

# **WP1 E-Payment Authentication Study - Final Deliverable**

**Version number: v1.0  
Date: 23/11/2007**

### Document Information

Document Title:	WP1 E-Payment Authentication Study - Final Deliverable
Issue Date:	23/11/2007
Project Reference:	MARKT/2006/08/F
Document Archival Code:	WP1 SIE - 1.0
Authors:	<ul style="list-style-type: none"> <li>- Sylvie Lacroix (SEALED)</li> <li>- Olivier Delos (SEALED)</li> <li>- Marijke De Soete (Security4Biz)</li> </ul>

### Version control

Version	Date	Description / Status	Responsible
0.1	30/09/2007	First input version	SEALED, Security4Biz
0.2		Quality review	Siemens
0.5	07/11/2007	Further refining, start to integrate Mr. Fernandez-Salas' comments	SEALED, Security4Biz
0.6	09/11/2007	Quality review	SEALED, Security4Biz, Siemens
1.0	23/11/2007	Editorial changes + minor technical addition and European Commission comments's integration	SEALED, Security4Biz,

### External Distribution

Version	Company	Name	Action required
0.2	30/09/2007	M. Fernandez-Salas	Review
0.6	09/11/2007	M. Fernandez-Salas	Review
1.0	23/11/2007	M. Fernandez-Salas	Review

### Annexes provided in a separate document

- [A1] WP1 – Methodology
- [A2] WP1 - Experts and Industry - EPI Providers - Payment Schemes Providers questionnaires v1.0
- [A3] WP1 - Experts and Industry - EPI Providers - Banks questionnaires v1.0
- [A4] WP1 - Experts and Industry - Security & Technology Experts questionnaires v1.0
- [A5] WP1 - Experts and Industry - Technology Providers questionnaires v1.0
- [A6] WP1 – Authentication methods
- [A7] WP1 – Card Payments

[A8] WP1 – E-Payments

[A9] WP1 – M-Payments

[A10] WP1 – Banks and eID Cards

## Table of content

<b>TABLE OF CONTENT .....</b>	<b>4</b>
<b>1. FOREWORD .....</b>	<b>6</b>
<b>2. EXECUTIVE SUMMARY.....</b>	<b>7</b>
2.1 MOST FREQUENTLY USED PAYMENT AND USER VERIFICATION METHODS.....	7
2.2 BEST USER VERIFICATION METHODS PER PAYMENT TYPE.....	8
2.2.1 <i>Best user verification methods for card payments</i> .....	8
2.2.2 <i>Best user verification methods for e-payments</i> .....	9
2.2.3 <i>Best user verification methods for mobile payments</i> .....	11
2.3 EMERGING TECHNOLOGIES.....	12
2.4 BARRIERS TO THE IMPLEMENTATION OF BEST USER AUTHENTICATION METHODS .....	14
2.5 FRAUD CONSIDERATIONS AND IMPACT ON USER VERIFICATION METHODS .....	17
<b>3. INTRODUCTION .....</b>	<b>18</b>
<b>4. USER VERIFICATION METHODS .....</b>	<b>19</b>
4.1 DEFINITIONS .....	19
4.1.1 <i>Identification</i> .....	19
4.1.2 <i>Authentication</i> .....	19
4.2 HOW DOES AUTHENTICATION WORK – AUTHENTICATION FACTORS .....	20
4.3 ENTITY AUTHENTICATION TOOLS IN THE FINANCIAL WORLD .....	21
4.3.1 <i>PINs, Passwords &amp; Passphrases</i> .....	21
4.3.2 <i>PINs</i> .....	22
4.3.3 <i>Passwords &amp; Passphrases</i> .....	22
4.3.4 <i>Challenge-response authentication schemes</i> .....	23
4.3.5 <i>Biometric systems</i> .....	24
4.4 DATA AUTHENTICATION IN THE FINANCIAL WORLD .....	25
4.5 LINKED SECURITY CONCEPTS.....	25
4.5.1 <i>Confidentiality</i> .....	25
4.5.2 <i>Privacy</i> .....	26
4.6 LEGAL AND REGULATORY IMPLICATION ON AUTHENTICATION METHODS .....	26
4.7 AUTHENTICATION METHODS LIFECYCLE .....	28
<b>5. ANALYSIS OF THE CURRENT AND PROSPECTIVE CARD HOLDER/USER VERIFICATION/AUTHENTICATION METHODS .....</b>	<b>29</b>
5.1 INTRODUCTION .....	29
5.2 CARD PAYMENTS .....	31
5.2.1 <i>Introduction</i> .....	31
5.2.2 <i>Security challenges</i> .....	31
5.2.3 <i>Selection, assessment and analysis for the most used card payments</i> .....	32
5.2.4 <i>Facts and figures</i> .....	35
5.2.5 <i>Possible barriers to the implementation</i> .....	36
5.3 E-PAYMENTS .....	36
5.3.1 <i>Foreword and structure</i> .....	36
5.3.2 <i>E-payments security challenges</i> .....	37
5.3.3 <i>E-banking</i> .....	38
5.3.4 <i>E-commerce</i> .....	50
5.3.5 <i>Prospective e-banking and e-commerce authentication methods</i> .....	66

5.3.6	<i>Selection, Assessment and Analysis for the most used technical cashless payments.....</i>	<i>66</i>
5.3.7	<i>Facts and figures .....</i>	<i>68</i>
5.3.8	<i>Possible barriers to the implementation .....</i>	<i>68</i>
5.4	<b>M-PAYMENTS.....</b>	<b>69</b>
5.4.1	<i>Mobile Payments categories .....</i>	<i>69</i>
5.4.2	<i>Analysis of m-payment schemes.....</i>	<i>71</i>
5.4.3	<i>Prospective Mobile Payments &amp; Mobile Users Authentication Methods.....</i>	<i>82</i>
5.4.4	<i>Selection, Assessment and Analysis for the most used technical cashless payments.....</i>	<i>84</i>
5.4.5	<i>Facts and figures .....</i>	<i>84</i>
5.4.6	<i>Possible barriers to the implementation .....</i>	<i>84</i>
<b>6.</b>	<b>EMERGING TECHNOLOGIES .....</b>	<b>86</b>
6.1	MOBILE PHONE .....	86
6.2	EID CARDS .....	86
6.3	CONTACTLESS TECHNIQUES AND PROXIMITY PAYMENTS.....	87
6.4	BIOMETRY .....	87
6.5	IDTV.....	88
<b>7.</b>	<b>PAYMENT INDUSTRY PERCEPTION .....</b>	<b>89</b>
7.1	INTRODUCTION .....	89
7.2	MAIN RESULTS.....	89
<b>8.</b>	<b>CONCLUSIONS AND RECOMMENDATIONS .....</b>	<b>93</b>
8.1	MOST USED AND BEST USER VERIFICATION METHODS .....	93
8.2	EMERGING TECHNIQUES.....	95
8.3	BARRIERS AND RECOMMANDATIONS.....	95
	<b>REFERENCES .....</b>	<b>97</b>
	<b>ABBREVIATIONS.....</b>	<b>103</b>

## 1. Foreword

With the fast dissemination of public on line interactive services such as the internet and interactive TV and the increasing use of customer devices like PCs, mobile phones and PDAs, the European “on line market” is expanding rapidly.

Electronic payments, which cover any kind of non-cash payments that do not involve a paper check, are considered as an essential cornerstone for this on line market. However, electronic payments cannot be sustainable without a secure and trusted environment in order to obtain and maintain the confidence of all stakeholders, more in particular the customers..This trust in the system can only be achieved through an appropriate protection of its users against the various security threats. For example, one of the main security concerns for the users of an electronic payment system is to receive debits for a transaction they never agreed upon. This could happen as a consequence of an end-user privacy violation, e.g., when personal information is re-used for another purpose than the original intended one (e.g., having card or account data stolen and re-used in a so-called replay attack). Identity theft, which is the fraudulent exploitation of another entity’s identifying information for criminal purposes is emerging as one of the most important type of crime nowadays. However, identity theft can be avoided by ensuring the right security measures and policies, including the appropriate authentication of all the principals acting in a transaction system to guarantee proof of their identity.

The objective of the present study is to analyse current and prospective card holder verification/authentication methods on card payments, as well as user verification methods on e-payments and mobile payments in this “on line” market. The document provides an overview of existing and prospective verification methods with a security assessment of each of the methods described. These assessments are presented by type of electronic payment and by type of technical solution and further provide information on which of the existing methods are the most frequently used, their actual protection against certain fraud types, the potential barriers regarding the use of these techniques and their economics and collateral dependencies.

## 2. Executive Summary

This section provides an overview of the most important results and conclusions of WP1 in terms of trends in the field of user's authentication methods to e-payment and summarises the aspects related to the methods most used and the emerging technologies. It further highlights the methods that are selected as "the best ones in use" and also aims to provide an overview of the possible barriers that might prevent or hinder the deployments of these methods. The reader may find a more detailed analysis of all these methods in the subsequent sections.

Together with the outcome of WP2 and WP4 of the present study, all these findings are provided as basis for WP5 to derive recommendations to the European Commission in order to help circumventing the potential barriers to the best user's verification methods in e-payments.

### 2.1 *Most frequently used payment and user verification methods*

In the context of this study on user identification methods in card payments, mobile payments and e-payments, each of the payment methods most used has been assessed in view of its level of security, vulnerability and fraud resistance and last but not least its user perception. From these assessments the best user identification and verification techniques have been selected from a security perspective.

WP2 has concluded on the following order for the user preference on payment methods:

1. Cards
2. On line
3. Mobile.

Also in terms of trustworthiness, user friendliness and relevance in day to day life, card payments appear at the top of the list but nevertheless, are closely followed by the internet payments which gain in importance. This order of preference is also aligned with the observations made by WP1 on the awareness and usage of the cashless payment solutions, where clearly card payments are the most common payments means in the European countries. This observation does not only apply to card present payments (e.g., at a point of sales), but is also valid for e-commerce (e.g., buying on the internet).

Irrespective the payment type (card, e- or m-payment), the **two-factor authentication** is the **expected and recommended minimal level of authentication** for cashless payments. This is not only reflected by the security analysis but is also re-enforced by the legal and regulatory framework. However, this does not mean that this level of security is already commonly applied.

The **most frequently** employed user authentication method is a "secret you know" (e.g., password, PIN code) based authentication often combined with a "**something you have**" as an additional authentication factor. Payments cards in combination with a PIN are the most

frequently used method for cashless transactions. The main reason for the usage of the PIN are its ease of use, the concept is well understood and established amongst users, and no sufficient fraud exists which is directly related to this verification method which could create a sense of distrust.

**Best user authentication method in cashless payments relies on something you know (e.g. dedicated payment PIN), supplemented by an additional “something you have” authentication factor, in order to implement 2-factor authentication**

## 2.2 Best user verification methods per payment type

### 2.2.1 Best user verification methods for card payments

The best user authentication/verification method for card present based transactions relies on the provision of the PIN code at transaction time. For credit cards in particular, this is far more secure than relying on the provision of the card holder signature (additionally to the card information capture). Whereas the mag-stripe cards with an on line verification of the PIN only offered limited security due to the possibility of counterfeit cards (using skimming attacks), the migration to chip cards considerably increased the security. Indeed, the usage of IC Card technology allows the dynamic authentication of the card at transaction time. This is, in combination with the card holder verification by means of a PIN, the best card holder authentication/verification method available today for card payments.

The combination of the usage of IC Card technology allowing the dynamic authentication of the card at transaction time and the provision of the card holder PIN code is the best (2-factor) card holder authentication/verification method available today for card payments.

The adoption of IC card authentication in combination with a PIN as user verification method will also be followed by the SEPA Cards Framework (SCF) for implementation in the European member countries. This framework will define a set of minimum requirements, including security, which allow for functional interoperability of elements of the processing chain for the different SCF compliant schemes (global or national, alliances and any new schemes). These minimum requirements will be based on the EMV specifications and adopt PKI-based authentication of the cards (static or dynamic). Furthermore three types of PIN verification methods will be specified:

- on line PIN verification by the Issuer based on symmetric crypto,
- off-line clear text PIN verification by the card,
- off-line encrypted PIN verification by the card based on asymmetric crypto.

With this framework at least a harmonisation of a minimum security level for card based transactions will be realised in Europe.

### 2.2.2 *Best user verification methods for e-payments*

For e-payments the study has made a distinction between e-commerce (payments using the internet) and e-banking.

#### **E-commerce**

##### *e-Payment schemes in general*

Payments on the internet can either be:

- direct from buyer to merchant (the transaction is not powered by an intermediary payment service provider, except the credit card company, e.g., Visa, MasterCard); or
- indirect and relying on a TTP (i.e. a transaction where an intermediary payment service provider secures the transaction (e.g., Paypal, Ogone).

Payment schemes whereby the merchants outsource some of the payments tasks are promising from a security perspective. A detected trend is the redirection from the merchant towards the customer's e-banking and/or web banking facilities. This redirection may occur via the intermediary of a TTP (e.g., Ogone), or directly from the merchant site when this merchant has agreements with banks (e.g., mainly applicable when selling local goods). This trend is indeed very important with respect to security. It not only increases the guarantee of a correct execution of these so-called payment tasks (such as user identification/verification) but also has an impact on the privacy. Indeed, the financial data and the goods related data follow two distinct channels. This separation of data improves the customer's privacy. In addition, the use of a well-known TTP also increases trust and user's confidence in the payment solution. Solutions where the payment is performed indirectly tend to overtake solutions where the payment is done directly to the merchant. This observation is EU-wide and was quite expectable since the goods and services that are paid via e-payment methods are provided by EU or even world-wide merchants such as eBay.

However, regarding the user perception, although the trend is to rely on TTP-based schemes, WP2 shows a slight preference from the end-users to directly deal with the merchant. This may be explained by the fact that end-users might not realise the benefits of the usage of a TTP.

##### *User verification methods*

**On the internet, card payment is the main payment channel** (independent of the payment scheme).

Chargeback rates for internet purchase transactions supported by bank cards are several times higher than face-to-face (e.g., card holder present) chargeback rates. The majority of the chargeback reasons are fraud-related or card holders claiming non-participation. According to VISA, 80% of all e-commerce chargebacks and fraud, as well as a substantial proportion of customer complaints, could be eliminated with the use of authenticated payments, a means to verify that the person making an e-commerce purchase is an authorised card holder.

For this purpose, different schemes such as 3D Secure, supported by payment card companies allow issuers to authenticate their customers. Card-based payments schemes that are based on 3D secure and where the issuer authenticates its customer seem very promising from a liability perspective; the issuer is responsible to choose the ad-hoc authentication method. In particular, EMV card based authentication meets the requirements.

Irrespective the payment scheme, from a security level perspective, the best user verification methods implemented so today rely on 2-factor authentication systems (e.g., user ID + password, whether static or dynamic and combined with the possession of specific device, card or security software). However, most of the payments schemes remain on a “1-factor” authentication system essentially based on a static password.

For payment schemes making use of an intermediary TTP with user account, one sees an evolution towards the use of a dynamic factor, while direct payments to merchant remain basically SSL based with no other user authentication than the card related information accompanied by the request for the related CvX numbers.

In the context of e-commerce and internet payment schemes, **the TTP based payments schemes are better payments schemes from a security perspective than those not powered by an intermediary payment service provider:**

- TTPs evolve towards the use of a dynamic factor
- Direct payments to merchants remain SSL based with a static factor (with no other authentication than the card related information accompanied by the request for the related CvX numbers).

Irrespective the payment scheme, from a security perspective, the **best user verification methods rely on 2-factor authentication systems** (e.g. user ID + password, whether static or dynamic combined with the possession of specific device, card or security software).

Irrespective the payments scheme, **cards payments are not only used most frequently but also offer** the best security. Card-based schemes whereby the card issuer authenticates the user are considered as the best payments schemes. In particular, an effective way of preventing the classical frauds linked to card-not-present is to use the EMV smart card authentication to perform user authentication or on line payment transaction authentication.

However, most of the payments schemes remain today on a “1-factor” authentication system (e.g., user ID + password).

## E-banking

Interestingly, there is a convergence of authentication methods in the e-banking environment towards 2-factor authentication methods. In particular, EMV authentication is more and more used.

In e-banking, the use of a PINPAD<sup>1</sup> reader producing a challenge-response signature based on the user’s bank card seems to generalise. This observation is EU-wide and was quite expectable since there are standards that uniform such payments schemes.

However, WP2 shows that the users prefer a static password for e-banking because of the convenience.

**Two-factor authentication methods implemented in the context of e-banking schemes are to be considered as the best user identification/ verification methods.**

In particular, an effective way of performing user authentication is to use the **EMV smart card authentication**. This technique based on a card reader **tends to generalise and appears to be the best technique for authentication in web banking**.

Security of e-banking schemes may be reinforced by the use of dedicated software (e.g. an applet from the bank). This solution helps to prevent attacks such as webspoofing (see Annex 8).

The use of e-signatures as specified in the European Directive on e-signature may offer an advantage for non-repudiation purposes related to liabilities and possible litigations.

### 2.2.3 *Best user verification methods for mobile payments*

With regard to mobile payments, the authentication methods most frequently used are based on 2-factor authentication which combines the usage of a PIN with the possession of the mobile device. However the sole reliance on the classic PIN protecting the mobile device is not to be considered sufficient to meet the e-banking requirement “to know their customers”. To address this requirement, the best user identification / verification methods are based on the delivery and implementation of an additional, dedicated PIN for the payment application available on the mobile device. The delivery of such a dedicated mobile payment PIN is processed through existing and secure electronic channels (e.g., through the use of bank card authentication in ATMs allowing mobile payment activation facilities) that were established based on a prior face-to-face authentication (e.g., opening of a bank account).

The required convergence and collaboration between financial services providers, mainly the banks, on one side and the mobile operators on the other side is observed to fragment the market into multiple and often incompatible initiatives such as in France, or to federate the market around one (monopolistic) scheme as in Belgium.

In the context of mobile payment schemes, the best user identification and verification methods are based on the use of **2-factor authentication combining the possession of a**

<sup>1</sup> The PINPAD reader is a smart-card reader with a dedicated keyboard enabling to enter securely the card PIN Code.

**(mobile PIN-protected) mobile device and the use of a specific PIN dedicated to the payment application** and delivered through a secure channel preferably established at a (prior) face-to-face authentication.

However, many of the m-payments means most used today are still based on a one-factor authentication method (e.g., SMS).

Finally, to conclude this section, it is worth mentioning that the weakest step identified by this study in all the authentication processes is **the user registration phase**. This is because all subsequent steps rely on this first crucial task. If someone manages to be enrolled under a false identity, the registration process will furthermore reinforce the link between this person and its false identity by providing him/her with official credentials validating initially corrupted information. And precisely these credentials will be relied upon in further authentication processes.

## 2.3 Emerging technologies

### The usage of mobile phones

Emerging technologies in the context of user authentication in electronic payments schemes are mainly related to the usage of mobile phones as part of a two-factor based authentication process. The noticeable element here is the combination of two Trusted Third Parties (TTPs). While normally payment schemes only rely on the Bank as the TTP, here an additional TTP, namely the Telecommunication Operator, is involved. The appearance of a new actor and the modification of the relationships and business models are one of the main challenges for the introduction of this new payment access channel. With the introduction of mobile phones, user verification for the payment transaction most often requires the presentation of a dedicated payment PIN. However, new user verification methods such as fingerprint are being investigated and start to be piloted.

### The usage of electronic identity cards (eIDs)

Besides the mobile phone, another new tool appears on the market to support user authentication, namely the electronic Identity (eID) card. Such eID cards have been or are being introduced in quite a number of European countries and hence, because of the widely spread, are becoming well-known to the citizens. Where in some countries the issuance for these eID cards is fully managed by the governments (acting as a TTP), in some cases, they result from Private-Public Partnerships (PPP) between banks and governments as issuing bodies, such as in Sweden, Estonia, or Luxembourg. As detailed in the “emerging technologies“ section, there is in this context, at least in some countries, a real interest of the e-banking sector to work with public authorities as close as possible on the topics of user authentication and e-signatures. In addition to the intrinsic added value with respect to security, the usage of eID cards can even be seen as a marketing advantage for the payment scheme providers (e.g., Keytrade bank). This is a rather new trend.

E-commerce providers are more and more concerned by security issues and investigate the migration to stronger authentication means such as the eID card.

### **Contactless cards or devices**

During the last years the usage of contactless technology is also emerging in the payment area. Proximity payments are being introduced using contactless cards as replacement for “small cash” transactions such as parking meters, movie tickets, etc... These new payment tools have firstly been introduced in the U.S. but now also European payment schemes are considering them. In most cases a user verification method such as a PIN is not used.

Even more recent the so-called “display cards” have been prototyped which have a battery (next to the contact and contactless interfaces) and provide a small screen and a couple of push buttons. These new features might become important to enhance the security for payments. However, first the trade-off issue between the price (mass production) and the enhanced functionality and security for these devices needs to be solved before real market introduction would be possible.

During the last years also the NFC (Near Field Communication) technology is being introduced for proximity payments by means of mobile phones. In this context user authentication methods will remain similar to those already used in mobile payment schemes.

### **Biometry**

Biometry is currently not really used in the payment context and is not expected to be a relevant prospective method for authenticating users in the near future due to the lack of stability, difficulty of use, cost effectiveness, and mostly due to the lack of added value compared to existing solutions. Indeed, it does not offer new advantages to the payment schemes to solve the problem of user verification in an open and interfering environment, with no possibilities to select or educate users on the appropriate usage. However, in the more distant future this might change. Already in Asia pilots are planned in rural areas where payments with a mobile phone with fingerprint will be considered as user verification methods. To what extent these solutions would also be adopted in Europe is very difficult to predict. Indeed, two main factors that are playing in Asia, namely the lack of banking infrastructure and the analphabetism, do not exist in Europe.

### **User’s perception on emerging technologies**

From a user perspective, WP2 shows that the following preference list on innovative payment methods:

1. Biometry,
2. RFID,
3. iDTV.

This ranking of preference is aligned with the observed fact that biometry could soon enter the cashless world, while RFID is not really seen as a convenient tool for all cashless payments (especially on the internet).

### **Best emerging technologies**

Amongst the technologies mentioned above, it seems that mobile phones, contactless technology and eID cards might be expected to play an increasing role in the next years, provided that some barriers (see below) are correctly addressed..

## 2.4 Barriers to the implementation of best user authentication methods

### eID usage barriers

While perceived as interesting, eID based schemes are not yet an accepted alternative for authenticating users in the context of cashless payments (e.g., as authentication method in e-commerce). Some of the barriers identified can be listed as follows:

- Lack of cross-border PKI interoperability and mutual recognition,
- Lack of control on the registration and issuance process in countries where the banks are not part of the issuing process of eID cards
- Liability issues, there are questions about the split of liabilities and who will take up the fraud,
- Co-existence of the standards supporting the EU directive on Electronic signatures and standards adopted by the banking sector that both would need to be applied:
  - o ISO TC68 standards *versus* ETSI TSs;
  - o EMV cards specifications *versus* the different SSCD and eID related CWAs.

The liability issues could possibly be solved through legislation.

The cross-border and mutual recognition issues should be tackled by 2010 within the i2010 programme.

### Mobile phone barriers

A possible barrier with respect to the availability of this payment channel comes from the fact that the mobile phone battery must be loaded.

In some cases, it can be an issue for the user to disclose its mobile phone number to its bank(s).

### Contactless technology

One of the main barriers in contactless technology is the unwanted interception or alteration of transaction data that might lead for instance to replay attacks. Therefore the investigation of technical solutions whereby the users “actively” approve the transaction on its token (e.g., via a push button on card after the display of the transaction amount on the card) or whereby the user token is protected against the “antenna attacks” should be promoted.

### Need for harmonisation and certification of security tools

The financial industry wishes a high level of security. However, except for what can be derived from the Anti-money laundering Directive [8] in terms of registration, there is no legal framework today requiring specific security measures for e-payments. Actually, the Anti-money laundering directive does not *strictly speaking* impose particular security features on payment instruments, but the directive requires well the banks to “know their customers” and has thus implication on the requirement to “register” clients, a face to face is highly recommended. Clients’ registration is a crucial step for initiating any user’s authentication method and sustaining subsequent security measures.

Nevertheless, there are already some schemes in place such as the BCE recommendations from 2003 that can be associated with the implementation of the Directive. Most of the recommendations criteria are based on assessment to be performed by Accreditation/Certification bodies. Some payment schemes such as Visa/Mastercard and some national schemes such as ZKA in Germany and CB in France also impose security evaluations.

