Banking, Sweden.
[^142]: According to the Finnish Bankers’ Association.
[^143]: In this sense, comments from Visa International, BBL Belgium.
[^144]: BBL Belgium.
[^145]: FIA-NET, France.
[^146]: Finnish Bankers’ Association.
information about EPIs and EPSs better echoed in the communication means used to approach consumers.

Customers are not always aware of refund obligations imposed in the financial institutions and other bank practices, although these are generally fair, in case that an e-operation is not carried out as due or if a technical failure occurs with the e-payment system.

Along with the financial institutions, the bank ombudsmen believe that harmonising the legislation about the technical requirements related to the use of EPIs/EPSs cannot be the ideal solution. The technical systems supporting e-payments are different all over Europe and the ideal interoperability cannot be achieved, at least in short term. The most realistic solution should be that legislators leave the actual market actors to take the lead in the shaping-up and introduction of best e-payment practices.

4.5.3 Recommendations Reflected in Documentation Received from Respondents

This section discusses a number of suggestions on the subject matter formulated on the basis of the documentation that we received together with the questionnaires, and of other information sources that we collected for the purposes of this study. Some of these suggestions also reflect the opinion of the respondents to our survey.

- **Improving the form**
  When communicating security-related information about their e-payment systems and tools, financial institutions and other service providers shall keep in mind that they usually target the average consumers. Vague messages about the functionality and uses of a given EPI should be eliminated. Typical problems and faults that may occur during the performance of the e-payment operation should be clearly and expressly stated.

In addition, the consequences of the bad performance of the given transaction, including those due to technical failures, should be indicated and, if possible, alternative procedures to remedy the fault(s) or prevent grave damage should be recommended.

- **Clarifying obligations and responsibilities**
  It is essential to make customers aware of their own liability risks at the use of an EPI, as well as of their rights and limits thereof towards the other intervening parties in an e-payment operation. The provider of the e-payment service shall provide correct and clear information regarding what applies in various situations. In case that the Payment Service Providers can benefit from special provisions of the local law alleviating its liability or the existence of other disclaimers, these clauses shall be explicitly drawn to the attention of consumers before engaging in e-payment operations.

Yet, it is not sufficient to provide information about the division of responsibility and risks in using an e-payment service. Customers shall also receive instructions regarding how

---

147 The table of this documentation is given in Appendix 4.
148 Excluding the provision of specialised services to particular categories of customers, whom level of knowledge and/or familiarity with e-payments may differ from this of the average consumer.
they should act in order to minimise the risk of unauthorised transactions or the impact of other security risks if realised. In particular, consumers should be aware of what responsibility the Payment Service Providers assume if a transaction cannot be conducted due to temporary technical glitches or capacity constraints.

- **Being realistic about the security capacities of an EPI or EPS**
It was discussed above that no definitive security solutions are available. Payment Service Providers and e-merchants shall help consumers to develop a realistic feeling about the security that the technology today can assure.

In this context, Payment Service Providers should explicitly reassure consumers about their efforts to implement state-of-the-art technology and on continual, conscientious security work.

- **Taking advantage of the Internet’s potential as communications channel**
In view of the considerable prospects offered by the Internet as an information channel, Payment Service Providers have great possibilities to supply updated information in a well-structured pedagogic manner. Not to exclude the possibilities of enhancing communication in an interactive way, by asking customers’ feedback and providing tailor-made instructions if necessary.

- **Accessibility of EPIs to all consumer categories**
Certain categories of consumers, like the elderly, less schooled or disabled people, are not familiar with the functionalities of, or simply cannot use certain EPIs.

Providing information that is adapted to these categories of population or publicity over the availability of alternative e-payment methods (e.g., more suitable for handicapped or blind people) can be a remedy in this regard.

