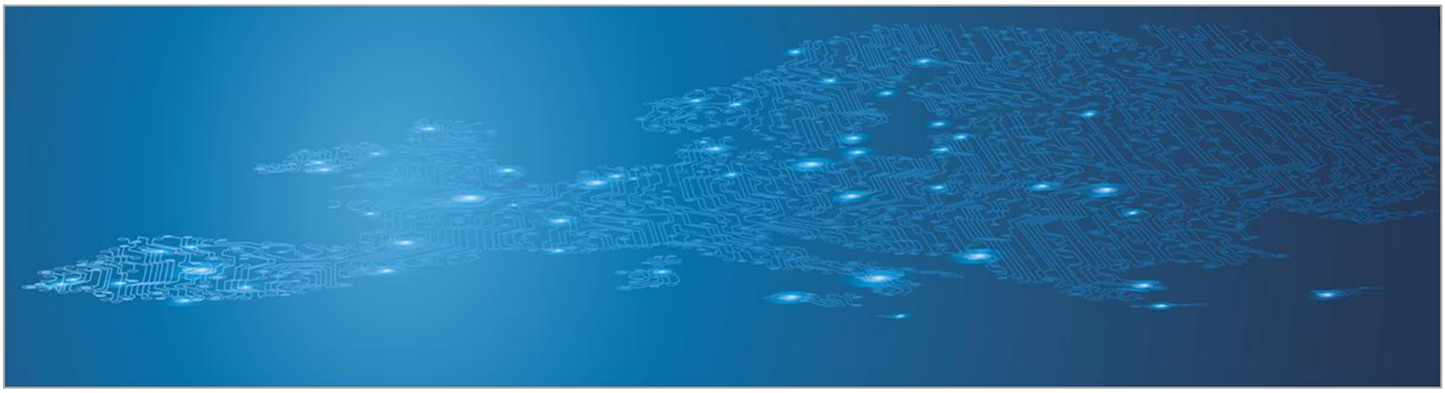


eID Authentication methods in e-Finance and e-Payment services

Current practices and Recommendations

Report, December 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This research was carried out by ENISA in conjunction with, BDigital and the Anti-Phishing Working Group (APWG) European chapter.

- Prof. Manel Medina (ENISA)
- Dr. Jetzabel Serna (APWG.EU and BDigital)
- Andreas Sfakianakis (ENISA)
- Jordi Aguilá (APWG.EU)
- Luis Ángel Fernández (APWG.EU and BDigital)

Contact

For contacting the authors please use manel.medina@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank the APWG.EU and BDigital for their collaoboration in launching the survey and drafting this report, and the Merchant Risk Council, SecuRePay, EU FI-ISAC, ECB, EPC, DG Market H3 and the FSUG for their valuable contributions to this study.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-077-2 doi: 10.2824/27272

Executive summary

This report collects the results of a survey launched by ENISA. The main purpose of the survey has been to collect information about the electronic IDentity and Authentication (eIDA) Systems used in e-Finance and e-Payment systems, to analyse the risks associated to each eIDA method, and produce a Guidelines report with the best practices recommended to the main actors of this sector: Financial institutions, Merchants and Payment Service providers.

An important role of ENISA is to provide its stakeholders with guidelines on topics that are related to Network & Information Security (NIS) – this particular report deals with those topics associated with the e-Identity of citizens and **concentrates on e-identity management risks in financial sector**: phishing, id-theft, session and identity hijacking, etc. Some financial institutions are still not considering the risk associated with the use of inadequate authentication mechanisms, and this report has collected information about the amount of fraud detected in financial institutions. Then it correlates that fraud with the different types of authentication mechanisms implemented by them. With this information, financial institutions could evaluate the cost/benefit associated to the implementation of additional authentication mechanisms in their particular environment, which is highly recommended here.

