

WP1 E-Payment Authentication Study - Final Deliverable - Annexes

**Version number: v0.7
Date: 30/10/2007**

TABLE OF CONTENT

ANNEX 1	WP1 METHODOLOGY	3
ANNEX 2	WP1 - EXPERTS AND INDUSTRY - EPI PROVIDERS - BANKS QUESTIONNAIRES	
V1.0	8
ANNEX 3	WP1 - EXPERTS AND INDUSTRY - EPI PROVIDERS - PAYMENT SCHEMES	
PROVIDERS QUESTIONNAIRES V1.0.....		17
ANNEX 4	WP1 - EXPERTS AND INDUSTRY - SECURITY & TECHNOLOGY EXPERTS	
QUESTIONNAIRES V1.0.....		25
ANNEX 5	WP1 - EXPERTS AND INDUSTRY - TECHNOLOGY PROVIDERS QUESTIONNAIRES	
V1.0	33
ANNEX 6	USER VERIFICATION AND USER AUTHENTICATION METHODS.....	39
ANNEX 7	EMV CHIP CARD AUTHENTICATION METHODS	74
ANNEX 8	USER AUTHENTICATION TO E-PAYMENTS METHODS ANALYSIS	76
ANNEX 9	M-PAYMENTS RELATED TECHNIQUES: MOBILE SECURITY BASICS AND	
MOBILE PAYMENT SECURITY TECHNIQUES		99
ANNEX 10	BANKS AND EIDS CARDS SCHEMES	103

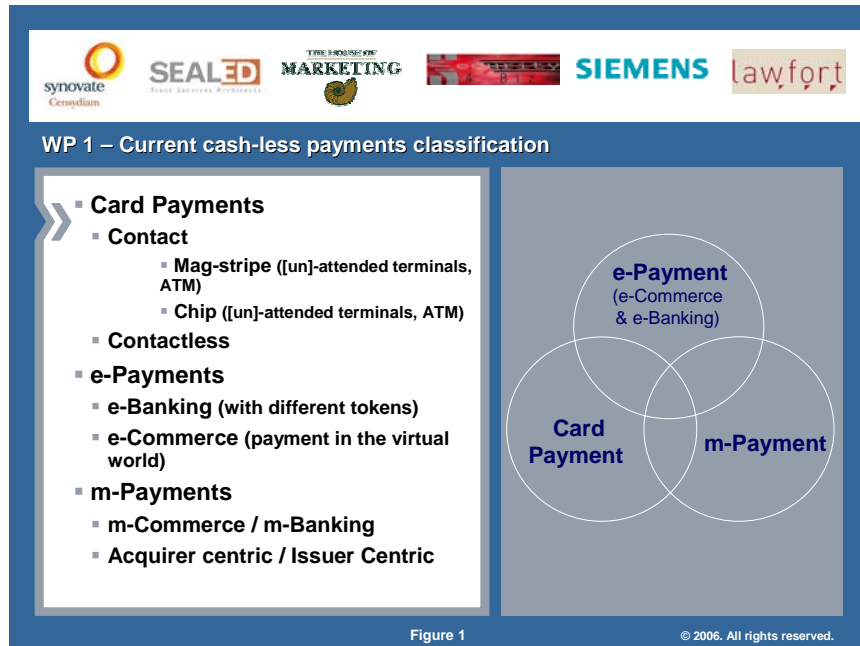
ANNEX 1 WP1 Methodology

In addition to the information available to the WP1 Team of Experts, and the results of WP2 on “User assessment”, the analysis performed during WP1 also takes into account Payment Industry and Experts information collected through interviews. These interviews specifically targeted three groups:

- **Security & Technology Experts** while focusing on the user/card holder verification method and security aspects,
- **Leading Payment Providers and Banks**
- **Technology Providers** mainly to collect valuable information on the prospective solutions.

ANNEX 1.1. Studied Payment Methods

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



Way of working and detailed methodology for User Identification / Verification methods analysis

Figure 2 depicts the detailed methodology that was used in WPI in order to perform the assessment and analysis of the User identification/verification methods (here after called “Authentication Methods”) in card, e-, and m-payments.

The first step consists in defining and classifying (listing) the different techniques and methods used to authenticate users. Authentication Methods are not restricted to the 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 depends 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.

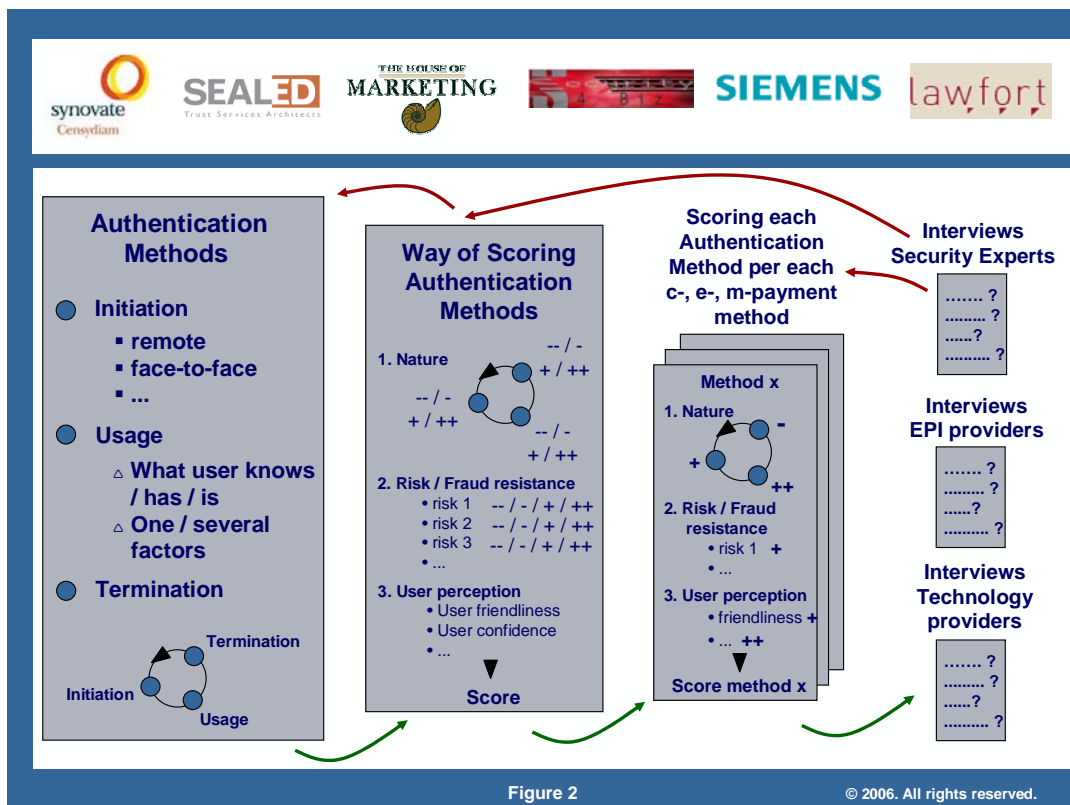


Figure 2

The second step consists in defining a way to score any authentication method that is applied to any card-, e-, or m-payment method. The scoring matrix first takes into account the nature of the authentication method and scoring each life-cycle step (initiation, usage and termination). Authentication methods are then also scored against their resistance to risks and frauds. Finally they are scored against their user perception (e.g., user friendliness, user confidence).

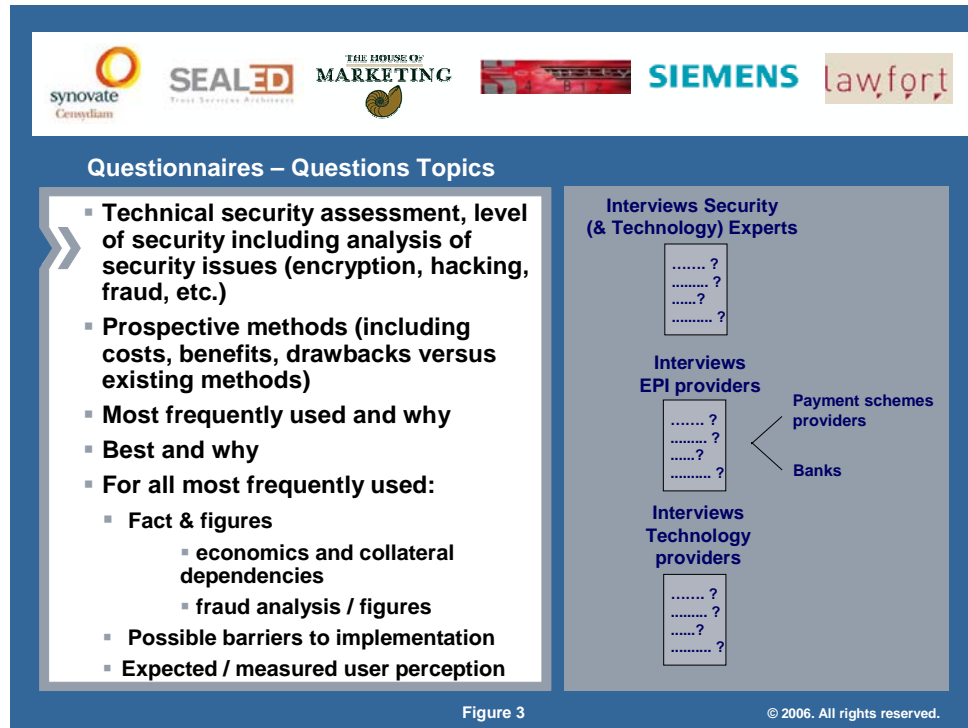
The third step consists in scoring each Authentication Method per each card-, e-, and m-payment method. Each of these payment methods is then scored against its nature, resistance to risk and frauds, and user perception.

In order to meet the objectives of the WP1, i.e.:

- providing an assessment on the (existing or prospective) level security of each verification method covered, including an analysis of issues such as encryption, protection against data hacking, etc,
- outlining the cost/benefits/drawbacks of new solutions over existing systems,
- further providing information on which of the existing methods are the most used, their actual protection against certain fraud types, the potential barriers regarding the use of these techniques and their economics and collateral dependencies,

The **next step** consists in collecting information, confirmation from a panel of experts and industry principals in the payment sector.

The questionnaire(s) have been organised around the following topics to maximise the collection of relevant information from the three groups of interviewees (i.e., Security & Technology Experts, Payment Schemes Providers and Banks, and Technology Providers):



As illustrated in Figure 2, the conduction of the interviews as supported by the questionnaires serves to complete the scoring of each User Authentication Method for each existing and prospective card-, e-, and m-payment methods, focusing on the most used. This process may also lead to the further refining of the Authentication Method list and the scoring matrix.

The blank questionnaires are provided in Annexes [A2], [A3], [A4] and [A5].

The collection and intake-of existing documentations, as well as the information collected from the Payment Industry, Security Experts, technology providers, banks and payment scheme providers enables the assessment structured per card /electronic / mobile payment method, per existing / perspective user authentication method, for each user authentication method on the following issues:

- Presentation of the user authentication method
- Security Level of the user authentication method (according to the methodology presented in the draft questionnaire document)
- Payment Industry perception on regulatory, contractual and commercial constraints – in function of the collected information from Industry & Experts
- Most used characteristic of the covered authentication method – depending on collected information from Industry & Experts
- Payment Industry feedback on user perception – in function of the collected information from Industry & Experts
- [Prospective] High level cost/benefit/drawbacks analysis versus existing methods – in function of the collected information from Industry & Experts

ANNEX 1.2. Scoring methodology

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

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

The following scoring matrix has been used in the context of the present study:

	Initiation	Usage	Termination	Risk & Fraud resistance	User perception
Authentication method X in card-, e-, or m-payment method Y	<ul style="list-style-type: none"> - Generation - Registration - Delivery - Storage & Access 	<ul style="list-style-type: none"> - Number of factors - Factor properties - Mechanism security 	<ul style="list-style-type: none"> - Termination 	<ul style="list-style-type: none"> - Risk 1 - Risk 2 - Risk 3 - ... - Risk n 	<ul style="list-style-type: none"> - Friendliness - Ease of use - Confidence - ...
...					
...					

Scoring per sub-category shall be granted amongst the following values: -- / - / + / ++

Value	Definition
++	Excellent, capable of meeting all objectives.
+	Good.
-	Insufficient but with limited possibilities for exploitation of the drawbacks/flaws
--	Critically flawed.

ANNEX 2 WP1 - Experts and Industry - EPI Providers - Banks questionnaires v1.0

ANNEX 2.1. Introduction

WP1 Objective

The objective of the European Commission study on User identification methods in card payments, mobile payments and e-payments is to analyse current and prospective **cardholder verification methods** on card payments, as well as **user verification methods** on e-payments and mobile payments. More in particular an assessment is to be made on the security provided and the user-friendliness, next to an analysis of possible regulatory, commercial and contractual barriers related to the use of best technologies.

The objective of the work package WP1 is to analyze current and prospective cardholder verification/authentication methods on card payments, as well as user verification methods on e-payments and mobile payments. It will provide an assessment on the (existing or prospective) level security of each verification method covered. This will include an analysis of topics such as encryption, protection against data hacking, etc. The analysis of new solutions will outline the cost/benefits/drawbacks over existing systems. The assessment will be presented by type of electronic payment and by type of technical solution. The assessment will further provide information on which of the existing methods are the most used, their actual protection against certain fraud types, the potential barriers regarding the use of these techniques and their economics and collateral dependencies. The analysis will be structured by technical method, within the payment method type (card, e- or m-payment).

WP1 Methodology

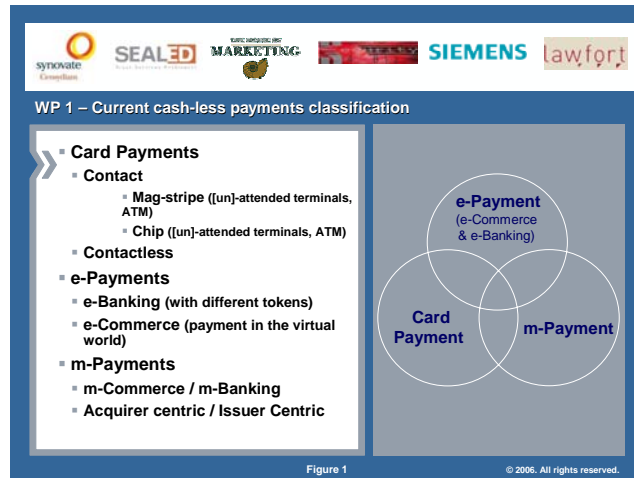
In addition to the information available to the WP1 Team of Experts, and the results of WP2 on “User assessment”, the analysis performed during WP1 shall also take into account Payment Industry and Experts information collected through interviews. These interviews will specifically target three groups:

- **Security & Technology Experts** while focusing on the user/card holder verification method and security aspects,
- **Leading Payment Providers and Banks**
- **Technology Providers** mainly to collect valuable information on the prospective solutions.

Studied Payment Methods

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

VERSION 0.7



ANNEX 2.2. EPI Providers Questionnaire - Banks

Interviewee Administrative Details

Please complete the following information:

Name of organisation/company, incl. website	
Name of contributor(s) to this Questionnaire	
Professional title / position with company	
Address	
Telephone	
Fax	
e-mail	

* Please include names and personal details of all persons having replied.

N.B.! You are invited to indicate (by ticking in the appropriate box) if you agree with the following:

YES	NO	You accept that your feedback to this Questionnaire becomes publicly available.
YES	NO	You accept that your personal name and the name of your organisation are included in the list of the entities having taken part in this survey (“list of survey participants”)
YES	NO	Please indicate if any information you provide in the Questionnaire should be treated as confidential information and, therefore, should not be published. If this is the case, please indicate the Question(s) for which we should treat your answer as confidential.

VERSION 0.7

	Question(s) n°.....
--	---------------------

Your organisation's/company's profile, area of business and activities
Answer:
Your organisation's/company's relation (and role) to card-, e-, or m-payment industry/technology
Answer:

Technical security assessment of existing methods

<p>1) For the existing payment methods (see section 1.3) can you comment on security issues (encryption, hacking, fraud, etc.) related to the associated authentication method(s) (including per authentication method lifecycle step – initiation, usage, termination), per payment method?</p>
<p>Answer:</p>
<p>2) It is likely that the implemented user authentication method is a compromise in terms of security, user convenience, risks and business objectives. What were the main barriers towards an improved security in terms of user authentication method?</p>
<p>Answer:</p>
<p>3) If Users possess different banking cards, do they put all PINs to the same values? Does your bank provide warning not to do so? Do you distribute anything to help the Users to remember their PIN? Where do they usually store the PIN values?</p>
<p>Answer:</p>
<p>4) In case several applications reside on the card is it acceptable that they have different PINs (a PIN is to be entered in the payment terminal after selection of the application debit, loyalty, etc...in other words, whence the user has chosen the application)?</p>
<p>Answer:</p>
<p>5) Do you have problems reported by Users caused by giving their card(s) to relatives (e.g. children) or friends with the PIN for a purchase or cash retrieval on your behalf?</p>
<p>Answer:</p>
<p>6) Do Users sometimes ask the banks to issue a kind of de-blocking PIN in analogy to the PUK of the GSM cards or will they loose the PUK anyway?</p>
<p>Answer:</p>
<p>7) With regards to e-commerce and e-banking what are the user authentication solutions that would worth to be harmonised and whether this would be desired or not? Are/were there plans towards such directions? Which barriers were encountered?</p>
<p>Answer:</p>

VERSION 0.7

8) With regards to m-commerce and numerous emerging initiatives in this area (e.g., sms based payments for parking, public transport but also GSM to GSM, and VISA mobile payment), User authentication seems to be reduced to PIN code and possession of a sometimes special type of SIM card. What are the security issues related to User authentication? What additional services or measures can be taken into account to increase authentication certainty and/or to reduce risks? How are the possible frauds and risks mitigated? How can Users be protected against abuses? Are there any proofs of User authentication related to performed payments? In particular with regards to <i>initiation</i> and <i>termination</i> steps of authentication methods.
Answer:
9) What are your commitments / procedures in terms of user identification / verification and in particular with regards to credential allocation? In case you need to strongly identify the user prior credential allocation and check the unambiguous link between credential and user, are you legally obliged to do so?
Answer:
10) Is user convenience (always) in contradiction with security? Can you comment? Do you see methods covering both aspects?
Answer:

Prospective user identification/verification methods

11) To what extent will government meet banking i.e., will or may e-Identity cards be used for identification purposes for payment transactions. What are here the legal or contractual barriers including the Trusted Third Parties involved (e.g. certificate issuers), the “liability” issues, insurance coverage, data privacy, etc.
Answer:
12) Usage of such eID authentication tools certainly implies a shift of ownership, liability and control about provisioning of such tools (e.g., eID issuing government). Are the differences in terms of usual commercial or contractual liabilities in contracts between banks and users, and use of eID card as authentication tool in e-banking?
Answer:
13) If mobile phones were to replace plastic cards for payments, what would be your assessment with respect to user identification/verification method (taking into account every step in authentication method lifecycle – initiation, usage, termination)?

VERSION 0.7

Answer:
14) What is your assessment with respect to user verification in the context of contactless and proximity payment technologies? What would be the preferred technology? Do you have experience in certain countries?
Answer:
15) Do you have knowledge of other prospective User authentication methods and/or new form factors?
Answer:
16) For the prospective user identification/verification methods can you inform us about costs, benefits, drawbacks versus existing authentication methods?
Answer:
17) For the prospective user identification/verification methods, can you comment on the security level (esp. compared to the classical methods)?