In particular, for card payments, EPC has chosen to use smart-cards and follow largely the EMV standard, with as prior objective, having the same EMV based implementations European wide. Moreover, they are also addressing the approval /certification process of devices such as smart cards and POS terminals. Having a more harmonised way to address authentication and security would certainly enhance the global level of security.

The Fraud Prevention Expert Group (FPEG) advising the Commission has prepared a report providing an overview of the procedures used for the security evaluation of payment products and components (cards, terminals, software, etc.) in the European Union. The report recommends to harmonise the security procedures at EU level to evaluate the security of payment cards and terminals (see [56]).

### **Costs and barriers of implementation**

Barriers for implementation are mostly cost related. Methods that present too heavy costs, for any of the stakeholders without a clear business benefit will not be endorsed by the market. Also the market size and business revenue for the vendors and suppliers plays an important factor which have a direct impact on the implementation costs for the financial industry. Harmonisation and interoperability of the solutions proposed are therefore a “key” element.

There are also some limitations on the ways the bank can enter within the end-user’s environment. When a financial institution installs security tools, especially on a user private device (e.g., PC), it must consider the following limitations:

- Regarding privacy issues
- Regarding user friendliness issues
- Regarding resources consumption
- ...

### **Limitation of user responsibility – lack of incentive for due care of authentication credentials**

When looking at the article 50 of the Payment Services Directive [76], one clearly sees a limitation of the end-users responsibilities. This perception of protection can be seen as a positive signal to promote the use of cashless payments on one hand. However, on the other hand, this also leads to the consequence that end-users may be less concerned with security issues and become careless with their credentials.

This limitation on user responsibility has thus a positive aspect on the economical side by constituting an incentive to use e-payments, but at the same time has also a negative side regarding the user responsibility with respect to security. To struggle against that kind of behaviour, the user awareness/education is really important, as well as the possibility to sue fraudulent or even “bad” use of credentials.

### **The need for a reinforced legal framework**

The Payment Services Directive [76] specifies an incitation for the bank to increase the security of the e-transactions (e.g., sustaining authentication of each principals in a transaction) in support to a possible arbitration in a dispute or litigation. Also, the set-up and recognition of an appropriate framework for the accreditation/evaluation/certification of payment tokens and devices is important in the process of detecting fraud or solve disputes and liabilities. However, it is very important to support these technical security methods implemented by the financial sector by an appropriate legal framework to appropriately address fraud cases such as identity theft, counterfeit cards, etc...

Furthermore the victims of payment fraud should be adequately supported. Hereby not only the short term support via a dedicated declaration, investigation and communication processes should be addressed but also a legal framework should be created that recognises and addresses the possible long term financial impacts on the victims.

### **Conclusion**

A number of factors can be identified towards overcoming some of these main barriers:

For the banks and retailers:

- The decision for migration in Europe to the EMV specification by the global card schemes such as Mastercard and Visa (with fixed deadlines) with the associated liability shift to non-chip parties;
- The migration of fraud to “less secure” countries has put pressure on issuers and acquirers in those countries.

For the vendors and suppliers:

- The harmonization of specifications and the guarantee of interoperability;
- The harmonization of the security certification processes for cards (CAS-Common Approval Scheme) and PIN peds (PCI-PED) and mutual recognition (e.g., by global and national schemes)
- The increasing market size for EMV products, even more in the near future with the EPC SEPA Cards Framework.

However, a number of related problems remain:

- Who will be the “ultimate” recognized certification body in Europe for card and PIN ped approvals?
- Who will be responsible for accrediting the appropriate certification laboratories?
- How will the minimum (security) requirements be enforced?

## **2.5 Fraud considerations and impact on user verification methods**

More than only a technical feature, security is a major cornerstone for ensuring trust in cashless payments. In some cases, security even appears as a real marketing tool. This may be explained by the fact that recent frauds have been put under the spotlight by the media, making security a “hot” topic.

It is also noticeable that fraud, without increasing drastically, has changed. Fraud has become the fact of the organised crime and is no longer a game for individual hackers challenging each other and not really trying to earn money from their acts, as it was the case a few years ago. However, official figures remain very difficult to obtain.

Fraud is very often the result of identity theft (see Annex 6). User authentication is a major method to fight against identity theft. As a matter of fact, one can observe that banks enhance the web-banking facilities more and more. Nowadays, 2-factor based authentication schemes seem to become the minimal level of security for web-banking, but also for card and mobile payments.

The increase in fraud and in the skills and the organisation of the fraudsters is adequately addressed in a well balanced approach by the increase of the security level offered by the financial world for cashless payments.

In this perspective, user and data authentication are major e-security features. There is a convergence towards 2-factor based authentication methods, and in particular EMV authentication for card-based payments and/or e-banking transactions. Moreover, the financial sector organises itself to provide standards and recommendations (worldwide, EU-wide (e.g., EPC), nation-wide, ...).

Banks may also brand their security credentials (e.g., the EMV pinpad readers) to their logos to increase trust towards their customer by showing compliance to state of the art (security) technology.

E-commerce remains unfortunately basically tight to a low level of security, although pretty good techniques (similar to web-banking) exist to protect e-commerce transactions. Although important e-commerce stakeholders care about security, user authentication remains at a rather low level of security.

### 3. INTRODUCTION

As an introduction to this study it is important to define what is exactly covered by a so-called “Electronic Payment Instrument” (EPI).

The Recommendation of the European Commission concerning transactions by Electronic Payment Instruments and in particular the relationship between issuer and holder (97/489/EC) defines an EPI 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 e-banking** applications.”*

Conform the request by the European Commission; this document classifies the **user identification/verification methods** for EPI using three pillars:

- **Card-payments:** relating to card-payments on network other than internet or mobile, i.e., attended terminals (e.g., POS), unattended terminals (e.g., vending machines, parking meters) and ATMs.
- **E-payments:** dealing with e-payments occurring via PC, laptop, or another internet enabled device,
- **M-payments:** where mobile devices (gsm, pda, gps, etc.), are used as e-purse or authentication factor (e.g., via the SIM card) or as support for another authentication mechanism (mobile as PIN entry device).

After a general introduction on user verification methods which is provided in section 4, a detailed technical analysis is executed in section 5. This assessment is structured by payment type whereby for each type the different user verification methods are treated according to a methodology described in Annex 1. Section 6 provides an overview and brief analysis of emerging technologies appropriate to cashless payments. The payments industry perception on user verification methods is reflected in section 7 and is based on the outcome of dedicated questionnaires which were used to gather this information. Finally section 7 contains the conclusions and recommendations for WP1.

## 4. User verification methods

Identity theft, this is the fraudulent exploitation of another entity's identifying information for criminal purposes, is emerging as one of the most important type of crimes nowadays. Identity theft can be avoided by ensuring appropriate security measures and policies, amongst which the due authentication of all the principals acting in a transaction, in order to guarantee the proof of their identity. This section will introduce, define and briefly explain the authentication and related e-security concepts. The reader will find more detailed information on this topic in Annex 6 which aims to provide a more complete basis for the sequel of this study.

### 4.1 Definitions

#### 4.1.1 Identification

User **Identification** is the association of personal data with a specific user, e.g., surname, first name, date of birth, etc... , according to a set of data that is commonly fixed within a system to be representative of the "identity".

Formal definition<sup>2</sup>: **Identification** is the process of using claimed or observed attributes<sup>3</sup> of an entity to deduce who the entity is.

(e.g., in the context of the present study, in an e-banking transaction, the provision by the user of his/her "User ID" is an identification).

#### 4.1.2 Authentication

**User Authentication** is the proof of who the user claims to be, i.e., the proof of the exactness of the association of the identification data with a specific user.

Formal definition<sup>2</sup>: **Entity Authentication** is the corroboration<sup>4</sup> of the claimed identity of an entity and a set of its observed attributes.

User authentication should not be confused with **Data Authentication** that refers to the verification of data integrity (the fact that data has not been altered), and can be combined with the authentication of the data origin and some non-repudiation assurance about this origin.

Formal definition<sup>2</sup>: **Data Authentication** is the corroboration that the origin and integrity of data is as claimed.

---

<sup>2</sup> "Common terminology Framework for Interoperable Electronic Identity Management", Consultation paper, Modinis Study on Identity Management in eGovernment, v2.01, November 23, 2005.

<sup>3</sup> An attribute is a distinct, measurable, physical or abstract named property belonging to an entity.

<sup>4</sup> Corroboration is the confirmation by provision of a sufficient evidence and examination thereof that specified requirements have been fulfilled.

User authentication serves, in the context of cashless payments, for the authentication of the user accessing to either e-payments application, or towards the payment device whether a payment card or a mobile device enables or operates a cashless payment. Note that we are not concerned yet about transaction itself but only about the corroboration of a claimed identity from which the transaction originates.

(e.g., in the context of the present study, in an e-banking transaction, the provision by the user of his/her “password” is an authentication.

Data Authentication helps to commit on a set of data that can be a payment transaction or a document. Examples of how data authentication may be assured include the use of a check sum, a message authentication code, or digital signature. PKI based **digital signature** mechanisms ensures integrity, origin authentication and non-repudiation of having digitally signed the signed data. The assurance of those type of digital signature effects are conditioned to the correct authentication of the signer during the provision of the tools or credentials that will enable the signer to effectively sign the data and to the security and protection of these signing tools. Under some specific circumstances set by the European Directive 1999:93/EC and its implementation in the Member States, digital signatures cannot be denied legal effect and even be recognised as equivalent to a handwritten signature.

Let us illustrate these definitions by applying them to the case of e-banking:

- As a first step the user must logon on the system; for this purpose he will authenticate himself/herself (*user authentication*)
- Then, once he/she needs to confirm a transaction, he/she will perform a *data authentication* (a *signature*).

## 4.2 How does authentication work – Authentication factors

User Authentication procedures are applied for the corroboration of the identity of the user (to prove that the person really is who (s)he claims to be).

An authentication factor is a piece of information and process used to authenticate or verify a person's identity for security purposes. Two-factor authentication is a system wherein two different methods are used to perform the authentication. Using two factors as opposed to one delivers a higher level of authentication assurance.

There are three universally recognized factors, or a combination thereof, for authenticating individuals:

- Something the user knows,
- Something the user possesses,
- Something the user is.

Using **something only the user knows** is the classical way to corroborate any user’s identity based on a “shared secret” information such as a **password**, a PIN code, a pass-phrase, etc.

Using or providing **something the user possesses**, is usually based on a physical token like an identity badge, a proximity card, a **magnetic strip card**, a smart card (a hand-held

computer the size of a credit-card), an authentication token, etc. This factor is usually combined with something the user knows for authentication purposes, usually towards the token itself.

**Something the user is** deals with biometrics making use of *biometric* attributes of the user in order to corroborate its identity.

Authentication schemes based on something a user really *knows* is limited, since the user's memory is limited, and it should not vary too much over time. Whether it is a password, a PIN code or a user-id, all these items are being defined at a certain time and often are re-used a certain number of times. This makes that someone who can eavesdrop this information, will later be able to impersonate the user. A similar observation holds true for a magnetic strip card or memory chip. All these systems provide static authentication only (also called “weak” authentication). It is crucial to move to more secure ways of authenticatin methods which are not re-playable.

In other words there is a need for much **stronger authentication means**. Stronger authentication is obtained when moving from something you know, to something you have and even something you are. In addition, it is even more secure to combine two or more such authentication factors; one can then distinguish between “one-factor authentication” and “several factor authentication”. A system is said to leverage **two-factor authentication** (T-FA) (or multi factor authentication) when it requires at least two (or more) of the authentication form factors mentioned above. This contrasts with traditional password authentication, which requires only one authentication factor (such as knowledge of a password) in order to gain access to a system. For example, in a strong authentication schemes, the user should authenticate itself with respect to the device, using something he/she is the only one to know (e.g., a PIN Code). This makes the device useless if it is stolen. Note that the PIN code can be replaced by a biometric (e.g., fingerprint) to unlock the device (replacing the show “something you know” part of the protocol, by show “something you are” towards the device).

### **4.3 Entity Authentication tools in the financial world**

The authentication methods listed in this section are independent of the payment scheme or protocol used for a given transaction. Annex 6 provides a full description and security analysis on authentication mechanisms that are widely used as common building blocks in user identification / verification processes in card-, e-, and m-payment methods or protocols. Here below they will only be briefly presented.

#### **4.3.1 PINs, Passwords & Passphrases**

The very basic authentication factor that can be used to authenticate a User in the context of cashless payments is for instance the credit card number associated with a User Identifier (UID). Credit card numbers and holder information are such very basic authentication couple.

Certainly the credit card number is the most endangered and at the same time very often used. Also UID/Password techniques are still frequently used to secure home- and web-banking.

#### 4.3.2 PINs

A payment PIN (Personal Identification Number) is a means of verifying the identity of a customer within an electronic funds transfer (EFT) system. It is a code consisting of not less than 4 and not more than 12 characters in length. While there is a security advantage to use longer PINs, for usability reasons an assigned numeric PIN should not exceed 6 digits in length. It should also be noted that many international systems do not accept more than 6 digits and do not accept alpha PIN entry (including alphabetical characters).

The secrecy of the PIN needs to be assured at all times during its life cycle which consists of its selection, issuance, activation, storage, entry, transmission, validation, deactivation, and any other use made of it.

#### 4.3.3 Passwords & Passphrases

##### 4.3.3.1 (Static) Password or Passphrase

Together with Personal Identification Numbers (PINs), passwords and passphrases are the most widely used forms of authentication factor. They are used along with user identifiers (UID) in many of today's authentication schemes.

To gain access to a system resource or to confirm an electronic payment operation, the user enters a UID / Password pair. The UID is a claim of the user's identity and the password is the evidence supporting this claim. Passwords are supposed to be known only by the factor-holder and consist usually in at least 6 characters that are shared between the verifying entity and the factor-holder. In many systems they are not stored in cleartext at the verification side but stored in encrypted form.

One-factor authentication methods that are based on the sole use of passwords are rarely providing adequate protection due to their numerous vulnerabilities. But this does not mean that passwords are insecure authentication factors that should not be used at all. They can be used in combination with alternative authentication mechanisms (presented here below), in multi-factor implementations, to improve the overall security of the authentication system.

##### 4.3.3.2 One-Time Password - Dynamic Passwords

A way to increase security of UID password based authentication mechanisms is to use passwords only once. This introduces the difficulty for both parties to agree on the next to be used password. Predefined lists of passwords can be provided to a User on paper or plastic card media for example.

If the user possesses a device that can perform simple computations, the security can be increased significantly by producing a new password for each transaction (**dynamic password**).

In this case, the authenticated party has a device that generates a new password for each transaction (this avoids the replay of the static password) and the verifier, at the other side of the transaction, has the equivalent device to compare local password generation with the received password. There are sometimes referred to as One-Time-Passwords (OTPs)

#### 4.3.4 *Challenge-response authentication schemes*

In most of the password based schemes the authenticating and verifying parties are sharing the same secret information. **Challenge-response** authentication schemes are even more secure. In this case, when a user tries to identify itself to a verifying system, the system generates a random challenge and sends it to the person or more exactly to his/her device. Such a specific device (e.g., a mini-calculator, a microprocessor) will then compute the corresponding response, using (unique) secret information which has been generated for this = device and which is linked to its owner. This response is then sent back to the system, which verifies if it matches the expected response based on a verification mechanism, verification information associated to the user and on the assurance the system gives on the link between this verification information and the user. The following cryptographic solutions may be used for this type of challenge-response authentication scheme.

##### 4.3.4.1 Authentication through symmetric cryptography

Such authentication schemes are based on sharing a secret key between the authenticating party and the verifier, i.e., in the context of payment schemes between the issuer authentication system and the user. The authenticating user demonstrates its knowledge or possession of a secret key by using a PIN or password to unlock the secret key to be used in the authentication process. The challenge sent by the verifier to the authenticating user is then encrypted with the secret key or more generally speaking is used in a cryptographic calculation that employs the secret key. The result is then sent to the verifying party. This party verifies the cryptographic calculation by using the same secret key and checks whether the resulting cleartext information links to the original challenge. When both data match the identity of the authenticating party is then corroborated.

##### 4.3.4.2 Authentication through asymmetric cryptography

Asymmetric or so-called public key cryptography allows to proof the possession of a secret without having to share this secret with the verifier. Indeed, in asymmetric cryptography the key used for the verification process, and which is associated to the secret (private) key, is public. Moreover authentication schemes based on asymmetric cryptography also provide non-repudiation. Indeed, if the user employs its (unique) secret key in a cryptographic calculation, it cannot deny afterwards to have made this calculation (e.g., a digital signature). This results from the fact that the link between the owner of the secret and the secret is non-ambiguous provided the scheme is correctly implemented and in particular the user is correctly registered.

The authenticating party has a key pair consisting of a private key known or possessed only by its owner and a mathematically related public key that is made public to the relying parties. Public keys are made available (published) through so-called digital certificates. These

certificates guarantee the unique link between the owner (of the private key) and its public key and are issued by a trusted party, called a Certification Authority (or Certification Service Provider). The system is generally referred to as a “public key infrastructure” (PKI).

When such asymmetric cryptographic techniques are used to implement challenge-response authentication mechanisms, the authenticating party can demonstrate knowledge or possession of its private key:

- Either by decrypting a challenge encrypted by the verifying party under the certified public key of the claimant party,
- Or by electronically signing a challenge whose resulting signature is then corroborated by the verifier using the public key certified as being associated to the claimed identity of the authenticating party..

Both implementations will require the verifier to validate the authenticating party’s certificate as well as the certificate (chain) of the Certification Authority(ies) having issued the user certificate and the CA certificates up to a trusted (Root) Certification Authority.

When a key pair has been “officially” allocated to (or generated by) a user, and the corresponding public key has been certified as linked to the user’s identity by the Certification Authority, then the verifier can be ensured that the person claiming to be the owner of the public key is REALLY that user.

#### 4.3.5 *Biometric systems*

During the last decade, new technologies have emerged that are enabling many industries and governmental services to confirm the identity of people conducting transactions. Biometrics is one such technology, recording and comparing a template of an individual’s unique physiological characteristics or behaviour to verify identity. Biometrics, when combined with smart card technology, could make payment transactions more secure for consumers, merchants and the payment industry that serve them. Consumers would appreciate the convenience of not having to carry multiple forms of ID to prove their identity, while merchants and the payment industry would welcome the reliable and cost-effective ways this technology may reduce unauthorized card use.

More recently, not only governments but also the payment industry started to evaluate authentication schemes that went beyond personal identification numbers (PINs) for establishing card holder validation. PIN-based networks, while highly successful, are sometimes compromised because the Card holder Verification Methodology or CVM (PIN/password) is transferred. Unwise consumer practices, such as writing PIN numbers on cards, choosing short PINs based on personal information or using the same PIN for multiple accounts, could also make an account vulnerable to unauthorized access.

Biometric systems are usually used in the context of a several-factor authentication scheme in case of card, e- or m- payments. Several types of biometric schemes can be used depending on the intrinsic reliability, security and user acceptance, amongst others:

- Face
- Eye
- Fingerprint
- Dynamic signature
- Behavioural (other than signature)
- etc.

#### 4.4 Data Authentication in the financial world

Although there is a European Directive on e-signatures providing a legal framework for certain types of e-signatures (the Qualified Signatures, based on PKI), most of the time electronic signature implementations are based on a implementation of the simplest form of electronic signature (see art.2 para.2 of the e-signature Directive). Often schemes where electronic or digital signatures are used are governed by contractual agreements providing a sufficient legal framework to operate them.

However, banks are more and more involved in the establishment of PKI systems. This happens in different application areas such as in the context of Intranet, corporate e-banking, e-banking, deploying EMV smart cards, or even when actively participating to the deployment of national eID schemes as in Sweden or in national PKI services as in Luxembourg.

#### 4.5 Linked security concepts

##### 4.5.1 Confidentiality

Data **Confidentiality** aims to protect data by making it unavailable to any unauthorised party. In order to provide confidentiality, it is necessary to transform the message in an appropriate “non-readable” form, this is called “encryption”.

Formal definition<sup>2</sup>: **Data Confidentiality** refers to the state of keeping the content of information secret from all entities but those authorised to have access to it.

**Data Confidentiality** deals with the protection against unauthorized disclosure of the protected data (e.g., message, transaction). If someone sends a message to a recipient, but a third (malicious) intercepts it, both authorised communicating parties want to make sure that this unauthorised third party never understands its contents. Confidentiality protection is very important in the payment sector. World-wide there are several billion transactions each day and all of these have to be passed from one financial institution to another. If there were no ways to protect confidentiality, everybody would be able to see who had purchased what, who has made what kind of withdrawal, and so on. Clearly this would violate individuals and companies privacy rights.

#### 4.5.2 *Privacy*

Privacy is the freedom of a natural person to sustain a “personal space”, free from interference by other entities. In the context of the study of user identification in card-, e-, or m-payments, privacy can be mostly used as a synonym of ‘informational privacy’, i.e., the interest of a natural person to control or at least to significantly influence the handling of data about itself, also taking into account the nature of the applicable attributes and the entity in charge of data management.

Formal definition<sup>2</sup>: **Privacy** is the right of an entity – in this context usually a natural person – to decide for itself when and on what terms its attributes should be revealed.

#### **4.6 *Legal and regulatory implication on authentication methods***

Preventive policies (see Directives [4, 7, 8]) against the use of financial systems for money laundering require from the covered institutions and persons which are subject to these Directives, to “know their customers”, and in particular to identify them. In general, this is done by having a face to face meeting with the customer, at least at the moment of the registration.

When non face to face operations are allowed, additional measures are required to be taken, in order to reduce risks:

- Additional documentary evidence or supplementary measures used to verify or certify supplied documents, or
- Confirmatory certification by an institution subject to these Directives, or
- A first payment carried out by an account opened in customer name with a credit institution subject to these Directives

The implementation of these measures revealed to suffer from the following issues:

- Difficulties of implementation due to the Data Protection legislation, making it complex and cumbersome;
- Reliance on third parties and their reluctance to provide identification information either for commercial reasons or data protection legislation compliance;
- Difficulties in obtaining specific information (e.g., information on identity and power of attorney of persons operating on behalf of legal persons).

Costs are also associated to the implementation of these additional measures, both for the customers subject to additional constraints and for the covered institutions in terms of procedures, training, controls, tools for detection, and appropriate systems.

The current regime based on a comprehensive risk-based approach, as recognised in the Anti-money laundering Directive, [8], allows the covered institutions and persons to implement more cost effective measures by determining the extent of the measures related to the customer due diligence procedures on a risk-sensitive basis, depending on the type of

customer, business relationship, product or transaction, still assuming that non-face to face situations would entail a higher risk.

In order to increase the efficiency and effectiveness of the system, customer due diligence procedures can be based on third parties acting as introducers, or first in the chain of the provision of services to the same customers, and on the possible reliance on the identification performed by them.

In respect of acquiring information from identity documents or other sources of identity information, electronic signatures can be considered to be particularly helpful in speeding up the process while ensuring the same (if not higher) level of security, provided they are appropriately implemented and taking into account anti-money laundering needs (e.g., the issuer of the supporting certificate has to identify the customer on a face to face basis).

**In particular, from the Anti-money laundering Directive [8] it can be observed that:**

- A face to face (F2F ) for user registration is highly recommended
- If there is no F2F, additional proof (of identity, ...) is required and/or should rely on a previous F2F (trust by transitivity).

**Besides the mentioned Directives, there are sectoral regulations and recommendations whose applicable rules have consequences on user authentication:**

The e-banking (world) recommendation, which are similar in Europe (see the reports from the Financial Action Task Force, Groupe d'action financière, [73]), and in the US according to Basel II and the US Federal Financial Institutions Examination Council guidance regarding internet banking, focusing on more effective modes of authentication, specifies that:

- Financial institutions offering internet-based products and services should use effective methods to authenticate the identity of customers using those products and services.
- Single-factor authentication methodologies may not provide sufficient protection for internet-based financial services.
- Single-factor authentication, when used as the only control mechanism, is NOT consider to be adequate for high-risk transactions involving access to customer information or the movement of funds to other parties.
- Risk assessments should provide the basis for determining an effective authentication strategy according to the risks associated with the various products and services available to on line customers.
- Customer awareness and education should continue to be emphasized because they are effective deterrents to the on line theft of assets and sensitive information.

Financial institutions should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their internet-based financial services.

The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are

frequently the result of single factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of single factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

These elements are considered when assessing user authentication methods.