This information has been collected in a survey replied by more than 100 professionals, which has allowed also to **Identify Authentication mechanisms used in financial and payment services**, and the associated risks. The analysis of the survey results has allowed ENISA to produce 4 groups of recommendations about the best eIDA method to be used in the authorisation of ePayment operations, depending on the risk associated with them:

1. **Promote adequacy of eIDA method to Context**: i.e. Proportionality of method and risk, but encouraging also the use of 2 factor authentication even in low risk operations.
2. **Improve the knowledge and the behaviour of customers and professionals**: Professionals have to take into consideration the evolving risks associated with each authentication method, and customers have to be aware of the need to use strong authentication methods and protect their credentials.
3. **Improve the security of the e-Finance environment**, through: Risk Analysis of the Specific environment (customers profile and size of institution), improvement of customers' awareness and skills, implementation of context based authentication of transactions, and early detection of customer's device compromise through registration, testing and evaluation of the device security.
4. **Improve the security of e-Finance application development and distribution**: encouraging the traditional security by design, taking account of the new personal data protection Directive, and also using trusted distribution channels to install applications in the customers' device.

To summarise, there are many risks that current eIDA practices in the sector don't cover, ECB and EC are developing recommendations and regulations that are aligned with the recommendations of this report of ENISA, trying to identify and set up the tools to improve fraud statistics.

Table of Contents

1 Introduction

1.1 Summary of legislative work regarding e-Payment systems in EU

The EC has launched the following initiatives:

- The E-Money Directive (2009/110/EC) (EMD[1]) aims to enable new, innovative and secure electronic money services to be designed. Will be reviewed soon.
- The Payment Services Directive (PSD[2]) (Directive 2007/64/EC). For which a new proposal (PSD2[3], Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC), has been submitted by the European Commission to the European Parliament and the European Council on July 24th.
- The e-Invoicing[4] directive states that invoices must include authentication of origin.
- The new Regulation about personal data Protection (General Data Protection Regulation, GDPR[5]), which is expected to be applicable to all sectors, is expected to be approved by the European Parliament in 2014 or Q1 2014.
- The review of the EU electronic communications regulatory framework and, in particular, the new provisions of articles 13a and 13b of the Framework Directive and the amended article 4 of the Protection of Personal Data or e-Privacy Directive[6], aim at strengthening obligations for operators; to ensure security and integrity of their networks and services, to notify breaches of security, integrity and personal data to competent national authorities and assign to ENISA specific tasks. In June 2013, the Commission has put in place new specific rules to ensure that personal data breaches in the EU telecoms sector are notified in the same way in each Member State[7]. The new GDPR includes a requirement to notify about personal data breaches to all sectors, just like in the current telecommunication directive[8] requires telecom operators to notify any relevant security incident to their regulator.

1.2 Inputs from Stakeholders

1.2.1 Methodology

The project was developed according to the following steps:

[1] http://ec.europa.eu/internal_market/payments/emoney/index_en.htm

[2] http://ec.europa.eu/internal_market/payments/framework/index_en.htm
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007L0064:EN:NOT

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013PC0547:EN:NOT (COM/2013/0547 final - 2013/0264 (COD))

[4] http://ec.europa.eu/internal_market/payments/einvoicing/index_en.htm

[5] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[6] Old PPDD: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[7] Commission Regulation on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications" online: https://ec.europa.eu/digital-agenda/en/eprivacy-directive-data-breach-notifications

[8] Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)