Most used user identification/verification methods

18) According to you what are the most frequently used user identification/verification methods and why? For these most frequently used methods, can you provide information on <ul style="list-style-type: none">○ economics and collateral dependencies○ fraud analysis / figures
Answer:

Best methods

19) According to you what are the best authentication/identification methods and why?
Answer:

Possible barriers to implementation

20) Do you see any barrier to implementation of authentication/identification methods and why?
Answer:

VERSION 0.7

21) In particular do you see any barrier to implementation of the – according to you – best authentication/identification methods and why?
Answer:
22) Are you subject to any legal liability rules for user identification? Do you experience contractual issues that you feel may hinder the use of certain technologies related to user identification/verification?
Answer:

Expected / measured user perception

23) What are the expected / measured user perceptions related to existing / prospective user identification/verification methods you can provide information on?
Answer:
24) How well are users informed about the security issues related to user identification/verification e.g., PIN handling, authentication device for home banking, sms or mobile security. Does your bank issue special User manuals/leaflets to create awareness in this area?
Answer:
25) Do you encounter User complaints in this area e.g., with authentication for home banking, PIN, etc...?
Answer:
26) Are your Users interested in multi-application cards such as debit/purse/loyalty or do they prefer different cards?
Answer:
27) Have Users the same trust in using the bank card at an ATM abroad as in their home country. If not, why?
Answer:
28) Which ATMs do Users use more often? Inside banks, outside for convenience etc...?
Answer:

VERSION 0.7

29) In most of the countries the PIN is not used for a purchase with an e-purse. Is this perceived by the users as less secure or do they prefer the convenience of it?
Answer:
30) Do Users perceive a debit card (such as Maestro, VisaElectronic) or a credit card of the same security level?
Answer:

Other questions

31) To what extent are regulations such as liability shifts a good instrument to enhance the introduction of stronger User identification/authentication?
Answer:
32) To what extent can you enhance their User verification/authentication?
Answer:
33) To what extent is it (not) important to have common requirements/specifications for User verification/authentication? Is this an area for possible competition between banks and their products or should there be a common approach for reasons such as interoperability (of terminal basis) or User friendliness. To what extent are you willing as a bank to accept a common /standardised / EU harmonised approach?
Answer:
34) What are the main incentives for you as a bank to have enhanced user verification/authentication methods (e.g. fraud too high, bad press, etc.)?
Answer:
35) Will SEPA have an influence on the Users, more in particular on the identification/verification of Users?
Answer:
36) What is your view on the role of the European Commission in the matter of User verification/authentication? Should they work on policies in this area?
Answer:
37) Please add any information you consider useful in the context of this questionnaire.

VERSION 0.7

Answer:

ANNEX 3 WP1 - Experts and Industry - EPI Providers - Payment Schemes Providers questionnaires v1.0

ANNEX 3.1. Introduction

ANNEX 3.1.1 WP1 Objective

The objective of the European Commission study on User identification methods in card payments, mobile payments and e-payments is to analyse current and prospective **cardholder verification methods** on card payments, as well as **user verification methods** on e-payments and mobile payments. More in particular an assessment is to be made on the security provided and the user-friendliness, next to an analysis of possible regulatory, commercial and contractual barriers related to the use of best technologies.

The objective of the work package WP1 is to analyze current and prospective cardholder verification/authentication methods on card payments, as well as user verification methods on e-payments and mobile payments. It will provide an assessment on the (existing or prospective) level security of each verification method covered. This will include an analysis of topics such as encryption, protection against data hacking, etc. The analysis of new solutions will outline the cost/benefits/drawbacks over existing systems. The assessment will be presented by type of electronic payment and by type of technical solution. The assessment will further provide information on which of the existing methods are the most used, their actual protection against certain fraud types, the potential barriers regarding the use of these techniques and their economics and collateral dependencies. The analysis will be structured by technical method, within the payment method type (card, e- or m-payment).

ANNEX 3.1.2 WP1 Methodology

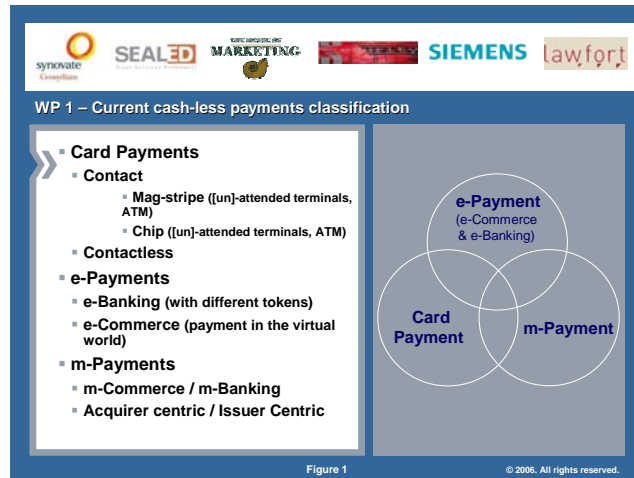
In addition to the information available to the WP1 Team of Experts, and the results of WP2 on “User assessment”, the analysis performed during WP1 shall also take into account Payment Industry and Experts information collected through interviews. These interviews will specifically target three groups:

- **Security & Technology Experts** while focusing on the user/card holder verification method and security aspects,
- **Leading Payment Providers and Banks**
- **Technology Providers** mainly to collect valuable information on the prospective solutions.

ANNEX 3.1.3 Studied Payment Methods

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

VERSION 0.7



ANNEX 3.2. EPI Providers Questionnaire - Payment Schemes Providers

Interviewee Administrative Details

Please complete the following information:

Name of organisation/company, incl. website	
Name of contributor(s) to this Questionnaire	
Professional title / position with company	
Address	
Telephone	
Fax	
e-mail	

* Please include names and personal details of all persons having replied.

N.B.! You are invited to indicate (by ticking in the appropriate box) if you agree with the following:

YES	NO	You accept that your feedback to this Questionnaire becomes publicly available.
YES	NO	You accept that your personal name and the name of your organisation are included in the list of the entities having taken part in this survey (“list of survey participants”)
YES	NO	Please indicate if any information you provide in the Questionnaire should be treated as confidential information and, therefore, should not be published. If this is the case, please indicate the Question(s) for which we should treat your answer as confidential.

VERSION 0.7

	Question(s) n°.....
--	---------------------

Your organisation's/company's profile, area of business and activities
Answer:
Your organisation's/company's relation (and role) to card-, e-, or m-payment industry/technology
Answer:

Technical security assessment of existing methods

18) For the existing payment methods (cfr section 1.3) can you comment on security issues (encryption, hacking, fraud, etc.) related to the associated authentication method(s) (including per authentication method lifecycle step – initiation, usage, termination), per payment method?
Answer:
19) It is likely that the implemented user authentication method is a compromise in terms of security, user convenience, risks and business objectives. What were the main barriers towards an improved security in terms of user authentication method?
Answer:
20) What is the position of your organisation with regards to the introduction of multi-application cards for payment applications only?
Answer:
21) To what extend is EMV CAP available as “universal” authentication method for different payment products. To what extend is it being introduced by banks and used by Users?
Answer:
22) To what extend does your organisation play a role in improving current User verification methods (e.g. PIN shielding at ATMs, physical requirements for ATMs)? Is a vendor approval programme in place to evaluate their products in that respect? If yes, what was the incentive to do it and does it prove to be useful in enhancing the security around user identification/verification?
Answer:
23) Bank PINs are in most cases limited to 4 digits although the ISO standard allows longer ones. Are there any plans to move to longer PIN codes. Are some banks doing it in specific geographical areas/ for certain products?
Answer:
24) Have you ever considered with your banks the introduction of a PUK, a deblocking PIN for payment cards?
Answer:
25) With regards to e-commerce and e-banking what are the user authentication solutions that would worth to be harmonised and whether this would be desired

VERSION 0.7

<p>or not? Are/were there plans towards such directions? Which barriers were encountered?</p>
<p>Answer:</p>
<p>26) With regards to m-commerce and numerous emerging initiatives in this area (e.g., sms based payments for parking, public transport but also gsm to gsm, and VISA mobile payment), User authentication seems to be reduced to PIN code and possession of a sometimes special type of SIM card. What are the security issues related to User authentication? What additional services or measures can be taken into account to increase authentication certainty and/or to reduce risks? How are the possible frauds and risks mitigated? How can Users be protected against abuses? Are there any proofs of User authentication related to performed payments? In particular with regards to <i>initiation</i> and <i>termination</i> steps of authentication methods.</p>
<p>Answer:</p>
<p>27) What are your commitments / procedures in terms of user identification / verification and in particular with regards to credential allocation? In case you need to strongly identify the user prior credential allocation and check the unambiguous link between credential and user, are you legally obliged to do so?</p>
<p>Answer:</p>
<p>28) Is user convenience (always) in contradiction with security? Can you comment? Do you see methods covering both aspects?</p>
<p>Answer:</p>

Prospective user identification/verification methods

<p>29) What is your approach with respect to new technologies for user verification? In particular such as biometrics? What would be the preferred technology? Do you have experience in certain countries?</p>
<p>Answer:</p>
<p>30) To what extend could e-Identity cards play a role for User identification in for instance electronic banking?</p>
<p>Answer:</p>
<p>31) Usage of such eID authentication tools certainly implies a shift of ownership, liability and control about provisioning of such tools (e.g., eID issuing government). Are the differences in terms of usual commercial or contractual liabilities in contracts between banks and users, and use of eID card as</p>

VERSION 0.7

authentication tool in e-banking?
Answer:
32) If mobile phones were to replace plastic cards for payments, what would be your assessment with respect to user identification/verification method (taking into account every step in authentication method lifecycle – initiation, usage, termination)?
Answer:
33) What is your approach on the usage of contactless cards?
Answer:
34) What is your assessment with respect to user verification in the context of contactless and proximity payment technologies? What would be the preferred technology? Do you have experience in certain countries?
Answer:
35) Do you have knowledge of other prospective User authentication methods and/or new form factors?
Answer:
36) Are the prospective payment methods always associated to prospective authentication methods? And vice versa?
Answer:
37) For the prospective user identification/verification methods can you inform us about costs, benefits, drawbacks versus existing authentication methods?
Answer:
38) For the prospective user identification/verification methods, can you comment on the security level (esp. compared to the classical methods)?

Most used user identification/verification methods

22) According to you what are the most frequently used user identification/verification methods and why? For these most frequently used methods, can you provide information on <ul style="list-style-type: none"> o economics and collateral dependencies o fraud analysis / figures
Answer:

VERSION 0.7

--

Best methods

23) According to you what are the best authentication/identification methods and why?
Answer:

Possible barriers to implementation

24) Do you see any barrier to implementation of authentication/identification methods and why?
Answer:
25) In particular do you see any barrier to implementation of the – according to you – best authentication/identification methods and why?
Answer:
26) Are you subject to any legal liability rules for user identification? Do you experience contractual issues that you feel may hinder the use of certain technologies related to user identification/verification?
Answer:

Expected / measured user perception

27) What are the expected / measured user perceptions related to existing / prospective user identification/verification methods you can provide information on?
Answer:
28) To question mentioned above: “Bank PINs are in most cases limited to 4 digits although the ISO standard allows longer ones. Are there any plans to move to longer PIN codes. Are some banks doing it in specific geographical areas/ for certain products?” What is the User perception here?
Answer:

Other questions

29) To what extent are regulations such as liability shifts a good instrument to
--

VERSION 0.7

enhance the introduction of stronger User identification/authentication?
Answer:
30)To what extent can you enforce banks to enhance their User verification/authentication?
Answer:
31)To what extent is it important to have common requirements/specifications for User verification/authentication? Is this an area for possible competition between banks and their products or should there be a common approach for reasons such as interoperability (of terminal basis) or User friendliness. To what extend can or are you willing to enforce banks into a common approach?
Answer:
32)What are the main incentives for you as payment organisation to have enhanced user verification/authentication methods (e.g. fraud too high, bad press, etc.)?
Answer:
33)Will SEPA have an influence on the Users, more in particular on the identification/verification of Users?
Answer:
34)What is your view on the role of the European Commission in the matter of User verification/authentication? Should they work on policies in this area?
Answer:
35)Please add any information you consider useful in the context of this questionnaire.
Answer:

ANNEX 4 WP1 - Experts and Industry - Security & Technology Experts questionnaires v1.0

ANNEX 4.1. Introduction

ANNEX 4.1.1 WP1 Objective

The objective of the European Commission study on User identification methods in card payments, mobile payments and e-payments is to analyse current and prospective **cardholder verification methods** on card payments, as well as **user verification methods** on e-payments and mobile payments. More in particular an assessment is to be made on the security provided and the user-friendliness, next to an analysis of possible regulatory, commercial and contractual barriers related to the use of best technologies.

The objective of the work package WP1 is to analyze current and prospective cardholder verification/authentication methods on card payments, as well as user verification methods on e-payments and mobile payments. It will provide an assessment on the (existing or prospective) level security of each verification method covered. This will include an analysis of topics such as encryption, protection against data hacking, etc. The analysis of new solutions will outline the cost/benefits/drawbacks over existing systems. The assessment will be presented by type of electronic payment and by type of technical solution. The assessment will further provide information on which of the existing methods are the most used, their actual protection against certain fraud types, the potential barriers regarding the use of these techniques and their economics and collateral dependencies. The analysis will be structured by technical method, within the payment method type (card, e- or m-payment).

ANNEX 4.1.2 WP1 Methodology

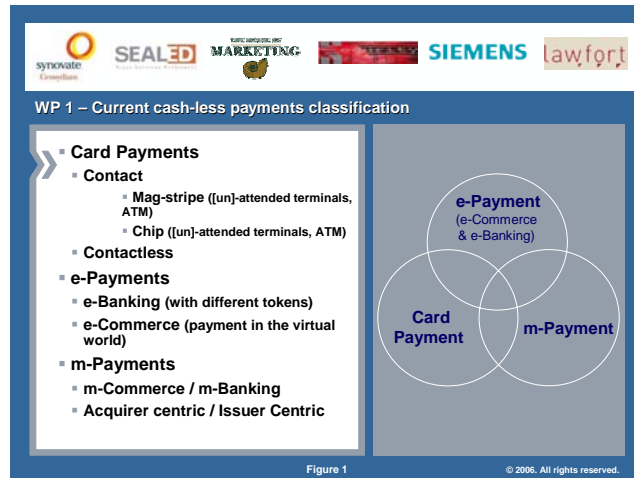
In addition to the information available to the WP1 Team of Experts, and the results of WP2 on “User assessment”, the analysis performed during WP1 shall also take into account Payment Industry and Experts information collected through interviews. These interviews will specifically target three groups:

- **Security & Technology Experts** while focusing on the user/card holder verification method and security aspects,
- **Leading Payment Providers and Banks**
- **Technology Providers** mainly to collect valuable information on the prospective solutions.

ANNEX 4.1.3 Studied Payment Methods

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

VERSION 0.7



ANNEX 4.2. EPI Providers Questionnaire - Payment Schemes Providers

Interviewee Administrative Details

Please complete the following information:

Name of organisation/company, incl. website	
Name of contributor(s) to this Questionnaire	
Professional title / position with company	
Address	
Telephone	
Fax	
e-mail	

* Please include names and personal details of all persons having replied.

N.B.! You are invited to indicate (by ticking in the appropriate box) if you agree with the following:

YES	NO	You accept that your feedback to this Questionnaire becomes publicly available.
YES	NO	You accept that your personal name and the name of your organisation are included in the list of the entities having taken part in this survey (“list of survey participants”)
YES	NO	Please indicate if any information you provide in the Questionnaire should be treated as confidential information and, therefore, should not be published. If this is the case, please indicate the Question(s) for which we should treat your answer as confidential.

VERSION 0.7

	Question(s) n°.....
--	---------------------

Your organisation's/company's profile, area of business and activities
Answer:
Your organisation's/company's relation (and role) to card-, e-, or m-payment industry/technology
Answer:

Technical security assessment of existing methods

39) For the existing payment methods (cfr section 1.3) can you comment on security issues (encryption, hacking, fraud, etc.) related to the associated authentication method(s) (including per authentication method lifecycle step – initiation, usage, termination), per payment method?
Answer:
40) It is likely that the implemented user authentication method is a compromise in terms of security, user convenience, risks and business objectives. What were the main barriers towards an improved security in terms of user authentication method?
Answer:
41) What is the position of your organisation with regards to the introduction of multi-application cards for payment applications only?
Answer:
42) To what extend is EMV CAP available as “universal” authentication method for different payment products. To what extend is it being introduced by banks and used by Users?
Answer:
43) To what extend does your organisation play a role in improving current User verification methods (e.g. PIN shielding at ATMs, physical requirements for ATMs)? Is a vendor approval programme in place to evaluate their products in that respect? If yes, what was the incentive to do it and does it prove to be useful in enhancing the security around user identification/verification?
Answer:
44) Bank PINs are in most cases limited to 4 digits although the ISO standard allows longer ones. Are there any plans to move to longer PIN codes. Are some banks doing it in specific geographical areas/ for certain products?
Answer:
45) Have you ever considered with your banks the introduction of a PUK, a deblocking PIN for payment cards?
Answer:
46) With regards to e-commerce and e-banking what are the user authentication solutions that would worth to be harmonised and whether this would be desired

VERSION 0.7

<p>or not? Are/were there plans towards such directions? Which barriers were encountered?</p>
<p>Answer:</p>
<p>47) With regards to m-commerce and numerous emerging initiatives in this area (e.g., sms based payments for parking, public transport but also gsm to gsm, and VISA mobile payment), User authentication seems to be reduced to PIN code and possession of a sometimes special type of SIM card. What are the security issues related to User authentication? What additional services or measures can be taken into account to increase authentication certainty and/or to reduce risks? How are the possible frauds and risks mitigated? How can Users be protected against abuses? Are there any proofs of User authentication related to performed payments? In particular with regards to <i>initiation</i> and <i>termination</i> steps of authentication methods.</p>
<p>Answer:</p>
<p>48) What are your commitments / procedures in terms of user identification / verification and in particular with regards to credential allocation? In case you need to strongly identify the user prior credential allocation and check the unambiguous link between credential and user, are you legally obliged to do so?</p>
<p>Answer:</p>
<p>49) Is user convenience (always) in contradiction with security? Can you comment? Do you see methods covering both aspects?</p>
<p>Answer:</p>

Prospective user identification/verification methods

<p>50) What is your approach with respect to new technologies for user verification? In particular such as biometrics? What would be the preferred technology? Do you have experience in certain countries?</p>
<p>Answer:</p>
<p>51) To what extend could e-Identity cards play a role for User identification in for instance electronic banking?</p>
<p>Answer:</p>
<p>52) Usage of such eID authentication tools certainly implies a shift of ownership, liability and control about provisioning of such tools (e.g., eID issuing government). Are the differences in terms of usual commercial or contractual liabilities in contracts between banks and users, and use of eID card as</p>

VERSION 0.7

authentication tool in e-banking?
Answer:
53) If mobile phones were to replace plastic cards for payments, what would be your assessment with respect to user identification/verification method (taking into account every step in authentication method lifecycle – initiation, usage, termination)?
Answer:
54) What is your approach on the usage of contactless cards?
Answer:
55) What is your assessment with respect to user verification in the context of contactless and proximity payment technologies? What would be the preferred technology? Do you have experience in certain countries?
Answer:
56) Do you have knowledge of other prospective User authentication methods and/or new form factors?
Answer:
57) Are the prospective payment methods always associated to prospective authentication methods? And vice versa?
Answer:
58) For the prospective user identification/verification methods can you inform us about costs, benefits, drawbacks versus existing authentication methods?
Answer:
59) For the prospective user identification/verification methods, can you comment on the security level (esp. compared to the classical methods)?

Most used user identification/verification methods

23) According to you what are the most frequently used user identification/verification methods and why? For these most frequently used methods, can you provide information on <ul style="list-style-type: none"> ○ economics and collateral dependencies ○ fraud analysis / figures
Answer:

VERSION 0.7

--

Best methods

24) According to you what are the best authentication/identification methods and why?
Answer:

Possible barriers to implementation

27) Do you see any barrier to implementation of authentication/identification methods and why?
Answer:
28) In particular do you see any barrier to implementation of the – according to you – best authentication/identification methods and why?
Answer:
29) Are you subject to any legal liability rules for user identification? Do you experience contractual issues that you feel may hinder the use of certain technologies related to user identification/verification?
Answer:

Expected / measured user perception

29) What are the expected / measured user perceptions related to existing / prospective user identification/verification methods you can provide information on?
Answer:
30) To question mentioned above: “Bank PINs are in most cases limited to 4 digits although the ISO standard allows longer ones. Are there any plans to move to longer PIN codes. Are some banks doing it in specific geographical areas/ for certain products?” What is the User perception here?
Answer:

Other questions

36) To what extent are regulations such as liability shifts a good instrument to
--

VERSION 0.7

enhance the introduction of stronger User identification/authentication?
Answer:
37)To what extent can you enforce banks to enhance their User verification/authentication?
Answer:
38)To what extent is it important to have common requirements/specifications for User verification/authentication? Is this an area for possible competition between banks and their products or should there be a common approach for reasons such as interoperability (of terminal basis) or User friendliness. To what extend can or are you willing to enforce banks into a common approach?
Answer:
39)What are the main incentives for you as payment organisation to have enhanced user verification/authentication methods (e.g. fraud too high, bad press, etc.)?
Answer:
40)Will SEPA have an influence on the Users, more in particular on the identification/verification of Users?
Answer:
41)What is your view on the role of the European Commission in the matter of User verification/authentication? Should they work on policies in this area?
Answer:
42)Please add any information you consider useful in the context of this questionnaire.
Answer:

ANNEX 5 WP1 - Experts and Industry - Technology Providers questionnaires v1.0

ANNEX 5.1. Introduction

ANNEX 5.1.1 WP1 Objective

The objective of the European Commission study on User identification methods in card payments, mobile payments and e-payments is to analyse current and prospective **cardholder verification methods** on card payments, as well as **user verification methods** on e-payments and mobile payments. More in particular an assessment is to be made on the security provided and the user-friendliness, next to an analysis of possible regulatory, commercial and contractual barriers related to the use of best technologies.