#### 4.7 Authentication methods lifecycle

Authentication methods are not restricted to this widely known distinction (or combination) between *what the user knows*, *possesses* or *is*. Any authentication method and in particular its efficiency and security will be dependent on its full life-cycle that can be divided into three steps:

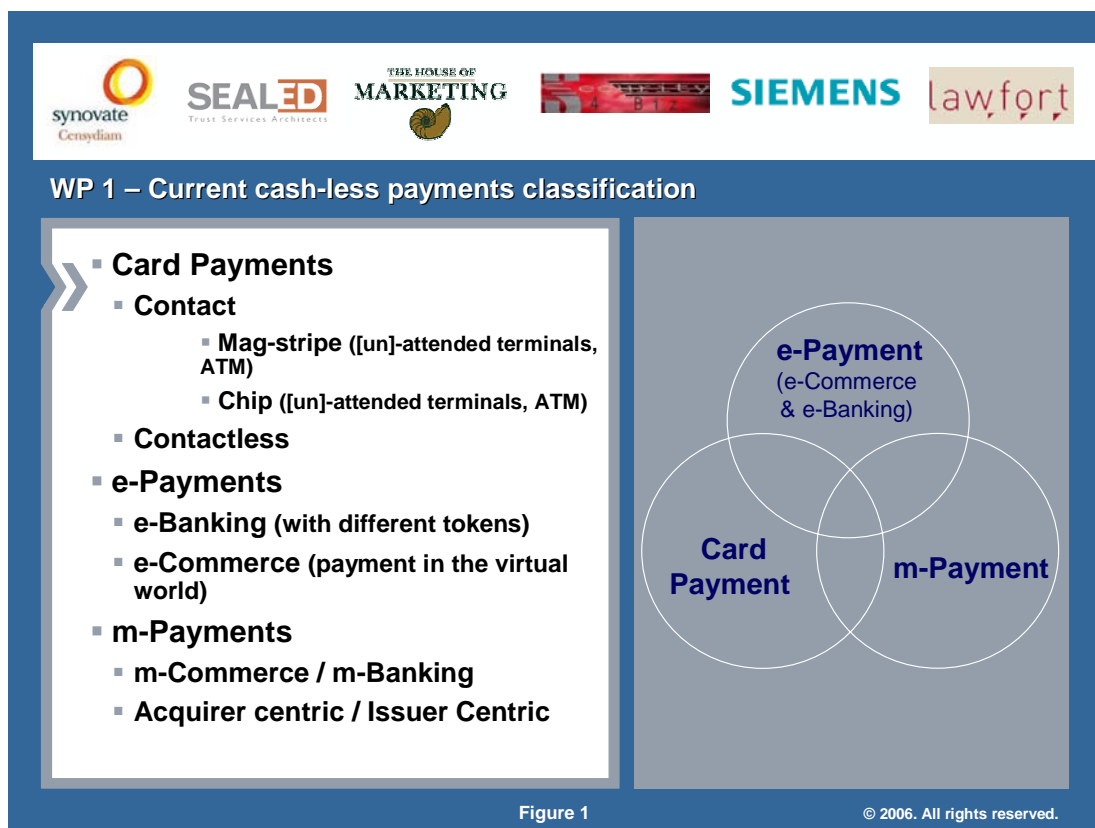
- **Initiation:** this step is covering the registration of the identified user and the delivery of authentication credentials. It is easy to understand that this step is even more critical than the use and security level of the provided credential since any failure in this step may jeopardize the entire authentication method.
- **Usage:** this step is related to the use and correct implementation of the authentication techniques based one or more authentication factors widely known as *what the user knows*, *possesses* and/or *is*. The security level of the authentication method will certainly depend on the nature of the used factor(s), their possible combination, and their correct implementation.
- **Termination:** the termination step is certainly part of and to be considered as fully defining an authentication method. Failure in properly terminating the life-cycle of user authentication credentials may jeopardize the entire authentication method.

When dealing with authentication, the lifecycle of ALL credentials (password, devices, ..) must be managed correctly, from the design to the termination of the user account, to avoid large scale attacks. The methodology used in this study to evaluate authentication methods will consider the full lifecycle of the related credentials (see Annex 6).

## 5. Analysis of the current and prospective card holder/user verification/authentication methods

### 5.1 Introduction

The card-, e-, and m-payments for which the user identification / verification method are being analysed during this study have been classified in the following categories:



To score an authentication method in the context of the present study, not only the security of this authentication method is considered, but also its *user perception*, that is amongst other topics, the user friendliness of the authentication method, the level of confidence the user in the method, etc.

Annex 1 defines a metrics to score every authentication method that is applied in the specific context of the card-, e-, or m-payments that are analysed in the present study. The scoring matrix first takes into account the nature of the authentication method and each life-cycle step (initiation, usage, and termination). Authentication methods are then analysed on their resistance against risks and frauds. Finally, they are assessed against their user perception.

In the analyses of the authentication methods, diverse criteria are considered:

- legal and regulatory compliances
- security aspects related to the different stakeholders:
  - o Issuers:
    - *Non-repudiation*: Issuers do not want the end-users to repudiate a transaction he/she has effectively conducted. This will be supported by *secure standards and interoperable* solutions.
    - *Reduced chargebacks*: Issuers want as few chargebacks and associated costs as possible.
    - *Minimal investments & ease of implementation*.
  - o Merchants and Acquirers need to avoid:
    - Transacting with end-users that are using stolen or fake payment data, which will eventually lead to repudiation of the payment data by the legitimate owner or end-users denying having ordered a particular purchase that has been correctly performed.
    - Loss of confidentiality (of transaction details to competitors, leading to loss of competitiveness or of consumer transaction details, leading to breach of regulatory conditions governing consumer privacy)
    - Loss of reputation (and hence volume of business) through breaches to server security.
  - o End-users
 

They want solutions that are easy to use and that require neither tedious installations nor extra costs and that allows them mobility (they would like to be able to make payments at different locations (e.g. when travelling) and to use different internet-enabled devices (such as Personal Computers (PCs), Personal Digital Assistants (PDAs) or mobile phones). Hence, mobility and device independence of the payment instrument should be supported as well as multiple devices.

Today, it is the merchant side of the business that bears the cost of fraudulent transactions. But the risk for merchants is also that their investment in the implementation of a solution does not bring the expected revenue, especially if the solution is not adopted by end-users. On the other hand, if they wait before investing, end-users will also wait before using the solution; the typical chicken-and-egg problem.

## **5.2 Card payments**

### **5.2.1 Introduction**

In the mid seventies magstripe financial transaction cards have been introduced on a worldwide basis. Where in the first years after the only handwritten signatures were used as card holder verification method, more in particular for credit cards, later on PINs were introduced as user verification method for financial transactions, mainly for debit transactions. But one of the main cause for fraudulent transactions were the counterfeit cards, despite the efforts by the e-banking industry which raised the barriers year after year with the introduction of additional (visual) technologies such as card embossing and holograms. It is only in the mid eighties with the introduction of chip card technology that a major step forward was taken with respect of the genuity of the financial transaction card. Still nowadays the PIN remains “the method” used for user verification for chip card based banking applications such as debit, credit and purse.

In this section the payments where cards are used at ATMs and POS terminals (attended or not) are considered. These are the so-called “card present” transactions whereby the card holder physically needs to insert the (contact) card in the payment terminal to perform a transaction.

Financial transaction cards fully adhere to international standards to ensure interoperability. ISO/IEC 7810 is one of a series of standards describing the characteristics of identification cards. It aims to provide criteria to which cards shall perform and to specify the requirements for such cards used for international interchange. It takes into consideration both human and machine aspects and states minimum requirements. Together with the multipart standards ISO/IEC 7816 on Integrated Circuit Cards it provides the technical basis for the today’s banking cards.

### **5.2.2 Security challenges**

Cards are mostly used in banking applications as a means for two factor authentication in combination with the usage of a PIN. The main security challenges with respect to this two-factor authentication are:

- The protection of the PIN in all its stages of its life cycle (generation, storage, transfer, etc...). Since in most stages in storage and transfer the PIN is encrypted using cryptographic technology the weakest place is really the user who should (personally) store the PIN separately from the card and should be extremely cautious when entering a PIN at a terminal.
- The genuity of the card. While counterfeit cards were a major problem with the magstrip technology (card cloning), the introduction of chip cards allows for an off-line (dynamic) authentication of the card by the card accepting device (terminal), generally based on PKI technology for interoperability reasons or for an on line verification by the back-end server, generally based on symmetric crypto technology.

### 5.2.3 *Selection, assessment and analysis for the most used card payments*

#### **5.2.3.1 Magnetic stripe cards**

Traditional credit and debit payment cards carry a magnetic stripe, a hologram, a specimen signature of the card holder, and one or more payment brands, and they may be embossed with the card holder's name, their account number and the expiry date of the card. Magnetic stripe technology provides little in the way of card authentication. Point-of-Sale terminals cannot authenticate magnetic stripe cards and, even if sent "on line" for authorization by the card issuer, because of the static nature of the magnetic stripe, the issuer is not able to distinguish card data originating from a genuine card from replayed card data or card data read from a copied (cloned) card.

With magnetic stripe credit cards mostly a handwritten signature is used as user verification which clearly offers very limited assurance about the genuity of the card holder.

With magnetic strip debit cards mostly on line PIN verification by the Issuer is used. ISO/IEC 7813 specifies the data structure and data content of magnetic tracks 1 and 2, which are used to initiate financial transactions. The PIN entry, transmission and verification follow the process as described in Annex 6. Hereby the PIN entered by the user is encrypted in a secure PIN pad for its protected transmission to the Issuer.

#### **5.2.3.2 Chip or IC cards**

##### **EMV debit and credit**

With the advent of chip cards, card authentication can be performed by the terminal or issuer using dynamic techniques that distinguish genuine cards from clones. Both the card and terminal implement offline risk management processes that control whether a transaction is approved or declined offline, or whether on line authorization should be sought.

European banks migrated during the last years to the EMV standard for debit and credit chip transactions. EMV defines different mechanisms for chip card authentication. In the so-called on line authentication method (on line CAM) the authentication of the payment card and transaction is done through an on line communication to the card issuer during the transaction while the off-line authentication method (off-line CAM) enables the payment terminal to authenticate the card without this on line communication. A description of these card authentication methods is provided in Annex 7 (see Annexes document).

With respect to the card holder verification method (CVM), the introduction of chip cards allows Issuers to choose whether their cards support on line PIN and/or offline PIN verification. With on line PIN the PIN entered by the card holder is encrypted and sent over the network to the issuer for verification in the usual way (as per magnetic stripe). With offline PIN verification the PIN entered by the card holder is sent from the PIN pad to the card for verification. In order to perform offline PIN verification the card must securely store a reference copy of the card holder's PIN.

EMV specifies two methods for offline PIN verification: plaintext and enciphered.

- With offline plaintext PIN verification the card receives the PIN in clear from the terminal.
- For offline enciphered PIN verification the card must be an RSA-capable card. The card will receive the PIN encrypted under a card public key and using a randomized RSA encryption method specified in EMV. The card will decrypt the PIN using its corresponding private RSA key.

For simple lost and stolen cards the use of offline PIN verification will vastly reduce fraud as compared to the use of handwritten signatures.

In addition to the PIN verification and the card authentication chip cards allow for an additional increase in security through the usage of risk management. Indeed, the decision for off-line or on line authorization for a given chip card transaction is based on the outcome of the card and terminal risk management, consisting of

- Floor limit checking. Merchant terminals contain a floor limit value. If the transaction value exceeds this number then the terminal should request on line authorization.
- Random transaction selection by the terminal, ensuring that transactions go on line periodically.
- Velocity Checking, where the terminal can choose to go-on line depending on card risk management aiming to limit the number of consecutive offline transactions performed by the card.

Moreover chip card technology allows the issuer to block or unblock the card, change the PIN and some of the card risk management parameters using issuer to card script processing. These scripts are protected using symmetric cryptography ensuring integrity and/or confidentiality as appropriate.

### **Purses**

The European Committee for Banking Standards (ECBS) started work on electronic purse standardisation in September 1997, uniting experts from all purse schemes in Europe and developed the EBS 111 standard on the European Electronic Purse. Subsequently, based on the results of the work of ECBS, major European card schemes completed the Common Electronic Purse Specifications (CEPS), an implementation specification on which an interoperable electronic purse product could be built.

However, as of today, most of the European countries have implemented their own (proprietary) purse scheme which does not offer interoperability abroad. Typically most of the schemes are not CEPS based. Most of the purse schemes execute mutual authentication of chip card and payment terminal. (based on a Secure Authentication Module-SAM in the terminal).

In the purse schemes, an ordinary POS transaction does not require the presentation of a card holder verification method i.e. a PIN. All schemes however require the entry of the PIN for the (cashless) load of the purse at an ATM or other load device. This PIN is then typically handled as described in Annex 6 for an ATM transaction.

### 5.2.3.3 Best method

The best user authentication/verification method for card present based transactions relies on the provision of the PIN code at transaction time. For credit cards in particular, this is far more secure than relying on the provision of the card holder signature (additionally to the card information capture). Whereas the mag-stripe cards with an on line verification of the PIN only offered limited security due to the possibility of counterfeit cards (using skimming attacks), the migration to chip cards considerably increased the security. Indeed the usage of IC Card technology allows the dynamic authentication of the card at transaction time. This is, in combination with the card holder verification by means of a PIN, the best card holder authentication/verification method available today for card payments.

The combination of the usage of IC Card technology allowing the dynamic authentication of the card at transaction time and the provision of the card holder PIN code (2-factor authentication) is the best card holder authentication/verification method available today for card payments.

The adoption of IC card authentication in combination with a PIN as user verification method will also be followed by the SEPA Cards Framework (SCF) for implementation in the European member countries. This framework will define a set of minimum requirements, including security, which allow for functional interoperability of elements of the processing chain for the different SCF compliant schemes (global or national, alliances and any new schemes). These minimum requirements will be based on the EMV specifications and adopt PKI-based authentication of the cards (static or dynamic). Furthermore three types of PIN verification methods will be specified:

- on line PIN verification by the Issuer based on symmetric crypto,
- off-line cleartext PIN verification by the card,
- off-line encrypted PIN verification by the card based on asymmetric crypto.

With this framework at least a harmonisation of a minimum security level for card based transactions will be realised.

**Evaluation summary**

	<b>Initiation</b>	<b>Usage</b>	<b>Termination</b>	<b>Risk &amp; Fraud resistance</b>	<b>User perception</b>
<b>Magstripe &amp; handwritten signature</b>	Registration - card holder identification by bank: ++	2-factor authentication: -	Card stop 24/7 help desk to block the card	Risk of counterfeit cards because of skimming: --	Ease of use: ++ Trust: -
<b>Magstripe card &amp; PIN</b>	Registration - card holder identification by bank: ++	2-factor authentication: -	Card stop 24/7 help desk to block the card	Risk of counterfeit cards because of skimming: -	Ease of use: ++ Trust: +
<b>Chip card &amp; PIN</b>	Registration - card holder identification by bank: ++	2-factor authentication Static card authentication & PIN: + Dynamic card authentication & PIN: ++	Card stop 24/7 help desk to block the card	++	Ease of use: ++ Trust: ++

**5.2.4 Facts and figures**

The migration to EMV cards for financial transactions is now well underway in the 27 European member countries. In Q2 2007 approximately 58% of the payment cards, 66% of ATMs and 51% of POS terminals have been converted to EMV<sup>5</sup>. A full migration in time for SEPA is envisaged for 2010 although there remain significant country differences.

With the introduction to EMV cards, the fraud is moving to card not present payments, although it is hard to get access to exact statistics. Furthermore, for acceptance reasons in view of the mobility of card holders travelling abroad, magstripe technology is maintained in parallel to EMV chip cards on the so-called hybrid cards. This lowers the global security level and quite often fraud is directly linked to this.

<sup>5</sup> Figures provided at the 2<sup>nd</sup> Cards Standardisation Workshop of EPC, September 27<sup>th</sup> 2007.

### 5.2.5 Possible barriers to the implementation

The main barriers for implementation are the following:

- investment costs for issuers, acquirers and retailers;
- market size and business revenue for the vendors and suppliers.

However, a number of factors can be identified towards overcoming these main barriers:

For the banks and retailers:

- The decision for migration in Europe to the EMV specification by the global card schemes such as Mastercard and Visa (with fixed deadlines) with the associated liability shift to non-chip parties;
- The migration of fraud to “less secure” countries has put pressure on issuers and acquirers in those countries.

For the vendors and suppliers:

- The harmonisation of specifications and the guarantee of interoperability;
- The harmonisation of the security certification processes for cards (CAS-Common Approval Scheme) and PIN peds (PCI-PED) and mutual recognition (e.g., by global and national schemes)
- The increasing market size for EMV products, even more in the near future with the EPC SEPA Cards Framework.

However, a number of related problems remain:

- Who will be the “ultimate” recognized certification body in Europe for card and PIN ped approvals
- Who will be responsible for accrediting the appropriate certification laboratories
- How will the minimum (security) requirements be enforced.

## 5.3 e-Payments

### 5.3.1 Foreword and structure

Conform to the structure required by the European Commission, this section deals with user identification/verification methods for e-payments occurring via PC, laptop, or other internet enabled devices.

Basically e-payments dealt in this section can be classified into two main areas: e-banking (i.e. transferring money through an **e-banking** application) and e-commerce (i.e. paying on an **e-commerce** website (e.g., with a credit card))<sup>6</sup>.

---

<sup>6</sup> Note that 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 a merchant’s site (see also E-commerce section of this chapter). 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

Whereas e-banking are payment services that rely on a bank account and use the internet as a means of moving funds to or from a bank account, e-payments methods are used for payments of goods (material or immaterial (software, access to content,...) in the on line world. E-payment methods for e-commerce are based on payment services that are mostly provided by non-bank institutions and are only indirectly associated with a bank account.

It is noticeable that e-banking and e-commerce are however closely linked, e-banking being a major tool to perform e-commerce transactions. However, the e-banking framework differs from the e-commerce framework as follows.

- The business model is rather simpler in e-banking than in e-commerce. Indeed, the principals in e-commerce may include both the banks and their customers as is the case in e-banking, but in addition also the customer – merchant relationship. Moreover, e-commerce deals with goods and services and some additional risks regarding the possible non-delivery of goods to the customer and/or the possible non-payment to the merchant.
- E-banking is ruled by contractual relationships between a customer and his/her bank. The contractual relationships themselves are regulated under a legal framework (in particular related to this study, the 2005/60/EC Directive) and fall within banking associations guidelines (see further in this document). On the side of e-commerce, regulation is less stringent and some transactions occur without any contractual framework.

The next clauses identify e-banking and e-commerce payment methods giving a brief description of the method and a presentation of the user identification/verification method.

### 5.3.2 *E-payments security challenges*

Although the on line world, thanks to the dematerialisation of many processes, allows users, banks and merchants to handle a larger number of transactions more quickly in a more cost-effective way, the remote nature of these transactions and the inherent lack of human involvement in these transactions is also a cause of concern from a security perspective.

In the physical world, when a card holder wants to pay with his/her debit or credit card at a store, the parties rely upon a number of mechanisms to build security and trust, including the physical presence at the store of the goods that can be seen and touched. In particular, regarding authentication purposes, the card holder payment card, besides its payment means function, provides a quite trusted way of authentication. The merchant can not only check the physical authentication characteristics of the card (such as the embossing, hologram, brand and signature panel) but he can also compare the signature provided by the card holder with the one on the back of the card. Some merchants even require the card holder's passport/identity card to ensure that the card holder is the genuine owner of the card and also

---

bank transfer systems may very well be one and the same application (such as with Nordea Solo). Especially from the user authentication perspective, we refer the reader to the E-banking sections.

cross-check the authenticity of the signature. Following this authentication process the payment is made.

In the on line world however, there is no possibility of using the physical characteristics of a card as in the physical world. Moreover, payment instructions containing account information are generally transmitted from card holders to merchants on public (and unprotected) networks such as the internet or mobile networks that are no longer entirely controlled by the banks, as it is the case in the physical world. Without further securing, data can be copied on a large scale and reused in other transactions.

Therefore, in order to maintain an acceptable level of security and trust for transactions in the on line world, it is necessary not only to replace the traditional face-to-face mechanisms by new digital ones, but also to rely on ad-hoc tools to manage the specific risks of e-commerce.

### 5.3.3 *E-banking*

#### 5.3.3.1 Introduction

As identified along the conduction of this study, electronic banking is a key distribution channel for financial services. A growing number of private and public bodies are establishing technologies, techniques, standards and policies for the delivery of electronic banking.

E-banking relates to payment services that rely on a bank account and use the internet as a means of moving funds to or from a bank account. internet is the major banking channel but other channels do exist as well, some of them being themselves internet Provider channels: call centres, iDTV and mobile banking (see 5.4). Electronic banking is thus the provision of *banking services* by a *bank* to a *customer* supposed to *have a bank account* and *using a customer device* (e.g. PC, WebTV, PDA, mobile phone) *connected to a network*.

#### 5.3.3.2 Electronic banking security challenges

As explained in the beginning of this WP1, doing e-business via a public network introduces new challenges for security and trustworthiness. It is necessary to protect customer information, in order to comply with requirements to prevent money laundering and terrorist financing, to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

Basically, any internet based banking system must ensure that:

- only authorised people can access an internet banking account,
  - o the information viewed remains private,
  - o the information viewed cannot be modified by third parties,
- any transactions made are traceable and verifiable.

This means financial institutions must solve the issues of authentication, confidentiality, integrity, and non-repudiation. On the side of the end-users in particular, it is necessary to have a certain level of guarantee that:

- they really work on an e-account dully linked to their bank,
- they do not have their privacy violated,
- their personal financial information is not re-used for another purpose.

It is important to keep in mind that e-banking transactions rely in general on a 2-steps user verification;

1. **Login:** this is the step where the end-user enters his/her personal account section within the bank portal (and potentially authenticate his bank).
2. **Transaction confirmation:** this is the step where the user “signs” the transaction. It can be done via the same authentication means as for the login step, or it can rely on another credential.

### 5.3.3.3 Security building blocks underlying e-banking schemes

The e-banking methods rely on a variety of technologies and methodologies that financial institutions can use to authenticate customers. These methods include and combine the use of diverse tools as presented in Annex 6 such as customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of tokens, transaction profile scripts and biometric identifications. Clearly the level of risk protection offered by each of these techniques varies. Obviously, the selection and the use of the authentication technologies and methods should depend upon the results of risk assessment processes conducted by the financial institutions.

As already mentioned earlier in this study, authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/ password is a typical single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication method may also include “out-of-band” controls for risk mitigation. “Out-of-band” generally refers to additional steps or actions taken beyond the technology boundaries of a typical transaction. Call-back [voice] verification, e-mail approval or notification, and cell-phone based challenge/ response processes are some examples.

Before analysing authentication schemes, the e-banking authentication methods most used are summarised here below. More detail may be found in Annex 6.

## **SSL/TLS**

The scope of the SSL/TLS protocols is to secure the transfer of any data between two entities, generally between a browser and a server (providing thus a client-server secured channel). SSL/TLS allows for data encryption during the communication, as well as for mutual authentication of the principals. Mutual authentication is not mandatory and in a lot of cases, only the server is authenticated by the client. In the current context, this enables the customer to authenticate his/her bank by checking the url he/she is connected to, dully belongs to the bank. In general, the customer is authenticated by the bank by other means (e.g., a card).

Hence, SSL/TLS covers the following security requirements:

- authentication of the bank towards the end-users
- (in some cases) authentication of the end-users towards the bank
- confidentiality of data exchanged.

Although some care must be taken in order to avoid phishing and web spoofing attacks (see Annex 8), SSL remains a basic building block for securing e-banking transactions. Even though SSL/TLS on its own lacks some of the required security features, when associated with one of the next payments techniques below, it brings at least some level of security for e-banking.

## **Passwords and OTP in e-banking solutions**

E-banking applications extensively use passwords. Passwords mainly support user authentication (see Annex 6), and by extension, can be used to confirm a transaction (although the fact that this confirmation does not constitute a signature in the sense of the EU directive on e-signature since the signature and the signed data are not bound).

Annex 6 shows that using static passwords alone is definitely not a secure solution (this is less and less used as main authentication means). Typical solutions on the market make use of a (static) “password” in combination with additional security feature (e.g., the password authorised session is generally SSL encrypted).

Static passwords are generally combined with (or replaced by) one-time passwords (OTP), also called dynamic passwords or short time passwords, used once and for a particular transaction, hereby preventing replay of the transactions.