- **Enhancing the role and responsibilities of trusted third parties**
In the suggestions put forward by the respondents to our survey, it has been claimed that if data processing (especially, related to the carrying-out of a payment through SSL) takes place under the control of, or if directly entrusted to a third supervisory authority (bank institution or other), some problems of confidence in e-payments may be resolved.

In this hypothesis, consumers should of course be well aware of the role and responsibilities of these trusted third parties. The functioning thereof should also be transparent.

Finally, direct access by consumers to such authorities should be ensured.
4.6 Comparative Analysis of the Results in the Light of the Levels of Public Confidence in EPIs

Having completed the qualitative and quantitative survey of the quality and level of information provided to consumers, a comparative analysis of the results in the light of the levels of public confidence in EPIs (as derived in Part 1 of this study) was made. This analysis is presented in tabular form below.

Countries represented in descending order of confidence level as defined by the levels of public confidence, i.e. most confident first.
### 4.6.1 Finland

Finland Confidence Indicator Value 8.41  
EU-15 Confidence Indicator Value 7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>It appears that security requirements in relation to EPIs from the point of view of the Finnish consumer are similar to the ones inherent to the supply of secure e-services in general. Applications involving e-payments, in particular e-banking systems, have been used in Finland for over 20 years and the target user groups have progressively been broadened from experts to amateurs. Accordingly, information has been progressively adjusted to fulfil the requirements of this broadened audience. Finnish consumers are used to looking for security-related information alone and they have sources to find it.</td>
<td></td>
</tr>
<tr>
<td>A few complaints/queries only were reported through our survey regarding the quality and level of the security-related information. Isolated cases addressed notably the appropriate identification of the parties involved in an e-payment operation and questions in relation to security matters in general when performing e-payments (i.e., “How ensuring that a specific e-shop is reliable and that everything is going well? “Can a given EPS be considered as safe?”), without questioning explicitly the communication of information <em>per se</em>. Security-related information is mostly provided as standard on the websites of Payment Service Providers, but also in service agreements (in some cases, in separate annex or section thereof) and other accompanying documentation (user’s guides, explanatory brochures etc.).</td>
<td></td>
</tr>
<tr>
<td>In general, information is made available before signing of the general services agreement or prior to performing a transaction. The language in which the information is communicated is in general clear and consumer-friendly. On average, it was reported that the level and quality of security-related information available to consumers is satisfactory.</td>
<td></td>
</tr>
<tr>
<td>Answers to our survey confirm the findings of Part I of the study, thus Finnish consumers are quite confident in the use and functionalities of EPIs/EPSs.</td>
<td></td>
</tr>
<tr>
<td>This is probably explained by the fact that the practice of financial institutions is to provide security-related information tailored to each user group. Moreover, the large majority of the e-banking websites ensures easy accessibility to this information (83%).</td>
<td></td>
</tr>
<tr>
<td>Surprisingly enough, the high level of consumer confidence cannot be explained if comparison is made with the level of information provided in websites of e-merchants. The availability of security-related information is very low on these sites (36%).</td>
<td></td>
</tr>
<tr>
<td>As it was stressed in our survey, however, it appears that Finnish consumers are proactive enough to look for sources of information by themselves. This proactive approach is a probable explanation why confidence in EPIs in Finland is remarkably high even if security-related information is not provided by e-merchants as systematically as by Payment Service Providers.</td>
<td></td>
</tr>
</tbody>
</table>
### 4.6.2 Netherlands