- The objectives of the eIDA project were discussed in a meeting organized by the APWG.eu in Dublin (e-Crime Researchers Sync-Up), March 2013. The attendants to the workshop validated the objectives.
- Once the main objectives were delimited, a questionnaire was elaborated by ENISA, with contributions from the APWG.EU and BDigital, the questionnaire was then validated by FSUG, MRC and SecuRe Pay forums.
- We received important comments, which allowed us to produce a final version of the Survey that was launched by ENISA and distributed by the above-mentioned groups as well as EU FI-ISAC and EPC, through which the European Member States central banks were reached.
- The Survey was available for participants during a period of 6 weeks; we received 54 responses from representatives of end users groups, and 112 from the professionals, once merged the responses collected through different sessions, and removed those invalid, e.g. coming from IP addresses outside EU.
- A results analysis was performed with the conclusions summarised in this report, as well as identifying a set of recommendations for improvement.
- Those draft recommendations have been distributed for comments to FSUG, MRC and SecuRe Pay forum. They have been presented also in several workshops and conferences, to get feedback from industry, which was positive in all cases. In the World-eID conference it was possible to interchange ideas with STORK2.0 partners, and in ISSE2013 we had the opportunity to chair a whole session, with contributions from the Commission, Merchant and financial sectors.
- The received comments have been integrated in the document, and finally aligned with the recommendations made by ECB on its report "**Recommendations for the security of Internet payments**"[9] (the "Recommendations").
- Finally, an internal evaluation has also been carried out by ENISA in order to produce the final version of this report.

1.2.2 Partners for the project:

This research was carried out by ENISA in conjunction with, BDigital and Anti-Phishing WG (APWG) European chapter.
Also contributed to the launching and the analysis of the survey results:

- Anti-Phishing Working Group (APWG.EU) EU chapter
- European Central Bank (ECB) and Forum on the Security of Retail Payments (SecuRe Pay)
- Merchant Risk Council (MRC)
- Financial Services User Group (FSUG)[10]
- Payment Services Directive (PSD2) preparation team: DG Market H3
- Financial Services Information Sharing and Analysis Center European Chapter (EU FI-ISAC)
- European Payment Council (EPC)

1.2.3 APWG.EU chapter

Some members of the APWG.EU chapter, mainly from the financial sector, made the following contributions to the project:

- Identified eID practices used in the e-Banking and e-Payment systems:

[9] Published on 31 January 2013 on the ECB's website http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf
[10] http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2010:199:SOM:EN:HTML

  - In the e-Banking applications, the application of eID mechanisms to different types of operations, e.g. read data, modify credentials, money transfer, etc.
  - In e-Payment services, they suggested to use indirect methods of assessment of fraud, to avoid having to provide absolute data.
- Analysed the Robustness of each eID method and the associated Risks, based on the known Phishing and other Attack Patterns that have been successfully threating each eID method.
- Defined some best practice guidelines recommending the use of adequate eID methods depending on the risk associated to the transaction or payment.

1.2.4 MRC (Merchant Risk Council)

On top of the known problems with mafia and organised criminals, MRC[11] is highly concerned about “account takeover”: the criminal / hacker uses directly the payment data stored by the merchant, logging in as a real user of the merchant. Then, they may “exchange” the goods purchased electronically in the physical store, if the merchant has multiple channels, which allows “monetizing” the fraud. MRC is interested in analysing how this kind of identity /account spoofing, that allows to get into the merchant website with a fake identity, can be avoided.

MRC is willing to contribute to improving the security of the user identification, and the related data storage security. Meaning that, the merchants tend not to store any personal or financial data, but only a randomly generated token to launch new purchase orders without having to introduce again the payment details through the merchant site. However, they still handle personal data, because the token identifies the user between the merchant and the payment service, and it has to be considered also for data storage security controls.

MRC also contributed with a presentation about “Incident management”, that informs merchants about how to react in case of incident. MRC is interested in getting information about the skills that merchant infrastructure managers should have in order to protect their assets from attacks and incidents, as well as about data breach notifications that they will need to make, when the EU Directive will be applicable.

1.2.5 Financial Services User Group (FSUG)[12]

The Commission set up a Financial Services User Group (FSUG). In its *White Paper on Financial Services Policy 2005–2010*[13], the Commission stated that it attaches great importance to ensuring proportionate user representation in the policy-making. In the *Communication for the European Council – Driving European Recovery*[14], the Commission put the interests of European investors, consumers and SMEs at the centre of the financial market reform.