The OTPs are used in one-way processes or in so-called “challenge-response” processes. Typically, a challenge or instruction is provided by the bank web site and the customer needs to perform an action on this request (e.g., sign a random with his/her card, select a number on the TAN cards, etc ...).

In all cases, in order to use his/her web banking account, the user has to prove that he/she knows something (e.g., his/herpassword) and that (s)he is in possession of something (e.g.,his/her card, phone or token). This process fits thus well in two-factor authentication methods.

The process can be achieved in one or two steps:

- 2 step process:
  - (i) the user logs on with a user ID / password proving he/she knows the password
  - (ii) the user provides the OTP
- 1 step process: the user provides the OTP itself after the user has unlocked the OTP using a PIN code (user authentication toward OTP token required).

The OTPs for e-banking are provided by means of something the user has (as opposed to something the users knows such as the static password).

The dynamic password can be provided by diverse means basically falling into one of the following categories:

- OTP list or token received in advance by the user (e.g., printed on a card),
- OTP generated on a need-to-know basis and communicated at the moment of the transaction (e.g., via the use of a mobile phone; communication of the OTP from the bank authentication server towards the user via SMS).
- OTP generated on a need-to-know basis at the moment of the transaction (e.g., generated by a token). Using that kind of OTP (sometimes also called short-time password) from an offline hardware tokens (e.g., a card-reader) combined with a (EMV) card can be considered as a subcase of the one mentioned above. However, this case is sufficiently important in e-banking that it deserves dedicated focus. The last category of OTP can even be split into two ways of working;
  - o Card-reader not connected to the PC (in this case, symmetric cryptography is often used to generate the OTP, which is actually the “signature” of a random number proposed by the bank via the logon page);
  - o Card-reader connected to the PC (in this case, asymmetric cryptography (PKI) is often used to generate the OTP, which is actually the signature of a random number proposed by the bank via the logon page). When PKI is used, beyond end-user authentication towards the bank, the card can also be used to sign transactions (in the sense that the signature is linked to the data and can be archived as such). One can imagine systems where the signature is performed by a non-connected reader, but this would impose the user to enter manually long data string without errors and this is not feasible from a user friendliness perspective.

Examples and more details on OTP generation modes are provided in Annex 6.

The following factors must be taken into consideration when studying an OTP based solution:

- Mobility: OTP tokens and plastic cards such as a smart-cards or bank-cards are easy to be carried. This is significantly less true when they need to be employed in combination with a dedicated reader. A mobile phone is a particular case where the reader, the card (SIM) and the network are all together present ... and mobile.
- Complex devices can break more easily or stop functioning. Battery-life normally is sufficient for the expected life-time of these tokens (3-4 years).
- Hardware protection: OTP-devices have tamper-detection and tamper-prevention technology on-board to avoid compromise / copy of sensitive keys inside. This is not true for OTP-cards: when not under control of their users (in their wallet), they can be copied easily (manually or on a copier).

One can see that EMV cards can be used to issue passwords in an authentication scheme. EMV allows much more than password issuance. Let us thus briefly describe the EMV authentication protocol, since many schemes highlighted in this document rely on it (more details may be found in Annexes 6 and 8).

### **EMV**

EMV smart card authentication is a two-factor based authentication scheme. In addition, a user can at the same time:

- Be authenticated to a particular application by a one-time passcode; and
- Provide on line transaction authentication in the form of an electronic signature.

EMV authentication can be used in a variety of different applications, the most common being on line banking applications. It can also be used in any situation that requires user identification to a requested service or authentication of on line transactions, i.e. e-commerce in general.

EMV authentication uses a combination of the end users standard EMV card with an (un)connected terminal capable of reading smart cards:

With unconnected devices, EMV symmetric keys are used to ensure card authentication (proof of the possession of the card during a transaction by signature of a challenge):

1. The smart card is inserted into the EMV card reader
2. The user is prompted to enter its 4-digit PIN number
3. The reader then presents the user with a one-time passcode which can be used to authenticate itself towards the required service; or
4. For authentication of an on line payment transaction, the user is presented with a numeric challenge on the webpage which it enters onto the EMV card reader. The card then produces an electronic signature from this challenge which is displayed on the reader. The user enters this signature onto the same webpage and submits the transaction. The signature can then be verified by the system ensuring strong authentication of the transaction and the card holder.

As the passcode or signature generated is different every time, card identities, passwords or electronic signatures cannot be compromised through phishing, skimming or other fraud attempts.

User authentication can be used for a range of on line or offline access channels (e.g., the internet, mobile phone, digital TV etc.) giving users a single, simple means to authenticate themselves. Electronic signatures can be used as a strong authentication method during an on line payment transaction, across a variety of channels (such as internet and telephone banking and on line shopping).

With connected devices, EMV PKI features can be used in order to issue digital signatures with a data authentication purpose (this proves not only the possession of the card, but also the origin and integrity of the data since the signature can now be bound to the data to be signed).

**5.3.3.4** User verification methods in e-banking schemes analysis

According to the way the banks combine and use the here above presented building blocks, different levels of security can be achieved. One can quasi identify a specific e-banking method per banks; it is not the scope of this study to establish the exhaustive list of e-banking methods.

In the e-banking schemes review, simple (and considered as not secured) authentication methods are left out and the study starts from the fact that a user/ID password connection will always occur under a secure (such as SSL/TLS) connection enabling the authentication of the bank server towards the customer browsers and providing confidentiality to the transferred data. Moreover, only methods whereby the security level conforms to the sectoral regulations presented in the introduction of the present document (i.e. at least based on two factor authentication) are considered

Let us remind that e-banking transactions rely in general on a 2-step user verification;

1. **Login:** this is the step where the end-user enters its personal account section within the bank portal (and potentially authenticates his bank). The customer generally provides his/her user identification (userID) and uses a password to log onto the system and access his/her personal web banking environment.
2. **Transaction confirmation:** Whenever a transaction needs to be performed, this is the step where the user “signs” the transaction. It can be done via the same authentication means as for the login step, or it can rely on another credential; e.g., the user is requested to re-introduce his/her password (or a second different password) to confirm the transaction.

**Methods description**

Different methods are possible according to the type of password, with increasing level of security generally going hand in hand with higher costs for the bank and, in some cases, less user friendliness (see also Annex 6):

	User logon	Transaction confirmation
1	Static password	Static password (same as from login)
2	Static password	Static password (different as from login)
3	Static password	OTP
4	Static password	Digital Signature of the transaction
5	Static password	PKI Digital Signature of the transaction in the sense of the EU directive
6	OTP	OTP (generally different)
7	OTP	Digital Signature of the transaction
8	OTP	PKI Digital Signature of the

		transaction in the sense of the EU directive
--	--	--

It is important to note that OTP can be generated in various ways, ranging from:

1. OTP based on printed card (TAN),
2. OTP based on mobile phone connection,
3. OTP generated by a token (e.g., VASCO),
4. OTP generated by an EMV card challenge with a symmetric crypto based signature,
5. EMV PKI signature.

Except for the printed card (TAN) all devices described above are generally PIN protected and rely on the use of cryptography.

As specified in the WP1 methodology (Annex 1), the methods are compared in their entirety and their complete lifecycle. Also aspects such as user friendliness, risk and fraud resistance are analysed.

**Initialisation**

The initialisation evaluation strongly depends on the way the bank registers the user and associate his/her credential.

In the foregoing it was already mentioned that it is useless to invest in very secure systems or credentials if the registration step is not correctly implemented. In this perspective, a PKI scheme with a bad registration procedure is less secure than a password based scheme with a good registration procedure.

If a face to face meeting is performed to enrol the user and to strongly associate the user to the password or the credential, the registration system can be considered as very secure. When there is no such a face to face, the bank must follow the “additional” requirements such as prescribed by the 2005/06/EC Directive (e.g. document proving the user identity for his/her enrolment) or rely on an authentic channel where data origin can be authenticated as coming from the genuine user thanks to a previous face to face used for the secure channel establishment. In general, the previous face to face is the user’s first registration to the bank (when he/she created the account). In this way, the exact identity and postal address of the user is established and the PIN letters and/or tokens and/or cards may be sent to his/her address with a high level of guarantee that the correct person will receive the token.

From a risk analysis perspective, the bank shall check whether identity theft is possible and how it is prevented. For all cases, if this step is not dully performed with the necessary care, the security is belittled to zero. This is NOT a TECHNOLOGICAL matter, but a matter of policy and procedures. However for the specific cases:

- SIM card authentication: where the communication of the OTP from the bank authentication server towards the user is performed via SMS, an additional security in the registration process is due to the fact that another TTP actor (the mobile provider)

has already enrolled the user (however, this is only valid for subscribing customers, not with pre-paid card users).

- EMV card authentication: the registration step is in fact the card registration step, which is generally highly secured.

## Usage

### *Login authentication:*

- Static password: The use of static passwords, even when a second password is used for transaction confirmation, cannot be seen as a second authentication factor. This case is quite unsecure, unless SSL/TLS protected.
- For all other password based authentication methods, the strength of the password depends on the token:
  - Crypto-based authentication OTPs are the stronger authentication tools than non-crypto based ones.
  - A security advantage of the mobile approach can be seen in the use of two different channels which can be assumed to be present in almost of the cases. This means to stage a successful attack, an attacker must be able to either compromise both channels (seems almost impossible), or to stage a MITM attack on the internet-channel (this can be detected). The residual risk is identical to other OTP-solutions. However there are associated costs:
    - SMS Gateway to be coupled with the bank authentication server. These costs are similar to the cost relating to TAN cards management,
    - Costs from the cellular phone network operators. The main cost difference is likely to come from the per-use model versus one-time costs.
  - EMV: The strength of the password depends on the symmetric crypto functions on board of the card. They can be considered as highly secure. Challenge-response tokens are 'two-factor authentication' tokens, meaning that an attacker needs both the PIN and the token (as well as an appropriate card reader) to succeed in masquerading the card holder. This enhances the security of card holder's authentication.

### *Transaction authentication:*

- For all non PKI signatures, in case of litigation on the correct association of the password with the customer, the non-repudiation effect will depend on the strength of the token, and essentially on the quality of registration (initialisation) procedures.
- A PKI digital signature would be the ideal way of working, but this solution calls for PKI and this requires a connected device for doing so (see Annex 6). Indeed PKI is the only tool that allows for true non-repudiation. An even better method would be the issuance of a Qualified signature in the sense of the EU directive on electronic signature (with same legal value as a handwritten signature).

## Termination

The bank shall take care to close the account when the user left the bank or decided not to use the service anymore. This is to prevent that a user which is no more a customer still gets

access to the bank resource via his/her web banking application by simply trying to log on with his/her user ID password. In particular:

- PKI based schemes: as with any PKI system, suspension, revocation and certificate validity status services needs to be put in place.
- EMV: termination is linked to card termination (end of validity and/or revocation).

### **Risk and fraud resistance**

Static password based schemes:

1. Procedures from the banks shall allow (oblige) the user to frequently change the password and shall impose a minimal length for the password , including special characters in order to be resistant to dictionary attacks;
2. Specific measures need to be implemented to avoid that the confirmation password is the same as the login password.

Other schemes, in particular based on crypto tokens: cryptogram should include data that prevent replay attacks (e.g., as is the case for EMV cards).

### **User friendliness**

- Static password based schemes: These systems are rather simple to use. In a lot of cases, the confirmation password is the same as the login password, making it very ease to remember for the end-user.
  - Example of such scheme is provided by Keytradebank.
- Mobile phone based schemes: a mobile phone seems a well-accepted interface for most users (SMS-messages). On the other hand, this method requires users to disclose their cellular phone number to their bank. However, some barriers have been pointed by WP2, due to the fact that people:
  - are not knowing how to make mobile payments and the technology behind the application,
  - do not have the necessary technology to make payments via the mobile,
  - do not trust the technology behind the application (although the level of trust is higher when the transaction is PIN protected).
- EMV: The main advantages of this authentication scheme are:
  - *Ease of use*: Card holders need only to remember a PIN to access their token, and only one.
  - *Portability*: The EMV card reader need not be connected to any device, permitting the Card holder to carry it with him/her and authenticate him/herself to any internet-enabled device.
  - *Reuse of Infrastructure*: The token is the actual debit/credit card used for the e-commerce transaction. When issuing EMV cards, the Issuer has already made investments in its infrastructure in order to validate the cryptographic processes involved in EMV transactions. This infrastructure can be used to validate the cryptogram generated in the authentication process. Additionally, the ordinary

distribution process for debit/credit cards is used to re-issue the token (the card).

However, this authentication scheme has also some drawbacks, including:

- *Costs*: The cost of distributing the card readers must be considered. Although the ordinary distribution method can be used to distribute the cards, the card reader has to be distributed to the card holders. This is a one-time cost since card renewal does not require re-distribution of the card reader. Redistribution of card readers is only required in the case of loss.
- *Lower mobility*: This scheme implies that Card holders must have the EMV card reader in their possession each time they want to authenticate themselves to a system. If the replacement costs are high and supported by card holders, they will fear to lose their card reader.
- PKI has been perceived as difficult to use for the end-user, but nowadays, many applications (such as browsers) have endorsed PKI and have really integrated its use, making it very easy (e.g., an example of such scheme is provided by ING). Also EMV cards in connected mode allow for PKI signatures.

### Evaluation summary

	<b>Initiation</b>	<b>Usage</b>	<b>Termination</b>	<b>Risk &amp; Fraud resistance</b>	<b>User perception</b>
<b>Static password</b>	depends on procedure	--	depends on procedure	--	Ease of use: ++ Trust: +
<b>OTP based on printed card (TAN)</b>	depends on procedure	-/+	depends on procedure	-/+	+
<b>OTP based on mobile</b>	depends on based on mobile: ++	++ (but costly for the banks)	depends on based on mobile: ++	++	++
<b>OTP based on token</b>	depends on procedure	++	depends on procedure	++	++
<b>OTP based on EMV</b>	Based on card registration: ++	++	Based on card registration: ++	++	+ (*)
<b>PKI (signature)</b>	depends on procedure  When EMV, based on card	+++ (**)	depends on procedure  When EMV, based on card	+++	+ (***)

	registration: ++		registration: ++		
--	---------------------	--	---------------------	--	--

*(\*) considered as less convenient than some other tokens because of the mobility constraint.*

*(\*\*) The superiority on the rest is mainly due to the “transaction signature” step which is far stronger with a PKI based signature, since it has more strength in case of litigation thanks to its legal value and non-repudiation characteristics.*

*(\*\*\*) considered as less convenient because of the mobility constraint (needs a connected device).*

By comparing the different methods scored here above, one can easily see that solutions based on EMV for the logon and the transaction signature appear to be very good user friendliness – cost efficiency – security compromise. When used in PKI mode for transaction signature, the highest level of security is reached, but this requires a connected reader. In all cases, the same credential is used for the user logon and the transaction signature, while offering a high level of security.

One can observe that more and more banks opt for the EMV solution, “offering” the reader to their customer. Business case seems to be profitable; the gain in security and convenience being sufficiently valuable and balancing the costs.

In some cases, the user needs specific software to connect to the bank. This reduces the mobility of the user (the software being installed on his/her personal PC), but enhances the security of the bank by avoiding that user that do not have the software connects to its resources. It also protects the user from man-in-the middle attacks (see Annex 8, section SSL). The user is impacted at registration, as he/she has to download a program (e.g., a thin applet) to his/her internet-enabled access device. Although the presence of the programme on the end-user PC is often regarded as a drawback of the solution, it is important to note that this end-user application is mostly automatically activated, and it is transparent for the end-user.

Having this feature slightly affects the here above scored methods, expect in the “usage” assessment since it really reinforce the security of the e-banking transactions.

- **Initialisation**  
User needs to install the application (from the bank web-site or from a CD rom provided by the bank).
- **Usage**  
Once the application is installed, all operations occur transparent.
- **Termination**  
Whether the user keeps the application or not on its environment, this does not matter for the bank. From a security point of view, the closing of the account shall be done similarly as any userID based system + confirmation scheme.
- **Risk and fraud resistance**  
The use of secure module can help preventing man-in-the-middle attacks. Indeed the hacker cannot redirect the card holder wallet application to a fake

issuer server, since this application is build to always connect to the appropriate issuer server<sup>7</sup>.

- User friendliness

This way of working is generally well perceived by end-users since only the first occurrence of e-banking requires the download and installation of the program (which is generally correctly supported by the bank). However, when the user needs to use another device (have a new PC, is on holyday ...) this requires the re-installation of the program.

**Cumulative effect of using specific software on here above scoring matrix**

	<b>Initiation</b>	<b>Usage</b>	<b>Termination</b>	<b>Risk &amp; Fraud resistance</b>	<b>User perception</b>
	- (installation required)	na (*)	na	++	+

(\*) not applicable

**5.3.3.5 Conclusion on users authentication methods in e-banking schemes**

Basically, financial institutions providing any form of internet banking should have effective and reliable methods to authenticate customers prior giving them access to their e-account.

For confidentiality, integrity and bank authentication towards the end-user, SSL/TLS (Secure Socket Layer) is the de-facto internet banking standard. For authentication and non-repudiation no single scheme has become predominant yet, although one can see a strong convergence toward 2-factor based authentication schemes (see Annex 6 on authentication tools for more detail). In particular, EMV authentication is more and more used.

In e-banking, the use of a PINPAD reader producing a challenge signature based on the user's bank-card seems to generalise. This observation is EU-wide and was quite expectable since there are standards that uniform such payments schemes.

**Two-factor authentication methods implemented in the context of e-banking schemes are to be considered as the best user identification/ verification methods.**

**In particular, an effective way of performing users' authentication is to use the EMV smart card authentication. This technique based on a card reader tends to generalise and**

<sup>7</sup> However the hacker may display a window *just like* the issuer provided applet window and prompt the user for the necessary authentication information. Although this is possible in principle, it is not simple to achieve and a way in which the attack described above could be avoided would be to require the card holder to initiate the operation of the module (or may be the applet). That is, if the applet was something which the card holder was required to run, then there would be no ambiguity about whether or not it is operating.

**appears to be the best technique for authentication in web banking.**

Security of e-banking schemes may be reinforced by the use of dedicated software (e.g. an applet from the bank). This solution helps to prevent attacks such as webspoofing (see Annex 8).

The use of e-signatures as specified in the European Directive on e-signature may offer an advantage for non-repudiation purposes related to liabilities and possible litigations.

### 5.3.4 E-commerce

#### 5.3.4.1 Introduction

This section deals with user identification methods for e-payments methods used for payments of goods (material or immaterial (software, access to content,...) in the on line world. They are payment services mostly provided by non-bank institutions and are thus only indirectly associated with a bank account.

For all the schemes described and analyzed in this document, the actors involved in those transactions are:

1. *The end-users (or buyers)*: they are consumers shopping for goods or services and wishing to pay. E.g., they may pay using a credit card issued by an issuer bank.
2. *Issuers*: Mostly the end-users' banks. They represent the financial institutions extending credit to their customers through bank card accounts or by providing access to demand deposit accounts via a debit card. Issuers have contractual agreements with credit card companies such as VISA or MasterCard to issue their respective products and distribute them to their card holders (end-users).
3. *Merchants*: they are vendors accepting payment of goods or services. Merchants can accept credit cards through relationships with their acquirers.
4. *Acquirers*: Mostly the merchant's banks. They are financial institutions doing business with merchants who wish to accept payments. E.g., acquirers have a relationship with their merchants for the processing of debit and credit card authorizations and can make payments for card transactions to their merchants.
5. *Payment Systems providers*: they establish relationships with issuers and acquirers.

#### 5.3.4.2 E-commerce security challenges

The growth in internet use has expanded at an exponential rate and is expected to continue. It is likely to lead to an increase in e-commerce. But this increase in on line commerce and virtual transactions is not without significant security concerns. As identified in WP2, security issues are the most commonly cited reasons for individuals who choose not to engage in on line shopping. As already stated, internet communication networks are insecure, and all parties – end-user, merchants, issuers and acquirers – face a number of risks when

transactions are conducted through these insecure public networks. Other weaknesses rise from merchant servers that are insufficiently protected, leading to unauthorized access to payment data stored in their databases.

From the European Consumer Centre, ECC, (Belgium aisle) April 2007, one learns that in 2005, it registered 3780 requests from consumers linked to their purchases on internet, among which 1834 cross-border complaints, compared to 831 complaints treated in 2004.

Most of the complaints relate to purchased goods not delivered (46 %). Fraud is one of the causes, in particular fraud sustained by false trusted third party. ECC discourages the consumer to work with « trusted third party ». But one can also quote transaction sites that are created, collect payment data and then disappear after fraudulently charging the end-user.

As a consequence, many users are reluctant to perform e-payments on the internet, especially to provide their credit card number. Issuers would like to avoid the risk that their card holders adopt another issuer's solution that they find more attractive, and/or that merchants delay implementing the solution until it is proven to be profitable. The parties involved in a transaction need thus a secure environment to conduct the transaction. In particular, the buyer and the seller want to protect the details of the order and the payment. The buyer wants to be sure that his/her account information is not stolen and inappropriately used.

From an end-user perspective, the main security issue is to receive debits for a good or service it never agreed to buy or agreed but never received (e.g., following a transaction with a fraudulent merchant who may bill the transaction and never deliver the goods purchased). This can also happen as a consequence of the end-user privacy violation, when personal information is re-used for another purpose (e.g., having card or account data stolen and re-used for another purpose, which can occur when hackers breach the security at on line merchants and manage to retrieve their credit card databases).

Hence, the main security requirements for the end-users are the following:

1. the confidentiality of the information exchanged (including card details);
2. the integrity of the information exchanged; the card holder requires that the transaction he/she approved and that the payment information he/she sent cannot be modified.
3. the authentication of the merchant: the card holder requires assurance that the merchant is actually who he/she claims to be and is trustworthy. In fact, the card holder needs to build a transacting trust environment equivalent to that of the physical marketplace. He/she needs also to identify the entity towards which to address an eventual complaint. Hence, merchant authentication is a building block for this trust process.
4. replay protection: the card holder does not want the data used for genuine transactions to be re-used to conduct fraudulent transactions.

For principals other than the end-user, and due to the increase of chargebacks and of the associated costs due to fraudulent transactions, non-repudiation is becoming a major business requirement. Indeed, chargebacks originating from "card holder not authorized" transactions represent more than 70% of all e-commerce chargebacks (including "not authorized" transactions due to fraudulent merchants that do not deliver the goods, where it is sometimes easier for the card holder to repudiate the transaction rather than sue the merchant).

Regarding the merchant in particular, payment guarantee (which is actually the main objective), needs to rely on proper end-users authentication (the merchant requires assurance that the end-users is authorised to conduct a payment transaction (e.g., with the card he/she is presenting, and that the card the card holder is using is a genuine one), that the buyer is legitimate and will provide payment in exchange for the goods), and non-repudiation of the transaction. Merchants do not want the end-users to repudiate a transaction he/she has effectively conducted.

As a matter of fact, one easily understands that authentication, entity authentication and data authentication (with non-repudiation purpose) are crucial features to sustain e-commerce and help to sort out liabilities in case of litigation:

- As it leads to chargebacks for issuers and acquirers and potentially no payment for merchants, non-repudiation by the end-users is thus the main business requirement,
- Authentication of both parties is crucial to ensure trust; the buyer must believe that the seller is legitimate and will actually deliver the goods as described.

#### **5.3.4.3 E-commerce schemes**

There are numerous e-commerce schemes<sup>8</sup>, (more details are provided in Annex 8). It is not the goal of the present study to list them all, but it is important to group them in order to be able to make a comparison from a user verification perspective. This is quite easily achieved since e-commerce schemes can be classified in categories sharing the same authentication tools.

According to FEVAD, (the French Professional Organisation representing remote sales enterprises), e-commerce transactions in France are supported by bank cards for more than 65% of the cases (cheques support 14% of the transaction, private cards support 14% of the

---

<sup>8</sup> Note on E-Cash, eInvoice and EBBP

Electronic cash payment systems has been described in the 2003 PwC study, however they do not represent a large proportion of e-payment transaction. Examples of such payment systems are DigiCash, MicroMint, PayWord. It is the card-issuing bank and its partners who determine how card accounts can be funded. Prepaid-cards draw on a prepaid account that can be funded in a variety of ways. Many methods rely on credit transfers from a bank account or credit card. From the user verification perspective (which is the aim of this study) we thus refer the reader to the very complete section related to E-commerce card based payments.