Netherlands Confidence Indicator Value 7.91  
EU-15 Confidence Indicator Value 7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>A few complaints only reported. In their majority, they address security issues in general (not explicitly the information communicated thereupon) and they are forwarded to the bank involved in the given e-payment operation.</td>
<td>There is a slight contradiction between this high level of confidence of Dutch consumers and the quality of security-related information available to them.</td>
</tr>
<tr>
<td>The security issues that seem to worry consumers are EPIs’ usability, the risks of fraud, timely execution of payment and appropriate identification of the counter-party.</td>
<td>This is probably explained by the fact that financial institutions are far more attentive to make available to consumers user-friendly and easily accessible information about the security of EPIs compared to Dutch e-merchants. It is noteworthy that the scanning of all Dutch e-banking websites of our sample reflects this statement.</td>
</tr>
<tr>
<td>Security-related information is most of the times provided as standard, on the website of the Payment Service Provider and through other accompanying paper-based documentation (user’s guides, brochures etc.).</td>
<td>The high degree of compliance of financial institutions to a high level of information probably counterbalances the inadequate level of information provided by e-merchants. Indeed, the scanning of e-commerce websites confirmed the statements communicated through our survey, about the language and accessibility of security-related information. The Dutch e-merchant websites scanned revealed compliance percentages far below the EU average level (availability of information: 28%, accessibility: 8%, comprehensibility: 16%).</td>
</tr>
<tr>
<td>It was reported that the information is supplied at the moment of signing the services agreement. As to the form in which the information is communicated, it was reported that the language is sometimes confusing and complicated. Also, it is not always easy to find this information. However, the overall quality level is considered to be adequate.</td>
<td></td>
</tr>
</tbody>
</table>
### 4.6.3 Sweden

Sweden Confidence Indicator Value 7.79  
EU-15 Confidence Indicator Value 7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Respondents to our survey stressed that, although Swedish consumers were worried about security at the early stage of Internet applications, the situation today has considerably changed. However, it appears that Swedish consumers are still concerned to be informed about the capability of Payment Service Providers to encounter security risks relating to identification, fraud and technical failures of the operating system. Specific consumer complaints directed to some Swedish banks concerned usability issues. It seems that Swedish bank institutions make efforts to clarify these queries in a more systematic way, by addressing them in the FAQ section of the website. It was explicitly reported through the survey that almost all websites offering e-payment services include information about security and reliability (this is also confirmed through the assessment of the Swedish banking websites). It was stressed that the tradition of the Swedish legal system protecting consumers’ rights through fair trade practices secured the habit of communicating the security-related information in a standardised way at a standardised place. Therefore, the security-related information is most of the times communicated as standard on the website of the Payment Service Provider. Additional means of communication are services agreements - stipulating security-related information in the section of general terms and conditions (T&C) of the contract or in a separate annex thereof – and paper-based documents (user’s guides, explanatory brochures etc.). As for the form used, it was explicitly stated that the information is communicated in a legally acceptable format and in a visible place. However, it is not always easy for a layman to understand it. On an average basis, it appears that the level and quality of the information provided is satisfactory.  

The high level of confidence in using EPIs correlates with the level and quality of security-related information provided to Swedish consumers.  

The websites’ survey revealed a significant gap between the levels of care that financial institutions and e-merchants take in order to provide consumers with easily accessible and clear information.  

The fact that the websites of Payment Service Providers attain a high degree of compliance in the provision of adequate, easy-to-find and clear information probably counterbalances the lack of clarity of security-related information supplied by Swedish e-merchants.
4.6.4 Luxembourg

Luxembourg Confidence Indicator Value 7.79
EU-15 Confidence Indicator Value 7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>We received no feedback from Luxembourg through our survey. However, on the basis of the website assessment, it appears that only 33% of the e-commerce websites visited make available to consumers information about the security features of EPIs. On the contrary, bank institutions seem to be much more attentive in this respect (all the e-banking websites surveyed disclose security-related information in a clear, comprehensible language). But even in this case, only in the half of these websites it was easy to identify the security-related information. With regard to the information available about specific security threats, it was found that 83% of the Luxembourg websites surveyed do not provide clear information about how resolving problems that consumers may encounter with their credentials. Regarding data protection issues, it was found that none of the e-commerce websites surveyed mentions explicitly the party collecting the communicated payment information. In the light of the above, it seems that the level of security-related information provided to consumers is satisfactory with respect to e-banking websites but that further improvements are needed to streamline the information available on the e-commerce websites.</td>
<td>The quite high level of confidence of Luxembourg consumers in the use of EPIs does not always correspond to a high level of information. Financial institutions have probably played a role in enhancing the general feeling of confidence. It appears from our findings that all banks of our sample make available to consumers explanations about the security features of EPIs/EPSs and this in a clear language. The picture is not so positive when looking at the websites of e-merchants. The level and quality of information supplied on the e-commerce websites is below the EU average level (availability of information: 33%, accessibility: 17%, comprehensibility: 50%).</td>
</tr>
</tbody>
</table>
### 4.6.5 United Kingdom