The objective of the work package WP1 is to analyze current and prospective cardholder verification/authentication methods on card payments, as well as user verification methods on e-payments and mobile payments. It will provide an assessment on the (existing or prospective) level security of each verification method covered. This will include an analysis of topics such as encryption, protection against data hacking, etc. The analysis of new solutions will outline the cost/benefits/drawbacks over existing systems. The assessment will be presented by type of electronic payment and by type of technical solution. The assessment will further provide information on which of the existing methods are the most used, their actual protection against certain fraud types, the potential barriers regarding the use of these techniques and their economics and collateral dependencies. The analysis will be structured by technical method, within the payment method type (card, e- or m-payment).

ANNEX 5.1.2 WP1 Methodology

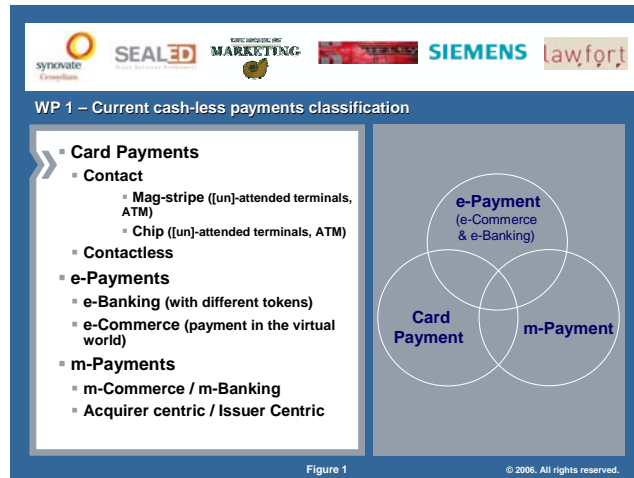
In addition to the information available to the WP1 Team of Experts, and the results of WP2 on “User assessment”, the analysis performed during WP1 shall also take into account Payment Industry and Experts information collected through interviews. These interviews will specifically target three groups:

- **Security & Technology Experts** while focusing on the user/card holder verification method and security aspects,
- **Leading Payment Providers and Banks**
- **Technology Providers** mainly to collect valuable information on the prospective solutions.

ANNEX 5.1.3 Studied Payment Methods

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

VERSION 0.7



ANNEX 5.2. Technology Providers Questionnaire

Interviewee Administrative Details

Please complete the following information:

Name of organisation/company, incl. website	
Name of contributor(s) to this Questionnaire	
Professional title / position with company	
Address	
Telephone	
Fax	
e-mail	

* Please include names and personal details of all persons having replied.

N.B.! You are invited to indicate (by ticking in the appropriate box) if you agree with the following:

YES	NO	You accept that your feedback to this Questionnaire becomes publicly available.
YES	NO	You accept that your personal name and the name of your organisation are included in the list of the entities having taken part in this survey (“list of survey participants”)
YES	NO	Please indicate if any information you provide in the Questionnaire should be treated as confidential information and, therefore, should not be published. If this is the case, please indicate the Question(s) for which we should treat your answer as confidential.

VERSION 0.7

	Question(s) n°.....
--	---------------------

Your organisation's/company's profile, area of business and activities
Answer:
Your organisation's/company's relation (and role) to card-, e-, or m-payment industry/technology
Answer:

Technical security assessment of existing methods

60) For the existing payment methods (cfr section 1.3) can you comment on security issues (encryption, hacking, fraud, etc.) related to the associated authentication method(s) (including per authentication method lifecycle step – initiation, usage, termination), per payment method?
Answer:
61) Do you participate in vendor approval programs for user verification devices (e.g., PIN entry devices)? Is it a useful/necessary initiative? What are the general problems related to such certification process that you encounter?
Answer:
62) Is user convenience (always) in contradiction with security? Can you comment? Do you see methods covering both aspects?
Answer:

Prospective user identification/verification methods

63) What is your approach with respect to new technologies for user verification such as biometrics? What would be the preferred technology? Do you have experience in certain countries?
Answer:
64) To what extent will government meet banking i.e., will or may e-Identity cards be used for identification purposes for payment transactions. What are here the legal or contractual barriers including the Trusted Third Parties involved (e.g. certificate issuers), the “liability” issues, insurance coverage, data privacy, etc?
Answer:
65) If mobile phones were to replace plastic cards for payments, what would be your assessment with respect to user identification/verification method (taking into account every step in authentication method lifecycle – initiation, usage, termination)?
Answer:
66) What is your assessment with respect to user verification in the context of contactless and proximity payment technologies? What would be the preferred technology? Do you have experience in certain countries?

VERSION 0.7

Answer:
67) Do you have knowledge of other prospective User authentication methods and/or new form factors?
Answer:
68) For the prospective user identification/verification methods can you inform us about costs, benefits, drawbacks versus existing authentication methods?
Answer:
69) For the prospective user identification/verification methods, can you comment on the security level (esp. compared to the classical methods)?

Most used user identification/verification methods

11) According to you what are the most frequently used user identification/verification methods and why? For these most frequently used methods, can you provide information on <ul style="list-style-type: none"> o economics and collateral dependencies o fraud analysis / figures
Answer:

Best methods

12) According to you what are the best authentication/identification methods and why?
Answer:

Possible barriers to implementation

13) Do you see any barrier to implementation of authentication/identification methods and why?
Answer:
14) In particular do you see any barrier to implementation of the – according to you – best authentication/identification methods and why?
Answer:

VERSION 0.7

Expected / measured user perception

25)What are the expected / measured user perceptions related to existing / prospective user identification/verification methods you can provided information on?
Answer:

Other questions

16)How do you perceive the payment sector's technology approach with respect to User verification/authentication (e.g., not pro-active enough, moving too slowly...) etc... compared to other market sectors?
Answer:
17)Please add any information you consider useful in the context of this questionnaire.
Answer:

ANNEX 6 User verification and User Authentication Methods

- 1 INTRODUCTION
- 2 DEFINITIONS
 - 2.1 Identification
 - 2.2 Authentication
- 3 HOW DOES AUTHENTICATION WORK – AUTHENTICATION FACTORS
 - 4.1 PINs, User ID / Password, and Passphrases : introduction
 - 4.2 PINs
 - 4.3 Passwords & Passphrases
 - 4.4 Asymmetric authentication schemes
 - 4.5 Biometric systems
- 5 AUTHENTICATION METHODS LIFECYCLE
 - 5.1 Authentication Mechanisms Initiation
 - 5.2 Authentication Mechanisms & Usage
 - 5.3 Authentication Mechanisms Termination
- 6 IDENTIFICATION/AUTHENTICATION SCHEMES SCORING
 - 6.1 Introduction
 - 6.2 Security Level

ANNEX 6.1. Introduction

Identity theft, this 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 insuring pretty good security measures and policies, amongst which the due authentication of all the principals acting in a transaction that will guarantee the proof of their identity. This section details the authentication and related e-security concepts.

ANNEX 6.2. Definitions

ANNEX 6.2.1 Identification

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

Formal definition¹: **Identification** is the process of using claimed or observed attributes² of an entity to deduce who the entity is.

¹ “Common terminology Framework for Interoperable Electronic Identity Management”, Consultation paper, Modinis Study on Identity Management in eGovernment, v2.01, November 23, 2005.

² An attribute is a distinct, measurable, physical or abstract named property belonging to an entity.

ANNEX 6.2.2 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 definition¹: **Entity Authentication** is the corroboration³ 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 definition¹: **Data Authentication** is the corroboration that the origin and integrity of data is as claimed.

User authentication serves, in the context of cashless payments, for the authentication of the user accessing to either e-payments application (e.g., logon to Web-banking service), or towards the payment device whether a payment card or a mobile device enables or operates a cashless payment. Note that we do not deal here yet about transaction itself but only about corroboration of a claimed identity from which the transaction originates.

Data Authentication helps to commit on a set of data that can be a payment transaction, a document. Examples of how data authentication may be assured include the use of a check sum, double keying, 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, 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, such digital signatures cannot be denied legal effect and even be recognised as equivalent to a handwritten signature.

Let us illustrate this definition 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 (*user authentication*)
- Then, once he needs to confirm a transaction, he will perform a *data authentication* (a *signature*).

ANNEX 6.3. How does authentication work – Authentication factors

User Authentication procedures are responsible for the corroboration of the identity of the use (whether that person really is who (s)he says 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

³ Corroboration is the confirmation by provision of a sufficient evidence and examination thereof that specified requirements have been fulfilled.

VERSION 0.7

different methods are used to authenticate. 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 «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 necessary to move to more secure way of authenticating, not based on a re-playable credential in order to **make these means of authentication stronger**.

Stronger authentication is obtained when moving from something you know, to something you have and even something you are. In addition it is also 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 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 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 (by replacing the “something you know” part of the protocol, by the “something you are” towards the device).

ANNEX 6.4. Authentication tools - General considerations on authentication mechanisms in payment systems

The authentication methods described in this section are independent of the payment scheme or protocol used for a given transaction. The next sub-sections aim to provide a description and security consideration 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.

ANNEX 6.4.1 PINs, User ID / Password, and Passphrases : introduction

The very basic authentication factor that can be used to authenticate a User in the context of cashless payment is the password associated to a User Identifier (UID). Credit card numbers and holder information are such very basic UID Password couple. In this case the credit card number is certainly the password that is the most endanger and in the same time the most used. UID/Password techniques are also used to secure home- and web-banking.

A second password can even be requested to authenticate specific actions or transactions, and used as confirmation code. However those passwords that are repetitively used must be adequately protected.

ANNEX 6.4.2 PINs

6.4.2.1 What is a Payment PIN?

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. The objective of PIN management is to protect the PIN against unauthorised disclosure, compromise, and misuse throughout its entire life cycle and in so doing to minimise the risk of fraud occurring within EFT systems. After the selection of the PIN and until the deactivation, the PIN, if stored, shall be enciphered when it cannot be physically secured. This means that PIN security also depends on sound cryptographic algorithms used for its encipherment and the associated key management.

The following clauses provide some high level description of the different stages in a PIN life cycle in a POS or ATM context. More information can be found in ISO 9564-1.

6.4.2.2 PIN selection

A PIN is selected in one of the following ways: it is assigned by the Issuer using a derivation or a randomized process or it is a customer (cardholder) selected PIN. In the latter case the Issuer should provide the customer with the necessary selection instructions. This PIN is

VERSION 0.7

referred to as the “reference” PIN and its value is used by the Issuer for comparison with the “transaction” PIN, entered by the customer at the time of a transaction. Only if the two values match, the customer is successfully identified.

A PIN assigned by the issuer shall be conveyed to the customer in a PIN mailer which means that the plaintext PIN is printed in such a way that it cannot be observed until the envelope is opened.

A PIN is usually linked to a card and customer account. However, multiple cards may be in issue on the same account, each with a different PIN. In this case the PIN mailer should display on the outside the appropriate details for customer identification. Moreover, PIN and card are never mailed in the same mailer nor at the same time.

A customer selected PIN is normally conveyed to the issuer via a secured PIN entry device (PED) at an issuer’s location (bank branch). Hereby, the PIN entry device is integrated in a physically secure terminal or is remotely connected via a protected communication link to the terminal. It should be installed in such a way that the customer can prevent others from observing the PIN value as it is being entered. As soon as the PIN is entered by the customer, it is enciphered for further transmission to the Issuer system.

6.4.2.3 PIN change

PIN change is to be performed on the issuer system in the home country. In case of an attended terminal it will follow the same procedure as for a customer selected PIN as described above. In the case of an unattended terminal such as an ATM, the customer must present its current PIN and twice the new selected PIN, whereby the last two entries shall be identical.

For forgotten PINs generally the same procedure(s) as for the generation of a first reference PIN is followed.

When a PIN is believed to have been compromised it shall be deactivated as soon as possible and the customer informed of a replacement value or given the opportunity to select one. A replacement PIN shall not be intentionally the same as the compromised PIN.

6.4.2.4 PIN activation

A PIN may be activated either implicitly or explicitly. Under a system of implicit PIN activation the issuer assumes successful PIN delivery, unless advised to the contrary. When a PIN is to be explicitly activated the issuer only activates the PIN after the return of a signed, and subsequently verified receipt of the customer or some other means that confirm PIN receipt.

6.4.2.5 PIN storage

A PIN stored in the computer files of the issuer shall be enciphered. Generally PIN encipherment incorporates the account number (or other data) such that the verification process would detect substitution of one value for another stored value.

When the PIN (assigned or customer selected) is stored on the magnetic stripe of a card, it shall never be stored as plain text, always in an enciphered form. When the PIN (assigned or

customer selected) is stored in the Integrated Circuit (IC) of a card, it should be stored within the protected area of the IC or it should also be enciphered. ISO 9564-2 specifies the approved algorithms for PIN encipherment during storage and transmission (see clause 3.5.1.8).

6.4.2.6 PIN deactivation

Solely the Issuer is responsible for deactivating a PIN. This generally occurs in one of the following cases:

- the PIN is compromised (or suspected to be compromised);
- all of the customer's accounts associated with the PIN are closed;
- the customer requests deactivation of the PIN;
- the issuer otherwise determines that deactivation of the PIN is appropriate.

In the case of PIN compromise, or a deactivation request by the customer, the customer shall be advised by the issuer of the action taken.

6.4.2.7 PIN entry

The present document is mainly concerned with PINs associated with payment cards, where the payment cards may be either chip cards or magnetic stripe cards (or hybrid cards.) In the ‘classic’ world, the PIN is generally used by the cardholder (customer) to prove its legitimacy in one of the following contexts:

- In a “face-to-face” context at the point-of-sale (POS) at a merchant's premises;
- At a cash dispenser (ATM) or electronic purse loading device;
- At a vending machine
- At an unattended terminal
- At a cardholder activated terminal (CAT).

Hereby, the protection of the PIN during the entry process is with the customer, the card acceptor (e.g., merchant), and the acquirer or its agent.

More recently, technological developments have now made feasible the use of PIN based financial transactions in open networks. When a PIN is used for cardholder verification in an open network transaction, the transaction acquirer has no control over the PIN-entry device into which the PIN is entered. This differs from the ATM and POS environments where the acquirer is responsible for the operation and security of the PIN-entry device. If PIN security in this environment is deficient, there is a high probability, if card data is also disclosed, that both (card data and PIN) may be fraudulently used in the ATM, POS or open network environments.

ISO TR 9564-4 specifies minimal PIN security practices in the open environment. This ISO Technical Report does not support the usage of magnetic stripe cards in this open environment. It defines the concept of a Minimally Acceptable PIN Entry Device composed of an Integrated Circuit Card (ICC) reader and an input device capable of allowing the cardholder to enter his PIN for offline verification (see clause 3.5.1.9). It is further recommended that the appropriate physical and/or cryptographic protection of the PIN is provided between the PIN entry device and the ICC.

6.4.2.8 PIN transmission

A PIN must always be protected during transmission (including, for example, storage at network nodes) either by adequate physical protection (e.g., a physical secure device) or by encipherment of the PIN. Whenever it is necessary to decipher and encipher a PIN during transmission, this must happen in a physically secure device.

For interoperability purposes PINs are stored and transmitted in special formats, the so-called PIN block formats which are specified in ISO 9564-1.

6.4.2.9 PIN verification

Depending on the type of card and on the type of PIN verification, important differences arise in the way that PIN verification is performed. For international interchange, the PIN associated with a magnetic stripe card can only be verified online by the issuer, since the card cannot perform any computations. However, the PIN associated with a chip card can be verified online as with a magnetic stripe card or offline by the card itself.

Four basic PIN verification techniques exist to verify the validity of the PIN entered at a PIN Entry Device (PED).

- PIN verification at a terminal (PED) by the terminal,
- PIN verification by the issuer,
- PIN verification by a service provider other than the issuer
- PIN verification at a terminal (PED) by the card (chip cards only)

The first three methods are also sometimes referenced as on-line PIN handling while the latter is an off-line PIN handling technique.

The principle behind all three techniques is to compare the PIN as keyed in (the transaction PIN) with reference data originating from the issuer, e.g. the reference PIN. For a comparison to be valid the transaction PIN or the reference data, or both, may require processing e.g., encipherment, decipherment. Irreversible encipherment, for example using a one-way function, may provide a higher level of security when reference data are exchanged.

PIN verification at a terminal

Obviously, to achieve PIN verification at a terminal the device, next to the transaction PIN, needs to have access to the reference data needed for the verification process. This reference data is either:

- obtained or derived from the customer's card; or
- obtained/transmitted from the issuer

Clearly, if the reference data are obtained from the customer's card the disclosure of the secret cryptographic keys utilised within the terminal may expose all of the PINs of those issuers.

PIN verification by the Issuer

When the verification of a PIN is carried out by the issuer concerned, the issuer needs to have access to the transaction PIN (or a derivative). Obviously the issuer has already access to the reference data. The enciphered transaction PIN therefore needs to be transmitted from the terminal to the issuer.

*VERSION 0.7****PIN verification by a service provider other than an issuer***

PIN verification by a service provider other than an issuer is carried out neither at the terminal at which the transaction PIN is entered, nor by the issuer. Both sets of data required for the comparison need to be provided to the service provider concerned. Thus, the transaction PIN or a derivative needs to be transmitted from the terminal. The reference data may be either obtained from the issuer or derived from data on the customer's card (e.g., using a PIN Verification Value (PVV) stored on the magnetic stripe) and transmitted with the transaction PIN (or a derivative). When this technique is used the PIN security of the issuer depends entirely upon the integrity of the facility of the service provider.

Offline verification (chip cards only)

In this case, the PIN entered by the customer is transferred to the chip card, either in cleartext form or, if the card is equipped with an asymmetric key pair, encrypted under the chip card's public key (see ISO 9564-2,3). Whether in cleartext form or encrypted, the card has an internal method for verifying the PIN's correctness (e.g., as per EMV). The card indicates to the terminal whether or not the supplied PIN is valid.

There are important differences between the different types of verification, and what they achieve in terms of security. Following a successful online PIN verification by the issuer or service provider at a POS, the merchant will be given an assurance via the acquirer that the PIN is valid for the card details. There is no assurance, however, that the physical card itself is valid. In the case of a magnetic stripe card, it may be a bogus card manufactured using valid account details.

During the period in which chip cards are introduced, hybrid cards will also exist (cards equipped with both a chip and a magnetic stripe). These cards will be capable of being used with magnetic stripe only terminals, chip card terminals and dual mode terminals. Such cards will typically have only a single PIN, where the PIN will be used to authorize transactions of both magnetic stripe and chip type.

6.4.2.10 PIN protection at Point of Entry

This section provides an analysis of the various means by which an attacker might fraudulently obtain cardholder PIN values at the point of PIN entry and the resulting risks. It is important to consider and evaluate these risks in order to be able to implement appropriate levels of security.

A list of general attack scenarios for SCDs is provided in ISO 13491-1.

This section analyses the most important threats by which PIN values may be fraudulently obtained at PIN entry.

Substitute terminal

A PIN might be compromised through the deployment of a "false" POS terminal introduced by an unauthorized replacement of the device. This may incorporate both PIN pad and/or terminal, or may just be a false PIN pad. There are various possible sub-cases for this type of attack ranging from pure PIN capture in case of an unconnected false terminal to complete transactions if the false terminal is connected to the network and fully impersonates a genuine terminal.

Bugged terminal

VERSION 0.7

A PIN might be compromised through use of a “bugged” genuine POS terminal that operates normally in every way except from leaking PINs via the “bug.”

Entry monitoring

A PIN might be compromised through “shoulder surfing,” that is, through an attacker watching the PIN being entered into the keypad by the genuine cardholder. The term “shoulder surfing” includes not only a human observer standing nearby, but also more sophisticated techniques such as the use of video cameras or the likes.

If cardholders and merchants are not honest and diligent, the attacks described above are difficult to prevent. In fact, if the merchant POS attendant or vending machine owner is dishonest then it may be impossible to prevent them from using a completely bogus disconnected terminal or a bogus intermediating terminal. Thus the task of protecting PINs at the point of entry reduces to the task of ensuring that such merchants are honest and diligent in mitigating all threats, that they use only legitimate unbugged terminals and that terminals are designed and located to minimize the monitoring threat. Unattended terminals must either not require PIN entry or be specially designed and operated in an environment that provides a very high level of tamper protection and tamper evidence. Finally, the acquirer is responsible to ensure that only legitimate unbugged terminals are used.

6.4.2.11 PIN security and card technology

PIN security policy and rules are in place in the banking world to protect cardholder PINs when the cardholder and merchant are assumed honest. If either is dishonest, protection becomes virtually impossible. However, the industry should provide adequate PIN protection for legitimately completed transactions, irrespective of whether in reality a substantial threat may exist for uncompleted transactions.