Let us also note that EBPP systems (Electronic bill presentment and payment (EBPP), most US oriented) and/or e-invoicing solutions (more EU oriented) also uses the Internet as a speedier and less expensive delivery infrastructure to present bills electronically and proceed to payment. E.g. Nordea, Telefact, Certipost, ... The bill payment process involves at least five main participants: the consumer, the consumer's financial institution, the biller, its financial institution, and a payment network. As the reader can see in Annex 8, these schemes relate to E-commerce as well as from the business model (principals are the same, the biller being assimilated to the merchant) and consequently, as from the principals' expectations. The payment methods are also the same as for any other goods or services in E-commerce (debit or credit card based, or bank transfer based).

The analyse of the related security requirements and in particular, authentication methods are thus covered in this E-commerce section and do not call for a specific section.

transaction whiel the rest is paid through different means, e.g., at the moment of delivery of the goods). Although it might be dangerous to directly extend the French figures to Europe, the WP2 study also confirms that bank cards payments are the most spread for e-banking in Europe. More than being the most used e-commerce payments schemes, bank cards (debit/credit) are also recommended and promoted by the Office Européen des fraudes and the ECC. Therefore this section is thus strongly focusing on card payments.

According to ECC, credit cards are the most secure payment means for buying on the internet because the consumer is protected by legislation (the issuer is required to reimburse in case of fraud). Our study will thus address in particular the credit card based payment.

Another scheme that appears to be more and more used is the re-direction from the merchant toward the customer's banks web banking facilities. This re-direction may occur towards the intermediary of a TTP (e.g., Ogone), or directly from the merchant site when this merchant has agreement with banks (this is more for local goods selling).

Payment over the internet can either be direct from buyer to merchant (the transaction is not powered by an intermediary payment service provider, except the credit card issuer (e.g., Visa, Master Card), or can rely on a TTP (i.e. electronic transaction where an intermediary payment service provider secures the transaction (e.g.,: Paypal, Ogone)).

From a high level view, one may distinguish two payment schemes categories:

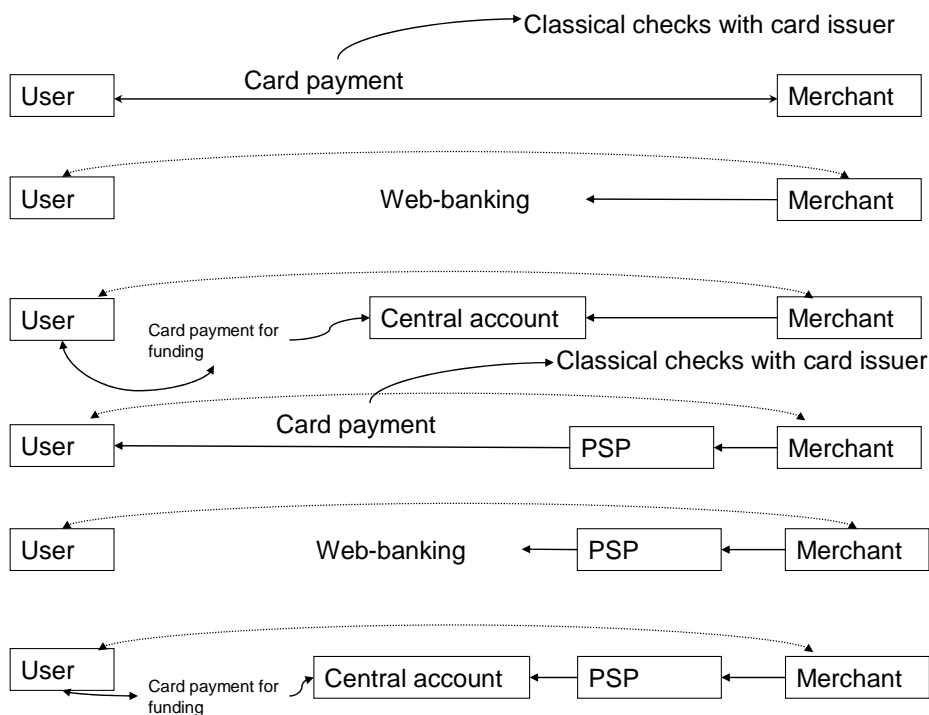
- (i) Direct with the merchant:  
These are generally credit card payments. In this case, in its simplest form, the merchants embed on their sites software modules responsible for communicating information with the acquirer's payment gateway, and retain the card holder's details in a database on their own site. More elaborated schemes described here below, require the card holder to authenticate itself towards its issuer and require a transaction authorisation to be provided to the merchant in order to allow the transaction. 3D-Secure is an example of such a schemes.
- (ii) Indirect with the intervention of a Trusted Third Party:
  - Payment service provider (PSP). In this case, merchants do not embed any software on their site but embed hyperlinks for each product into web pages. When card holders click on one of these hyperlinks, they are redirected to a payment server hosted by a service provider (e.g., Ogone).
  - Web banking re-direct solutions. Merchants and/or payment services providers can redirect the customer to their web banking solution.
  - Centralised account providers (Paypal) or other e-money where the credit card is used to fund an account.

Where these payment services do not rely directly on a bank account, such as PayPal, individuals can transfer funds, shop on line, or participate in on line auctions, using a (pre-funded) account.

The service provider usually will not have a face-to-face relationship with its customers. Depending upon the accessibility of the internet payment service, these activities can involve payments or funds transfers across national borders.

The tools to carry out the on- line payment operation are thus basically:

- internet/web-site payment associated with any kind of payment cards,
- internet/web-site payment associated with an e-banking methods,
- internet/web-site payment associated with a centralised account (this last category can be seen as a sub-set of the first one, the account being actually generally funded by means of the end-user credit card or bank account).



**5.3.4.4 Analysis of card user verification methods in e-commerce schemes**

The quality of the user verification methods according to the aims of the present study (security, user friendliness etc) depends on one hand on the schemes global architecture and on the other hand on the underlying tools.

The global architecture security is influenced by the way the end-users are enrolled in the system, the relationships between principals and the possible security breaches between them (the weakest link security level being the actual security level the overall scheme), the segregation of sensitive information between actors, etc...

As an example, in a lot of cases with a direct payment relationship between the end-user and the merchant, unless specific protocols such as SET are used, the payment information (card holder's name, credit card details, etc.) is sent to the merchant system. Then the merchant sends an authorisation request to its acquirer. The request is transferred to the issuer, and the authorisation response is sent back to the acquirer, which forwards it to the merchant. In this case the merchant has access to all end-user's information (including the financial information) in addition to the information related to the goods purchased. At this stage, one can already identify the risk that the merchant database, if not well protected, could be hacked and the end-user's financial information disclosed.

As previously stated, card payments are at the basis of the majority of the e-commerce transaction payments; as well direct to merchants payments and payments relying on an intermediate Trusted Third Party. Before comparing e-commerce schemes, it is necessary to understand the major building blocks that are the card payments protocols. The present section describes and analyses the security techniques existing to counter the various threats and risks linked to credit card payments conducted in the on line world in general.

### **Minimal requirements**

Even before the rise of the internet, there was a need to conduct transactions without the card holder 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. 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 card holder at the merchant.

Without any additional security measures, the card holder 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. This is even more true on the internet where information can easily be found and re-use indefinitely.

The first threat when dealing with credit card is thus **eavesdropping** on the connection between the browser and the web server.

The second threat is that an attacker tries to imitate the site from a legitimate organisation, in order to extort users' confidential information (web **spoofing**).

It is important to know that, in order to comply with the VISA International and MasterCard International security rules published in April 2001, all CNP transactions will need to include the CVV2/CVC2 (CVx2) security code of the corresponding card<sup>9</sup>. The CVx2 was made compulsory in 2003 for French selling sites. From a pure security point of view, this code is however comparable to a static password.

Minimal requirements:

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. E.g., SSL prevents eavesdropping by providing data encryption and helps to support merchant site authentication against web spoofing (with the restrictions explained in Annex 8 regarding SSL).

The next paragraphs will highlight diverse schemes for securing CNP transactions.

**No security**

Although this solution is clearly easy to use and to implement (no device or software to use), the risk of fraud is huge. This case is thus not pertinent and does not comply with the minimal criteria requested here above.

**Evaluation overview**

	<b>Initiation</b>	<b>Usage</b>	<b>Termination</b>	<b>Risk &amp; Fraud resistance</b>	<b>User perception</b>
<b>Card holder</b>	n.a.	Merchant authentication: --	n.a.	Confidentiality: -- Integrity: -- Replay protection: -	Ease of use: ++ Trust: -
<b>Issuer / Acquirer</b>	n.a.	Card holder auth./ non-repudiation: --	n.a.	Confidentiality: -- Integrity: -- Interoperability: ++	Ease of use: ++ Trust: --
<b>Merchant</b>	n.a.	Card holder auth./ non-repudiation: --	n.a.	Confidentiality: -- Integrity: -- Interoperability: ++ Replay protection: --	Ease of use: ++ Trust: --

<sup>9</sup> CVx2 is a code unique and specific to each card, corresponding to the 3 last figures of the number printed on the card verso (near the signature pan). According to the issuers, the others numbers corresponds for part of them or the whole to the card number. The CVx2 is requested by the merchant in e-transaction in order to verify that the customer is (or has been) in possession of a genuine card. This number can be validated by the issuer thanks to a cryptographic computation.

### Transaction SSL (TLS) protected

As mentioned before, this protocol provides data confidentiality and merchant authentication (as it does for bank authentication toward end-user when underlying e-banking scheme). It shall be reminded that SSL is generally used in unilateral authentication mode (the end-user authenticates the merchants but does not authenticate himself toward the merchant via the SSL protocol).

### Evaluation overview

	Initiation	Usage	Termination	Risk & Fraud resistance	User perception
<b>Card holder</b>	n.a.	Merchant authentication: ++	n.a.	Confidentiality: ++ Integrity: ++ Replay protection: --	Ease of use: ++ Trust: ++
<b>Issuer / Acquirer</b>	n.a.	Card holder auth./ non-repudiation: --	n.a.	Confidentiality: na Integrity: na Interoperability: na	Ease of use: ++ Trust: --
<b>Merchant</b>	Needs to have an SSL certificate. When issued by well known CSP: ++	Card holder auth./ non-repudiation: --	+	Confidentiality: ++ Integrity: ++ Interoperability: ++ Replay protection: --	Ease of use: ++ Trust: --

### Virtual and pseudo Card Numbers

These features are provided by the issuers to the attention of their end-users and allow them to use one-time (or limited in time or for a limited amount of transaction) credit card number. These numbers present the same advantage as OTP passwords over static passwords: replay protection. Even if the merchant database is hacked, the disclosed information is of no use for the hacker.

In the e-commerce perspective, it also has the advantage of being transparent for the merchants.

### Evaluation overview

	Initiation	Usage	Termination	Risk & Fraud resistance	User perception
<b>Card holder</b>	Depends on the registration process. Performed by issuers: ++	Merchant authentication: --	Auto-Expiration is possible: ++	Confidentiality: - (*) Integrity: -- Replay protection: ++	Ease of use: - /+ Trust: ++
<b>Issuer / Acquirer</b>	n.a.	Card holder auth.: ++ Card holder non-rep.: +	Auto-Expiration is possible: ++	Confidentiality: - Integrity: - Interoperability: ++	Ease of use: - (requires investments for issuers) Trust: +

<b>Merchant</b>	n.a.	Card holder auth.:++ Card holder non-rep.:+	Auto-Expiration is possible: ++	Confidentiality: -- Integrity: -- Interoperability: ++ Replay protection: ++	Ease of use:++ Trust:++
-----------------	------	--	---------------------------------	---	----------------------------

(\*) Not the case if pseudo card numbers are used in conjunction with another technique, e.g., SSL.

### SET and 3D SET

SET, and its enhanced version 3D SET, were very secure protocols both from a data protection as from a privacy perspective.

However, because of its high implementation costs (mainly due to the underlying complexity of the scheme), SET and 3D SET were never fully endorsed by the market. This is an important lesson le when studying security aspects of e-payment; the balance security – cost shall always be considered.

### Evaluation overview

	Initiation	Usage	Termination	Risk & Fraud resistance	User perception
<b>Card holder</b>	Depends on the registration process. Performed by issuers: ++	Merchant authentication: ++	Depends on the process. Performed by issuers: ++	Confidentiality: ++ Integrity: ++ Replay protection: ++	Ease of use: - -/+ SET: --- 3DSET: ++ Trust: ++
<b>Issuer / Acquirer</b>	n.a.	Card holder auth.: SET: ++ 3D-SET: Depends on implementation Card holder non-rep.:++	n.a.	Confidentiality: ++ Integrity: ++ Interoperability: ++	Ease of use: SET: -- 3DSET:- Trust:++
<b>Merchant</b>	Needs a certificate	Card holder auth.: SET: ++ 3D-SET: Depends on implementation card holder non-rep.:++	n.a.	Confidentiality: ++ Integrity: ++ Interoperability: ++ Replay protection: ++	Ease of use: SET: -- 3DSET:- Trust:++

### 3-D Secure

3-D secure is fully detailed in Annex 8. This protocol is a payment industry standard and uses SSL encryption to protect payment card information. Similar to 3D-SET it **allows the Issuer to choose a mechanism which is sufficiently strong to authenticate the card holder.**

There are diverse implementations of 3D Secure. The VISA (marketed as Verified by Visa) and the MasterCard implementation of 3-D Secure (forming part of the MasterCard SecureCode family of card holder authentication techniques), are two schemes built upon 3D-Secure (for further details see Annex 8).

3-D Secure permits merchants to use a single implementation to handle payments originating from MasterCard, Maestro, VISA and other card brands, and also allows a certain degree of customisation by the payment system provider.

3-D Secure is not an authentication method but a payment architecture on the internet where:

- Buyer's bank authenticates its customer.
- Merchant's bank authenticates its customer.
- Inter-bank domain allows the merchant to start the buyer's authentication in a unique way, whatever the authentication means used by the buyer

Trust is ensured between acquirer and issuers domains in the following ways:

- Following the buyer's authentication, the merchant verifies a "generic" proof computed by the issuer.
- During authorisation, the merchant sends an authentication token which has been communicated by the issuer during authentication.

### **Initialisation**

The registration process can be performed entirely on line or it can be a combination of a physical mail out of the password and on line registration. In the United States the registration process is often entirely on line and involves the card holder answering a series of security questions 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 can be done entirely on line too, e.g., by the use of information on previous account statements.

The lifecycle of all authentication devices must be managed correctly, from the design to the delivery to the card holder, to avoid large scale attacks.

The ease of obtaining evaluation is '+'. This affirmation is based on the fact that there is a registration procedure. However this procedure may vary according to the authentication method proposed by the issuer.

### **Usage**

SSL is used in order to protect the confidentiality of information in transit, and to enable the card holder to verify the merchant's identity.

However, although the use of a strong method of authentication by the Issuer is expected, 3-D Secure offers a level of security that is strongly dependent upon the type of authentication chosen by the issuer. Authentication systems username/password based may have inherent weaknesses such as use of a static password, ... In principle, however, 3-D Secure can provide good technical security. Usage security evaluation is '+'; again this evaluation is to be fine-tuned according to the authentication method proposed by the issuer.

### Termination

Besides the proper closing of the account, this phase is again, depending on the authentication method proposed by the issuer.

### Risk and fraud resistance

These schemes offer relatively good protection of the web/application server against hacking.

### User friendliness

The merchant is the unique entity responsible for the security of the storage of the information, so the card holder must trust that the merchant will guard its credit card information securely. However, the card data can be disclosed by attacks on the merchant's system or by fraudulent merchants. This is a real issue, as the lack of protection of the merchants' databases is the cause of many frauds.

To counter this issue, the use of CVx2 is an additional security feature knowing that card issuers do not permit this value to be stored and that creation of the CVx2 value requires access to secret keys known only to the issuers. However, this supposes to have fair implementations at the merchant's side (not storing the number, such as prescribed).

### Evaluation overview

	Initiation	Usage	Termination	Risk & Fraud resistance	User perception
<b>Card holder</b>	Depends on the registration process. Performed by issuers: + E.g. when EMV based: ++	Merchant authentication: + (SSL based)	Depends on the process. Performed by issuers: + E.g. when EMV based: ++	Confidentiality: ++ Integrity: ++ Replay protection: ++	Ease of use: + Trust: +
<b>Issuer / Acquirer</b>	n.a.	Card holder auth./non-rep.: + <b>(less than SET, more than SSL)</b> E.g. when EMV based: ++	n.a.	Confidentiality: ++ Integrity: ++ Interoperability: ++	Ease of use: acquirer: + issuer: - Trust: ++
<b>Merchant</b>	n.a.	Card holder auth./non rep.: + E.g. when EMV based: ++	n.a.	Confidentiality: ++ Integrity: ++ Interoperability: ++ Replay protection: ++	Ease of use: +/- Trust: ++

## **Most used and best payments authentication schemes in e-commerce**

On the internet, card payment is the main payment channel.

The fact that SET and 3D SET were never endorsed by the market is an important lesson learned; the balance security – cost shall always be considered and it appears that security will never be at the expense of too high costs.

The 3D secure scheme appears to be a good compromise between security and implementation costs. However 3D Secure is not yet very wide spread although precise figures were not really available to the WP 1 team.

SSL appears to be the method most used to secure e-commerce. As previously explained, it offers a quite good merchant authentication, but in general (and at least as used in most of the schemes), no user authentication at all.

### **5.3.4.5 E-commerce schemes impact on security**

As presented above, all the methods studied in the sequel that support e-commerce payment schemes may be classified as follows:

- (i) Direct with the merchant:
- (ii) Indirect with the intervention of a Trusted Third Party:
  - Payment service provider.
  - Web banking solution.
  - Centralised account providers

## **Direct with the merchant**

### ***Classical cards payments***

In this case, merchants embed on their sites software modules responsible for communicating information with the acquirer's payment gateway, and retain the card holder's details in a database on their own site (except with SET, but this protocol is no longer used).

The merchant is the unique entity responsible for the security of the storage of this information, so the card holder must trust that the merchant will guard their credit card information securely. However, the card data can be disclosed by attacks on the merchant's system or by fraudulent merchants. This is a real issue, as the lack of protection of the merchants' databases is the cause of many frauds.

The problem of storage of the card holder's card details in merchant databases can be smoothed by the usage of the CVx2 code.

The problem of storage of the card holder's card details in merchant databases can be avoided by outsourcing the payment server and the management of credit card details to a service

provider, rather than to choose to implement the payment server, and send payments to a payment gateway (see intervention of a TTP, next sub-section).

**The quality of the payments when performed in direct with the merchant is directly linked to the quality of the underlying protocol;** no security, SSL only, virtual or pseudo card number based, or 3D Secure based. As stated above, 3D-Secure appears to be the best solution. However, it shall be kept in mind that 3D Secure security highly depends on the authentication method employed by the issuers.

Similar to the conclusion on the e-banking section, and following the same reasoning, a crypto based authentication, and more precisely a PKI-based authentication would be the most secure authentication solution (e.g., using EMV). However, nowadays, many of the e-commerce schemes are only SSL / TS based.

### *Private card payments schemes*

Private cards can be pre-paid card and there are various systems in place; e.g., Paysafe. Paysafecard is a prepaid card that allows users to pay on the internet (users do not need a bank account or a credit card).

1. The user buys a paysafecard at a retailer (he/she decides which value paysafecard he/she chooses).
2. The user employs his/her paysafecard to pay on line.

Each paysafecard has a 16-digit PIN code. The users do not have to disclose any personal details or access to his/her bank account.

This kind of systems provides a very good privacy level for the user. Indeed, the user only has to proof the possession of the card with the PIN code, and stays anonymous to the outside. It is however difficult to have an idea on the rate of use of such systems.

### **Indirect with the intervention of a Trusted Third Party (TTP)**

#### *Payment services provider*

In this case, merchants do not embed any software in their site but embed hyperlinks for each product into web pages. When card holders click on one of these hyperlinks, they are redirected to a payment server hosted by a service provider. Hence merchants do not need to implement a payment server. Using this 'outsourcing' model provides greater security to the card holder, as the merchant web site does not store the credit card details, which could potentially be hacked or misused. This assumes that the payment service provider does not store credit card numbers, or, if it does, that it strongly protects them. If this assumption does not hold, then outsourcing may actually make things worse, since it provides a single point of attack, giving the attacker a much better pay-off than having to attack multiple merchants (note that some merchants still want to capture the card holder information and control the shopping process and remain reluctant to use an intermediary TTP).

#### *Example of TTP based payments scheme where the end-user has no account: Ogone*

Ogone e-commerce is a payment solution designed for electronic commerce. When the customer indicates that he/she wishes to make a payment, the merchant's e-commerce site redirects him/her to the Ogone site. Ogone e-commerce collects the necessary information and processes the payment request. After payment verification, Ogone

notifies the merchant's e-commerce site and returns the customer to it. This process can be transparent for the customer. The merchant can then connect to the Ogone site to administer his/her payments. The advantages are the following:

- Payment service providers (PSPs) offer the service of handling payments to internet merchants. By using a PSP, a merchant need not to 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 as an *Integrated Solution*.
- protection of end-users
  - o privacy: financial data is transferred to financial institution;
  - o commercial data stay at merchant;
- enhanced trust (end-user only trust the PSP) and have a good level of assurance regarding the merchant (officially affiliated to the PSP);
- some of them (e.g. IdTronic) also add security value (e.g.; protect the credit card number transfer).

### ***Web-banking redirect***

It is to be noted that very important merchants (e.g., the Fnac) use the redirect to web-banking solutions. For assessment of the related end-user verification methods the reader is referred to the e-banking section.

### ***Centralised account systems***

Centralised account systems are electronic payment systems involving transferring money to/from money accounts. Amongst other centralised account systems feature person-to-person payments and avoid the financial clearing process.

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 disappear if improved security measures (such as strong authentication) would have to be implemented.

Let us describe one of the most widely spread system in Europe; PayPal. Paypal appears indeed to be the emerging centralised account systems. Paypal is detailed in Annex 8. Due to the shareholder relation between eBay and PayPal (PayPal is the on line payments unit of auction website eBay Inc.), this payment scheme tends to take more and more market share. PayPal is spread all over Europe (and even worldwide) and has nearly 35 million customer accounts in Europe; about a quarter of all its accounts (June 2007). PayPal enables individuals and businesses to send and receive electronic money on line. It also provides other financial and non-financial services closely related to on line payments. These services are collectively referred to hereafter as the "Service". However, PayPal does not provide credit, banking and/or escrow services.

The Service is provided by a new PayPal company, PayPal (Europe) S.à r.l. & Cie, S.C.A. (PayPal Luxembourg), founded on July 2<sup>nd</sup> 2007, which became the service provider for

PayPal in the EU. This is a Luxembourg entity regulated as a bank by the Commission de Surveillance du Secteur Financier (CSSF), the Luxembourg equivalent of the FSA. PayPal primarily functions as a payments intermediary for individuals and organisations that wish to trade with each other or transfer funds via the internet. PayPal operates by allowing an individual to set up a pre-paid account in his/her name with PayPal that can be funded from a credit or debit card or a bank account via a credit transfer. Using those pre-paid funds, individuals can buy items or transfer funds to other PayPal account holders. The payment or transfer of funds occurs as a book-entry transaction between the PayPal accounts. When an individual wishes to access the funds in his/her PayPal account, he/she directs PayPal to credit his/her credit or debit card or bank account via a credit transfer or even a paper check.

#### *Paypal authentication issues*

Regarding user authentication, in its simplest way if working, Paypal uses ownership of an e-mail 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.

Regarding the verification of payee identity, payees are identified by their email address, which is a weak method. Mistakes can happen by making a typo, or by attackers obtaining an address which suggests they are from a certain organisation. In case of ordinary bank transfers stronger checks exist on the account number through 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.

When used in its simplest expression, Paypal may induce a decrease of security compared with direct payments with card where traceability of liabilities in case of litigation is more straightforward (e.g., merchants are well-known by the acquirer). However, Paypal now offers enhanced security features (see Annex 8), which provides both the buyer and the payee with a quite good level of authentication.

In particular e-commerce providers are however concerned by security issues, and eBay has recently announced that they would try to integrate the Belgian eID card on its Belgian site in order to strengthen Paypal user authentication (Tanguy Peer, eBay Belgium general manager, RTBF, September 2007).

#### **Impact of the e-commerce scheme on security aspects**

E-commerce payments can either be:

- Direct from buyer to merchant (the transaction is not powered by an intermediary payment service provider, except the credit card company, e.g., Visa, MasterCard); or
- Indirect and rely on an TTP (i.e. an electronic transaction where an intermediary payment service provider secures the transaction (e.g., Paypal, Ogone). In this particular context, a more and more used trend is the redirection from the merchant towards the customer's e-banking and/or web banking facilities. This redirection occurs towards the intermediary of a TTP (e.g. Ogone), or directly from the

merchant site when this merchant has agreements with banks (e.g., mainly applicable when selling local goods).