[11] The MRC organises webinars and writes reports to raise the awareness of their members, which are mostly merchants and payment service providers. They also collaborate with public security agencies, which membership fee is free and have a Committee to manage the collaboration with the LEA. ECB wants to force the use of safer communication means between payment services and merchants. Their European Congress takes place at London from the 17th to the 19th of April (expected 500 participants).

[12] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:199:0012:0014:EN:PDF
http://ec.europa.eu/internal_market/finservices-retail/fsug/fsug_en.htm

[13] White Paper on Financial Services Policy 2005–2010

[14] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0114:EN:NOT

1.2.6 European Central Bank and Forum on the Security of Retail Payments (SecuRe Pay)

SecuRe Pay was established by the European Central Bank as a voluntary cooperation between overseers and supervisors of Payment Services Providers (PSPs) aiming at:

- Facilitating common knowledge and understanding with regard to electronic retail payment services, instruments and PSPs.
- Addressing major security weaknesses and vulnerabilities.
- Issuing harmonized recommendations.

The security recommendations made by SecuRe Pay, as well as the different contributions on security-related topics received in the different public consultations launched by the Commission last year will be a valuable input for the Commission in the review of the Payments Services Directive foreseen for the second half of 2013.

The ECB is also interested in working on security requirements together with the Secure Payment forum. The SecuRe Pay has issued recommendations for the security of Internet payments, which, have been published on 31 January 2013 and can be accessed on the ECB's website[15]. As future directions, ECB planned working on secure payments with mobile phones[16].

1.2.7 Payment Services Directive

The PSD[17] is currently proposing to implement high-level security requirements for the payment institutions. The new directive is intended to enforce the usage of strong used authentication for remote payment transactions. As it is stipulated in the **Article 87** of the proposed regulation: "Member States shall ensure that a payment service provider applies strong customer authentication when the payer initiates an electronic payment transaction unless EBA guidelines allow specific exemptions based on the risk involved in the provided payment service."

1.3 Motivation

In July 2013 the European Central Bank published its "Second Report on Card Fraud"[18]. This report contains interesting information regarding the so-called "Card not Present-Fraud (CNP-Fraud)", which, is by far the predominant type of fraud within card payments. Whereas remote transactions known as "card not present-transactions" represent only a share of around 10 % of all card payments, the share of CNP-Fraud of the total card payments fraud has increased from 47 % in 2007 to 56 % in 2011. Accordingly, the ECB concludes that Internet payments result in higher rates of fraud. Therefore, in 2011 the European Forum on the Security of Retail Payments, where relevant public authorities overseeing and supervising payment service providers cooperate voluntarily, focused its work on developing "recommendations to improve the security of Internet payments". These findings have been enforced by further country-specific statistics. The 2012 Annual Report of the French Observatory for Card Payment Security[19] stipulates "*the fraud rate for CNP payments fell*

[15] http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

[16] http://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf

[17] Edited by: DG Market H3

[18] http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf

[19] http://www.banque-france.fr/observatoire/telechar/gb/2012/rapport-annuel-OSCP-2012-gb-fraud-statistics-for-2012.pdf

to 0.299%, but was still 20 times higher than the rate for face-to-face payments. The fraud rate for Internet payments, in particular, declined to 0.290% from 0.341% in 2011. A mid sustained growth in electronic commerce, CNP payments accounted for just 9.2% of the value of domestic transactions but for 61% of the total amount of fraud (the same as in 2011)". Similar information can be found for the UK market, where Financial Fraud Action UK publishes regularly information on fraud in payments[20]. CNP fraud is responsible for 63 % of the total fraud in the UK as well. A calculation of the loss over volume for all payments fraud in UK the ratio is at 7.1 basis points[21], whereas the ratio only for e-commerce fraud is at 20.6 basis points. Total e-commerce fraud losses only in the UK accounted 2012 already for 140.2 M GBP.