The level of protection that is needed will vary depending on:

- Level of criminal activity
- Merchant operating environment
- Payment application
- Card technology.

As previously discussed, the level and type of risk associated with different card technologies (magnetic stripe and chip) is very different. If a PED of a magnetic stripe terminal is bugged to reveal PIN values, the attacker with access to both PIN and magnetic stripe card data could for instance conduct fraudulent transactions at cash dispensers. This attack would not require that the attacker steal the cardholder’s card. However, if a PED of a chip-only terminal is bugged, the attacker would not be able to perpetrate the above fraud without actually stealing the actual card.

Because offline PIN verification primarily protects against the theft of chip cards, it is under the control of the card issuer and cardholder as to whether the PIN need be entered into such a merchant PED. For instance, irrespective of whether there is concern about the theft of PINs in chip-only merchant terminals, the issuer has the option to program their chip cards so that PIN entry is not requested as part of a chip transaction. The enforcement of straightforward “card locking and unlocking” mechanisms can then be deployed to minimize the risk

VERSION 0.7

associated with card theft. Such mechanisms might typically require that the cardholder enter a PIN using a personal PED or could even involve biometrics.

With two types of card technology, there are two different types of PIN risk and potentially two levels of tamper evidence requirements. From a risk perspective, terminals providing online PIN verification need to meet requirements that are more stringent than those offering only offline PIN verification (see ISO 9564-3 and ISO 13491). Thus, terminals supporting both online and offline PIN verification, including those designed to operate with both magnetic stripe and IC cards, must meet the more stringent requirements for online terminals. However, if a chip card has corresponding magnetic stripe data, for example, a hybrid card, the associated PIN must be protected similarly for chip as for magnetic stripe. This is because magnetic stripe data is not assumed to be protected and thus, one must assume that databases of such data could exist and are accessible to attackers.

Acquirers must ensure that their PEDs which accept PINs for magnetic stripe cards or chip cards that have corresponding magnetic stripe data are legitimate, that is, unbugged. This typically will require the use of tamper evidence techniques, and these techniques may include the ability for the PED to authenticate itself to the merchant or to the acquirer.

ANNEX 6.4.3 Passwords & Passphrases

6.4.3.1 (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.

Main benefits

As for Payment PINs, the main benefits of using passwords are:

- their *technical simplicity* as, for the most basic implementation, they can be implemented entirely in software without need of additional hardware;
- their *low cost*, as they are cheap and easy to implement;
- their *user familiarity and friendliness*, as users are generally familiar with passwords and are relatively comfortable with their use.

Main vulnerabilities

However, the use of passwords as authentication factors has several vulnerabilities, including:

- *Sniffable passwords*: When sent across the network in cleartext, passwords are extremely vulnerable to attackers eavesdropping on the traffic. Once intercepted,

VERSION 0.7

passwords can then be easily replayed in so-called “replay attacks” allowing attackers to impersonate the password holders. Encryption can prevent such attacks. Examples of encryption implementation on the Internet are the use of the SSL or TLS protocols.

- **Weak passwords:** Null, default or easily guessable passwords do not offer appropriate protection against so-called dictionary attacks that consist for an attacker, via specially developed programs, in searching a large number of possibilities from those that are most likely to succeed, typically derived from a list of words in a dictionary. Blocking UID access after three wrong attempts is usually implemented as prevention against dictionary or brute force attacks.
- **Weak policies:** Strong password selection policies should be implemented in order to limit the risk of selecting weak passwords. Awareness policies should accordingly be in place in order to inform password holder about risks related to the use of weak passwords but also to weak protection of passwords as it is often experienced that users are writing them down in highly visible areas. A good balance must also be found between the selection of strong passwords and the need for users to remember such passwords without endangering them.
- **Social engineering:** Many users are revealing their passwords when someone claims, either by phone or per e-mail, to be from the technical support of their bank. Again user awareness should here be improved, and even enforced.
- **Improper password storage:** Improper password storage is not only experienced at the user side as some software programs can store password in a manner such that they can be easily retrieved. Password protection shall also be correctly implemented at the generator / issuer side (e.g., database protection). EMV, for example, has issued recommendations for generating and distributing cards and related Pins or passwords.
- **Weak distribution processes:** The intrinsic security of passwords relies not only on their strength, on their storage but also on the security of the distribution scheme.

Recommendations

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.

In the context of payments, examples of such combination include:

- Password + Homebanking security modules whether PKI based or not
- Password + OTP systems either based on the use of TAN list, TAN cards
- Password + Hardware token implementing OTP schemes, including mobile devices with OTP per SMS

- Password + smart card (e.g., EMV) and smart card reader
- Etc.

6.4.3.2 One-Time Password - Dynamic Passwords

Definitions

- **One-Time Password**

A way to increase security of UID passwords 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.

- **Dynamic Passwords**

To reduce the inconvenience of using really one-time used passwords, and changing such list too frequently, some limited list of passwords can be used (e.g., on plastic cards). In case of such, so-called TAN-List, for each transaction, one of these numbers is randomly asked by the verifying application and needs to be provided by the user to prove that he owns the secret printed on the TAN List. Such lists can be used in combination with usual UID-Password in order to provide some more assurance on correct entity or data origin authentication (a kind of combination of what you know UID-Password and what you have, the TAN-List).

- **One-Time Password – Dynamic Password Devices**

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.

The token can also be protected by a simple (e.g., Pin-Code), or more complex (e.g., biometrics) to ensure correct authentication between the User and the device.

The token can also require the introduction of a challenge provided by the authenticating party for prevention of synchronisation issues, replay attacks and further ensuring time related authentication.

Such schemes making use of One-Time Passwords (OTP) implemented using hardware tokens are the most popular. Examples of such hardware tokens contain a microprocessor, an accurate clock that uses Universal Coordinated Time (UTC), a battery, an LCD capable of displaying up to an 8-digit number, and a unique 64-bit seed value. The token is initialised with a 64-bit seed value and every 60 seconds, the microprocessor runs a cryptographic algorithm (e.g., RSA) combining the seed value and UTC time to generate a pseudo-random number. When logging into a system, the token holder enters a PIN along with the pseudo-random value displayed on the token at that moment. An authentication server at the other end knows the seed value, the UTC and the PIN for each user. It is then able to compute the same

VERSION 0.7

pseudo-random number that the user presents. A 2-factor authentication is in this case achieved combining something the user knows (the PIN) and something the user has (the token).

The token can also be protected by a more complex authentication factor (e.g., biometrics) than a simple (e.g., Pin-Code) in order to ensure a stronger authentication between the User and the device.

The token can also require the introduction of a challenge provided by the authenticating party for prevention of synchronisation issues or replay attacks, and further ensuring time related authentication.

OTP classificationOTP-Cards or devices received in advance by the user

These devices should be able to produce a code which can be verified by a central authority to be coming from this device only. How these codes are generated and how they are communicated to an application, or to the user of an application, is often very specific for the technology chosen. An overview of the possible variants is provided here:

- Techniques for code-generation :
 - o Randomised list of codes (pre-calculated by central security server)
 - 1 specific “response-code” is requested
 - o Sequential Codes (Counters)
 - After 1 response-code is used, a range of next codes can be pre-calculated
 - o Time-based codes (clock-based)
 - Based on an internal clock of the small device, a code is calculated
 - o Challenge-response based
 - Based on User-input (limited nr. of digits)
 - MAC-based : message-authentication code, using symmetric keys
 - Digital signatures of a server-challenge, PKI-based
- Different “Token” form-factor :
 - o Plastic Cards (size of credit cards)
 - with a set of characters or codes
 - Smart Cards with cryptographic keys and/or PIN-protection
 - o Small unconnected devices with LCD screen
 - o Small USB-connected devices with crypto-keys inside
 - These use often similar techniques as smart-cards

The first technique does not require ‘intelligence’ of the authentication-device, whereas all other techniques require some sort of calculation power on the device itself. The last two ways for challenge-response based authentication require a larger set of data (at least the equivalent of some 20-25 characters, often “random” sequences. This is unfeasible for users to manually enter them from an LCD screen, these require a direct communication from the device to the application itself.

Common to all these techniques is that a central server is required which can validate the code entered to be the right code for this device, from this user.

Possible devices are:

VERSION 0.7

- A pre-printed plastic card with a set of human-readable OTP-codes (“OTP-Card”)
 - o Example : TAN-Card
- A Token with only an LCD-Screen (“OTP-Device”)
 - o Example : Secure-ID Token
- A Token with LCD and Pin-Pad (“OTP/MAC-Device”)
 - o Example: Secure-ID Tokens, Vasco-like tokens
- A plastic card with chip
 - o Example: PKI Smartcards

In general, the order of described solutions is rising in the cost and complexity.

The use of a Mobile Phone for communicating an OTP

The user mobile phone can be used as a token in an authentication process 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 achieving 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).

Payment schemes, supported by such mobile authentication, benefit from using two separate communication channels for the conduction of the authentication process. Basically, when attempting to finalise a financial transaction, the user contacts / is directed to the Issuer Authentication System requesting authentication to be performed. The Issuer has a protected database in which the user account number is associated with his mobile phone number. The Issuer system either calls the user’s phone asking him to enter a specific PIN or password travelling back to the Issuer system, or sends a specific one-time password to the user’s mobile phone to be used in the initial authentication channel (e.g., Internet web page). Once the identity of the user is verified, the authentication system communicates the result to the authenticating party via the initial channel or through a separate channel between the Issuer Authentication system and the verifying party.

Authentication of mobiles users in the GSM network can be obtained where each SIM card contains a secret key, and where proof of possession of this key is established by means of the A3 algorithm.

Benefits of using GSM as authentication factor include the ease of use, an easy distribution and the mobility of users. However it bears as well some hidden issues that must be carefully taken into account and securely resolved including the maintenance of the database associating mobile phone or SIM card numbers and user accounts as any change may affect the access to the payment services. Another issue resides in the enrolment of the mobile phone numbers in order to prevent any unauthorised access to the payment services. In such cases, dedicated PINs should be used differently from the mobile phones or the card PINs.

Such uses of mobile phones or devices in supporting more classical electronic payment schemes have already been discussed in the previous chapters dedicated to card-payments and e-payments.

VERSION 0.7

The use of an out-of-band communication can eliminate Man-in-the-middle attacks by “signing” or having dependence of OTP with earlier content submitted (dynamic match). This is not possible with cards (static values)

(From COSIC paper “Combining WWW and wireless security”, Claessens, Preneel & Vandewalle, 2001, rephrased summary).

On-line services using SSL/TLS and user-ID & Password systems or even specific OTP-tokens as well as Mobile Services using GSM Mobile devices are used everyday. Both approaches however provide security weaknesses and/or a lack of functionality.

A combination of WWW-technology with GSM Mobile Phones (using SMS-text messages) is regarded as being the most practical and low-cost way to come to a (more) secure and mobile solution to fully exploit the broad functionality of the internet, more specifically the WWW.

“... The concept of using an out-of-band channel ..., and the combined use of a mobile device together with a normal PC, will remain very useful. For the PC and its big screen will always be far more advanced than the mobile device, but will never be mobile.”

Following the here above mentioned paper, the use of GSM to communicate OTP offers the best possible match for functionality, security, mobility and (thus) user-acceptance, as well as an optimal re-use of what can be regarded to be existing infrastructure in 95 % of the cases ...

The main security advantage of this approach resides in the use of 2 different channels which can be assumed to be present in (almost ?) 95 % 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, with the added advantage of using:

- Existing (already deployed) solutions (hardware, networks, ...)
- (very) interoperable protocol (GSM-SMS)
- Well-accepted Interfaces for most users (SMS-messages)

OTP issued from bank card

In most of the password based schemes the authenticating and verifying parties are sharing the same secret information.

Asymmetric based **challenge-response** authentication schemes are even more secure.

In this case, when a User tries to identify himself to a verifying system, the system generates a random challenge and sends it to the person or more exactly to his device. Such a specific device (e.g., a mini-calculator, a microprocessor) will then compute the corresponding response, using secret information which has been generated only to this device and linked to its owner only. This response is then sent back to the system, which verifies if it fits the expected response based on public verification mechanism, public verification information associated to the User and on the assurance the system can have in the link between this public verification information and the User. The next solutions are used for this type of challenge-response authentication scheme.

Challenge-response authentication schemes rely on cryptography methods that are explained here below.

Off-line reader

Using short-time passwords from offline hardware token (a card-reader) combined with a [EMV] card can be considered as a sub-cases of the here above section, but this case is sufficiently representative in e-banking to have a dedicated section.

The card reader is typically a portable reader, including a Pin-Pad and digital display, and does not have to be connected to the Cardholder's Internet-enabled device. This scheme is based on symmetric cryptography, as described in the ad-hoc section on authentication.

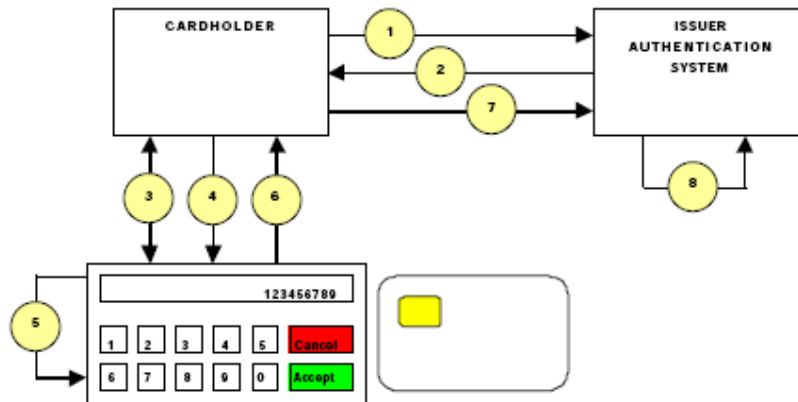
User authentication then works as follows:

1. The user connects to his Internet banking server via SSL/TLS with server-side authentication; by this way the user may ensure to be connected with a genuine banking server by explicitly validating the server certificate.
2. The user claims his identity by entering his account number on the bank's login form and, in turn, the banking server displays an n-digit challenge, asking for a matching m-digit response.
3. The user opens his smart card by entering the corresponding PIN on his smart-card reader before entering the given challenge. The smart card then calculates the matching response by encrypting the challenge and the incremented on-card login counter with its symmetric cryptographic key and encoding the result as an appropriately presentable response string.
4. The user manually copies the shown response to the bank's login form to be checked by the bank's authentication server redoing the same calculation independently. Since the login counters on the smart card and on the server may diverge (e.g., if a user playfully calculates some responses), the server tries to synchronize its local counter within a small range of, say, 32 counter values.

When the card is an EMV Card, the incorporated cryptography in EMV debit/credit cards is used.

The figure below describes a possible authentication process with an EMV card:

VERSION 0.7

*On-line reader (FINREAD)*

Making use of a hardware-token based PKI (see here below) and a FINREAD secure smart-card reader, connected to the end-user PC. FINREAD - Financial Transactional IC Card Reader - is a European solution to meet the need for advanced security for smart card transactions via public networks. The founding members of the FINREAD consortium consists of seven European partners, comprising six key European payment systems and the leading card reader manufacturer. The partners are Banksys, MasterCard Europe, Groupement des Cartes Bancaires "CB", Ingenico, Interpay Nederland, SIZ (the computer processing centre of the German Saving Banks), Visa EU, Canal+ Technologies, France Telecom, GTA, Omnikey AG, Orga, Sagem, SCM Microsystems. The design and promotion of FINREAD are co-ordinated by Groupement des Cartes Bancaires "CB".



FINREAD is defining the specifications of an interoperable intelligent smart card reader to be connected to a personal computer. Parallel to achieving this goal, FINREAD has developed a set of open standards - freely available to any terminal developer worldwide. This set of software specifications is applicable to various forms of mass-market terminal equipment, such as, portable devices (Cell Phones, Personal Digital assistants), set-top boxes, etc. The driving principle is that each device would accept payment cards with the same level of security and user-friendliness.

The advantage is that a PKI signature can be provided since the reader is connected (with an off-line reader, the signature may also be calculated but difficult to manually enter in the web interface).

Some cost and other Considerations on OTP

VERSION 0.7

As an indication, an overview of costs for some of such devices is provided

System	Number of Users	Estimated Deployment Cost
Authenex	1000	\$37,000 - \$42,000 ¹
RSA SecureID	1000	\$116,776 ²
Challenge-Response Tokens	1000	\$60,000 - \$100,000 ³
Smart Cards	1000	\$60,000 - \$65,000 ⁴
Biometrics	1000	\$100,000 ⁵
Hardware Tokens	1000	\$80,000 ⁶
Software Tokens	1000	\$60,000 ⁷
PKI	1000	\$100,000 - \$200,000 ⁸

(The above data is based on input by Authenex, which uses data from RSA Security, Gartner, Information Security Magazine, Computerworld, Ibid and @stake. This data is based on 2002 pricing levels).

From the @Stake paper one can identify the 3 major cost-factors for the technology used. These are:

- Deployment Cost
- Maintenance Cost
- Remediation Cost (Revoke / Re-issue of 1, or all Tokens)

Arguably, this last factor of cost can also be considered the residual “risk” resulting from the technology-choice. The replacement cost for revoking or re-issuing devices can be considered to be part of the maintenance costs.

With the remarks above, one can then determine the cost-factors that can lead to the choice of the preferred technology:

- Deployment Cost
 - o Production / Purchase Cost per token
 - o Cost for physical delivery to person
 - o Cost for central security server
- Maintenance Cost
 - o Replacing failing and/or lost devices
 - Revocation of Tokens
 - Redistribution of Tokens
 - o Running the central security service

As a basis for comparison: Manufacturing Plastic Cards with pre-generated random codes can be estimated to be under 1 €/ card, including the packing inside a tamper-evident envelope for delivery to the final user. This delivery can be done quite easily because the Tokens themselves are (should be) wrapped in a secure envelope, which makes it easy for a user to detect possible fraud or compromise.

OTP-Tokens run around 10-15 € some even up to 20 €/ piece, being at least 8 € more expensive in initial purchase. Shipment-costs of these devices can also be regarded to be (slightly) more expensive because of the higher value of the Token-devices and thus security-requirements of such transport. For a population of 1.000 users, the difference would be around 9.000 to 10.000 € from Plastic Cards to the cheapest OTP-solution.

VERSION 0.7

The following factors however do have to be taken into consideration as well:

- **Mobility:** A plastic card such as a smart-card or bank-card is easy to be carried inside a wallet. This is not, or significantly less, true for OTP-tokens. Risk of loss of a token or card is also reduced.
- **Many OTP-Tokens** instead can be attached to a key-ring.
- **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 –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).
 - o It must be highlighted that this tamper-protection is of most use during provisioning and transport of Tokens before, or during the deployment. OTP-cards can be protected in the same way as OTP-tokens are during this phase, by using tamper-evident packing.



Main benefits

The main benefits for the usage of such OTP tokens are the following:

- **Ease of use:** one single PIN is required to be known by the user to be able to access and use such tokens. No other skill is required since the token is displaying automatically the next pseudo-random value. Non reader or additional hardware is needed at the user side.
- **Mobility and portability:** such tokens are portable and can be used in any Internet-based configuration, anywhere.
- **Security:** such tokens are 2-factor authentication tools meaning that an attacker would need to collect both the PIN and the device to be able to impersonate the user.

Main vulnerabilities and drawbacks

The main vulnerabilities and drawbacks of using such OTP tokens are the following:

- **Costs:** The costs of such an implementation must be considered, including the tokens, the issuing, distribution and other life-cycle management of such tokens (e.g., expired, lost and defect tokens).
- **Availability:** Token needs to be in possession of the holder to be used. Timing impact of replacement for expired, lost or defect tokens should be considered
- **Limited lifetime:** Usual lifetime for such token ranges between 3 and 5 years.

- **Single versus multi-application domain:** One single token can usually be used in one single application domain. Cross-recognition or usage in multiple domain is possible but leads to complex and security-sensitive procedures.
- **Security of used cryptographic algorithms:** While algorithms that are under public scrutiny since a long time such as RSA algorithm can be usually considered secure provided they are correctly implemented, most of the proprietary algorithms may reveal being quite weak leading to security issues. As a general statement, guarantee of robustness of such algorithm implementations is quite difficult to obtain when even possible.

ANNEX 6.4.4 Asymmetric authentication schemes

In most of the password based schemes the authenticating and verifying parties are sharing the same secret information.

Clearly asymmetric based **challenge-response** authentication schemes are even more secure.

In this case, when a User tries to identify himself to a verifying system, the system generates a random challenge and sends it to the person or more exactly to his device. Such a specific device (e.g., a mini-calculator, a microprocessor) will then compute the corresponding response, using secret information which has been generated only to this device and linked to its owner only. This response is then sent back to the system, which verifies if it fits the expected response based on public verification mechanism, public verification information associated to the User and on the assurance the system can have in the link between this public verification information and the User.