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>It appears that consumers are not much aware of how to use less common means of e-payments than payment cards.</td>
<td>Indeed, Part I of the study reveals that “pay later” products, being primarily credit cards, and to a lesser extent, “pay now” EPIs, are far more widely used than “pay before” products. More information about less widely known means of e-payment could probably enhance the consumers’ confidence in using them.</td>
</tr>
<tr>
<td>Most of the complaints/queries received concern EPIs usability (reported questions as basic as these ones: “How to go about using EPIs?”,”What are EPIs?”,”How would you get one?”). Other concerns relate to identification issues (“How is the parties’ identity proved?”), and the good performance of the e-transaction in general (questions addressing the integrity principle). With respect to the data protection issue, it seems that consumers in UK are eager about taking a more proactive role (i.e., they often ask how to verify appropriate processing of personal data and which are the measures they would be in a position to take by themselves in order to ensure adequate protection etc.).</td>
<td>Surprisingly enough the indicator of confidence and the results of the public survey contradict to a certain extent the findings of the websites’ assessment, probably because input in the former case was received by consumer protection bodies, which are more critical about the information provided to consumers than financial institutions.</td>
</tr>
<tr>
<td>Security-related information is provided as standard in typical credit/debit card contracts. However, in general, it is not easy for the average consumer to find, read and understand it.</td>
<td>Accordingly:</td>
</tr>
<tr>
<td>The respondents to our survey qualified the level and quality of information supplied in relation to EPIs as very poor and inadequate to inspire consumers’ confidence.</td>
<td>The website scanning revealed that the UK websites are generally classified above the average EU level in terms of the availability, accessibility and comprehensibility of the security-related information posted on them. On the contrary, the findings of the public survey point out that the level and quality of information is still very poor.</td>
</tr>
</tbody>
</table>
4.6.6 Denmark

Denmark Confidence Indicator Value 7.46
EU-15 Confidence Indicator Value 7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Providers of e-payment services in Denmark have the legal obligation to communicate detailed information about the use of EPIs, including security requirements. The major part of the issuers of EPS indeed comply with this rule and usually explain on their websites the security and the security precautions which the issuer offers to consumers with the use of the given EPI/EPS. This practice is more or less an established routine for all payment service providers in Denmark nowadays. Respondents to our survey stressed that consumers who wish to learn about EPI/EPS have ample possibilities of finding such information easily. This explains probably that no complaints relating to the availability of security-related information have been communicated to us through the survey. The level of the information provided was qualified as satisfactory.</td>
<td>Taking into account that both Payment Service Providers and e-merchants take due care for making available security-related information about EPIs in a clear and easily accessible way, one could probably expect herein a higher confidence indicator.</td>
</tr>
</tbody>
</table>
4.6.7 Germany