Payment schemes whereby the merchants outsource some of the payments tasks are promising from a security perspective. A detected trend is the redirection from the merchant towards the customer's e-banking and/or web banking facilities. This redirection may occur via the intermediary of a TTP (e.g., Ogone), or directly from the merchant site when this merchant has agreements with banks (e.g., mainly applicable when selling local goods). This trend is indeed very important with respect to security. It not only increases the guarantee of a correct execution of these so-called payment tasks (such as user identification/verification) but also has an impact on the privacy. Indeed, the financial data and the goods related data follow two distinct channels. This separation of data improves the customer's privacy. In addition, the use of a well-known TTP also increases trust and user's confidence in the payment solution. Solutions where the payment is performed indirectly tend to overtake solutions where the payment is done directly to the merchant. This observation is EU-wide and was quite expectable since the goods and services that are paid via e-payment methods are provided by EU or even world-wide merchants such as eBay.

These schemes appear to be candidates for the best *payment schemes* in this section. The two major advantages of TTP based payments schemes being the trust induced by the intervention of a well-known actor, the TTP and the increased privacy level.

#### 5.3.4.6 Conclusion on users authentication methods in e-commerce schemes

Chargeback rates for internet purchase transactions supported by bank cards are several times higher than face-to-face (e.g., card holder present) chargeback rates. The majority of the chargeback reasons are fraud-related or card holders claiming non-participation. According to VISA, 80% of all e-commerce chargebacks and fraud, as well as a substantial proportion of customer complaints, could be eliminated with the use of authenticated payments, a means to verify that the person making an e-commerce purchase is an authorized card holder.

For this purpose, different schemes such as 3D Secure, supported by payment card companies allow issuers to authenticate their customers. Card-based payments schemes that are based on 3D secure and where the issuer authenticates its customer seem very promising from a liability perspective; the issuer is responsible to choose the ad-hoc authentication method. In particular, EMV card based authentication is particularly well suited.

Whatever the payment scheme, from a security level perspective, the best user verification methods implemented so far rely on 2-factor authentication systems (e.g., user ID + password, whether static or dynamic combined with the possession of specific device, card or security software). However, most of the payments schemes stay on a "1-factor" authentication systems e.g., user ID + password, whether static or dynamic.

For payment schemes making use of an intermediary TTP with user account, one can see an evolution towards dynamic factor, while direct payment to merchant stays basically SSL based with no other authentication than the card related information accompanied by the request for the related CvX numbers.

In the context of e-commerce and internet payment schemes, **the TTP based payments schemes are better payments schemes from a security perspective than those not powered by an intermediary payment service provider:**

- TTPs evolve towards the use of a dynamic factor
- Direct payments to merchants remain SSL based with a static factor (with no other authentication than the card related information accompanied by the request for the related CvX numbers).

Irrespective the payment scheme, from a security perspective, the **best user verification methods rely on 2-factor authentication systems** (e.g. user ID + password, whether static or dynamic combined with the possession of specific device, card or security software).

Irrespective the payments scheme, **cards payments are not only used most frequently but also offer** the best security. Card-based schemes whereby the card issuer authenticates the user are considered as the best payments schemes. In particular, an effective way of preventing the classical frauds linked to card-not-present is to use the EMV smart card authentication to perform user authentication or on line payment transaction authentication.

However, most of the payments schemes remain today on a “1-factor” authentication system (e.g., user ID + password).

### 5.3.5 *Prospective e-banking and e-commerce authentication methods*

All methods described in section 6 of the present study present emerging techniques applicable to any payment type, including e-commerce. Regarding e-commerce in particular, one can say that a new sort of internet channel may be seen in iDTV (interactive television). iDTV is indeed a new device that could be the support for payment. However, it is expected that iDTV supported payments will be very similar to internet payments (i.e. same payments methods, and thus same user identification and authentication methods. Only the interfaces toward the user would be different (i.e. be the iDTV instead of classical browsers). For example, the credit card number would be submitted via the iDTV.

The iDTV authentication modules as such might also be used as authentication tool in the framework of e-payment. Technically speaking, there is indeed an authentication module within iDTV allowing further authorisation to access certain content according to the type of subscription of a particular user, but it seems that this authentication feature will not serve any other purposes, and e-payment in particular does not seem to be in the roadmap. However, since a set up box could be used as a payment terminal offering more security than an internet payment via a PC without a card reader this possibility could be considered in the future.

### 5.3.6 *Selection, Assessment and Analysis for the most used technical cashless payments*

#### **E-banking**

As stated in the E-banking section, one observes the emergence of schemes based on the use of EMV card as credential to support as well the user login as the transactions signatures.

**Two-factor authentication methods implemented in the context of e-banking schemes are to be considered as the best** user identification/ verification methods.

In particular, an effective way of performing user authentication is to use the **EMV smart card authentication**. This technique based on a card reader **tends to generalise and appears to be the best technique for authentication in web banking**.

Security of e-banking schemes may be reinforced by the use of dedicated software (e.g. an applet from the bank). This solution helps to prevent attacks such as webspoofing (see Annex 8).

The use of e-signatures as specified in the European Directive on e-signature may offer an advantage for non-repudiation purposes related to liabilities and possible litigations.

### E-commerce

As stated before, one observes that, independently of the e-commerce scheme (with or without TTP), credit-card payments are the most used e-payment system for e-commerce on the internet (whether secured with protocols such as 3D Secure or not).

Regarding the e-commerce schemes themselves, schemes with reliance on a TTP tend to be more and more used. In particular, PayPal appears to be the most widely used non-bank, internet-based method. PayPal primarily functions as a payments intermediary for individuals and organizations that wish to trade with each other or transfer funds via the internet.

In the context of e-commerce and internet payment schemes, **the TTP based payments schemes are better payments schemes from a security perspective than those not powered by an intermediary payment service provider:**

- TTPs evolve towards the use of a dynamic factor
- Direct payments to merchants remain SSL based with a static factor (with no other authentication than the card related information accompanied by the request for the related CvX numbers).

Irrespective the payment scheme, from a security perspective, the **best user verification methods rely on 2-factor authentication systems** (e.g. user ID + password, whether static or dynamic combined with the possession of specific device, card or security software).

Irrespective the payments scheme, **cards payments are not only used most frequently but also offer** the best security. Card-based schemes whereby the card issuer authenticates the user are considered as the best payments schemes. In particular, an effective way of preventing the classical frauds linked to card-not-present is to use the EMV smart card authentication to perform user authentication or on line payment transaction authentication.

However, most of the payments schemes remain today on a “1-factor” authentication system (e.g., user ID + password).

### 5.3.7 *Facts and figures*

While e-banking authentication methods seem to present a quite harmonised approach and high coherent level of security amongst the different banks, the authentication methods in e-commerce schemes are much more diverse.

It was really difficult for the WP1 team to receive figures on the rate of fraud (global figures for the whole section are provided in the introductory section). One can however note that most of the card payments are still occurring under simple SSL/TLS connection. The 3D-Secure scheme is identified as a very powerful tool, especially when relying on EMV authentication, not only from a pure security point of view, but also because of this collateral effect that it enables to solve liability issues. Nevertheless it is not generalised and widely used yet.

### 5.3.8 *Possible barriers to the implementation*

Barriers of implementation are mostly cost related. Methods that present too heavy costs, for any of the principal, will not be endorsed by the market.

Cost can be linked to the complexity (and thus cost) of integration (this concerns more the payment industry and, to some extent, the merchant). First implementations of 3D Secure may fall in that category, and referring the section above, it indeed appears that security will never be at the expense of too high costs (e.g., the SET case). As far as it is not strictly required (either by regulations or because of an unbearable level of fraud), expensive systems will not be deployed.

A priori, there is no other major *commercial* barrier to user authentication means. On the contrary, it is even well possible that the emergence of new easy and secure authentication/payment means (like mobile phones), is a commercial *incentive* to the use of e-payments.

Nevertheless a number of other concerns need to be raised:

- (i) user privacy concerns (see WP4),
- (ii) some fears on the way litigations issued from hacking would be managed (who is liable for what – who will pay a merchant that could not get money for goods it sent / who will reimburse an end-user for a good it paid and that was never delivered),
- (iii) user friendliness problems (see WP2).

The emergence of eID cards as authentication tools is somehow linked with this liability issue, such as explained in Annex 9.

However, the latest evolutions show, at least in some countries, real interest of the e-banking sector to work with public authorities as far as possible in that precise matter of user authentication. This is a rather new trend.

This is to be considered as well with the consideration on the need for more regulation (e.g., prosecution of ID fraud,...) that are highlighted in Annex 6.

## **5.4 M-payments**

### **5.4.1 Mobile Payments categories**

Mobile payments can be considered as a new type of payment instrument on one hand, and simply an access method to activate an existing means of payment for financial transactions processed by banks between bank customers on the other hand. It is noticeable that when constituting a new payment instrument, mobile payments can activate financial transactions processed by Mobile Services Providers (MSP) between MSP customers while MSPs are not necessarily banking institutions.

In the present study the m-payments methods are classified using the following two subclasses<sup>(10)</sup>:

- Mobile payment based on bank account
- Mobile payment not directly based on a bank account.

The mobile payment models can also be categorised as ranging from Issuer to Acquirer centric models (with increasing impact on the merchant) and from the server wallet based solutions to mobile based (with increasing complexity of mobile application).

Mobile payments refer generally to the use of mobile phones and other wireless communication devices to pay for good and services. Payments are initiated from a mobile communications device using voice access, text messaging protocols (such as short/single messaging service or SMS), or wireless application protocols (WAPs) that allow the device to access the internet. Authorization often occurs by keying in a unique personal identification number (PIN) associated with the customer or mobile device. Adoption of mobile payments varies from country to country. Use of mobile phones as a means to initiate payments is relatively widespread in Southeast Asia and in some European countries.<sup>11</sup>

Most mobile payment services simply use the phone as an access device to initiate and authenticate transactions from existing bank accounts or payment cards.<sup>12</sup> This is the equivalent of using the internet to initiate a direct debit or credit transfer from a bank account, or a credit or debit card transaction. This is an extension of traditional payment methods.

In new mobile payments, where mobile payment services are not based on an underlying bank or payment card account, the telecom operator typically acts as a payment intermediary to authorise, clear, and settle the payment.<sup>13</sup> Telecom companies engaged in these activities may not be overseen by a country's central bank or other banking regulator but may be subject to AML/CFT measures.

---

<sup>10</sup> Source for the two subclasses: FATF-GAFI – Financial Action Task Force – Groupe d'action financière: Report on New Payment Methods – 13 October 2006.

<sup>11</sup> See CPSS, « Policy issues for central banks in retail payments, » BIS, CPSS #52, March 2004, at [www.bis.org/publ/cpss52.htm](http://www.bis.org/publ/cpss52.htm)

<sup>12</sup> See CPSS, “Survey of developments in electronic money, and internet and mobile payments,” BIS, CPSS #62, March 2004, at [www.bis.org/publ/cpss62.htm](http://www.bis.org/publ/cpss62.htm)

<sup>13</sup> Telecom companies offering mobile payment services provide for the settlement of the payment transactions completed via their systems through normal banking channels.

The telecom operator may either allow the phone owner to let charge certain transactions to the phone bill (postpaid) or may permit the phone owner to fund an account held by the telecom operator or other service provider for the purposes of making payments (prepaid). Prepaid mobile payments accounts operate in the same manner as a prepaid card or an electronic purse. When the phone is used in the same manner as a prepaid card, the phone owner uses the phone as a payment system access device to authorize the deduction of value from the prepaid account. When the phone functions as an e-purse, the prepaid value is stored on the subscriber identify module or SIM card within the mobile phone.

Post-paid and prepaid card-like mobile payments are much more common than e-purse mobile payments. In the case of prepaid mobile payments, telecom providers often offer this service in conjunction with a bank.

More information can be found in Annex 6.

### ***Mobile Payments based on Bank Account***

Mobile Payments based on bank account (as an extension of traditional retail electronic payment systems) can be listed as follows:

- The telephony is used to facilitate the payment as an **authentication tool**, such as the use of mobile devices as authentication factor (SIM) or the use of mobile device to support another authentication mechanism (mobile as PIN entry device), in:
  - Direct debit
  - m-banking
  - centralised accounts
- GSM to GSM payments (brand names include M-Banxafe/Pay2Me from Banksys and the three Belgian mobile operators – Belgium, MOVO – France) implementing also so-called Person-to-Person payments

In these cases the mobile devices are used for the support of other classical e-payment systems, e.g., a server wallet based implementation of the PC Authentication Program which performs most of the payment related tasks. The mobile is not necessarily the access device to the internet. The mobile device is used in most implementations for authentication purposes, helping to achieve authentication either as an authentication factor (e.g., call-back mechanism, one-time password sms, etc.), or as support for authentication mechanisms (e.g., several factor based mechanisms).

### ***Mobile Payments not based directly on a Bank Account***

Mobile Payments not based directly on a bank account include telephony account systems, closely related to (GSM) telephony subscription accounts that enable payment to merchants. The telephony is here used as the payment instrument as such and the telephony account is related to the payment.

- **“Premium rate” model:** The merchant has a contract with the telephony operator which provides the merchant with a specific phone number.

Whenever a consumer accesses this specific number, the consumer's account is charged at a significantly higher rate than for ordinary dial numbers. This "premium" is shared between the mobile operator and the merchant. One can distinguish various versions within this category:

- **Premium-rate SMS:** Specific cost per message
    - Example: parking, public transport, culture and entertainment (ticketing), traffic management.
  - **Premium-rate voice** (connection time dependent but accessible from all phones)
  - **Premium-rate dial-up** (widely used in cases where consumers need to pay to gain access to a website or website based service. Paid content is available only from a private computer accessible by modem connected to a premium-rate phone number (use of a specific software may be required). The consumer is then charged accordingly (usually time based).
- **"Direct Transfer" model:** The telephony account is directly charged when a payment has been made. The telephony account is then used as a general-purpose payment account. Payment software installed by the operator is usually used rather than premium-rate services.
    - Example: additional menu available application allowing to perform debit payments from the user's pre-paid credit (or subscription account) with the operator. Such applications can make use of encrypted SMS messages.
  - **GSM to GSM payments not directly based on a bank account** (brand names include Crandy from NCS (DE), Luup (DK), PayPal (US)) implementing also so-called Person-to-Person payments.

#### 5.4.2 Analysis of m-payment schemes

The reader may find a high level overview of the basics of Mobile Security and a general overview of the security techniques used in Mobile Payment in Annex 9 as background to this clause.

Most mobile payment systems use the mobile phone as a device to access a bank account or credit card. These systems establish customer identification when the underlying bank or credit card account is opened. A similar customer identification process takes place when a telecommunications service provider mobile phone service is prepaid and the funds used to facilitate mobile payments are also prepaid, the service provider may not be motivated to fully identify customers because of the absence of credit risk.

The following criteria shall be considered in the study of m-payments methods:

**Value limits.** Where mobile phones are access devices to underlying bank and credit card accounts, limits may not be necessary.

**Method of funding.** Mobile payment programs that draw on a prepaid account can be funded in a variety of ways. Payment sources that have independently verified the identity the phone owner and that maintain a record of the funds transfer to the mobile payment account present a low risk. The use of cash to fund a mobile payment account, independent of other risk factors or risk mitigation strategies, may present some limited Money Laundering (ML)/Terrorist Financing (TF) risk.

**Geographic limits.** Mobile payment systems currently do not facilitate cross-border transactions due to incompatible systems. An attempted joint venture (SIMPAY) of several European telecommunications service providers failed in 2006.

**Usage limits.** Payments can only be received by a participating merchant or fellow service subscriber.

**5.4.2.1** Security analysis of user verification methods in M-Payment schemes based on a bank account

## **Introduction**

Because of the emerging and still moving characteristics of m-payment services, it is not easy to list and analyse all the systems currently in place. This section will thus highlight as an example, the Pay2Me technology allowing payments via a mobile phone which has recently become available. This service was presented on the 20<sup>th</sup> of March 2007 by Banksys, the Belgian company operating the electronic payment networks MisterCash/Bancontact and by the three Belgian mobile operators. This mobile-to-mobile payment technology allows merchants who are not equipped with bank card reading devices (e.g., liberal professions, taxi drivers, courier and other delivery services, but also the (wo)man in the street) to propose an alternative to their customers.

Other examples are presented at the end of the present section.

## **How does it work**

In order to be able to pay with its GSM and enable connection of the SIM card and its bank account, the SIM card of the GSM owner must be equipped with a specific application (M-Banxafe).

As a prerequisite the buyer will have to activate the M-Banxafe OTP ion of its SIM card through its GSM menu, select a 4-digit secret PIN and ensure once for all the connection between its SIM card and its bank account through the use of a Banksys terminal. The merchant will have to register to the M-Banxafe/Pay2Me application through the [www.m-banxafe.be](http://www.m-banxafe.be) website from mid-May 2007.

The mobile-to-mobile payment process is quite simple, requires two GSM, one for the buyer and one for the merchant, and is split into 5 steps:

- 1) The merchant enters the M-Banxafe menu of its GSM. It introduces the GSM number of the buyer (or its M-Banxafe activation number) and finally the amount of the purchase;
- 2) These data are sent to the M-Banxafe server that controls them before sending a payment request to the buyer under the form of an SMS;
- 3) The buyer receives the SMS asking confirmation of the transaction and requiring the presentation of the secret 4-digit PIN;
- 4) After approval from the buyer, merchant and buyer will both receive, from the payment service (3815), an SMS confirming the financial transaction linked to the buyer's M-Banxafe reference number and the merchant's Pay2Me ID, respectively. At the same time the buyer's bank account is debited, while the merchant's bank account is credited. In optimal conditions, the whole transaction from GSM to GSM will take less than 20 seconds, and up to 35 seconds in case of network congestion.
- 5) On their respective bank statements, both merchant and buyer will retrieve the transaction record.

In case the buyer's bank account is not sufficiently provisioned, the transaction will fail at step 4 and both the buyer and the merchant will receive an SMS confirming the failure of the transaction.

Buyer and merchant must not be located next to each other. Such M-Banxafe supported transactions and payments can occur remotely. This possibility enables electronic commerce to benefit from such a payment method. Similarly payment requests can be sent to buyers located abroad.

It will be possible to associate many M-Banxafe SIM cards to only one bank account (e.g., taxi drivers employed in the same company) and in the future it will be possible to link one M-Banxafe SIM card to several bank accounts

Note that the M-Banxafe application allows the SIM card holder not only to pay with its GSM, but also to reload a prepaid mobile card and to have access to bank account status information.

### **Value Limits**

A value limit has been set to a minimum of 6 euros and the upper limit is the same as for the bank card. Transaction costs have been set to 0,49€(VAT excl.) for the merchant and 0,25 € (VAT incl.) for the buyer. These transaction costs are likely to be reduced once the transaction volumes will rise.

### **Expected volumes**

100 millions of transactions are expected by 2010.

## User Authentication Security Level Analysis

In practice, the transaction should be as secure as a card-payment through Bancontact / Mistercash.

### Initiation

Buyer activation is a three-step process:

- 1) **M-Banxafe enabled SIM:** The buyer has to check whether the SIM card is M-Banxafe enabled and holds the corresponding logo. When this is not the case the buyer is requested to request a new Banxafe enabled SIM card from its mobile operator.
- 2) **Activation:** In order to activate the application, the buyer has to enter the M-Banxafe OTP ion of its SIM card through its GSM menu, select a 4-digit secret PIN. Once this is done, the buyer will immediately receive back a M-Banxafe reference code.
- 3) **Activation confirmation:** and ensure once for all the connection between its SIM card and its bank account through the use of a Banksys terminal or via one of its mobile operator agencies. In the Banksys terminal, the buyer will have to enter its bank card into the terminal, select the GSM Services / M-Banxafe menu, insert its M-Banxafe reference code and its GSM number, and confirm by entering the Bank Card PIN. In the mobile operator agency, the buyer will have similarly to indicate to the agency vendor the bank card to be link to the GSM, its M-Banxafe reference code and its GSM number. The vendor will insert the buyer's bank card in the terminal and treat the received data. The buyer will confirm the operation by typing its Bank Card PIN.

### Usage

It is a 2-factor authentication method for which an attacker would need to collect both the secret PIN-code and the GSM (SIM card). Actually there are two PINs, one for activating the GSM (the SIM card) and one specific to the M-Banxafe application, such that even when the GSM is stolen or lost activated, there is still one PIN protecting the M-Banxafe payment application. Three wrong PIN values will result in blocking the card.

The security level is transitively equivalent to the bank card security.

### Termination

In case of lost GSM or when it is stolen, it is recommended to contact the (Card Stop) Call desk in order to block the M-Banxafe application activated on the lost or stolen SIM card.

### Risk & Fraud resistance

The security level is transitively equivalent to the bank card security.

No detail about the M-Banxafe application has been made available yet or obtained from Banksys.

### User perception

Belgium, a 10 million citizen country, registers 9,5 millions GSM users whose 64% would appreciate to pay with their GSM, according to Banksys (Payment Industry).

The service is claimed by the Payment Scheme Provider to be:

- Quick,
- Easy,
- Secure, and
- Allowing the GSM holder to have always money in its pocket, provided it holds its GSM.

In such a joint offering of added value service may result in confusion at user's side about the owner of the customer relationship, on who is the registration authority, on who is liable for what between banks, Banksys and the user's mobile telecommunication operator.

### Evaluation overview

	Initiation	Usage	Termination	Risk & Fraud resistance	User perception
<b>2-Factor Authentication Method (PIN + SIM Card) in m-payment method M-Banxafe</b>	<ul style="list-style-type: none"> <li>- Generation: SIM card level ++</li> <li>- Registration: Bank Card Holder based ++</li> <li>- Delivery: new SIM card</li> <li>- Storage &amp; Access: ++</li> </ul>	<ul style="list-style-type: none"> <li>- Number of factors: 2 (+)</li> <li>- Factor properties: PIN (+) + SIM Card (++)</li> <li>- Mechanism security: ++</li> </ul>	<ul style="list-style-type: none"> <li>- Termination: Card Stop 24/7 call desk to block application (++)</li> </ul>	<ul style="list-style-type: none"> <li>- Risk 1: +</li> <li>- Risk 2: + (see below)</li> </ul>	<ul style="list-style-type: none"> <li>- Friendliness ++</li> <li>- Ease of use ++</li> <li>- Confidence (unknown)</li> </ul>

Risk 1: SIM/WIM chips are not yet evaluated and current operator's SIM do not necessarily meet banks' security standards. In this scheme specific M-Banxafe approved SIM are required and certified by Banksys on behalf of the Belgian Banks.

Risk 2: PIN will be entered into a device that is not tamper evident, nor complying with EMV requirements. The danger of eavesdropping, tapping or "shoulder surfing" is however limited as the device is in the personal possession of the user.

### Other similar schemes in Europe

#### France

In France, the MOVO system allows Person-to-Person money transfer ([www.movo.fr](http://www.movo.fr)). Users need to adhere to the MOVO system and to transfer an amount the sender needs to hold a

bank account (Groupe Caisse d'Épargne). To receive a transfer there is however no need to hold a bank account but only to adhere to the system.

The transfer can be made either through an SMS, or using a vocal server, or using i-mode or WAP applications. Using SMS, the principal ordering the payment (transfer) to the recipient simply sends an SMS to a specific number and containing the code MOVO followed by the principal's MOVO specific 4-digit PIN, the 3-digit security code on the rear of the principal's bank card, the mobile phone number of the recipient, and the amount in euros to be transferred, all separated by a blank character. The recipient will then receive an SMS with the confirmation of the transfer on his bank account or if the recipient has not yet subscribed to the system instruction on how to subscribe within the next 72 hours. The sender receives an SMS to confirm the execution of the transfer or its cancellation in case the recipient did not subscribe within the 72 hours. Transaction flow is quite similar when using the I-mode portal or the WAP services (logging to the services through application level UID/PIN, writing transfer order, receiving confirmation SMS).

The user identification is, similarly to the M-Banxafe Belgian system, based on a non-face to face registration process. It implements as well however additional measures to verify and certify to some extent the identity of the subscriber. In this MOVO case the subscription process is made through an internet-based webpage collecting personal identification details and detailed information on the bank account of the subscriber (RIB – RICE information, i.e., bank account number, bank name, bank phone number, bank code ID, locket code, RIB/RICE key, and account name). The collection of this information allows one-to-one recognition of the bank account holder provided sufficient a posteriori verification is done.