Challenge-response authentication schemes rely mostly on cryptography techniques. The next sections provide highlights on the technique, in particular on one of the most used technology that sustains such challenge-response authentication schemes; PKI (Public Key Infrastructures).

6.4.4.1 Cryptographic Keys

Cryptographic methods are commonly use in authentication schemes usually combined with other authentication factors like passwords and/or cryptographic tokens. Cryptographic keys that can be used as authentication factors are of two kinds:

- Secret keys used in symmetric cryptographic algorithms such as DES, Triple-DES or AES
- Public/Private key pairs that are used in asymmetric cryptographic algorithms such as RSA where the private key is used to authenticate the user

The corresponding secret or private keys can be stored in either software or hardware means. For software versions, the key is stored in file, preferably encrypted, protected by a password. Higher protection of secret/private key storage (and use) can be achieved by using tamper evident/resistant devices with even computational cryptographic devices (e.g., smart card,

VERSION 0.7

USB token). The basic principle in which the authentication is performed is independent of the implementation such as through token or client-side software. Obviously the security of the keys relies on the chosen storage media, as well as on the generation process, distribution process and the authentication mechanism they support.

The main general benefit of using cryptographic keys as authentication factor are the ease of use and the higher level of security. On the one hand, to use their keys, users only need to know about the PIN or password that is protecting their usage whether they are implemented in software or on a removable (secure) token. On the other hand the intrinsic security level of cryptographic methods usually relies on well-recognised, well-tested and well-security scrutinised cryptographic algorithms.

However there are also several drawbacks linked to the usage of cryptographic methods compared to other solutions like OTP-based schemes. The main ones are the complexity of installation and the potential mobility / portability issues. The complexity of installation may reveal to be significant for systems requiring complex software installation or even card reader installation for smart card based systems. These installation processes have significantly be improved by the software industry to a point that can even introduce another type of drawback that is the unawareness of the type of technology that is underlying the authentication mechanisms. To an extreme, user may use PKI (public key cryptography supported by identity certificates issued by trusted third parties) based authentication factor that reveal to allow non-repudiation and even true implementation of legally binding electronic signatures while not being aware of this fact. On the other hand the portability / mobility of the cryptographic key based authentication factor may be drastically limited when based on token requiring installation of specific readers on every machine from which the system should be used or lead to security issues when keys (even protected) are allowed to be installed on several environments as it is usually the case for software based implementations.

In an authentication process, the proof of possession of a (secret/private) cryptographic key is usually implemented by means of a **challenge-response** mechanism. In such a mechanism, the authenticating entity is proving its identity to the verifying party by demonstrating its knowledge or possession of a secret / private key without revealing it to the verifier. This is done by the authenticating party by computing a response to a (pseudo)-random and/or time-variant challenge, where the correct response depends on both the authenticating party's secret/private key and the challenge.

6.4.4.2 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 demonstrate its knowledge of a secret key by using a PIN or password to unlock the secret key (when so protected) 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 would not be possible without the possession of the secret key (e.g., compute a Message Authentication Code – MAC as a function of the challenge). The result is then sent to the verifier. The authenticating party which possesses a copy of the secret key verifies the encrypted data by decrypting it and comparing the resulting cleartext information with the

VERSION 0.7

original challenge. When both data match the identity of the authenticating party is then corroborated.

Examples of implementations of symmetric cryptography based challenge-response authentication mechanisms are:

- SIM card authentication on the GSM network: Each SIM card contains a secret key whose proof of possession is established by means of the A3 algorithm. Since Users are authenticated to the SIM using a PIN, such authentication is implementing a 2-factor authentication towards the GSM network.
- On-line authentication of EMV cards for which the generation of a correct application cryptogram by the card, using a secret key, proves the possession of the card.

Challenges may be fully (pseudo)-random as in the first example or include some transaction context information as in the second example. In this latter case the identity corroboration of the authenticating party is linked to its acceptance of the transaction provided such acceptance context is clearly displayed and explained to the user so that he is fully aware of this fact.

Main drawbacks of symmetric cryptography are the lack of non-repudiation and the required key management especially in cross-domain implementations. Both the authenticating party and the verifier has to share the same secret information preventing a formal non-repudiation as the claimant could point out that the verifying party could have the ability to generate valid responses to challenges. Key management may reveal to be difficult to implement and to secure especially in large systems involving the acceptance of secret key based factors issued by different parties. IN such cases the secret keys must be distributed to all verifiers resulting in a complex and security-sensitive procedure.

6.4.4.3 Authentication through asymmetric cryptography: PKI based authentication schemes (or “strong authentication”)

PKI based authentication schemes allows proving the possession of a secret without having to share this secret with the verifier, and allows a very strong way of authenticating since non-repudiation can easily be provided, 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 correctly registered.

This authentication mechanism is based on the interchange of digital certificates guaranteeing the authenticated link between the identity of a user and its public key linked to its private key and the security of that private key (including generation, distribution, storage, usage and termination processes). The authenticating party possesses a key pair made 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 publicly available (published) in digital certificates, signed by a trusted party called a Certification Authority (or Certification Service Provider) which so affirms the authenticity of the certificate securely establishing the mapping between the identity of the owner of a specific public key.

VERSION 0.7

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 claimant.

Both implementation will require the verifier to validate the authenticating party 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 key pair has been officially allocated to (or generated by) a user, and the public key certified as linked to the User's identity, the verifier can be sure that the person he (she) expects to discuss with and claiming to be owner of a public key is REALLY that user.

One can easily understand that the registration process used to provide the User with such PKI-based key pair and to certify the link between the public key (information) and the user's identity is crucial for the security of the PKI-based authentication mechanism and that the private key protection is another crucial element of a PKI based authentication mechanism. Someone in possession of a user's private key can impersonate this user. For this reason, the private key can be protected:

- Software based: the private key is encrypted on the PC and is accessed via a password only known by its owner
- Hardware based: the private key is stored, protected and used on the hardware (smart-cards are a sub-set of such secure hardware) and the access to the key within the hardware is protected (e.g., PIN, password, biometrics). The security level of the hardware is thus an important feature determining the security level of the PKI based authentication mechanism (e.g., EAL, FIPS, etc.).

Mutual authentication can also be implemented such that both parties (user and verifier, cardholder and Issuer Authentication Server) will authenticate each other. Such mutual authentication has an additional security added value when establishing a secure communication channel between the communicating parties.

Examples of such asymmetric cryptography in challenge response authentication mechanisms include:

- SSL / TLS protocols: In these protocols, a party proves his possession of a private key associated with a public key certificate by signing a message provided by the other party. Mutual authentication is possible as well as the establishment of a confidential channel based on symmetric key cryptography whose "session" secret key is exchanged using the asymmetric key cryptography. SSL is mainly used in website

VERSION 0.7

authentication on the Internet or user/website mutual authentication. This can be visualised by the lock in the header or footer of the Internet browser.

- Off-line authentication of EMV cards: When Dynamic Data Authentication is used, the generation by the card of a digital signature on a terminal-provided (pseudo)-random challenge using the card's private key authenticates the card towards the terminal.

The key pair generation can take place at either the user's location or at the issuer's location. In the latter case, the generated private key must be delivered to the user in such a manner that the private key is not compromised and that the user is the only entity being able to access the private key. In case key generation is performed by the user, the integrity of the certificate request containing the public key to be certified must be ensured as well as the proof of possession of the private key by the user.

Besides the ease of use and the good level of security, the main advantages of using asymmetric cryptography resides in the possible implementation of formal non-repudiation and easier cross-recognition and key management compared to symmetric cryptography.

The main drawbacks are however the costs and complexity of such mechanisms, in particular the implementation of a full PKI based infrastructure and services, and the difficulty of correct implementation of true non-repudiation mechanisms.

ANNEX 6.4.5 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 cardholder validation. PIN-based networks, while highly successful, are sometimes compromised because the Cardholder 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- payment. Several types of biometric schemes can be used depending on the intrinsic reliability, security and user acceptance, amongst others:

- Face

VERSION 0.7

- Eye
- Fingerprint
- Dynamic signature
- Behavioural (other than signature)
- Etc.

6.4.5.1 The process

The use of PINs and passwords as a means of verification is based on actual values. The outcome of any verification process gives either a correct or incorrect response. Biometric methods, behavioural or physiological, however, use variable values, the results of which will be almost right or almost wrong, and in many cases a scale in between. An automated biometrics process can be used to verify an individual based on physical and/or behavioural characteristics. That is, based on things it does and or things it is. Although there are a variety of individual biological and behavioural characteristics, the basic process of measuring differences between people is essentially the same and many of the same factors are common across several biometric processes.

There are many biometric methods, but for any method used, an individual must first enrol, and create a template of his/her characteristics. This template can either be stored within the verification terminal, which may be a standalone system, or a central database for on-line systems, or on an integrated circuit card (chip card) which the enrolled individual carries with him/her.

When an individual needs to be identified, he/she simply enters a new sample of his/her characteristics which is compared with the stored template. Provided the template and the new sample are sufficiently similar to each other, the system will verify them as being correct. Typically, this process takes no longer than a few seconds.

Biometrics however do have one significant drawback. Unlike the PIN where the comparison process is very clear (comparison of two values) and provide a definite yes/no outcome, biometrics do not have that clear cut benefit. No matter what biometric is used, it is extremely unlikely that the template and the new offered image will produce an exact match. This is not because the characteristic changes, but because recording of the image for verification will vary. For example, it would be virtually impossible for a fingerprint always to be placed in exactly the same location, at the same angle and with the same pressure each time a verification is required. What the biometric process does provide, is the confidence that access to the system is being given to a genuine user. In most devices this level of accuracy will not be 100%, and therefore this means that the biometric system must incorporate a degree of tolerance. If a system requires an exact 100% match between the template and the newly offered image, then the vast majority of legitimate users would be rejected.

Biometric systems therefore have to be set to accept different tolerances depending on the needs of the user and the environment in which the biometric is being used. For example, a banking application may require that a high percentage of impostors are detected, and very few legitimate customers are rejected. These tolerances are expressed as being false

acceptance rates and false rejection rates. That is, the probability that the biometric verification device will either fail to reject an impostor or fail to verify the legitimate person.

6.4.5.2 Biometric methods

A distinction needs to be made between two classes of biometric methods: those based on physiological characteristics (based on measurements and data derived from direct measurement of a part of the human body) and those based on behaviour (based on measurements and data derived from an action by a human body, thus indirectly measuring characteristics of the human body).

Physical Biometrics

Physical biometrics, i.e. systems that measure biological characteristics unique to individuals, are techniques such as fingerprint, eye retina pattern, iris scan, facial recognition, hand geometry and vein patterns.

Fingerprint verification

Fingerprint systems operate by identifying the location of small marks, known as minutiae, which are found in the fingerprint. Most verification units store data which relate to the location and type of minutiae details, for example, the distance between two lines, or the length of a line before it is broken. The ability to read a fingerprint depends on a variety of work and environmental factors. These include age, gender, occupation and ethnic origin. Enrolment can take only a few seconds. The resulting template tends to be one of the largest in the field of biometrics, ranging from several hundred bytes to over 1000 bytes. However its stability and uniqueness is well established.

These systems are easy to operate as all the user needs to do is place his/her finger on a reading surface. The characteristics are then compared to those held on the individual's template. This verification may happen online by a back-end server or off-line for instance by means of a smart card. The technology is available from a number of vendors, some of them incorporating additional features such as the check that it is a print of a "live" finger.



Retina scanning

Retina scanning provides a unique basis for identification. To obtain a reading the user is required to focus on a small target while looking through a binocular style lens. An infra-red

VERSION 0.7

light, directed through the pupil to the back of the eye, then takes a 45 degree circular image of the blood capillaries, which is reflected back to a camera capturing the image. Enrolment takes less than 1 minute. The template for eye retina data is comparatively small e.g. 96 bytes and the verification process is very fast. For verification, the retina pattern is scanned in a few seconds and compared with the stored retina data.

To date the main usage of eye retina scanning has been restricted to high and medium security areas within military, space and police institutions although some prisons also use this method. There has been a general opinion that the public would prefer not to use retina scanning if given the option.

Iris Scan

The iris scan uses standard video optics to capture an image of the subject's iris. Infra-red light is used instead of natural light, allowing a clearer image of the iris to be captured. The enrolment method requires the user to place his eye to a telescopic style lens. The user sees a reflection of the eye and is required to hold still for a number of seconds. The image is then displayed on a monitor, analysed and the iris pattern is mathematically encoded into a database. It operates successfully with or without glasses/contact lenses. As well as eye patterns being unique they also remain stable from early infancy throughout a person's life, only being affected by a few rare diseases. The technique is already used today within prisons. The identification/verification speed is quick due to the low number of bytes stored on the template (typically between 120 to 256 bytes) and gives an extremely good level of accuracy producing almost zero error rates.

Facial Recognition

The facial recognition systems currently available generally require the user to be looking straight into the camera although very minor deviations, such as head movement, are acceptable. Other factors also need to be considered. The person needs to be standing a certain distance away from the camera (this can vary depending on the specific manufacturers design) with an uncluttered background and good lighting. As these systems first have to locate the face within the image and then locate such features as the eyes, mouth and nose, the need to capture a good image is imperative. The size of the template stored by facial recognition systems can vary depending on the supplier but they generally range between 500 bytes and 2000 bytes. Ultimately, facial recognition systems will be commercially available and able to identify persons as they walk naturally towards a door, however full commercial implementation remains some time off.

VERSION 0.7



Hand geometry

Hand Geometry systems operate by looking at the length of the fingers, hand thickness and palm shape. There is also a version whereby the geometry of just two fingers is measured. These systems are relatively easy to use, mostly incorporating guide posts to ensure the hand is placed correctly. They are not affected by environmental factors such as dirt and grease although rings with large stones or structures may need to be removed or positioned downwards if they were not worn at the time of enrolment. Enrolment can be accomplished in a few minutes. Special equipment is needed. Template sizes are less than 20 bytes. The verification process takes less than five seconds. The prime application areas for hand geometry devices are generally as an access at military, nuclear and other high security locations such as prisons. One biometric device, the ID3D was used in the INSPASS Passport Immigration Control pilot in the US but has been abandoned subsequently to the 9/11 events.

The systems tend to be perceived as “good all-rounders” with a single try false acceptance rate of under 0,1% and a three try false rejection rate of 0,1%.



Vein Patterns

This system compares the vein tree pattern, formed from the sub-cutaneous blood vessel on the back of the hand. This pattern is picked up by a video camera when the skin is held tight. It utilises infra-red cameras to filter off only the vessels and ignore the rest of the hand. Whilst this system is still in its infancy, in operation and use it is similar to the hand geometry system. The size of the template is also very good and is reputed to be around 50 bytes.

Behavioural Biometrics

Behavioural biometric systems monitor the way in which an individual performs a particular action. Techniques include voice verification and dynamic signature verification (i.e. things the person does).

Voice verification

Voice verification techniques focus on characteristics of speech patterns formed by a combination of physical and behavioural factors rather than sound or pronunciation. They depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanisms of the body. As a result voice verification systems are safe from mimics but not from high quality digital tape recordings. To overcome this, most voice systems build in a random factor whereby words or numbers may be picked randomly by the system from a selection stored at the time of enrolment.

Voice verification systems come in two basic types; stand-alone and telephone-based systems. Telephone allows the user to access a system via a standard telephone which connects to a central voice verification system. Stand-alone systems are used for application areas such as physical access control and verification is performed internally. Although both systems are affected by background noise the telephone-based system is also affected by noise on the line, especially if it is performed over a great physical distance.

The user must enrol in the presence of a supervisor. Enrolment consists of speaking a dozen or more words, each several times, into a device that records them. The recorded words are stored in a central file. At logon the user is identified by three or four of these words, which can be transposed on the screen or into a telephone. The enrolment process is about 1 minute. The verification procedure takes 12 - 20 seconds. The template sizes for voice verification systems vary depending on whether the user has to say one word or a whole sentence. The template size is typically 300 - 1500 bytes, usually upwards of 1000 bytes.

Voice recognition has the advantages of minimal costs at the terminal point and ease of operation. The method is easily accepted by the users.

Signature dynamics

Signature verification devices record the way in which a signature is written rather than its appearance. This is measured by either:

- a special pen;
- a sensitive tablet upon which the signature is written with an ordinary pen;
- or with a tablet and stylus purchased as a standard computer peripheral.

The data and measurements obtained from the signature writing process vary between different systems, but usually include factors such as speed, direction, pressure, thickness, the number of line segments crossed, total writing time, overall height and width, time taken to each of the turning points, and the number of times the pen is on and off the paper. When all the measurements have been taken the results are used to calculate how close the offered signature is to the pre-stored enrolment template. Some systems are however unable to cope with people whose signature changes radically each time it is written. Unfortunately, about 2% of the population is wildly inconsistent in signing.

Dynamic signature verification devices are easy to use, acceptable to the public and have the advantage that information on how to write the signature cannot be obtained by simply looking at one previously written signature. A forger can copy the appearance of someone's signature, but has no way of knowing the speed and rhythm of the genuine signer. The size of the template stored by dynamic signature verification systems is quite small at 40 - 100 bytes but to reproduce the image, more information needs to be stored.

One area which may cause problems is the positioning of the biometric device, especially at POS, where counter space may be limited. The individual may be required to sign at different positions/angles/heights which could distort his/her signature and make verification difficult.

6.4.5.3 Benefits of biometrics

Biometrics could bring benefits to each of the stakeholders in a financial transaction as follows.

- For consumers the usage of biometrics appears to be a safe, convenient, privacy sensitive and reliable way to help deter the unauthorized use of consumer accounts. It is reliable because it uses data based on a person's unique physical characteristics. It is convenient because carrying multiple forms of ID are no longer necessary to prove consumers are who they claim to be. There are no PINs to forget, incorrectly enter or inadvertently share.
- For the merchants biometrics may reduce the number of chargebacks related to non face-to-face transactions due to unauthorized payment card use. At the same time, the equipment necessary for facilitating biometrics transactions becomes affordable and multiple vendors are already in the market today.
- For the payments industry the introduction of biometrics-based payment cards could be a valuable, deployable service issuers could offer customers with a growing concern over security and safeguarding personal information. Moreover, issuers would be able to reduce their losses associated with fraud types such as: lost, stolen, counterfeit, and non-received issued cards.

Fingerprint: the most promising?

Out of the biometrics technologies available today as described above, fingerprint minutiae thus far appears to be the most promising for adaptation to CVM. First of all, the method has been adopted for employment in the new e-passports which means consumer are getting acquainted with the technology at border controls. From a practical point of view, the process for recording fingerprints is less time-consuming, less intrusive and less expensive than taking measurements of eyes, hands and voice. Next, the merchant equipment necessary for approving fingerprint minutiae transactions is also relatively compact and inexpensive which likely makes the solution more attractive to merchants and issuers.

ANNEX 6.5. Data Authentication in the financial world

Although there is a European Directive on e-signature providing for a legal value to certain type of e-signature (the Qualified Signature, 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 eSignature Directive) or even operation of schemes governed by private law agreements allowing conferring a sufficient legal value to agreed systems to be used by the parties.

However, banks are more and more involved in the establishment of PKI whether in the context of Intranet or corporate or eBanking secure services (e.g., ING PKI), or when deploying multi-application EMV smart cards, or even when actively participating to the deployment of national eID schemes as in Sweden or national PKI services as in the Grand-duchy of Luxembourg.

ANNEX 6.6. 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.

ANNEX 6.6.1 Authentication Mechanisms Initiation

The initiation of authentication mechanisms 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.

ANNEX 6.6.2 Authentication Mechanisms & Usage

The usage step of authentication mechanisms 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

VERSION 0.7

certainly depend on the nature of the used factor(s), their possible combination, and their correct implementation. Authentication processes rely on the here above presented methods and combination of these tools:

- PINs, User ID / Password, and Passphrases
- One-Time Password
- Dynamic Passwords
- One-Time Password – Dynamic Password Devices
- Asymmetric authentication schemes
- PKI based authentication schemes
- Biometric systems

ANNEX 6.6.3 Authentication Mechanisms 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.

ANNEX 6.7. Identification/authentication schemes scoring

ANNEX 6.7.1 Introduction

As previously described, authentication methods are combinations of one or more authentication mechanisms. These mechanisms can be seen as processes allowing an entity to prove its knowledge or possession of one or a combination of authentication factors from the previously identified categories “something you know”, “something you have”, and “something you are”.

To score an authentication method in the context of the present study, (1) the security of this authentication method and (2) its user perception (e.g., friendliness, confidence) will be analysed.