Germany Confidence Indicator Value 7.34  
EU-15 Confidence Indicator Value 7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>No particular problems have been addressed by German consumers to the institutions responding to us in the survey.</td>
<td>There is a clear correlation between the level of confidence of Danish consumers to EPIs and the level and quality of the security-related information provided to them.</td>
</tr>
<tr>
<td>General concerns have been expressed from time to time relating to identification, fraudulent use of EPIs, usability, personal data protection, failure of the operating system and integrity of payments. However, the queries vary depending on the age, education and social level of consumers.</td>
<td>The relative high percentages resulting from the website scanning exercise confirm this.</td>
</tr>
<tr>
<td>In principle, information is supplied as standard somewhere on the website of Payment Service Providers or of the Internet shop. The time at which the information is provided varies from one website to another.</td>
<td></td>
</tr>
<tr>
<td>On an average basis, more of the half (57%) of the e-commerce websites visited through the websites’ assessment revealed that e-merchants do make available explanations about the security features of e-payment methods used and this in a clear and comprehensible manner.</td>
<td></td>
</tr>
<tr>
<td>The respective percentage is even higher with respect to the websites of financial institutions: The majority (93%) of e-banking websites provide security-related information. Similarly high is the level of e-banking websites (87%) supplying this information in a clear-cut and understandable way.</td>
<td></td>
</tr>
<tr>
<td>However, the view of the consumer organisations is that the overall level of security-related information provided is inadequate and that there is still room for improvement.</td>
<td></td>
</tr>
</tbody>
</table>
4.6.8 Belgium

Belgium Confidence Indicator Value  7.12
EU-15 Confidence Indicator Value  7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respondents to our survey confirmed the lack of confidence of Belgian consumers to perform e-payments. It is believed that EPIs are still not widely used and this explains the low number of complaints received in this respect.</td>
<td>The findings of the public survey confirm that the confidence of Belgian consumers in e-payments remains low.</td>
</tr>
<tr>
<td>A basic barrier is lack of knowledge on how EPI/EPS are used. Occasional questions address the security of EPI against fraudulent use thereof and unauthorised access to the operating system. Other questions related to the in-time execution of the e-transaction and the right identification of the counter-party.</td>
<td></td>
</tr>
<tr>
<td>The security-related information is generally provided as standard on the website of Payment Service Providers. A usual location to find user-friendly information about the security features is the FAQ section. Sometimes, links are provided to the website of the provider of the EPS. The essential features thereof are also outlined in the general services agreements (or T&amp;C accompanying the contracts). General security procedures and technical information is supplied in paper-based documents (users’ guides etc.).</td>
<td></td>
</tr>
<tr>
<td>The security-related information is in general provided prior to the signing of the general services agreement. The information is made available in clear and user-friendly language.</td>
<td></td>
</tr>
<tr>
<td>Although bank institutions responding to our survey qualified the level of information provided as satisfactory, it is admitted in general that there is still room for improvement.</td>
<td></td>
</tr>
</tbody>
</table>
### 4.6.9 France

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>The respondents to our survey believe that the lack of significant complaints reported is due to the fact that, apart from payment cards, the use of all other EPIs is still in an embryonic phase.</td>
<td>Indeed, Part I of the study reveals that “pay later” products, being primarily credit cards, and to a lesser extent, “pay now” EPIs, are far more widely used than “pay before” products. More information about less widely known means of e-payment could probably enhance the consumers’ confidence in using them.</td>
</tr>
<tr>
<td>Most of the concerns reported relate to the security of e-operations in general, not to e-payments specifically.</td>
<td>Surprisingly enough and contrary to the average situation in EU, e-merchants in France present a higher degree of compliance in the provision of security-related information than financial institutions (the availability, accessibility and comprehensibility of information on French e-commerce websites ranks above the EU average level).</td>
</tr>
<tr>
<td>Information is most of the times provided as standard on the website of Payment Service Providers and in a clear, consumer-friendly language.</td>
<td>The situation is less encouraging when looking at e-banking websites that seems to better reflect the rather low confidence indicator.</td>
</tr>
<tr>
<td>The overall quality level of the security-related information was qualified as satisfactory.</td>
<td></td>
</tr>
</tbody>
</table>
### 4.6.10 Ireland