Authentication of sender and receiver is based on the ID-Tronic technology (2-factor authentication based on UID/Password and OTP password send to user GSM through SMS) of the Caisse d'Épargne ([www.spplus.net](http://www.spplus.net)). Money transfers are secured by the SPPLUS technology of the same bank. These security measures make the MOVO scheme as secure as the card-based payment processes.

### **Value Limits**

A maximum of 1000€ per year can be received by recipients aggregated from all senders. Senders can send payments between 5€ and 150€ for a maximum amount of 600€ within 7 sliding days.

### **Costs**

The service is free for the recipients. The senders must pay a subscription of 7€ and a transaction fee of 0.5€ per payment not including communication costs.

### **Users' perception**

The MOVO scheme is still in its early stage or in even pilot phase.

Costs are usually considered heavy while the system is simple and easy. Questions have been raised about liability denial from mobile operators for non received or incorrectly received SMS.

### Spain

Other schemes include MobiPay, a Spanish Mobile payment service provider that allows to link SMS based mobile payments to a bank account or a mobile account.

#### **5.4.2.2** Security analysis of user verification methods in M-Payment schemes directly based on a Bank Account

Mobile Payments not based directly on a bank account include telephony account systems, closely related to (GSM) telephony subscription accounts that enable payment to merchants. The telephony is here used as the payment instrument as such and the telephony account is related to the payment. There are various models in this category of mobile payments not based directly on a bank account, in which one can distinguish two main groups, the premium rate model and the direct transfer model.

##### **5.4.2.2.1 Premium rate model**

The “**Premium rate**” model is likely to be the most employed model for using telephony as a payment instrument. In this model, the merchant has a contract with the telephony operator which provides the merchant with a specific phone number. Whenever a consumer accesses this specific number, the consumer’s account is charged at a significantly higher rate than for ordinary dial numbers. This so-called “premium” is shared between the mobile operator and the merchant. One can distinguish various versions within this category:

- **Premium rate SMS:** This scheme is based on a specific cost per message or per service associated to a specific SMS
  - Example: parking, public transport, culture and entertainment (ticketing), traffic management, m-Government, Person to person payment.
- **Premium rate voice** (connection time dependent but accessible from all phones)
- **Premium rate dial-up** (widely used in cases where consumers need to pay to gain access to a website or website based service. Paid content is available only from a private computer accessible by modem connected to a premium-rate phone number (use of a specific software may be required). Consumer is then charged accordingly (usually time based).

Since the limited possibilities of the two latter schemes, the present study will focus on the premium rate SMS model that is the one that allows the most variety of applications as detailed in the next subsection.

Access to the service only requires the user to send an SMS to a pre-defined premium rate number.

### **Mobile accessories and services**

The simplest version of such premium rate payment facility is the well known and used payment for downloading mobile phone ringtones, images, screensavers, wallpapers, mobile

games, sounds, mobile videos and any other mobile applications. In the provision of such services, there is neither customer identification nor authentication performed. The sole mobile device (or SIM card) PIN can protect the user from unauthorised subscription to such services initiated from his device. No registration at all is foreseen unless when subscribing to i-mode or WAP applications or through the corresponding website service.

### Additional services through premium rate SMS

In a more evolved version, additional services can be provided to the user through the usage of premium rate based SMS. In this category numerous applications are emerging such as:

- **Parking payment:** The user willing to pay for a parking, simply has to send an SMS to a specific number indicating the parking area zone (as displayed on the closest parking ticket machine), the desired parking time and the car plate. Variants can include the use of first SMS at parking arrival and a second SMS to stop or when this second SMS OTP ion is not used the maximal parking period for the indicated parking zone will be taken into account. In this latter case an SMS will warn the user of the expiration of this maximal parking period. The electronic ticket is instantly registered. A confirmation is usually sent to the user. The parking controllers are equipped with mobile devices (e.g., GPRS Blackberry or PDA) to the database of the Mobile Parking Service for verification of the electronic tickets paid for a specific car plate. Users can even extend or stop the parking at any time from anywhere through an SMS without going back to the ticket machine.

Different systems are in production since less than a year, e.g.:

- **Crandy** from **NCS** company, a German system, is in production in Gent (Belgium) and in Köln (Germany) and should be available in several additional European cities (UK, France, Belgium and Germany) and in the US in the coming future.
- **Mobile-For** equip the cities of Antwerp and Moortsel in Belgium.
- **Milano SMS parking Kit** is based on a similar principle but requires the preliminary purchase of an SMS kit containing a User identifier and a PIN.
- **Managing access rights to enter or stay in specific zones:** the same technology can be used for managing access to specific zones or areas (e.g., **Mobile-For** (BE))
- **Public transport:** Mobile tickets can be purchased using either SMS or WAP as the purchase channel. The purchased ticket can be delivered to the customer either in the form of SMS or MMS. In local transport the bulk of tickets sold tends to be time-limited one-ride tickets, for which purpose SMS is the easiest solution. In intercity transport there is a need to provide a large number of different tickets, varying by the date, departure and destination zones, travel class, etc. For this purpose MMS is the most feasible solution as a ticket carrier.

Different systems are in production or in pilot phase, e.g.,

- **Mobile-For** (BE) product is available but not yet in real life implementation.
- **Crandy NCS** (DE) the service is available through the sending of a specific SMS to a special number (each fare has its own number). The sender then receives an SMS with a virtual local transit e-Ticket that shall be showed at the bus controller who will verify the virtual ticket and confirm via his own PDA.
- **Plusdial - Örebro bus transports** (SE): Örebro passengers can use their mobile phones to pay their bus fare. SMS e-tickets are currently sold (since September 2006) in a trial program that will last until the end of the year, 2007. In order to pay his fare via SMS user has to have a mobile telephone that can send and receive SMS short-text messages. For now users do, however, need to be a subscriber of either TeliaSonera's or Tele2/Comviq's mobile phone service. The system works as easy as this: User writes a two-letter code for the type of fare he wishes to pay. "ÖV" for instance means "Örebro Adult", while "ÖU" means "Örebro Youth". Once user has written the code, he sends it off to telephone number 72372, which is Länstrafiken's dedicated SMS e-ticket number. Users don't even need to pre-register to use this service. The message is automatically forwarded to the computer system of the e-ticket service supplier, Plusdial, who automatically checks with user's mobile phone service provider to make sure that payment can be authorized. If user receives a monthly bill from his phone company, the fare will be charged to his next bill; if he has a pay-as-you-go SIM card, the system will check to make sure that there is enough money left on the card to cover the fare. Ordinarily this process takes only a very short period of time, after which an e-ticket will be sent to the user as an SMS message. If user accidentally wrote an invalid code in his original SMS message, he will receive a message that will inform him of his mistake. If there is too little money remaining on the card, the system will send a message suggesting refilling of the card as soon as possible. The user must show the e-ticket in his phone's display to the bus driver as he boards the bus so the driver can check that the SMS message is valid. Users are requested to keep the SMS message in the phone memory until the end of the journey in case of disembarkation check, which Länstrafiken reserves the right to carry out from time to time. Mobile phone service providers offer both companies and private customers the possibility to lock their phones for pay-by-call services. Since SMS e-tickets are a pay-by-message service, pay-by-call locked telephones cannot be used to order SMS e-tickets.
- **Vending machines:** Depending on the system used, anyone with a mobile phone can pay for their vending machine items through its mobile phone. **Crandy** (the NCS system, DE) allows the money to be charged on your Crandy account. In case not enough money is left on your personal Crandy account an immediate refilling function is available to transfer money on to your account. To purchase an item from a vending machine, the user simply has to call the vending machine number (e.g., 01621234567), select he desired product, and if the available credit is sufficient, the

vending machine will allow the sale. The chosen product is then dispensed immediately.

- **Culture and entertainment:** Mobile ticket's can be purchased using similar principles. The purchase channel, i.e. the way the customer orders a mobile ticket, can be either SMS or WAP or even i-mode. Mobile ticket's carrier, i.e. how the customer receives a proof of the mobile ticket to his or her mobile phone, can be either SMS with a unique control number returned from the central system or MMS with a unique ticket number and graphical control elements. Amongst other, we can find:
  - **Mobile-For (BE)**
  - **Crandy NCS (DE)** the service is available through the sending of a specific SMS to a special number (e.g., Crandy m CBRnnr 1500, "Crandy" for the payment system Crandy, "m" for the merchant, "CBRnnr" for the reservation number of the concert of Carla Bruni, "1500" for the amount of 15€). The sender then receives an SMS with a virtual 6-digit e-Ticket (e.g., ertz43) that shall be showed at the concert hall entrance. The concert hall agent will verify the virtual ticket and confirm (Blackberry display: For ertz43 1 person paid 04.04.07).
  - **TMN (PT):** Lusomundo cinemas have teamed with Portuguese mobile operator TMN to introduce m-tickets in July 2006. Customers can purchase m-tickets at the ticket counter, on line on Lusomundo's website or by calling Lusomundo's hotline. The ticket comes as an SMS to the customer's mobile phone, and contains a barcode that is scanned by an optic reader. To enter the cinema, the m-ticket holder opens the SMS and holds it to the reader. The reader then scans it and gives the customer a paper ticket. For the first 6 months, this service was available exclusively for TMN customers.
- **M-Government:** An additional area of application can be found by using such premium rate SMS based payments to pay for e-Government services. While some payment scheme providers (like Mobile-For) are expressing such possibilities no wide scale implementation has been registered so far.
- **Information request:** Specific information on various domains or content can be obtained on the GSM (either via SMS or MMS) can be purchased through the sending of SMS to a special number.

In these systems, the transaction amount will be either invoiced by the mobile operator in addition to the classic mobile services invoice or be invoiced separately by the Mobile Payment Scheme Provider (MPSP), such as for Mobile-For (BE), or will be debited from a pre-paid account established at the MPSP (e.g., Crandy – BE, FR, DE, UK).

#### **5.4.2.2.2 WAP & I-mode applications**

In order to proceed to purchasing or financial transactions for purchasing goods or services using a GSM, an alternative to the use of SMS resides in the usage of WAP or I-mode applications. Taking the example of purchasing train tickets in the Brittany region of France at SNCF, travellers *only* need to connect via their mobile phone on the tikefone.com mobile website. The sine qua non condition is however to hold a WAP enabled GSM. The process is usual, traveller selects its departure station, arrival station, the travel date and the payment is made through the insertion of the credit card number. At the end of the transaction, traveller receives a confirmation through SMS. The day before the departure traveller will receive an MMS (Multimedia Message Service) message being the e-Travel Ticket. This MMS will then have to be shown to the train controller.

Several i-mode, MMS or WAP based applications drawbacks make the system not as convenient as it is for SMS message based payment systems: low penetration for WAP enabled GSM (e.g. only 30% in France), GSM battery must be sufficient loaded (as for enabling SMS based ticketing schemes), WAP applications and/or WAP enabled GSMs are not that simple to use and require WAP activation from the mobile operator leading to some more costs compared to SMS services, and such schemes often requires being holder of a credit card.

#### **5.4.2.2.3 Direct transfer model**

In the **“Direct Transfer” model**, the telephone account is directly charged when a payment has been made. The telephony account is then used as a general-purpose payment account. Payment software installed by the operator is usually used rather than premium-rate services.

Example: additional menu available application allowing to perform debit payment from the user’s pre-paid credit (or subscription account) with the operator. Such applications can make use of encrypted SMS messages.

Most current implementations of such services are based on the sending of SMS and are covered by the previous sections when based on an existing bank account.

#### **5.4.2.2.4 Mobile to Mobile Payments not directly based on a bank account**

Brand names include Crandy from NCS (DE), Luup (DK), and the future solution proposed by PayPal (US) implementing also so-called Person-to-Person payments.

The system basically requires the opening of an account at the Mobile Payment Service Provider (e.g. Crandy). This can be done using various channels like a call desk and using a credit card, a credit voucher either offered by a merchant or purchased at a POS, a paper based bank transfer, or a full registration on a website and through bank standing orders, etc. No user identification is usually performed when subscribing to such a service.

In order to transfer money from a mobile (actually a MPSP user account) to another mobile (actually another MPSP user account), the order initiator:

- simply call the money transfer number, a dedicated IVR system (e.g., Crandy – DE). The Voice Dialog system asks the user to enter the amount in cents or euros and then press the asterisk key. The Voice Dialog system repeats the amount and asks for the MPSP number of the beneficiary. Once the number entered and the asterisk pressed, the amount is transferred. Once received the money can be similarly transferred to a classic bank account in case of having provided such bank details when having fully registered.
- Or using an SMS (e.g. Luup). LUUP lets you pay, send and receive money via SMS and on line. Once you sign up, you can connect your LUUP account to your bank account, credit cards and/or debit cards. This allows you to send and receive text messages which transfer money or send and receive money securely on line. You can use LUUP to pay companies for goods and services or to send money to friends. LUUP is regulated by the UK Financial Services Authority (FSA) and has a European E-Money license.

Sending money to anyone who has a mobile phone from a country where LUUP operates. If the recipient is not a LUUP user, he/she will receive an SMS with the amount you sent and an invitation to sign up for a LUUP wallet.

Example:

- Tim owes Jennifer £6 for a cinema ticket
- He knows her username is "Jennifer". He types a simple text message PAY JENNIFER 6 and sends it to LUUP's shortcode 81100. (Tim could also use Jennifer's mobile number instead of her username).
- Jennifer receives a notification of the payment in a text message...

Note: User can only send money from "cash" in his wallet (not from cards)

- Or on line: in this case, transfer is done via a login protected webpage and allows users to order transfer to other accounts either by indicating the account number or the mobile phone number of the transfer receiver.

Other schemes include MobiPay, a Spanish Mobile payment service provider that allows to link SMS based mobile payments to a bank account or a mobile operator account. Mobipay allows to send money to another person but also to pay (mobile) merchant, to pay on the internet, at a vending machine, recharge mobile pre paid account, pay cinema tickets, and pay invoices (e.g., electricity invoices).

#### 5.4.3 *Prospective Mobile Payments & Mobile Users Authentication Methods*

The following mobile payment platforms have been recently announced and needs further collection of information:

- **VISA Mobile Platform:** As announced in the press release of January 2007, this platform aimed to be a comprehensive suite of technology tools and applications, security standards, and business models that will enable Visa issuers and mobile operators to engage in market trials to drive product development and commercialisation of mobile payment services. Informed by years of experience in the mobile payments market and developed in partnership with mobile technology companies, including handset manufacturers, chip suppliers, mobile applications developers, over-the-air (OTA) service providers and mobile messaging providers, the platform aims to be both flexible and complementary to existing technologies so that it can seamlessly integrate with global wireless technology and payments infrastructures. Unlike other solutions available in the mobile application market today, the platform is claimed to be designed to make it easier for Visa issuers, mobile operators and technology providers to deliver an intuitive and integrated consumer experience across a range of compelling services such as mobile contactless payments, remote payments, person-to-person payments, and mobile coupons, as well as account management services that enable consumers to better monitor account activity and manage their funds. The initial version of the platform launched at the beginning of 2007 offers solutions for contactless mobile payment, OTA personalization, coupons and direct marketing. Subsequent versions of the platform, to be made available later in the year 2007, will include solutions for remote payment and person-to-person payment.
  
- **PayPal Mobile payment solutions:** PayPal has announced at the end of 2006 its new mobile payment service, so-called Text2Buy, in the US. Similar to the Crandy NCS (UK, FR, BE, DE) and Luup (DK, NO, UK, DE) in Europe, the system concept consists in transferring money from a person's account to another person's account by using specific SMS numbers or to pay goods and services by SMS debited directly from a PayPal account. The system has encountered barriers from mobile telecom operators (e.g. Cingular from AT&T) that were already providing SMS+ as billing method for services like content services. Reasons were business model protection as PayPal proposed fees between 2 and 4% only compared to the existing fees of 30 to 40% for an equivalent service performance at AT&T, and the argument that massive usage of SMS by millions of PayPal clients on internet would induce costs for mobile operators that would not be reflected in PayPal fees. PayPal Mobile Checkout, a new version of the PayPal mobile (micro-) payment solution is expected to be proposed in 2007 to mobile internet users.

The following Mobile (Payment) Security Technique has been referenced by an interviewee in Sweden: the **WPKI project and infrastructure** aims to stimulate/enable a whole market of services that require a secure identification of the user and enables legally accepted electronic signatures. The involved parties are BankID (BID), all BID-banks, mobile operators (TeliaSonera, Tele2, Vodafone) and Ericsson.

#### 5.4.4 *Selection, Assessment and Analysis for the most used technical cashless payments*

With regards to mobile payments, the most used user authentication methods are related to the use of 2-factor authentication combining usage of a PIN-code and possession of the mobile device. However the sole reliance on the classic PIN-code protecting the mobile device is not to be considered sufficient to meet banking regulations “to know their customers”. To that extent, the best user identification / verification methods are based on the delivery and implementation of an additional PIN-code that is dedicated to the payment application available from the mobile device. The delivery of such a dedicated mobile payment PIN is processed through existing and secured electronic channels (e.g., through the use of bank card authentication in ATMs allowing mobile payment activation facilities) that were established based on a prior face-to-face authentication (e.g., opening of a bank account).

The required convergence and collaboration between financial services providers, mainly the banks, and the mobile operators is observed to either parcel out the market into multiple and often incompatible initiatives such as in France, or to federate the market around one (monopolistic) scheme as in Belgium.

In the context of mobile payment schemes, the best user identification and verification methods are based on the use of **2-factor authentication combining the possession of a (PIN-protected) mobile device and the use of a specific PIN code dedicated to the payment application** and delivered through a secure channel preferably established on a face-to-face authentication.

However, many of the most used m-payments means today stay based on a one-factor authentication method (e.g., SMS only based).

#### 5.4.5 *Facts and figures*

Since the market of m-payment is still in its early adoption and emergence phase, no significant figures can be given as representative.

#### 5.4.6 *Possible barriers to the implementation*

One observes a rather large number of trends in supporting technologies (e.g., NFC, sms-based, specific applications embedded in SIMs, migration of internet based solutions to mobile world, etc.) coupled with rather local or regional implementations with often significant differences between them. The market is clearly not stabilised yet.

The slow growth of m-payment may also be due to the volume of players in the mPayments space.

Barriers towards mobile payment from the user side (see WP2 for more details) are that people:

- are not knowing how to make mobile payments and the technology behind the application,
- do not have the necessary technology to make payments via the mobile,
- do not trust the technology behind the application (although the level of trust is higher when the transaction is PIN protected).

Low penetration of some devices (e.g. WAP enabled GSM (e.g. only 30% in France).) is noticed.

A last, but not least technical limitation is due to the fact that GSM battery must be loaded.

## 6. Emerging technologies

Besides security, “mobility”, “interoperability” and “multi-application devices” are the key words driving the future of cashless payments.

### 6.1 Mobile phone

Emerging technologies in the context of user authentication in electronic payments schemes are mainly related to the usage of mobile phones as part of a two-factor based authentication process. The noticeable element here is the combination of two Trusted Third Parties (TTPs). While normally payment schemes only rely on the Bank as the TTP, here an additional TTP, namely the Telecommunication Operator, is involved. The appearance of a new actor and the modification of the relationships and business models are one of the main challenges for the introduction of this new payment access channel. With the introduction of mobile phones, user verification for the payment transaction most often requires the presentation of a dedicated payment PIN. However, new user verification methods such as fingerprint are being investigated and start to be piloted.

### 6.2 eID cards

Besides the mobile phone, another new tool appears on the market to support user authentication, namely the electronic Identity (eID) card. Such eID cards have been or are being introduced in quite a number of European countries and hence, because of the widely spread, are becoming well-known to the citizens. Where in some countries the issuance for these eID cards is fully managed by the governments (acting as a TTP), in some cases, they result from Private-Public Partnerships (PPP) between banks and governments as issuing bodies, such as in Sweden, Estonia, or Luxembourg. As detailed in the “emerging technologies“ section, there is in this context, at least in some countries, a real interest of the banking sector to work with public authorities as close as possible on the topics of user authentication and e-signatures. In addition to the intrinsic added value with respect to security, the usage of eID cards can even be seen as a marketing advantage for the payment scheme providers (e.g., Keytrade bank). This is a rather new trend.

While perceived as interesting, eID based schemes are not yet an accepted alternative for authenticating users in the context of cashless payments (e.g., as authentication method in e-commerce). Some of the barriers identified can be listed as follows:

- Lack of cross-border PKI interoperability and mutual recognition,
- Lack of control on the registration and issuance process in countries where the banks are not part of the issuing process of eID cards
- Liability issues, there are questions about the split of liabilities and who will take up the fraud,
- Co-existence of the standards supporting the EU directive on Electronic signatures and standards adopted by the banking sector that both would need to be applied:
  - o ISO TC68 standards *versus* ETSI TSs;
  - o EMV cards specifications *versus* the different SSCD and eID related CWAs.

The liability issues could possibly be solved through legislation.

The Cross-border and mutual recognition issues should be tackled by 2010 within the i2010 programme.

As concluding words, and such as observed at recent conferences on this topic, it seems, at least in some countries, that there is a real interest from the banking sector to work with public authorities on matters of user authentication and e-signatures. More in particular the eID cards distributed and funded by the governments are powerful tools which are brought in the hands of all citizens which come “for free” from a banking perspective. This rather new trend should be closely followed by the European Commission. The topic is further elaborated in Annex 10.

### **6.3 Contactless techniques and proximity payments**

In the context of proximity payment, contactless techniques are emerging in the e-payments scheme landscape (examples are mainly based on NFC technology). Proximity payments are defined as those in which the local data exchange takes place between the customer handset and the terminal at the POS through Bluetooth, infrared and RFID. These technologies appear more and more in specific applications roadmaps (e.g., tele-payments for the highway fees).

It is important to note at this stage that these techniques, while very easy to use (for instance the user only has to wipe a card in front of a reader), have their limitations with respect to the type of payments it could be used for (small amounts). Indeed, because of the wireless technology it is possible to capture data from the card using powerful antennas without the user’s authorisation and or knowledge. Hence dedicated methods should be investigated to protect the contactless cards against these types of attacks (e.g., card shielding, card activation/deactivation, etc...).

Even more recent the so-called “display cards” have been prototyped which have a battery (next to the contact and contacless interfaces) and provide a small screen and a couple of push buttoms. These new features might become important to enhance the security for payments. As an example they would allow the user to verify the transaction amount on the screen and push a buttom for transaction confirmation to address the antenna attack mentioned above. However, first the trade-off issue between the price (mass production) and the enhanced functionality and security for these devices needs to be solved before real market introduction would be possible.

### **6.4 Biometry**

Biometry is currently in Europe not really used in the payment context and is not expected to be a relevant prospective method for authenticating users in the near future due to the lack of stability, difficulty of use, cost effectiveness, and mostly due to the lack of added value compared to existing solutions. Indeed, it does not offer new advantages to the payment schemes to solve the problem of user verification in an open and interfering environment, with no possibilities to select or educate users on the appropriate usage. However, in the more

distant future this might change. Already in Asia pilots are planned in rural areas where payments with a mobile phone with fingerprint will be considered as user verification methods. To what extent these solutions would also be adopted in Europe is very difficult to predict. Indeed, two main factors that are playing in Asia, namely the lack of banking infrastructure and the analphabetism, do not exist in Europe.

It is important to note (see also Annex 6), that biometric information on the user can only be used to replace *one* authentication factor (e.g., a fingerprint can replace a password); it is not a full authentication scheme. A solution solely based on biometry for authenticating users is not secure and biometry shall always be combined with a second factor (e.g., something the user has, such as a card). This is important since new schemes relying on biometry start to be deployed nowadays providing a sense of security caused by the “new look” technology. However, they require a correct implementation in combination with other security features such as a hardware token (e.g., solutions where a user provide his/her fingerprint without any other second authentication factor are dangerous since the fingerprint template may be easily copied and maliciously reused).

## **6.5 iDTV**

A new device that could become a support for e-payments is the interactive television (iDTV). However, it is expected that iDTV supported payments will be very similar to internet payments; i.e. same payments methods, and thus same user identification and authentication methods. Only the interfaces towards the user would be different, namely the iDTV instead of the classical browsers. For example, the credit card number would be submitted via the iDTV.

The iDTV authentication modules as such might also be used as authentication tool in the framework of e-payment. Technically speaking, there is indeed an authentication module within iDTV allowing further authorisation to access certain content according to the type of subscription of a particular user, but it seems that this authentication feature will not serve any other purposes, and e-payment in particular does not seem to be in the roadmap. However, since a set up box could be used as a payment terminal offering more security than an internet payment via a PC without a card reader, this possibility could be considered in the future.