ANNEX 6.7.2 Security Level

To evaluate the overall security of an authentication method, it is necessary to analyse:

- The **number of factors involved**: Obviously, the larger the number of factors is, the better the security should be as an attacker would need to defeat a higher number of resources or systems. A 1-factor authentication system based only on a UID-password would only require guessing/known the user password while combined with the possession of a token (e.g., card, secret or private key, OTP token) in a 2-factor authentication system will require not only to know/guess the password but also to possess the token at the same time.

VERSION 0.7

- **Initiation:** whatever the generation/registration/delivery process that is used to allocate an authentication factor (or a combination of factors) to an entity, the link to the entity's identity must be properly established.
 - **Generation process:** The originator of the authentication factor can either be the factor-holder or its issuer.
 - **Registration:** the formal step of authenticating the entity and its identity during the initiation step of the provision of an authentication method can basically rely on two different modes of corroboration processes:
 - Non face-to-face
 - Face-to-face
 - **Delivery (or Distribution) method:** A secure distribution to its legitimate holder must be implemented when authentication factor(s) are generated by issuers. When factors are locally generated by their holders, some data must be securely transmitted to the issuer in order to ensure the link between this factor and its holder's identity.
 - **Storage and access method:** the factor storage technique and the method used to access the stored factor have direct impact on the security of the factor itself.
- **Usage:**
 - **Factor properties:** The strength of a factor is dependent on the difficulty of stealing, copying, accessing, borrowing, or counterfeiting it.
 - **Mechanism security:** The intrinsic security of the implementation of the security factors in the authentication mechanism are to be carefully considered as this may include, for example, the cleartext or encrypted presentation of the factor value, the proof or not of the possession/knowledge of the factor, etc.
- **Termination:** Security issues or failure in properly terminating the life-cycle of user authentication credentials may jeopardize the entire authentication method.

The payment scheme in its whole must be secured in order to ensure the correct and secure identification/authentication of the authenticating party.

One of the main challenges in authentication schemes is the very beginning of the procedure, i.e., the user enrolment or registration. Based on this registration step, every relying party should have a good assurance that the person performing the authentication is really who he/she claims to be.

VERSION 0.7

Considering the PKI based authentication scheme, one can easily understand that the association of a key pair and its owner is of major importance. This link needs to be guaranteed (certified) to a certain level and this level verifiable. In the example of a TAN list, one needs to be sure that a certain TAN list has been fully delivered to the user claiming to be the owner of that list.

It is thus of crucial importance to provide authentication credential to the right person. One can classify registration into 2 categories:

- Non face-to-face: in this case, the allocation of a credential to a particular user is based, e.g. on a paper (or on-line) registration file aiming to provide sufficient information on the user to have a certain level of guarantee that he/she is who he/she claims to be (e.g. by asking a copy of the Identity card, ...).
- Face-to-face: in this case, prior the allocation of a credential to a user, an official security officer check the identity of the user (e.g. against his/her identity card).

The delivery of the payment credential, their usage and the payment scheme in its whole must be secured in order to ensure the correct and secure identification/authentication of the authenticating party. In particular all associated risks must be taken into account and managed accordingly.

Whether you think to know your trading partners or not, whether you have confidence in them or not, now that you are doing business in the digital world you are definitely not alone, especially on intrinsically non-secure networks.

You will be facing or are already facing numerous external threats: Viruses and worms, Social engineering, Phishing and pharming, Denial of services, Hacking, Network or application breach

Online extortion, Spyware, malware, Brand highjacking, and one of the most growing threat, ***Identity Theft.***

Unfortunately threats cannot only come from the outside but also and usually even more frequently from the inside. Internal threats are certainly as numerous as external threats and consist of for example: Viruses and worms, Development practices, Insider fraud, Lack or breach of Security Policies, Leakage of customer data, Internal network breach, Lack or gaps in training and awareness, Loss of company data, Patch management, etc.

Identity theft is emerging as one of the crimes of the 21st century. It is the fraudulent exploitation of another entity's ID-corroborating information. Or in other words it involves the deliberate stealing of another person's identifying information for criminal purposes.

This can be performed by:

- Borrowing privileges in order to initiate parallel account access, or performing classic Credit Card fraud for example,
- Expropriating privileges, consisting in taking over existing accounts,
- Fraudulently obtaining new privileges, that is the fraudulent use of existing credentials to get new ones or to aid other real-world theft, like real estate frauds,

VERSION 0.7

- Full impersonation that may include all of the above, while being less attractive to organized crime and not scalable.

ANNEX 7 EMV chip card authentication methods

ANNEX 7.1. The EMV architecture

In a transaction based on EMV architecture, a card authentication session is executed to check the genuineness of the card prior to the cardholder verification. The off-line card authentication mechanism is either “static”, wherein the same authentication data is provided by the card to the terminal for every transaction, or “dynamic”, wherein the authentication data provided by the card will be different for each transaction. The EMV 2004 specifications define one static offline CAM (SDA) and two dynamic offline CAMs: Dynamic Data Authentication (DDA) and Combined Data Authentication (CDA).

For SDA the issuer pre-signs unique static card data to protect against alteration of the data after personalization. During a transaction the terminal can retrieve this signed static data from the chip card and verify the correctness of this data.

ANNEX 7.2. Off-line CAM

The off-line card authentication mechanism is either “static”, wherein the same authentication data is provided by the card to the terminal for every transaction, or “dynamic”, wherein the authentication data provided by the card will be different for each transaction. The EMV2004 specifications define one static offline CAM (SDA) and two dynamic offline CAMs: Dynamic Data Authentication (DDA) and Combined Data Authentication (CDA).

For SDA the issuer pre-signs unique static card data to protect against alteration of the data after personalization. During a transaction the terminal can retrieve this signed static data from the chip card and verify the correctness of this data.

For both DDA and CDA the issuer personalizes the chip card with a certified private RSA key unique to the chip card and then during a transaction the card produces a dynamic signature on a random challenge received from the terminal. By verifying this dynamic signature, the terminal can authenticate the chip card itself (under the assumption that the chip card’s private key is known only to the chip card), and confirm the legitimacy of static chip card data. Additionally with CDA the dynamic signature of the chip card covers all the transaction data necessary for the terminal to confirm the integrity of the chip card’s response for the current transaction.

The EMV specifications have specified CDA as a result of a study on the use of “wedge” devices for offline transactions. Wedge devices alter data exchanged between the genuine card and the terminal and such alterations may not be detected when using SDA or DDA. Thus whereas DDA authenticates the card but not the transaction data, with CDA the card digitally signs all the important transaction data including the value, and so any modifications to this data can be detected.

ANNEX 7.3. On-line CAM

In order to understand the significance of the offline CAMs other aspects of the EMV transaction must be introduced, namely application cryptograms. During an EMV transaction the terminal will obtain from the card at least one Application Cryptogram (AC) that can be verified by the card issuer. These cryptograms, which are dynamically generated, can be one of the following:

ARQC : generated when the chip card requests online authorization

TC: generated when the chip card approves the transaction

AAC: generated when the chip card declines the transaction

AAR: generated for authorization referrals.

If the card generates an ARQC then the terminal sends this to the issuer who responds with a cryptogram called the ARPC which can be verified by the card. This process is known as online dynamic data authentication or Online Mutual Authentication (OMA). TCs are retained by the terminal for inclusion in the clearing records.

These transaction cryptograms are dynamically generated by the chip card and use symmetric cryptography, employing a unique key derived from a master key shared between the chip card and the issuer.

ANNEX 8 User authentication to E-payments methods analysis

ANNEX 8.1. Building blocks underlying e-payment schemes

ANNEX 8.1.1 SSL

SSL remains a basic building block for securising e-banking transaction. Even though, when used alone SSL/TLS lacks some of the required security features, when associated with one or several of the next payments techniques, it brings a quite high level of securisation (encompassing the bank side authenticating towards end-user).

SSL (Secure Socket Layer) was originally developed by Netscape and published as an Internet draft document. It has been designed to provide an end-to-end secure Internet channel. The version of SSL used in current implementations is version 3. The Transport Layer Security (TLS) protocol is very similar to SSL version 3 and is not really a new protocol; it is actually an IETF5 initiative whose goal was to produce an Internet standard version of SSL. The Wireless Transport Layer Security (WTLS) protocol provides functionality similar to the TLS protocol but is optimized for low bandwidth mobile networks.

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 transaction). SSL/TLS allows for the 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 our cases, this enables the customer to authenticate his bank by checking the fact that the url he is connected to dully belongs to the banks.

SSL/TLS covers thus the security requirement of the end-users that are:

- authentication of the bank towards the end-users
- confidentiality of exchanged data

However, the cardholder must usually trust the merchant, as there is no policy or legal framework describing who can be trusted. In addition, with respect to the authentication in SSL, there is a risk that the merchant is not authenticated but only identified in some way. The merchant is indeed authenticated through a digital certificate obtained from a trusted Certification Authority (CA). This authentication is often not very effective, both because of the lack of checks during merchant registration for a digital certificate and also because of the lack of user awareness. Indeed, safe merchant authentication assumes that the end-user has not been subject to web spoofing attacks, meaning that he/she has not been redirected to a website different from the one he/she thinks to be visiting (e.g. Mybank.com instead of Mybanque.com). This may occur:

- If the connection is hijacked by some means by a fraudulent actor. There are various ways in which such hijacking of a connection could be achieved (one possibility would be that the hacker has managed to register one or more common misspellings of the URL of a well-known bank, another possibility would involve manipulation of Internet traffic). This could be achieved by the hacker putting up an html screen that

VERSION 0.7

looks like the screen provided by the genuine bank. Of course, the URL displayed by the browser will not be correct, but it is supposed here that the cardholder fails to notice this (this is actually a very reasonable assumption)

- If the cardholder is invited to go to this URL by a commercial e-mail that looks to come from a trusted source (his (her) bank).

In both cases, even if the end-user is attentive to the use of SSL, the hacker may also manage to get a dully recognised certificate from a well-known CA. Indeed, if the security and registration procedures of this Certification Authority are inappropriate it can sustain that type of attacks. An example of such an attack is the Microsoft impersonation in March 2001, where two digital certificates were issued by mistake by VeriSign in Microsoft's name, allowing hackers to fool people into running harmful programs. In addition, very few cardholders reject the certificate when they are warned by their browser that the certificate is not trusted.

The variant of the attack consisting of the conduction of a fraudulent transaction by a fraudulent but legitimate merchant, is also feasible. But this variant involves fraudulent merchants billing a transaction in their name; they are likely to be detected by fraud detection mechanisms.

These attacks where a hacker tries to get information from an end-user are often called "phishing". When the hacker does it via a web-site that looks very like the bank site, it is called "web spoofing". All cases where the hackers stands (transparently) between an end-user and his bank (either to steal information and/or to modify parameters in a transaction), are so called "man-in-the-middle" attacks.

A way to help to prevent web spoofing attack is the use of dedicated software (e.g. an applet from the bank). The user installs the software and at the occasion of the first connection, it is parameterised to connect to the bank server only. Although this solution is technically "hackable", and reduces a little bit the user mobility, it is an additional security.

ANNEX 8.1.2 OTP

OPTs are described comprehensively in annex 6.

ANNEX 8.2. Security building blocks underlying (Credit) Card payment based transactions

ANNEX 8.2.1 No security

Card details and other personal data are transmitted in clear (between cardholders and merchants) whenever a payment is conducted. There is no confidentiality or integrity of the data, and no participant is authenticated in the transaction. In addition, as all transmissions are unprotected, the credit card details can easily be copied and used in other Internet transactions (replay attacks) or can be used to produce counterfeit physical cards.

Although this solution is clearly easy to use and to implement (no device or software to use), the risk of fraud is huge.

Since the cardholder is often offered a ‘no liability’ guarantee in case of fraud since the merchant side of the business bears the costs of any fraudulent transaction, it is in the interest of merchants to make use of security techniques to support electronic transactions.

User(s) authentication / verification / identification

CRITERIA	Cardholder	Issuer	Merchant	Acquirer
<i>Confidentiality</i>				
<i>Integrity</i>	---		---	
<i>Merchant authentication</i>	---			
<i>Replay protection</i>	---		---	
<i>Cardholder Authentication</i>			---	
<i>Cardholder non-repudiation</i>		---	---	---
<i>Ease of use</i>	+++			
<i>Ease of implementation</i>		+++	+++	+++
<i>Interoperability</i>		+++	+++	+++

ANNEX 8.2.2 Transaction SSL (TLS) protected

SSL/TLS (see here above) it is very often used to secure the conduct of electronic transactions over the Internet, and hence is used to protect the transfer of debit and credit card details.

SSL allows for data protection (data are encrypted during the session) and for principals’ authentication in e-commerce as follows:

- Data encryption: All communications over the SSL channel are generally encrypted using 128-bit algorithms, but this protection is true only during transmission across the web, protecting the credit card numbers from hackers; it does not reduce intentional fraud by either the cardholder or the merchant. When the information arrives at the merchant’s web site, it is decrypted and accessible by the merchant (the card data can be disclosed by attacks on the merchant’s system or by fraudulent merchants).
- Merchant’s authentication: cardholders authenticate merchant by means of its SSL certificate⁴.
- User authentication: Such as already stated previously of the present document, in theory SSL may also sustain cardholder authentication towards the merchant, provided that the cardholder is in possession of a digital certificate. This function is however rarely used, the first reason being that there is lack of PAN European IDM interoperability, especially between commercial, public and bank CAs (e.g. a widely recognised commercial CA cannot by default make the link between the cardholder

⁴ When used with circumspection, see previous section

VERSION 0.7

and his credit card details, while a private bank CA will not be recognised by another bank in another country. SET, which was set-up in that purpose has failed, see below). In addition, the cardholder already disposes of an authentication credential; his (her) card. Therefore, in an on-line transaction, the cardholder authentication relies on the card only; the merchant has no proof that the user is the true owner of the credit card. This risk increases with the purchase of a service delivered on-line as well as ordered on-line.

The overall process takes only a few seconds.

From the cardholder's perspective, the use of SSL does not require any additional software or a digital certificate to be installed. SSL is built into all current browsers, as well as into many wireless web access devices, such as web-enabled mobile phones and PDAs.

From the merchant's perspective, the implementation of SSL is also easy, as SSL is integrated into most server software. The merchant only needs to request a server certificate from a trusted Certification Authority.

The SSL/TLS protocols are usually considered as a simple, cheap and quick solution to implement, which can be used on any Internet-enabled device. This is why this technique has gained widespread acceptance, and is used for the vast majority of on-line purchasing today.

User(s) authentication / verification / identification

CRITERIA	Cardholder	Issuer	Merchant	Acquirer
<i>Confidentiality</i>	++		++	
<i>Integrity</i>	++		++	
<i>Merchant authentication</i>	+			
<i>Replay protection</i>	-		-	
<i>Cardholder Authentication</i>			---	
<i>Cardholder non-repudiation</i>		---	---	---
<i>Ease of use</i>	+++			
<i>Ease of implementation</i>		+++	+++	+++
<i>Interoperability</i>		+++	+++	+++

ANNEX 8.2.3 Virtual and pseudo Card Numbers

Both virtual and pseudo card numbers avoid the need for cardholders to send their real credit card number over the Internet. They are both recorded against cardholders' real credit card numbers by the issuer. The difference is that pseudo card numbers are more flexible; lifetime, transaction value or the number of transactions can be set in advance (namely by the cardholder which will by this way limit his liability. Note that he still have to protect his authentication means (e.g., password), and to some extent be liable for misuse.). Virtual card numbers are real credit card numbers that are not necessarily associated with a physical card.

VERSION 0.7

Cardholders need to register for a virtual account (for virtual card number). Pseudo card numbers can be issued to cardholders either at the issuer's web site or in a digital wallet provided to cardholders by their issuer, rendering the request process simple. The digital wallets are used to store personal and financial information such as credit card details. They can be server-based, meaning that the information is stored on a central server allowing the information to be accessed at any time by any device connected to the Internet, such as a PC, PDA or mobile phone. The cardholder has to apply for a number before any transaction, and in many instances an applet is also required.

From the standpoint of making a purchase, merchants and payment systems will handle virtual OR pseudo card numbers the same as they would a real card number. In fact, it is unlikely that they would even know the card number is virtual. Virtual or pseudo card numbers can be used as a stand-alone program (easy to implement and to deploy) or can be integrated into solutions such as SSL.

When the cardholder wishes to buy something, he provides the pseudo card number (instead of the real card number, using the existing merchant infrastructure (this can include SSL/TLS but can also include nothing), then the merchant sends an authorization request to its acquirer. This request is transferred to the issuer, which has to map the pseudo card number by the real card number. The issuer then sends an authorization response, which is finally forwarded to the merchant. Once pseudo card numbers expire, e.g., any purchase attempt is invalidated, enhancing the protection against fraud.

Merchants do not have to implement anything or to modify their site, as pseudo card numbers are indistinguishable from real card numbers and can pass through their existing infrastructure transparently. The process is then easy for them.

However, a major drawback of using pseudo card numbers is the significant impact on the issuer authorization and clearing systems, since pseudo card numbers – as for virtual card numbers – need to be translated by the issuer to the real card numbers.

The main benefits are the following: by restricting the validity period or number of possible replay, the risk to face fraudulent transaction is limited.

User(s) authentication / verification / identification

Table below summarizes how well the requirements of cardholders, issuers, merchants and acquirers are met when pseudo card numbers are used as stand-alone solution. Note that the security requirements can vary if pseudo card numbers are used in conjunction with another technique.

CRITERIA	Cardholder	Issuer	Merchant	Acquirer
Confidentiality	- (*)		---	
Integrity	-		---	
Merchant authentication	---			
Replay protection	+		+	
Cardholder Authentication		+++	+++	

VERSION 0.7

<i>Cardholder non-repudiation</i>		++	++	++
<i>Ease of use</i>	+/-			
<i>Ease of implementation</i>		-	+++	+++
<i>Interoperability</i>		+++	+++	+++

(*) This assessment changes if pseudo card numbers are used in conjunction with another technique.

ANNEX 8.2.4 SET and 3D SET

SET is not used anymore today; however, it is still described here because SET is a good example of the duality that may exist between user friendliness and security (it was a very strong protocol from a security point of view, principals authentication in particular, but too complex to implement / use for all principals and consequently, never adopted). Lessons learned from the SET experience are very interesting in the framework of our study.

The main advantages of the SET protocol are that it provides integrity and confidentiality of the information, it guarantees the payment and non-repudiation to the merchant and it authenticates all the parties involved in a transaction using digital certificates (achieving thus a strong authentication in the sense of annex 6, letting thus some opportunities to merchants to shift the liability for fraud to the issuer). The digital certificates for merchant and cardholder authentication are issued by (different) Certification Authority using strict procedures.

In addition, through the use of dual signatures, the merchant does not see the payment information but only the order information, while the issuer does not see the order information but only the payment information. In particular, the risk of sensitive payment information stored at the merchant server being stolen is avoided and the cardholder privacy toward issuer is enhanced.

SET and 3D Set have been described in [44]

However, technical interoperability among different vendor solutions was not easy to achieve. Furthermore, for all parties, the implementation was complex and costly:

- It required cardholder wallet software (of approximately 4 Megabytes) and digital certificates to be installed on the cardholders PC, impeding cardholders' mobility but also requiring huge support. Moreover, due to the size of the software elements (approximately 4 MB), SET cannot be used with devices with scarce resources, such as mobile phones.
- There were also implementation issues for merchants. Issuers and acquirers were further required to distribute software and manage the issuing of certificates.

As a consequence, In August 2002, MasterCard announced it would phase out support for SET over the coming years. Thus, as of March 2006, all MasterCard certificates expired and the SET protocol may no longer be used with the MasterCard hierarchy.

VERSION 0.7

In an attempt to address the lack of adoption of SET and to promote the SET solution further, server-based implementations of SET were developed; 3D-SET⁵.

The model allows the Issuer and Acquirer to select from among a variety of different authentication mechanisms in their domain. In the 3D-SET model the user wallet and certificate reside on a server hosted by the Issuer (called a Server Wallet), instead of being installed at the Cardholder's PC, which was the case with SET. The Cardholder then has to authenticate to the Server Wallet before a payment transaction can occur. In parallel to that the Merchant software and certificate reside on a server hosted by the Acquirer. The transaction flow in the Interchange Domain in 3D-SET is the same as the original SET, but for the cardholder authentication the thin wallet redirects the SET payment initiation message to the SET server wallet at the issuer's side. Cardholder authentication takes place between the cardholder and the SET server wallet (e.g. using a password).

The issuer is responsible for choosing the authentication method. From a security point of view, 3D-SET is nearly as good as SET. **It is dependent on the Cardholder authentication mechanism the Issuer uses.**

It is easier to implement than SET. In 3D-SET, the Issuer can implement and operate a Server Wallet in its own controlled environment and needs only to distribute a Thin Wallet to the Cardholder's PC, (while SET required a Thick Wallet at the Cardholder's PC).