Ireland Confidence Indicator Value 6.91  
EU-15 Confidence Indicator Value 7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>We received no feedback from Ireland through our survey.</td>
<td>The low confidence indicator corresponds to the poor level of information appearing to be the rule for e-commerce websites.</td>
</tr>
<tr>
<td>Following our websites’ assessment, all Irish financial institutions offering e-payment services make available on their websites information about the security features in use and this in a clear and consumer-friendly way. However, in less than half of the e-banking websites scrutinised (33%), it was easy to find this information.</td>
<td>The correlation is not so obvious when looking at the e-banking websites scrutinised.</td>
</tr>
<tr>
<td>On the contrary, it was found that e-commerce websites make systematic way (33% of the websites surveyed communicated security-related information). The percentage of e-commerce websites making it easy for consumers to find this information is even lower (11%).</td>
<td></td>
</tr>
<tr>
<td>In the light of the above, it seems that the level of security-related information provided to consumers is satisfactory with respect to e-banking websites but that further improvements are needed to streamline the information available on the e-commerce websites.</td>
<td></td>
</tr>
</tbody>
</table>
4.6.11   Austria

Austria Confidence Indicator Value   6.66
EU-15 Confidence Indicator Value   7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>No complaints were communicated by the Austrian Consumer Bodies and Austrian Bankers’ Association addressing specifically the security of EPIs or the information provided thereupon. The queries to which these bodies were asked to answer related to traditional banking business, not at all to EPIs.</td>
<td>Contrary to the outcome of the responses received through the public survey, the results of the websites’ screening show that the level of security-related information supplied on both e-banking and e-commerce websites is indeed below the average EU level (and, with respect to the comprehensibility of information on the e-banking websites equal to it). These findings correlate with the low confidence indicator indicated herein.</td>
</tr>
</tbody>
</table>

Yet, it was reported that problems specific to e-payment operations may exist, but, apparently, consumers do not consider them as so significant to subject them to official complaints to the Austrian Ombudsman Bureau.

The security-related information is most of the times communicated as standard, on the website of the Payment Service Provider or in another paper-based document (user’s guide, explanatory brochure) and orally when asked. It is primarily provided before the signing of the general services agreement.

As to the form, it was indicated that information is in general communicated in clear, comprehensive language and in a visible manner.

The overall quality level of the information available was found to be satisfactory.
4.6.12  Italy

Italy Confidence Indicator Value  6.62
EU-15 Confidence Indicator Value  7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>A few complaints reported by consumer organisations addressed the lack or insufficiency of information concerning identification issues and the security surrounding an e-payment operation in general (e.g., existence of security protocols). Another problem that seem to worry Italian consumers is proving that the e-payment was executed as intended. Some questions addressed to bank institutions related to the use of EPIs in particular situations.</td>
<td>The results of the websites’ survey confirm the opinion expressed by consumer protection bodies in our survey. In most cases, the level and form of security-related information provided on both Italian e-commerce and e-banking websites range below the average EU percentage. Therefore, the confidence indicator and the findings on the security-related information about EPIs are not contradictory.</td>
</tr>
<tr>
<td>Security-related information is provided as standard through the website of Payment Service Providers or the standard services agreement (in T&amp;C thereof) or in a paper-based document (user’s guide, leaflet etc.).</td>
<td></td>
</tr>
<tr>
<td>Most of the times, information is provided at the moment of signature or after the signing of the general services agreement, in a user-friendly language and form.</td>
<td></td>
</tr>
<tr>
<td>Although the opinion of bank institutions is that the level of information provided is satisfactory, consumer protection bodies qualified it as rather inadequate.</td>
<td></td>
</tr>
</tbody>
</table>
4.6.13 Spain