## 7. Payment industry perception

### 7.1 Introduction

This section highlights the industry perception on the regulatory, contractual and commercial constraints on the usage of user verification methods. This is the result of a survey based on questionnaires (provided in Annexes 2 to 5) and of interviews that the authors had with different actors from the financial world. The questionnaires were intended to EPI Payment Scheme Providers, EPI Banks, Security & Technology Experts, and Technology Providers.

In general very little response was received in writing through these questionnaires. In total 47 interviewees from 13 European countries were contacted (17 EPI PSP, 7 EPI Banks, 11 STE, 13 TechProv). Only a few questionnaires have been fully answered. Some interviewees have indicated a delay in providing answers due to time and workload constraints and many of them responded that they were not entitled to answer because of confidentiality reasons. The security issues are a very sensitive problem in the financial world and stakeholders are quite reluctant in providing written information. However, the authors could meet and discuss with numerous persons from the financial world, including bank representatives or consumers associations.

With these good mix of interviewees addressed, it is hoped that to a large extend the relevant information has been collected. However, because of the different regulations and legislations, differences in payment products and their implementations and differences in banking environments throughout Europe, the results might not be a 100% representative for the entire financial sector in Europe.

### 7.2 Main results

The outcome of the questionnaires and interviews (with the necessary precaution due to the low number of responses) are largely confirming the “paper” based results. The following findings could be noted.

#### Authentication methods

- Two-factor authentication is the minimal level of authentication recommended for banking related electronic payments.
- Most frequently employed user authentication method is PIN based authentication while often combined with a “something you have” as an additional factor. Reasons for PIN being most used are mainly the ease of use, it is well understood and established, and there is remarkable little fraud with it and certainly not enough to create a sense of distrust.

- For card related payments, best used method is expected to be PIN supplemented by an additional “something you have” authentication factor in order to implement 2-factor authentication, generally based on PKI for interoperability reasons.
- Biometry is not currently used and is not expected to be a relevant prospective method for authenticating users in the near future due to lack of stability, difficulty of use, costs effectiveness, and mostly due to the fact that it does not provide added value compared to existing solutions. It seems not to address in an adequate manner the payment industry problem of user verification in a non specific context, in an open and interfering environment, with no possibilities to select or educate users for appropriate usage.
- eID is seen as an interesting while not yet an alternative for authenticating users, for example as authentication in 3D-Secure. However some questions (barriers?) are raised related to such usage of eID cards such as in countries where the banks are not part of the issuing process of eID cards, there are questions about the split of liabilities and who will take up the fraud. It is suggested that this could be solved through legislation. Cross-border and mutual recognition may also become issues.
- Digital signatures are cited but are mostly performed using a proprietary format, which means not necessarily complying with the standards set forth in the context of the Electronic Signature Directive.
- Mobile payments are emerging as/when they are based on the following features:
  - o implement the same level of security as with bank card schemes, at least when banks or payment institutions are taking part to the designed scheme,
  - o making use of PKI (e.g., WPKI)
  - o based on 2-factor authentication ( with specific PIN for payment application)
  - o requiring no connection to a computer or terminal device.
- Very limited information available on contactless used in Europe.

### **Need for harmonisation and certification of security tools.**

The financial industry wishes a high level of security. However, except for what can be derived from the Anti-money laundering Directive [8] in terms of registration, there is no legal framework today requiring specific security measures for e-payments. Actually, the Anti-money laundering directive does not *strictly speaking* impose particular security features on payment instruments, but the directive requires well the banks to “know their customers” and has thus implication on the requirement to "register" clients (a face to face is highly recommended). Clients’ registration is a crucial step for initiating any user’s authentication method and sustaining subsequent security measures. Nevertheless, there are already some schemes in place such as the BCE recommendations from 2003

that can be associated with the implementation of the Directive. Most of the recommendation criteria are based on assessments to be performed by Accreditation/Certification bodies. Some payment schemes such as Visa/Mastercard and some national schemes such as ZKA in Germany and CB in France also impose security evaluations.

In particular, for card payments, EPC has chosen to use smart-cards and follow largely the EMV standard, with as prior objective, having the same EMV based implementation European wide. Having a more harmonised way to organise authentication and security in general would certainly enhance the global level of security. It is important to note that **self regulation or regulation** through national and central banks is expected to be the **preferred** and best supervision model. From a risk and security point of view, overall policies are not always beneficial. However the European Commission is expected to play a role whenever there are any legal obstacles to obtain for instance interoperability.

The Fraud Prevention Expert Group (FPEG) advising the Commission has prepared a report providing an overview of the procedures used for the security evaluation of payment products and components (cards, terminals, software, etc.) in the European Union. The report recommends to harmonise at EU level the security procedures to evaluate the security of payment cards and terminals." You should then add a reference at the end of the paper to the report. You can get it from: [http://ec.europa.eu/internal\\_market/fpeg/work\\_en.htm](http://ec.europa.eu/internal_market/fpeg/work_en.htm), see [56].

### **Limitation of user responsibility – lack of incentive for due care of authentication credentials**

When looking at the article 50 of the Payment Services Directive [76], one clearly sees a limitation of the end-users responsibilities. This perception of protection can be seen as a positive signal to promote the use of cashless payments on one hand. However, on the other hand, this also leads to the consequence that end-users may be less concerned with security issues and become careless with their credentials.

This limitation on user responsibility has thus a positive aspect on the economical side by constituting an incentive to use e-payments, but at the same time has also a negative side regarding the user responsibility with respect to security. To struggle against that kind of behaviour, the user awareness/education is really important, as well as the possibility to sue fraudulent or even “bad” use of credentials.

### **The need for a reinforced legal framework**

The Payment Services Directive [76] specifies an incitation for the bank to increase the security of the e-transactions (e.g., sustaining authentication of each principals in a transaction) in support to a possible arbitration in a dispute or litigation. Also, the set-up and recognition of an appropriate framework for the accreditation/evaluation/certification of payment tokens and devices is important in the process of detecting fraud or solve disputes and liabilities. However, it is very important to support these technical security methods implemented by the financial sector by an appropriate legal framework to appropriately address fraud cases such as identity theft, counterfeit cards, etc...

Furthermore the victims of payment fraud should be adequately supported. Hereby not only the short term support via a dedicated declaration, investigation and communication processes should be addressed but also a legal framework should be created that recognises and addresses the possible long term financial impacts on the victims.

### **Ensure that the registration process is made with due care by the parties involved**

The weakest step in the authentication process has been clearly identified within this study as being the registration step. This is because all subsequent steps rely on this first crucial task: if someone manages to be enrolled under a fake identity, the registration process will furthermore reinforce the link between this person and its fake identity (by providing him/her with official credentials validating initially corrupted information).

It must be noted that in some cases, the legitimate owner of an identity may pretend to have been impersonated in order to repudiate a transaction. On the other side, it is also important to provide the user with means enabling him/her to prove that he/she has been abused (otherwise nobody will use his/her card anymore). In both cases, it is important to take care that the systems in place do not turn to some extent in means to sustain hackers. The vicious circle is that the more is imposed on “trusted-true ID”, the more it will become attractive for hackers to steal identities.

## 8. Conclusions and recommendations

Security has become a major cornerstone to circumvent cashless payment risks, essentially due to identity theft and/or transaction repudiation. The increase in fraud and in the skills and the organisation of the fraudsters is adequately addressed in a well balanced approach by the increase of the security level offered by the financial world for cashless payments.

In this perspective, user and data authentication are major e-security features. There is a convergence towards 2-factor based authentication methods, and in particular EMV authentication for card-based payments and/or e-banking transactions. Moreover, the financial sector organises itself to provide standards and recommendations (worldwide, EU-wide (e.g., EPC), nation-wide, ...).

Banks may also brand their security credentials (e.g., the EMV pinpad readers) to their logos to increase trust towards their customer by showing compliance to state of the art (security) technology.

The major goal of the present WP was to assess the most used user authentication methods for cashless payments (being card-, e- and m-payments) with the aim to identify the best ones. Conclusions and trends for each payment type are provided at the end of each of the sections in the present document. These conclusions are also gathered in the executive summary and are summarised below.

Potential barriers to the use of these best methods were highlighted along the document. Recommendations on possible ways to circumvent these barriers and the additional barriers raised from a user perception (see WP2) as well as the legal and regulatory barriers (see WP4) are provided in WP5 of the present study.

### 8.1 Most used and best user verification methods

#### Most used user verification methods

A major finding of the WP1 is that card payments are the most common way of paying in the European countries. This is not only true for card present payments (e.g., at a point of sales), but also for e-commerce (e.g., buying on the internet).

The **most frequently** employed user authentication method is password (e.g. PIN code) based authentication often combined with a “something you have” as an additional authentication factor. The (most used) password used in the specific case of card payment is a PIN code. Reasons for PIN being most used are: ease of use, well understood and established amongst users, and no sufficient fraud directly related to this verification method to create a sense of distrust.

### **Best user verification methods**

Regarding user verification, independently of the payment type (card, e- or m-payment), two-factor authentication is the **expected minimal level of authentication** for cashless payments. This is reflected by the security analysis and moreover re-enforced by the legal and regulatory framework. However, this does not mean that this level of security is commonly applied.

With respect to data authentication, a PKI-based signature is the ideal mechanism to support non-repudiation.

### ***Card payments***

The combination of the usage of IC Card technology allowing the dynamic authentication of the card at transaction time and of the provision of the card holder PIN code (as second authentication factor, is the best card holder authentication/verification method available today for card payments.

### ***E-banking***

Interestingly, there is a convergence of authentication methods in the e-banking environment towards 2-factor authentication methods. In particular, EMV authentication is more and more used.

In e-banking, the use of a PINPAD<sup>14</sup> reader producing a challenge-response signature based on the user's bank card seems to generalise. This observation is EU-wide and was quite expectable since there are standards that uniform such payments schemes. In particular, EMV authentication is more and more used and perceived as best user authentication method.

However, WP2 shows that the users prefer a static password for e-banking because of the convenience.

### ***E-commerce***

In the context of e-commerce and internet payment schemes, the TTP based payments schemes are better payments schemes from a security perspective than those not powered by an intermediary payment service provider:

- TTPs evolve towards the use of a dynamic factor
- Direct payments to merchants remain SSL based with a static factor (with no other authentication than the card related information accompanied by the request for the related CvX numbers).

Irrespective the payment scheme, from a security perspective, the best user verification methods rely on 2-factor authentication systems (e.g., user ID + password, whether static or dynamic combined with the possession of specific device, card or security software).

Irrespective the payments scheme, cards payments are not only used most frequently but also offer the best security. Card-based schemes whereby the card issuer authenticates the user are considered as the best payments schemes. In particular, an effective way of preventing the classical frauds linked to card-not-present is to use the EMV smart card authentication to perform user authentication or on line payment transaction authentication.

<sup>14</sup> The PINPAD reader is a smart-card reader with a dedicated keyboard enabling to enter securely the card PIN Code.

However, most of the payments schemes remain today on a “1-factor” authentication system (e.g., user ID + password).

### ***M-payments***

In the context of mobile payment schemes, the best user identification and verification methods are based on the use of 2-factor authentication combining the possession of a (PIN-protected) mobile device and the use of a specific PIN code dedicated to the payment application and delivered through a secure channel preferably established on a face-to-face authentication.

Along this e-payment authentication study, 2-factor based authentication methods have been identified as best authentication methods, independently of the e-payment type (e-, m-, or card-payments).

## **8.2 Emerging techniques**

Emerging security credentials such as eID cards, mobile phones and contactless cards are perceived to play a more important role in the near future in cashless payments (all devices are perfectly suited to support two-factor authentication schemes and in particular the first two are already in the hands of the consumers nowadays).

## **8.3 Barriers and recommendations**

Besides costs of implementation that should not be prohibitive, few barriers have been identified to the use of the here above presented best user authentication methods. However, the payment industry has raised some wishes:

- Need for harmonisation and certification of security tools
- The need for a reinforced legal framework
  - It is important to support the financial sector technical security means by a legal framework allowing adequate handling of fraudsters.
  - The appropriate regulation for the evaluation/certification of tools and products (see above) is considered to be important (certified applications are supposed to ease the detection of fraud as well as the determination of liabilities, see also below).
  - Appropriate support and legal framework for victims, including recognition of the financial impacts for the victims

Regarding the emergence of eID, liability and interoperability issues have been highlighted. Some liability issues would need to be solved (may be through legislation) and the cross-border and mutual recognition issues should be tackled by 2010 within the i2010 programme. Recommendation for this is developed in WP5.

Finally, e-commerce remains unfortunately basically tight to a low level of security, although pretty good techniques (similar to web-banking) exist to protect e-commerce transactions. Although important e-commerce stakeholders care about security, user authentication remains at a rather low level of security (e.g., most of the schemes are SSL based, with no other authentication than the card information + the related CvX numbers). Better techniques such as 3D Secure, potentially supported by EMV authentication, exist and shall be promoted.

## References

- [1] ANSI X9.8-1, 2003; Part 1: Personal Identification Number (PIN) Management and Security.
- [2] ANSI X9.84, 2003; Biometric Information Management & Security.
- [3] ANSI X9, TG-3-2006: Guideline for Financial Services - Retail Financial Services Compliance Guideline, On line PIN Security and Key Management
- [4] Directive 91/308/EEC of 10 June 1991 on the Prevention of the use of the financial systems for the purpose of money laundering, OJ L 166, 28.6.1991.
- [5] Commission Recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, OJ L 208, 02.08.1997.
- [6] Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures; OJ L 13, 19.1.2000.
- [7] Directive 2001/97/EC of 4 December 2001 amending Directive 91/308/EEC, OJ L 344/76, 28.12.2001.
- [8] Directive 2005/60/EC of 26 October 2005 on the Prevention of the use of the financial systems for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005.
- [9] ECBS EBS 100, 2004; Keyboard Layout for ATM and POS PIN Entry Devices.
- [10] ECBS EBS TR102, 2003; Overview of European Electronic Purse Products.
- [11] ECBS TR 410, 2002; Secure Card Payments on the internet.
- [12] ECBS TR 410 Addendum, 2003; Secure Card Payments on the internet.
- [13] ECBS TR 411, 2004; Security Guidelines for Electronic Banking.
- [14] ECBS EBS TR 601, 2001; EEBSF - European Electronic Banking Standards Framework.
- [15] ECBS EBS TR 603, 2003; Business and Functional Requirements for Mobile Payments.
- [16] ECBS EBS IG 606, 2005; Implementation Guidelines for Electronic Payments.
- [17] EMV Card Personalization Specification (CPS); version 1.1, 2006.
- [18] EMV Common Payment Application Specification (CPA); version 1.0, 2005.

- [19] EMV Contactless Specifications for Payment Systems; version 1.1., 2006.
- [20] EMV Integrated Circuit Card Specifications for Payment Systems; version 4.1, 2004.
- [21] ETSI TS 101 456, 2002; Policy requirements for certification authorities issuing qualified certificates.
- [22] ISO/IEC 7810, 2003; Information technology -- Identification cards – Physical characteristics.
- [23] ISO/IEC 7813: 2006; Information technology -- Identification cards -- Financial transaction cards.
- [24] ISO/IEC 7816-1, 1998; Information Technology - Identification cards -- Integrated circuit(s) cards with contacts – Part 1: Physical characteristics.
- [25] ISO/IEC 7816-2, 2007; Information Technology - Identification cards -- Integrated circuit(s) cards – Part 2: Cards with contacts - Dimensions and location of the contacts.
- [26] ISO/IEC 7816-3, 2006; Information Technology - Identification cards -- Integrated circuit(s) cards – Part 3: Cards with contacts - Electrical interface and transmission protocols.
- [27] ISO/IEC 7816-4, 2005; Information Technology - Identification cards -- Integrated circuit(s) cards – Part 4: Organization, security and commands for interchange.
- [28] ISO/IEC 7816-8, 2004; Information Technology - Identification cards -- Integrated circuit(s) cards – Part 8: Commands for security operations.
- [29] ISO/IEC 7816-11, 2004; Information Technology - Identification cards -- Integrated circuit(s) cards – Part 11: Personal verification through biometric methods.
- [30] ISO 9564–1: 2002; Banking – Personal Identification Number management and security, Part 1: basic principles and requirements for on line PIN handling in ATM and POS systems
- [31] ISO 9564–2: 2005; Banking - Personal Identification Number management and security, Part 2: Approved algorithm(s) for PIN encipherment
- [32] ISO 9564-3: 2003; Banking – Personal Identification Number management and security – Part 3: Requirements for offline PIN handling in ATM & POS systems.
- [33] ISO TR 9564-4: 2004; Banking – Personal Identification Number management and security – Part 4: Best practices for PIN handling in open network environments.
- [34] ISO 13491-1: 2007; Financial services – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods.
- [35] ISO 13491-2: 2005; Financial services – Security compliance checklists for devices used in financial transaction environments.

- [36] T. Dierks and C. Allen, *The TLS protocol version 1.0*, RFC 2246 – internet Engineering Task Force, January 1999.
- [37] SET Standard Technical Specifications, Books 1, 2 and 3 available at [www.setco.org](http://www.setco.org).
- [38] SPA and UCAF Detailed Specification version 1.0, MasterCard International, June 2001.
- [39] 3-D Secure Protocol Specification – Core Functions version 1.0.2, Visa International, July 16, 2002.
- [40] A. J. Menezes, P. C. van Oorschot and S .A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
- [41] Mudge and Kingpin, *Initial Cryptanalysis of the RSA SecurID algorithm*, January 2001.
- [42] I. C. Wiener, *SecurID Token Emulator with Token Secret Import*, December 2000.
- [43] MasterCard International, *MasterCard SecureCode™ – MasterCard and Maestro enrollment and implementation guide*. December 2002.
- [44] Study on the Security of Payment Products and Systems in the 15 Member States Internal Market DG (Contract No. ETD/2002/B5-3001/C/11) - Final Report (Tony Hegarty PwC Luxembourg (Part 1 and Editor), Eric Verheul PwC Netherlands (Part 2), Dirk Steuperart PwC Belgium (Part 3), Georgia Skouma Bogaert & Vandemeulebroeke (Part 4))
- [45] Study on the Security of Payment Products and Systems in the 15 Member States Internal Market DG (Contract No. ETD/2002/B5-3001/C/11) – Key Conclusions Accountis Press Release ; Accountis Web E-Payments Platform
- [46] Carte de crédit sur internet – [www.cec.belgique](http://www.cec.belgique), 03042007
- [47] Acheter sur internet, European Consumer Centre (commerce électronique internet, F. Basseres)
- [48] Les enjeux du paiement sécurisé pour la vente à distance et le e-commerce, Paris, 15 novembre 2005, Jean-Pierre Buthion, Groupement des Cartes Bancaires
- [49] The European On line Marketplace: Consumer Complaints 2005, *A summary and analysis of consumer complaints reported to the European Consumer Centre Network*, report coordinated and written by the ECC offices on behalf of the European Consumer Centre Network
- [50] Financial Action Task Force, Groupe d'action financière, report on new payment methods, 13 October 2006
- [51] Commission staff working document; “The application of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering in relation

to the identification of clients in non-face to face transactions and possible implications for electronic commerce, Brussels, 19.12.2006, SEC(2006) 1792

[52] Recommandation de la Commission du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire (Texte présentant de l'intérêt pour l'EEE) (97/489/CE)

[53] ID Theft report\_draft\_200704\_version FPEG subgroup\_1 DEPUIS MIS à JOUR (REPORT ON IDENTITY THEFT/FRAUD, FRAUD PREVENTION EXPERT GROUP1, Brussels, 22 October 2007, [http://ec.europa.eu/internal\\_market/fpeg/index\\_en.htm](http://ec.europa.eu/internal_market/fpeg/index_en.htm))

[54] The President's Identity Theft Task Force; "Combating IDENTITY THEFT » Volume II: Supplemental Information April 2007

[55] The President's Identity Theft Task Force; "Combating IDENTITY A Strategic Plan" April 2007

[56] The Fraud Prevention Expert Group (FPEG) report providing an overview of the procedures used for the security evaluation of payment products and components (cards, terminals, software, etc.) in the European Union.  
[http://ec.europa.eu/internal\\_market/fpeg/work\\_en.htm](http://ec.europa.eu/internal_market/fpeg/work_en.htm)

[57] SEC(2006) 104, Commission staff working document on the Review of the E-Money Directive (2000/46/EC), Brussels, 19.07.2006

[58] Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 97/7/EC, 2000/12/EC and 2002/65/EC

[59] Brussels, 20.10.2004, COM(2004) 679 final Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol, A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment

[60] Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment instruments and in particular the relationship between holder and issuer, Call for Tender XV/99/01/C FINAL REPORT – Part a) and b) 17th April 2001

[61] Presentations from the European conference "Maintaining the integrity of Identities and Payments - Nov 2006"MM; Aghroum, Anderson, Ates, Chaudun, Langeheine, Verwoerd, McCreevy, Pardos, Ratzel, Ravoet, Vulpiani, Wabnitz, Webb

[62] Application of the e-money Directive to mobile operators, Guidance note from the commission Services

[63] Application of the E-money Directive to mobile operators, Summary of replies to the Consultation paper of DG Internal Market

[64] Towards a Single Euro payments area Objectives and deadlines, Fourth progress Report - February 2006

[65] The Eurosystem's vision for SEPA (Single European Payments Area)

[66] SEPA brochure (2006)

[67] The Eurosystem's view of a "SEPA for cards", European Central Bank

[68] Electronic money System security Objectives, According to the common Criteria methodology May 2003, European Central Bank

[69] World Payments REPORT \_ 2006, Cap Gemini, ABN Amro, EFMA

[70] ESTA Biz (The Cash Logistic Industry Association - European Security Transport Association, rue Dieudonné Lefèvrestraat 252, 1020 Brussels, Belgium) Documents amongst which:

- Card Fraud in Europe - v8
- Cash in Europe - campaign\_for\_cash\_backgrounder\_210906
- ESTA response to SEPA consultation
- Standardization in Europe (David Milner Euricpa)
- Cash in Europe
- Cash substitution, issues & implications

[71] Service Description from PayPal ([www.paypal.com](http://www.paypal.com))

[72] Secure internet Banking Authentication, Alain Hiltgen UBS AG, Thorsten Kramp IBM Zurich Research Laboratory, Thomas Weigold IBM Zurich Research Laboratory, Submitted to *IEEE Security & Privacy*, March 15, 2005

[73] Financial Action Task Force, Groupe d'action financière, GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING, *High Level Principles and Procedures* JUNE 2007

[74] Payment Card Industry (PCI) POS PIN Entry Device Security Requirements, Version 2, 2007.

[75] Payment Card Industry (PCI) Encrypting PIN Pad Security Requirements, Version 2, 2007.

[76] "Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 97/7/EC, 2000/12/EC and 2002/65/EC". (NOTE: at the moment of the edition of this study, the draft payment directive is on the point to be published. The reader shall be attentive to the fact that the numbering of the referred article may change)

**Information from websites:**

CAS: [www.berlin-group.org](http://www.berlin-group.org)

EMVCo: [www.emvco.com](http://www.emvco.com)

PCI : [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

Ogone: [www.ogone.com](http://www.ogone.com)

EPC: [www.europeanpaymentscouncil.eu](http://www.europeanpaymentscouncil.eu)

## Abbreviations

ATM: Attended Terminal Machine  
CSP: Certificate Service Provider  
CvX(2): (2 stands for second) Card Verification (x stand for value” or “code” according to VISA or Mastercard wording)  
CWAs: CEN Workshop Agreement (**CEN**, the European Committee for Standardization)  
eID: Electronic Identity Card  
EMV: Europay – Master Card- Visa  
EPI: Electronic Payment Instruments  
F2F: face to face  
GSM: Global System for Mobile Communications  
IC Card: Integrated Chip Card  
iDTV: Interactive Digital Tele vision  
mag-stripe: magnetic stripe  
MSP: Mobile Services Providers  
OTP: One-Time Password  
PDAs: Portable Devices  
PIN: Personal Identification Number  
PKI: Public key Infrastructure  
PSPs: Payment service providers  
QES: Qualified Electronic Signature  
RFID: Radio Frequency Identification  
SEPA: Single European Payments Area  
SSL: Secure Socket Layer  
TTPs: Trusted Third Parties  
url: Uniform Resource Locator  
WAPs: wireless application protocols

### In Annexes:

CAs : Certification Authorities  
OIDs: Object Identifiers  
(S)SCDs: (Secure) Signature Creation Devices