It offers the possibility of several communication channels, which means that the solution is more suitable for alternative authentication channels, using such devices as mobile phone or PDA.

The Merchant can choose to have his SET Server hosted by the Acquirer.

Although these developments did improve the usability of SET, the protocol remained difficult to manage from an implementation perspective. In the end, 3-D SET improvements were not sufficient and (3D)- SET are not used anymore.

User(s) authentication / verification / identification

The following table summarizes how well the requirements of cardholders, issuers, merchants and acquirers are met with (3-D) SET.

CRITERIA	Cardholder	Issuer	Merchant	Acquirer
<i>Confidentiality</i>	+++			+++
<i>Integrity</i>	+++			+++
<i>Merchant authentication</i>	++			
<i>Replay protection</i>	+++			+++
<i>Cardholder Authentication</i>		+++ (SET) Depends on implementation (3D-SET)		++

⁵ 3-D stands for 3 domains, the 3 domains of authentication, (i) between cardholder and issuer, (ii) between merchant and acquirer and (iii) between issuer and acquirer.

VERSION 0.7

<i>Cardholder non-repudiation</i>		+++	+++	+++

	(SET)			
<i>Ease of use</i>	++			
	(3D-SET)			
<i>Ease of implementation</i>	---	(SET)	---	---
	--	(3D-SET)	(SET)	(SET)
		SET)	+	--
<i>Interoperability</i>		+++	+++	+++

ANNEX 8.2.5 3-D Secure⁵

This protocol is an industry-standard payment security mechanism and utilizes SSL encryption to protect payment card information. 3D-Secure, like 3D-SET allows the Issuer to choose a mechanism which is sufficiently strong to authenticate the Cardholder.

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

3-D Secure is not an authentication method but well a payment architecture on the Internet

- 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:

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

Possible authentication means are:

- static password
- dynamic password (possibly generated by a mobile phone)
- CVD (virtual dynamic card (see annexe6)
- EMV card reader, that can be:
 - a mobile phone
 - an off-line smart-card reader e smart-card reader
 - FinREAD : (on-line smart-card reader) (see annex 6)
 - ...

The VISA (marketed as Verified by Visa) and the MasterCard implementation of 3-D Secure (forming part of the MasterCard SecureCode family of cardholder authentication techniques), are built upon 3D-Secure (and will be further detailed here after).

3 DSecure in a nutshell, works as follows:

- Issuer enrolls Cardholders and register them,

VERSION 0.7

- The Merchant on his side must implement a component called a Merchant Server Plug-in (MPI),
- In a purchase transaction it is then the responsibility of the Issuer to authenticate the Cardholder by means of a chosen authentication mechanism,
- When a Merchant receives a payment initialisation transaction, the MPI is activated and passes a query to the issuer to find out whether the Cardholder is a participant. If so, the MPI initiates, through the Cardholder's browser, the authentication process between the issuer and the Cardholder. The result of the Cardholder authentication is sent as a signed response to the MPI, again through the Cardholder's browser. The MPI then checks the response from the issuer and performs a standard authorisation request through the Acquirer.

All transactions are SSL protected, in particular with client-server authentication. There is in addition a transaction signature from the issuer to the Merchant. In order to settle any disputes between parties Visa, e.g., hosts an Authentication History server that can keep track of all authentication results.

To authenticate themselves as the true owners of their credit cards, cardholders must at least provide a password to their issuer. Issuers can use other methods of authentication, e.g. based on chip cards, but password is the easiest method to implement for the issuer and is likely to be the most common form of cardholder authentication. The requirements for cardholders are therefore minimized, as they only need a browser to participate. They do not need to make use of any special software or hardware.

However, the server authentication issue as described earlier for the SSL/TLS protocols used in e-banking solutions, is also present here. In addition, man-in-the-middle attacks can take place, e.g. to redirect the cardholder to a location other than the genuine issuer ACS and capture his username/password. Such attacks were described previously.

Such as for e-banking solution, a solution to avoid this would be the installation by the cardholder of software integrated with 3-D Secure to improve security, but the introduction of client software at the cardholder level conflicts somewhat with the design aim of minimizing the impact on the cardholder. The same problem would occur if authentication methods based on chip card were considered.

Note that 3-D Secure does not protect confidentiality of card account details at the merchant server.

Within the issuer domain, the issuer must deploy a system consisting of enrolment and access control server modules. It is clearly vital that this process does not enable third parties to impersonate valid cardholders and set up false authentication details. It is up to the issuer to set-up strong authentication means (e.g. dynamic password, ...) and take care the enrolment procedures.

3-D Secure is, on the whole, a much simpler system than SET, even if it requires issuers and merchants to deploy and integrate certificates.

From the usability point of view, the fact that cardholders do not need any certificate or software is a significant improvement compared to SET. The authentication of the cardholder

VERSION 0.7

is a mean of reducing the incidence of fraud and chargeback. However, its vulnerability to phishing attacks exposing the cardholder's username and password is a security concern and could be improved (A possible solution could be the use of dynamic authentication instead of static authentication).

Finally, 3-D Secure has multiple redirects, and care must be taken in the merchant implementation to minimize incidences of disconnections and any resulting cardholder confusion or processing time impact.

3-D Secure offers two additional security services to the merchant: it provides cardholder authentication and also a message signed by the issuer containing cardholder and transaction details. 3-D Secure provides thus a clear merchant benefit by providing for access to enhanced payment guarantees. While the solution clearly falls well short of the level of security offered by SET, the implementation challenges are considered considerably less and the cardholder does not require certificates or applets.

SET offered cardholder strong authentication and other benefits not addressed by 3-D Secure. These benefits included protection for payment information stored at the merchant server (in 3-D Secure, the merchant is indeed able to store the credit card numbers on the merchant's server), as well as offering the highest possible levels of privacy protection for the cardholder and merchant. These benefits, however, were at a cost and complexity that the market has been unwilling to bear.

Advantages

- Easy for the Cardholder - no additional software required
- Full mobility for the user from any access device
- Cardholders are enrolled by Issuers – no explicit registration is required
- Less complex than 3D-SET

Disadvantages

- Merchant implementation complexity, requiring Merchant Server Plug-in.
- Payment information (e.g., card number, expiry date) revealed at the Merchant. Server (not the case with 3D-SET).
- Merchant able to redirect the Cardholder to fake ACS, thereby capturing User ID and password.
- Increased number of Internet links involved in a transaction.

User(s) authentication / verification / identification

The following table summarizes how well the requirements of cardholders, issuers, merchants and acquirers are met 3D-Secure is implemented

CRITERIA	Cardholder	Issuer	Merchant	Acquirer
<i>Confidentiality</i>	++		++	
<i>Integrity</i>	++		++	
<i>Merchant authentication</i>	+			
<i>Replay protection</i>	+++		+++	
<i>Cardholder</i>		++	+++	

VERSION 0.7

<i>Authentication</i>		(less than SET, more than SSL)		
<i>Cardholder non-repudiation</i>			+++	+++
<i>Ease of use</i>	++			
<i>Ease of implementation</i>			-	-
<i>Interoperability</i>			+++	+++

ANNEX 8.2.6 3-D - .* implementations**8.2.6.1 Verified by Visa⁶**

Verified by Visa is the Visa authenticated payment programme that implements the 3-Domain model with the 3D-Secure protocol. Verified by Visa is the service name that cardholders associate with the Internet authentication capability from their Issuer. Verified by Visa is used initially at the time of enrolment and on an ongoing basis during each online interface with Issuers for authentication.

The service aims to strengthen the authentication roles of Issuers (for their Cardholders) and Acquirers (for their Merchants) for Internet transactions.

How Verified by Visa Works

Cardholders must register their cards at the issuer's registration site. Typically, this one-time process involves answering several security questions to which only the issuer and the cardholder know the answer. The cardholder selects a password and agrees on a secret phrase, which will be used by the issuer during each transaction. Some issuers use a mass enrolment process, which allows cardholders to quickly register at the time of their first online purchase. After cardholders register their cards, they are ready to shop securely at any participating online merchant.

⁶ Visa has also collaborated with other payment card companies to create a single set of industry requirements, called the Payment Card Industry (PCI) Data Security Standard, for consumer data protection. The PCI Data Security Standard aligns Visa's Account Information Security program, (also known as Cardholder Information Security Program in the U.S.), with MasterCard's Site Data Protection (SDP) program to create streamlined requirements, compliance criteria and validation processes.

This PCI Data Security Standard also addresses the concerns of merchants' and acquirers' (financial institutions that enable merchants to accept Visa cards for payment) about having to meet more than one set of standards to accomplish a single goal. However this standard does not concerns directly end-user verification methods and is thus out of scope of the present study.

VERSION 0.7



The Technology

Verified by Visa is based on the Three Domain ("3-D") Secure protocol, the payment industry's Internet authentication standard used by major card brands. Developed by Visa, 3-D Secure allows card issuers to authenticate cardholders using passwords, chip cards, digital certificates, etc. during the purchase transaction. Verified by Visa can be integrated into existing merchant e-commerce systems with little impact on the existing checkout process. Visa has established partnerships with a number of global firms to support implementation of Verified by Visa.

With Verified by Visa, cardholder identity is confirmed with the use of a personalized password during the checkout process, as the cardholder's bank validates the password, ensuring that only authorized users of the account can use it to shop online.

Verified by Visa supports all consumers with magnetic stripe Visa cards. Participation by cardholders is easy – access to a PC with one of several widely used Internet browsers is all that is needed. Cardholders visit the Issuer's enrolment site and provide the information requested. Upon validation by the Issuer, the cardholder is enrolled and is able to use Verified by Visa at participating merchants.

The service also supports consumers with a smart Visa card, by using card readers and PC software provided by the Issuers, which allows cardholder to authenticate the card (in addition to them). As with a standard Verified by Visa request, the Issuer's server sends a pop-up window to the cardholder's browser, prompting the cardholder to enter a password for cardholder authentication and insert the smart Visa card for card authentication (card cryptogram).

Merchants have no additional requirements - the Issuer's server formats an authentication response message in which the smart Visa card authentication data are communicated within one of the existing transaction data fields forwarded for all Verified by Visa transactions. Additionally, participating merchants may use the Verified by Visa identity graphic on their web site to communicate support for this service.

8.2.6.2 MasterCard SecureCode™

MasterCard SecureCode is the name to be used for all existing and new MasterCard cardholder authentication solutions. Recognising that a single solution may not work for all Issuers, MasterCard SecureCode enables them to choose from a broad array of security solutions for authenticating their Cardholders. It includes the MasterCard implementations of:

- 3D-Secure,
- SPA (Secure Payment Application) -UCAF (Universal Cardholder Authentication Field)⁷ and
- CAP (Chip Authentication Program) - UCAF.

While the three solutions listed above appear rather different at a high level, all three schemes share important common elements. Hence the common program name – MasterCard SecureCode™.

After having been registered toward the SPA service from his bank, the cardholder downloads an SPA applet that will provide the necessary payment details to the merchant.

- **PC Authentication Program** – combine SPA with the Universal Cardholder Authentication Field (UCAF) hidden fields deployed by participating Merchants. Since based on SPA, this specification involves the use of a small downloaded applet by the Cardholder.
- **Chip Authentication Program (CAP)** – designed to integrate the ease of use and security of an EMV-compliant smart card for authentication through a user’s PC. This solution is designed to interoperate with the UCAF hidden fields and specifications and is supported by both standalone and connected smart card readers.
- **MasterCard’s implementation of 3-D Secure** – MasterCard is providing further Issuer choice by supporting a MasterCard implementation of the 3-D Secure specification. In June 2002, MasterCard completed negotiations with Visa for an agreement that allows for a MasterCard implementation of 3-D Secure that includes support for the SPA algorithm and UCAF without any changes to the core 3-D Secure specification or protocol. With this agreement, MasterCard’s implementation of 3-D Secure becomes the client-less (no Cardholder download) authentication solution for MasterCard and Maestro Issuers that prefer not to deploy applet-based security solutions.

In each case, two main events occur.

⁷ It is a variable length field transferred to the issuer in the payment authorization request to provide evidence that the cardholder is legitimate. As part of the SecureCode infrastructure, a series of HTML-based hidden fields on the merchant’s order confirmation page are specifically tagged using MasterCard UCAF field naming conventions. These fields are implemented on the web sites of participating merchants, to enable the collection and exchange of transaction-specific information. These hidden fields, including merchant name, sale amount, and cardholder authentication data, are recognized by SecureCode issuer applets, such as those used for the Chip Authentication Program and the SPA-based PC Authentication Program.

VERSION 0.7

1. The MasterCard or Maestro cardholder is authenticated using a secure private code unique to him (the SecureCode).

- For the Chip Authentication Program, a pop-up box appears on the order confirmation page with a challenge value. The cardholder enters his/her smart card into an offline card reader and enters both the challenge and the PIN. The chip generates a response which is displayed on the card reader and copied by the cardholder into the pop-window as the SecureCode.
- When using the PC Authentication Program or the MasterCard implementation of 3-D Secure, an issuer pop-up box appears on the order confirmation page requesting the cardholder to supply his/her SecureCode as established by the cardholder with the Issuer (e.g. a password).

2. The authentication data is transported from party to party via MasterCard's UCAF mechanism. Regardless of the implementation method, the cardholder authentication data is always transported between the merchant and the issuer using the MasterCard UCAF mechanism.

UCAF is a multi-purpose means of transporting cardholder authentication information, as generated by issuers and/or cardholders, between the cardholder, issuer, merchant, and acquirer communities.

Due to the infrastructure requirements for 3-D Secure, MasterCard is deploying a directory service and a multi-Issuer Access Control Server (ACS) to support these solutions worldwide. These systems are being deployed along with a hosted program option for Issuers who are not pursuing an in-house solution.

Merchant adoption of the associated MasterCard SecureCode™ platform components is expected to lead to a significant drop in their overall chargeback costs for e-commerce transactions. MasterCard and Maestro members benefit from increased customer confidence and an anticipated rise in electronic commerce activity. MasterCard members additionally benefits from fewer disputes.

PC Authentication Program

In this solution, the UCAF is used to transmit an Accountholder Authentication Value (AAV), generated by the issuer (after having dully successfully authenticated the cardholder), that links a particular cardholder and a specific purchase. The AAV is presented to the merchant via the UCAF Authentication Data hidden field, which then forwards it to the issuer for verification during authorization. Security requirements such as confidentiality and integrity are covered under SSL/TLS.

As for 3-D Secure, the PC Authentication Program does not necessarily protect the confidentiality of card account details at the merchant server when not used in conjunction with pseudo account numbers. As far as replay attacks are concerned, they are prevented through the use of transaction sequence numbers.

The advantages of the PC Authentication Program are:

- For the merchant; it does not require additional software implementation by the merchant. The only task for the merchant is to modify its check-out web page to incorporate some hidden fields (i.e. small HTML code that can be easily integrated). This is to encourage merchants to adopt the solution.

VERSION 0.7

- The acquirer must adjust its interface to its merchants and to its POS system to support the UCAF infrastructure and the transport of authentication data.
- The issuer must adjust its infrastructure to support the UCAF field. An authentication server is often the chosen option and in this case the issuer has to establish an authentication mechanism to verify the identity of its cardholders. The issuer must also implement a mechanism able to generate and verify AAVs. With respect to cardholder authentication, the issuer can choose any method, including username/password, smart cards, digital certificates or biometrics, but username and password is probably the easiest method to implement for issuers and is likely to be the most common form of authentication for credit card transactions.
- The cardholder is impacted at registration, as he/she has to download a thin applet to his Internet-enabled access device. This one-shot procedure could, for example, be achieved by the cardholder using his Internet banking facility. Note that the use of applets could simplify the prevention of man-in-the-middle attacks and allow the use of any authentication method other than classical user ID / pass-phrase, such as smart card/PIN or EMV cards (see also WP1 e-banking section). Although the presence of the thin applet on the cardholder PC is often regarded as a drawback of the solution, it is important to note that this cardholder application is automatically activated, and it is transparent for the cardholder's.

The PC Authentication Program and 3-D Secure systems are in many ways very similar. Both are based on continuing use of SSL/TLS to protect the cardholder-merchant link, and provide cardholder authentication. In both cases, cardholder authentication is performed by the issuer, and following successful cardholder authentication the issuer creates an 'authenticator' that is sent to the merchant. The nature of the authenticator produced by the issuer is different. As far as the protection from attacks by fraudulent merchants is concerned, the differences between both schemes appear also to be very small. The use of an applet by the PC Authentication Program may provide a somewhat higher level of resistance to man in the middle attacks than does 3-D Secure. In addition, one easy way to prevent such attacks exists and consists of requiring the cardholder to initiate the operation of the wallet application.

As for 3-D Secure, the PC Authentication Program offers an improved level of security over naïve use of SSL, but primarily in terms of offering the *merchant* additional security guarantees by providing a means for the issuer to actively authenticate the cardholder during an online transaction. Indeed, in addition to the services offered by the use of SSL/TLS to protect the cardholder merchant link, the PC Authentication Program offers two additional security services to the merchant: it provides cardholder authentication to the merchant and also an Issuer-verifiable AAV dependent upon cardholder *and* transaction details. Hence the PC Authentication Program certainly offers an improved level of security for the merchant.

The PC Authentication Program, as well as 3-D Secure, clearly offers less security than that offered by SET:

- SET relied on a strong cardholder's authentication, but at the issuer cost.

VERSION 0.7

- SET included protection for payment information stored at the merchant server (in the PC Authentication Program, the merchant is able to store the credit card numbers on the merchant's server)

User(s) authentication / verification / identification

The following table summarizes how well the requirements of cardholders, issuers, merchants and acquirers are met with the PC authentication program.

CRITERIA	Cardholder	Issuer	Merchant	Acquirer
Confidentiality	++		++	
Integrity	++		++	
Merchant authentication	++			
Replay protection	+++		+++	
Cardholder Authentication			+++	
Cardholder non-repudiation		+++	+++	+++
Ease of use	+			
Ease of implementation		-	+++	++
Interoperability		+++	+++	+++

MasterCard Chip Authentication Program (CAP)

The Chip Authentication Program (CAP) integrates the use of an EMV-compliant smart card with a downloaded applet. This assumes the cardholder to be supplied with a reader, into which is inserts the cardholder's EMV compliant chip card. This reader possesses a simple display and a numeric keypad, and is either connected or not connected to the cardholder PC (see e-banking section of this chapter for more details).

During a transaction using the Chip Authentication Program, the cardholder will see a pop-up window appearing on the order confirmation page, accompanied by a challenge value. The cardholder enters his/her smart card into an offline card reader and enters both the challenge and his/her secret PIN into the reader. The reader then passes the PIN and information derived from the challenge to the chip card. The chip card verifies the PIN and generates a response which is displayed on the card reader. This response is copied by the cardholder into the pop-window as the *SecureCode*.

The main differences between the CAP solution and the PC authentication program are the following:

- The applet running on the cardholder PC does not play the role of a wallet but rather acts as the interface between the merchant and the cardholder's reader.
- The role of the wallet is filled by the EMV application on the card as it securely stores cardholders' keys and generates the AAV.

VERSION 0.7

A main advantage of the CAP solution is to re-use the EMV cards currently deployed today. Cardholder authentication is performed using the current EMV offline PIN verification. A reader need to be distributed to cardholders.

The adoption of an EMV card as AAV-generating device makes easier the prevention of the man-in-the-middle attack because:

- The AAV is based on the generation of a cryptogram by the EMV card. It derives typically from a 3DES MAC, which is widely perceived as strong cryptography.
- The card cryptogram itself includes data that prevent replay attacks.

It must be noted however that the input challenge has to be entered manually by the cardholder. It results in short challenges that the non-repudiation of the transaction is not formally ensured because several input data may result in the same challenge (based on a hash). This is a limitation compared to PKI signed transactions.

The use of a reader makes it particularly suitable for performing security functions, e.g. PIN entry, as it is unlikely to be vulnerable to techniques like tampering or keyboard sniffing.

User(s) authentication / verification / identification

The following table summarizes how well the requirements of cardholders, issuers, merchants and acquirers are met with CAP:

CRITERIA	Cardholder	Issuer	Merchant	Acquirer
Confidentiality	++		++	
Integrity	++		++	
Merchant authentication	++			
Replay protection	+++		+++	
Cardholder Authentication			+++	
Cardholder non-repudiation		++	++	++
Ease of use	+++			
Ease of implementation		-	+++	++
Interoperability		+++	+++	+++

ANNEX 8.2.7 Security evaluation of 3-D Secure implementations

▪ Initialisation

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

VERSION 0.7

The lifecycle of all authentication devices must be managed correctly, from the design to the delivery to the cardholder, 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, it varies 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 cardholder to verify the merchant's identity.