Spain Confidence Indicator Value  6.46
EU-15 Confidence Indicator Value  7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>The few complaints received by financial institutions addressed the non-appearance of indicators (e.g., little locks on websites supporting e-payments) ascertaining that the transaction is carried out safely. Other queries related to adequate proof of payment and a few others addressed the usability of EPIS.</td>
<td>The criticisms received by Spanish consumer protection bodies through our survey seem to correspond to an equally low level of consumer confidence in e-payments.</td>
</tr>
<tr>
<td>Although financial institutions reported that information is always provided as standard on the website of Payment Service Providers and this in a clear wording and attractive appearance, consumer organisations appear to be more reluctant to confirm such statements. On the contrary, the latter emphasised that websites only supply vague and unclear information about the security of EPIS. Also, that there are very rare the cases in which clarifications are given at the time of performing an e-transaction.</td>
<td>However, the low confidence level, together with the outcome of the public survey, contradicts the findings of the websites’ assessment. The results of the website scanning indicated the availability, accessibility and comprehensibility of information on the Spanish e-merchant and e-banking websites as above the EU average level.</td>
</tr>
</tbody>
</table>

Accordingly, the banking institutions qualify the overall level of the information provided as satisfactory, whilst consumer organisations criticised it as inadequate.
4.6.14 Portugal

Portugal Confidence Indicator Value 5.51
EU-15 Confidence Indicator Value 7.08

<table>
<thead>
<tr>
<th>Summary of consumer feedback from websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>No complaints relating to the security features of EPIs have been received by the respondents to our survey. However, in a few cases only e-commerce websites in Portugal provide information about the security features in use. This low percentage (43%) was also confirmed through the websites’ assessment. The number of financial institutions making available such information is also considerably low (43%). In the cases in which security-related information is provided, this is done in a standard way and mainly through the website of the Payment Service Provider or in the standard services agreement. Most of the times, information is provided at the time of signing the services agreements. As for the form in which the information appears, it is mostly in a confusing language, with reference to many technical terms. Moreover, it is difficult to get access to this information (sometimes, providing through hidden links), even in the case of e-banking websites. In general, the quality level of security-related information provided in Portugal is qualified as poor and inadequate.</td>
<td>The inadequate level of security-related information provided on both Portuguese e-commerce and e-banking websites, being also confirmed through the website scanning exercise, goes together with a very low level of confidence.</td>
</tr>
</tbody>
</table>
### Greece

Greece Confidence Indicator Value  5.25  
EU-15 Confidence Indicator Value  7.08

#### Summary of consumer feedback from websites

<table>
<thead>
<tr>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surprisingly, this low level of confidence of Greek consumers in the use of EPIs cannot be explained either through the input received from the respondents to our survey or the websites’ assessment.</td>
</tr>
<tr>
<td>On the contrary, financial institutions seem to be very careful when making available security-related information to users of EPIs and, most of the times, such information is communicated in consumer-friendly language and through visible links. The situation is less positive with respect to e-commerce websites but, even there, the overall level of information is above the average EU indicator.</td>
</tr>
</tbody>
</table>

- Only a few queries have been received by the financial institutions responding to our survey.

- In their majority, these questions addressed the risks of fraudulent use of EPIs, the proof of payment, the usability of EPSs and the assurance against technical failures of the operating system.

- The information is mostly provided as standard on the website of the Payment Service Provider, the standard services agreement and by means of other paper-based documents (user’s guides, brochures etc.).

- The information is generally communicated before the signing of the services agreement.

- The language used to communicate security-related information is rather formal with few legal terms that are however explained in a clear and comprehensible way.

- The respondents to our survey qualified the overall quality level of security-related information as adequate.
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Electronic) Wallet</td>
<td>An encrypted storage medium holding payment card or other financial information that can be used to complete electronic transactions without re-entering the stored data at the time of the transaction. Wallets may also be employed to store electronic cash.</td>
</tr>
<tr>
<td>A3/A8</td>
<td>Techniques used to authenticate GSM subscribers. GSM operators can choose from several options, one such option is COMP128.</td>
</tr>
<tr>
<td>A5</td>
<td>Encryption used to protect the confidentiality of the communication on GSM networks.</td>
</tr>
<tr>
<td>Building Blocks</td>
<td>Technologies or concepts that are used for a variety of payment systems and which are explained in a separate sections of the report.</td>
</tr>
<tr>
<td>Card Not Present transaction (CNP)</td>
<td>Payment card transactions during which the payment card is not present at the merchant. The term of Card Not Present transaction is broader than the term of MOTO transaction as it is not related to mail or telephone. In practice both terms are often used synonymously.</td>
</tr>
<tr>
<td>Card Verification Value (CVV)</td>
<td>A number printed, but not embossed, on payment cards in addition to the card number and expiry date that can be used to verify possession of the card in MOTO transactions.</td>
</tr>
<tr>
<td>Https</td>
<td>Http secured with SSL or TLS.</td>
</tr>
<tr>
<td>Mail Order Telephone Order (MOTO)</td>
<td>MOTO transactions are payment card transactions during which the payment card is not present at the merchant. Originating from the time when this typically occurred when a cardholder ordered using mail or telephone, the term is used nowadays also the refer to Internet payment card transactions that are carried out by simply stating the card number and expiry date.</td>
</tr>
<tr>
<td>Payment Service Provider (PSP)</td>
<td>Payment service providers (PSPs) offer the service of handling payments to Internet merchants. Merchants redirect their customers to the PSP’s site. The PSP offers a range of payment methods. After payment is completed, the PSP will inform the merchant of this. In this way, the merchant deals with one rather than multiple parties while still offering payment flexibility to its customers.</td>
</tr>
<tr>
<td>Person-to-Person (P2P) payment</td>
<td>A non-cash payment (transfer) from one subscriber (consumer) to another subscriber of a compatible system. Also known as Peer-to-Peer payment (transfer)</td>
</tr>
<tr>
<td>Term</td>
<td>Explanation</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SET (Secure Electronic Transaction)</td>
<td>A payments protocol developed by Visa and Mastercard</td>
</tr>
<tr>
<td>SIM Toolkit</td>
<td>Software that makes it possible to place GSM operator specific applications on GSM phones. Such application typically have their own menus, can work together with the SIM card and can communicate via Short Message Service (SMS) with the GSM operator.</td>
</tr>
<tr>
<td>SSL (Secure Sockets Layer)</td>
<td>Generic method to cryptographically secure communication on the Internet taking place between a client and a server. SSL is based on public key encryption usually only the server is using a certificate. SSL is best known for securing the World Wide Web protocol http, resulting in https. However this is only one example of the use of SSL.</td>
</tr>
<tr>
<td>TLS (Transaction Layer Security)</td>
<td>A form of SSL that is adopted by the Internet Engineering Taskforce.</td>
</tr>
<tr>
<td>WTLS (Wireless Transaction Layer Security)</td>
<td>Form of TLS to cryptographically secure Wireless Application Protocol (WAP) communication.</td>
</tr>
</tbody>
</table>
### List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNP</td>
<td>Card Not Present</td>
</tr>
<tr>
<td>CVV</td>
<td>Card Verification Value</td>
</tr>
<tr>
<td>DG</td>
<td>Directorate General</td>
</tr>
<tr>
<td>EPI</td>
<td>Electronic Payment Instrument</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Telephony</td>
</tr>
<tr>
<td>http</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>https</td>
<td>Hyper Text Transfer Protocol (Secure)</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Taskforce</td>
</tr>
<tr>
<td>MOTO</td>
<td>Mail Order/Telephone Order</td>
</tr>
<tr>
<td>P2P</td>
<td>Person-to-Person or Peer-to-Peer</td>
</tr>
<tr>
<td>PSP</td>
<td>Payment Service Provider</td>
</tr>
<tr>
<td>PwC</td>
<td>PricewaterhouseCoopers</td>
</tr>
<tr>
<td>SET</td>
<td>Secure Electronic Transaction</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TLS</td>
<td>Transaction Layer Security</td>
</tr>
<tr>
<td>WTLS</td>
<td>Wireless Transaction Layer Security</td>
</tr>
</tbody>
</table>