However, although the use of a strong method of authentication by the Issuer is expected, 3-D Secure and SecureCode type of systems offer a level of security that is strongly dependent upon the type of authentication chosen by the issuer. Authentication systems used (username/password) may have inherent weaknesses such as bad choice of password.

For now, it seems that issuers are choosing username / password. In this case, security is improved to a limited extent only. In principle, however, 3-D Secure and SecureCode type of systems can provide good technical security.

Therefore usage security evaluation is (+). Again this evaluations 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 this information, so the cardholder 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.

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

ANNEX 8.3. PayPal

This section describes one of the most widely spread systems in Europe namely PayPal. Due to proximity in shareholding between eBay and PayPal (PayPal, the online payments unit of auction website eBay Inc.), this payment schemes 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 online.

PayPal enables individuals and businesses to send and receive electronic money online. It also provides other financial and non-financial services closely related to online payments. These services are collectively referred to hereafter as the “Service”.

PayPal does not provide credit, banking and/or escrow services

The Service is provided by PayPal (Europe) Ltd. to registered users in the European Union (each a “User”) and, as from 02 July 2007, a new PayPal company, PayPal (Europe) S.à r.l. & Cie, S.C.A. (PayPal Luxembourg), 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 Luxembourg provides the PayPal service throughout the EU.

PayPal primarily functions as a payments intermediary for individuals and organizations 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 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 PayPal account, he directs PayPal to credit his credit or debit card or bank account via a credit transfer or even a paper check.

How does it work?

Opening a PayPal account

The Service allows individuals and businesses to open an account maintained by PayPal (an “account”).

To be eligible for an account, a user must:

- either be an individual (at least 18 years old) or a business that is able to form a legally binding contract; and
- have satisfactorily completed our sign-up process
 - As part of our sign-up process, a user must:
 - register an email address, which will also act as their ‘User ID’;
 - submit details of the source(s) with which they wish to fund their PayPal account (e.g., details of the User’s bank account, debit card or credit card). This is the “funding source”; and

VERSION 0.7

- agree to PayPal privacy policy and the terms and conditions of our user agreement, including the policy documents incorporated within it (the “Agreement”)
 - Each User must create a password, which together with their User ID (email address), allows a User to access their account and use the Service

To fund an account, a User must either

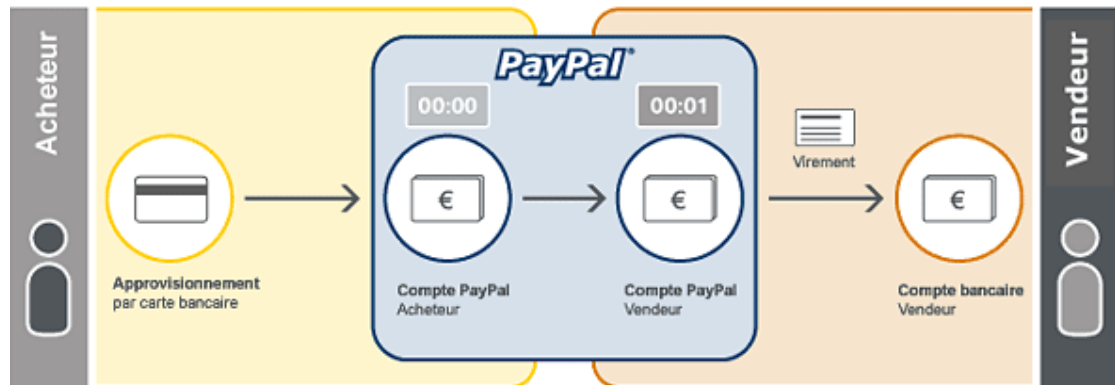
- purchase electronic money from PayPal via their funding source(s). In practice, this means that each time a User requests PayPal to send money, PayPal simultaneously debits the chosen amount from the User’s default funding source (bank account, debit card or credit card). PayPal then sends this online payment to the intended recipient; or
- accept an online payment that has been issued by PayPal and sent from another PayPal User

Sending payments

To send a payment to a third party via the Service, a User must provide the email address of the intended recipient (the “recipient”). By doing so, the User sending the payment (the “sender”) instructs us to transfer electronic money from their PayPal account to the account of the recipient. If the payment is accepted by the recipient, PayPal completes the transfer

Receiving payments

User is able to receive a payment via the Service by accepting a payment from another User. The recipient is able to return payments or, in some cases, use the Service to refuse payments that have been sent by another User



Seller Protection Policy: Under certain circumstances, PayPal will not hold the seller of goods who receives a payment via the Service liable if the buyer of the goods (i.e. the person sending the payment) claims that their transaction was unauthorised

Buyer Protection

- While PayPal are not generally liable for a User’s access to, and use of the Service, PayPal will not hold its Users liable for any unauthorised use of their account by any

VERSION 0.7

third person, provided that they are satisfied that the User has not acted deliberately so as to enable any third person to gain access to their user ID and/or password

- PayPal Buyer Protection Policy assists buyers of goods who send payments via the Service to recover a certain amount of funds from sellers who list on eBay and who are registered PayPal users in Austria, Australia, Belgium, Canada, France, Germany, Hong Kong, India, Ireland, Italy, Japan, Korea, The Netherlands, Singapore, Spain, Switzerland, Taiwan, the United Kingdom and the United States
- Users have the ability to claim against a merchant in case of litigation, according to the PayPal claim program and policies.

Protection against non-authorized payments from a user account.

- PayPal sends a confirmation email for any on-line PayPal payment.
- If a user receives a confirmation email for transaction he (she) does not authorise, he (she) is not liable.

Security

1) PayPal never shares user's financial information with or sells it to merchants.



1. User's sensitive financial information is securely stored on PayPal servers.
2. When users use PayPal to pay online, they provide only their PayPal email address.
3. The merchants/retailers receive payment from PayPal without ever seeing your financial information.

2) Information is automatically sent with a high level of data encryption.

3) Protection against non-authorized payments from a user account.

- o PayPal sends a confirmation email for any on-line PayPal payment.
- o If a user receives a confirmation email for transaction he (she) do not authorised, he (she) is not be liable.

Additional security

1. User strong authentication (dynamic password)

Optionally, users can quire a PayPal Security Key generating a unique six-digit security code about every 30 seconds. They enter that code when log in to their PayPal or eBay account with their regular user name and password. Then the code expires – no one else can use it.

2. Addition buyer's protection: merchant's verification:

VERSION 0.7

Verification increases the security of the PayPal network. Verified members have successfully completed PayPal's Verification system to establish their identity with us. The Verification process varies by country or region. For example, in the U.S., a Verified member has added and confirmed a bank account with PayPal. In Germany, a Verified member has completed a bank transfer or the Expanded Use Process. In most countries and regions where PayPal is available, a Verified member has added a credit card and completed the Expanded Use process.

Mobile Paypal is also possible

Mobile transactions are PIN-protected.

Activation

User activates his phone for PayPal Mobile – on the PayPal website or from the mobile internet – he'll create a unique mobile PIN that streamlines payment confirmation. To complete the activation, Paypal calls or text the user to verify his request.

Privacy

Credit card and banking information are never revealed.

Transaction control

A user confirms payment details for every transaction he makes. Otherwise, no money is sent.

Account is safe, even if phone is lost or stolen

PayPal account can only be accessed by phone if user uses his Mobile PIN or username and password.

PIN and password protection

PayPal will only ask for the PIN or Password for transactions that user initiates or to confirm ownership of the phone.

Conclusion on Paypal authentication

Regarding user authentication, Paypal uses ownership of an email address to authenticate users on first registration. In order to make withdrawals or make larger payments, ownership of a credit card or bank account is required to complete the transaction. These methods are reasonably secure.

However, when not used without the here above mentioned additional security measure, 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. This can go wrong by making a typo, or by attackers obtaining an address which suggests they are from a certain organisation. In case of ordinary bank transfers this is much stronger: an account number should often have specific properties (such as divisibility by 11) in order to prevent typographical errors, and the name and city of the payee are matched with the account number.

VERSION 0.7

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

ANNEX 9 M-payments related techniques: Mobile Security Basics and Mobile Payment Security Techniques

This sections aims to provide a high level overview of the basics of Mobile Security and a general overview of the security techniques used in Mobile Payment.

Basic Mobile Security

In a high level view of mobile security, the following security domains are considered:

- **Local Domains:** These local domains include the user and its mobile device, as well as the service provider and the web server acting as the access point to the service. The security of these domains is the responsibility of their owners.
- **Mobile Network:** The security of the over-the-air link and of the operator network is covered by telecommunication standards and techniques such as the GSM standards. When security functions are available, they are mainly implemented at the bearer level.
- **Internet:** Security at the transport layer is provided either by mobile specific protocols, such as WTLS or proprietary protocols, or, within the Internet domain, by classical systems such as SSL or TLS.

Several constraints impact the design of security services available on GSM mobile devices. The delay of the initial call set-up must be kept as short as possible for convenience reasons. The additional bandwidth requirements must be as small as possible. Limited computing resources available on platform items, in particular on SIM cards, require the system to be as simple as possible. And of course the cost impact must be as limited as possible.

The communications between the mobile devices and the base stations are protected using several secret algorithms:

- The **A3 algorithm** implements the SIM card authentication mechanism. SIM card authentication obviously aims to prevent SIM card cloning. This algorithm uses a challenge/response mechanism based on a key (the so-called subscriber identification key) stored in the PIN-protected SIM card.
- The **A8 key generation algorithm** generates the keys used for subsequent encryption of the voice channel. These keys are derived from the subscriber identification key that never leaves the PIN-protected SIM of the customer. The A3 and A8 algorithms are operator-specific, although an algorithm known as COMP-128 has been used by a many GSM operators to implement A3 and A8.
- The **actual encryption of the link is performed by the A5/1 or A5/2 standardized stream ciphers**, using the key generated by the A8 algorithm. Although A5/1 is the stronger of these two algorithms, many implementations have an A8 which only

VERSION 0.7

generates a 40-bit key, so for such implementations A5/1 has only an effective key length of 40 bits. Therefore, it can be regarded as a rather weak algorithm. A5/2 is an intentionally weakened version of A5/1, developed to overcome the legal limitations on the export of cryptographic systems.

Sufficient details about these secret algorithms, i.e. COMP-128, A5/1 and A5/2, have been released to allow extensive research on their security. Several attacks, either by direct access to the SIM card or by over-the-air queries to the phone, have shown intrinsic weaknesses of these algorithms. However, these attacks are not necessarily so simple to launch (and some networks have never used COMP-128), and it could be argued that in many ways GSM suffers from less problems than, say, using SSL/TLS.

GPRS does not feature any significant improvement with respect to security. UMTS is likely to provide a better level of security, e.g. by the use of publicly reviewed and approved algorithms and by a more sophisticated authentication procedure, but it will take several years before the use of UMTS becomes general.

The communications between the base station and the Mobile Switching Centres (MSC – handling the cell sites by directing the base station controllers) and the Gateway MSC (routing calls from classical networks to the mobile station) are not cryptographically protected. While not an open network, gaining physical access allowing interception of communication may not be that difficult. Furthermore, unencrypted transmission of data and keying material may take place over-the-air between the base station and the base station controller.

SMS security

The same protection applies to SMS messages as for the voice channel. SMS messages are encrypted using the A5 algorithm while travelling on the over-the-air link.

As such, they suffer from the same weaknesses as the voice communications. In addition, the store-and-forward nature of the SMS network allows even easier access by the network providers. Other security weaknesses exist, e.g. linked to the protection of the SMS public gateways.

Furthermore, the absence of delivery guarantee may be of concern when implementing reliable payment protocols.

Mobile Payment Security Techniques

The lack of communication privacy against the network operator and the lack of end-to-end security for the Internet connectivity, amongst other weaknesses, prevent the exclusive use of GSM Basic security protocols to support secure payment applications.

SIM Toolkit based proprietary systems

VERSION 0.7

Proprietary security systems have been developed to overcome weaknesses of basic GSM security with respect to authentication or payment applications. Implementations of such systems rely on the use of the SIM Toolkit. This standardised toolkit allows programming of the SIM with any type of application that may interact with the phone. From an issuer perspective, using such SIM Toolkit systems suffer from the fact that the SIM card belongs to the operator which keep total control on the application unless agreements can be found between issuers and operators as this has been the case in Belgium for the joint issuing of the M-Banxafe SIM cards between Banksys and the Belgian mobile operators.

In closed environments, such as e-banking systems, SIM Toolkit applications may embed secret keys for use with symmetric cryptographic techniques. These keys may then be used to ensure end-to-end confidentiality and integrity of data exchange, e.g. through SMS messages.

However, in open environments or in order to provide additional services such as non-repudiation, public key cryptographic functionalities within a SIM Toolkit application may certainly be of interest. Such applications typically contain a private key that is unique to the user. Certificates for the corresponding public key of the user may be publicly distributed. The private key is used to sign messages received as SMS messages. Obviously, this signature operation is subject to the entry of a dedicated PIN. The application responds by sending back the signature in another SMS message.

Such systems are generally implemented in combination with server wallets, which send payment approval requests for a transaction to the mobile for signature. By verifying the signature received, the server wallet performs in one single step both the cardholder authentication and the validation of the cardholder approval for that particular transaction.

WAP

Dependence on proprietary solutions may be avoided by making use of standardized WAP (Wireless Application Protocol) functionalities. The current main drawback of such standardized scheme is the low penetration of WAP enabled mobile devices.

In addition to the confidentiality service available at the bearer level, the Wireless Application Protocol (WAP) 1.x stack available on most mobiles offers additional security services:

- The WTLS protocol, which is the mobile counterpart of TLS, supports confidentiality, data integrity and authentication between two communicating entities. Just like TLS, WTLS is implemented at the transport layer.
- An application-level cryptographic library, allowing digital signature and encryption. These functions may be accessed through WML Script function calls.

Both security services rely on the use of a WAP/Wireless Identity Module (WIM). The WIM is a tamper-resistant device, typically an IC card, that:

- Carries PIN-protected asymmetric keys and the related certificates,
- Perform on-board encryption and digital signature operations, and
- Implements support for WTLS authentication and encryption.

VERSION 0.7

At the minimum, the WIM stores two private keys: a key used for WTLS authentication, and a key used for signature of data by use of the WMLScript SignText function. This latter key, the so-called non-repudiation key, can only be used by providing a dedicated PIN, called the non-repudiation PIN. The non-repudiation key provides an elegant way to verify transaction approval by a specific cardholder.

The functionalities of the WIM are often combined with the SIM functions in a single IC card.

The WAP 1.x security functionality seems to offer a sound basis for the implementation of end-to-end security services. Unfortunately, WAP 1.x separates the wireless and wired part of the Internet in two domains interconnected by WAP gateways. Consequently, a translation process between WTLS-encrypted data and TLS-encrypted data takes place at the WAP gateways. Furthermore, the server authentication offer by WTLS is limited to the authentication of the WAP Gateway, which is seen as the server for every WAP communication from a mobile perspective.

Obviously, this is only acceptable for banking applications if the WAP gateway resides in a trusted domain, i.e. if it is operated by the bank.

WAP 2.0, originally released in July 2001, introduces Internet protocols into the WAP environment. A wireless profile of the TLS protocol permits interoperability for secure transactions and defines the method for TLS tunnelling to support end-to-end security at the transport level.

From an issuer perspective, the WAP-based solutions share a drawback with the STK-based solutions; that is, as was the case for the SIM card, the WIM card belongs to the telecom operator. However, in the WIM case, this mainly has an impact on the ownership of the keys stored in the WIM. The application itself resides in the WML pages and in the WML scripts received from the issuer Web Server, and are not under the direct control of the telecom operator.

ANNEX 10 Banks and eIDs cards schemes

Members of the EPC (European Payment Council) reported that they experience a lack of a coherent adoption of the EESSI standards in the MS. The reason behind, and this is confirmed by the survey, is that the standards are perceived to be too complex and suffer from a rather theoretical approach. As already stated, as a consequence, practical implementations very often reduce this complexity in order to achieve cost effectiveness and/or develop applications according to local interpretation of the standards. As a consequence, there are PKI implementations with different levels of trust between them and, hence, a lack of interoperability between the PKI infrastructures and ES schemes which are put in place.

If the banks had to rely on these public PKI infrastructures for banking applications (or if they would be imposed on the banks by the governments for e-government applications such as e-tax declarations and e-invoices), then those interoperability problems would have to be endorsed by the banking industry. In particular, banks, as issuers of certificates and/or as relying parties, would be forced to adapt to this heterogeneous trust scheme.

In addition, the deployment of eID cards bearing electronic signature systems issued by public authorities to citizen (that are also bank customers at the end) raises the challenge for the banks that customers might desire to use these systems also for electronic banking (instead of the authentication methods issued by the banks, in order to alleviate the number of credential they have to use in their day to day life). In this case the security policy and the underlying infrastructure is no longer controlled by the banks but imposed by the public authorities. Moreover, in some countries (Germany e.g.) the banks MUST know their customers, making it quasi impossible to use eID cards for e-payments (because the eID F2F was performed by the government). Even when this requirement is not mandatory, there is still the question of liabilities that prevent banks to use eID cards. Indeed, who is liable in case of litigation on an impersonation? The end-user? The government in charge of the F2F registration? In addition, some governments (such as Belgium), have settled limitation on transaction value for transaction supported by eID cards. This is not affordable for the banking sector, although nothing prevent the bank to contractually agree with its customers to user their eID for truncations going beyond this value. In all cases, this remains a psychological barrier. A last issue concerns the control of OID Assignments. OID assignment is indeed under control of an ISO committee. As a recognized standards organisation ETSI has been assigned a sub-tree of object identifiers. Because ETSI has been producing and maintains several of the EESSI standards, the standards themselves as well as data elements and objects defined within them, are getting ETSI OIDs (e.g. the Q-Cert ETSI OID). The concern of the banking industry is that the OIDs are controlled by an organisation where they have very limited influence.

It is noticeable that even if eID cards are not directly used for authentication of end-users and/or transaction signatures, some banks use eID to support the on-line registration process of users to e-banking services (e.g. Keytrade Bank using the Belgian eID).

At the same time, simultaneously with the emergence of eID cards, when rolling out multi-application EMV smart cards some banks are involved in the establishment of public key infrastructures. In addition to the promotion of EMV cards as classical payment cards these

VERSION 0.7

banks envisage to use smart cards for identifying their customers over the internet and authenticating transactions (digital signatures) in a variety of internet banking applications such as internet payments or electronic banking. In some countries, banks assist to the construction of PPP where they join efforts with the government to offer their public key infrastructure to e-projects (e.g. LuxTrust in Luxembourg). The major concern for the use of smart cards as Secure Signature Creation Devices (SSCDs) is that there are important differences between the smart card interface of EMV and the one specified by EESSI. However there is sufficient similarity that makes it relatively simple and efficient for an EMV application and an electronic signature application to co-reside on the same smart card. Implementations are already in place in some member states.

Finally it must be noted also that the financial sector also has its proven standards suites, e.g., the ISO TC68 certificate management standards. A bank wishing to use certificates for transaction signatures will need to comply with this standard as well as with the correct implementation of the EU directive on electronic signatures. The standards which are relevant only in the context of digital signature are ISO standards about certificate management (ISO 15782) and Certification Authorities (ISO 21188). There are to be compared with ETSI TS 101 456, wider in its scope than certificate management (focus only on certificate related problems). ETSI TS 101 456 can thus not be directly mapped onto the ISO standards. Consequently the mapping between the EU Directive considerations and the ISO standards cannot and never will be perfect. For complete compliance with the EU Directive, the two existing TC 68 Standards would need to be supplemented by ISO Standards on signature formats, SSCDs, algorithms, etc. There is an ISO group (ISO TC68 SC2/WG12) supposedly covering signing mechanisms, but this is currently inactive.

Independently of the user of eID cards for signatures, there is a need for the financial sector to use electronic signatures at a European level for specific European wide applications (for example in authenticating an electronic direct debit mandate). It is important that the banking industry identifies a minimum set of implementation standards. This should be based on the most relevant and mature EESSI portfolio and the best practice from national PKI implementations. There is a wish from the financial sector to benefit from a legal recognition of their signatures. Indeed, the legal framework being there, it represents an additional level of trust for the bank customers to have their signature guaranteed by law *and* interoperability with services that are directly connected to financial services, such as e-invoicing.

As concluding words, and such as observed at the occasion of recent conferences, there is a real interest of the banking sector to work with public authorities as far as possible in matters of user authentication and e-signatures. This is a rather new trend that should be closely followed by the European Commission.

However some brakes for the use of (eID) QES signatures by the banks have been identified:

- Lack of cross-border PKI interoperability,
- Liability (and control on the issuance) issues,
- Co-existence of the EU DIR linked standards and Banking sector's standards that all need to be followed:
 - o ISO TC68 *versus* ETSI TS 101 456
 - o EMV cards specification *versus* the different SSCD and eID related CWAs

VERSION 0.7