The blooming of Internet technologies has revolutionized the way people transact with their financial institutions. Nowadays, it is estimated that globally 25% of Internet users, access e-banking services [1]. Given the surge of mobile technology, and according to a recent report published by Juniper [2], the number of people that use their mobile device for e-banking and e-financial services has drastically increased over the past years, i.e. over 590 million mobile users have used their mobile devices for banking purposes. Meaning that, e-banking users have considerably benefited from using e-banking services without time and location constraints (‘whenever you want’ and ‘wherever you are’), which is a compelling proposition to most banking customers. However, due to the sensitive nature of financial information, security has become a main concern [3], especially where ciber-fraud estimations range from 300MUSD to 1 billion USD per year[22], only in USA. The lack of proper security measures results in an barrier for the wider adoption of e-banking services.

Current e-banking systems are exposed not only to the set of known threats (now migrating from traditional PC-based e-banking to the mobile-based scenario), but, to emerging threats, specifically targeting mobile devices. Cybercrime is increasingly targeting e-banking systems (‘criminals go where the money is’), and being more and more organised. Nowadays, cybercriminals have the capabilities to target new technologies and launch attacks of increased sophistication, as in the two high impact attacks that took place during 2012, and shocked the e-banking sector (the High Roller[23] incident and the Eurograbber[24] attack). In the High Roller incident [4], 60 million euros were stolen, while in the Eurograbber attack 36 million euros were stolen and more than 30,000 bank customers were targeted [5]. Security is, therefore, a major issue, and must be considered, where, the security level of an e-Banking system is strongly influenced by the customer authentication methods, just as in the aforementioned incidents, attackers were able to hijack two-factor authentication (e.g. mTAN) and commit fraud.

Therefore, to be able to provide payment transaction security, and minimize the potential threats, e-banking systems must implement robust identification and authentication (eIDA) mechanisms when accessing sensitive information or performing risky operations. As a result, e-Banking authentication continues to draw important attention not only to security professionals, but also to security

[20] http://www.financialfraudaction.org.uk/publications/
[21] 1 basis point = one one-hundredth percent
[22] https://www.jpmorgan.com/cm/BlobServer/13th_Annual_2012_Online_Fraud_Report.pdf?blobkey=id&blobwhere=1320571432216&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs http://www.bloomberg.com/news/2011-08-04/hackers-take-1-billion-a-year-from-company-accounts-banks-won-t-indemnify.html
[23] http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps
[24] https://www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf

managers, decision makers and moreover, security researchers. In [6] authors discussed about general challenges and issues identified in e-banking systems. Authors of [7] and [8] have presented an extensive study on e-banking security and introduced a formal definition of e-banking threats and security models. In [9], the author presents a study on security threats towards proposing the use of biometrics for strong authentication in e-banking scenarios.

A taxonomy of attacks to e-banking authentication was introduced by authors of [10]. Additionally, a challenge/response authentication solution was proposed. An assessment of authentication methods for e-banking was presented by authors of [11], however, the presented study was focused only on the PC-based scenarios. Although, there are many interesting approaches, the evolution and sophistication of Internet and mobile attacks require the continuous study of emerging threats, issues and challenges in e-banking scenarios.

Similar to our study, authors of [12] analysed the eIDA methods used by major banks in English speaking countries. Nonetheless, their research was limited to data collected by mere observation (publicly available), contrary to our approach, which analyses these factors, taking into account current implemented e-banking systems, with information provided by the security professionals of major European banks.

Finally, our study provides an eIDA methods assessment and a set of recommendations taking into account the security professionals' perspective.

1.4 Survey Objectives

The main objective of the survey is to identify electronic Identification & Authentication (eIDA) mechanisms used in e-Finance and e-Payment services:

- Most relevant One-step mechanisms
- In the e-Banking applications, the application of eID mechanisms to different types of operations, e.g. read data, modify credentials, money transfer, etc.
- e-Finance professionals are asked to provide additional information about:
    - Internal authentication mechanisms, hidden to the customers.
    - Rough estimations about the improvements achieved in the fight against identity theft and cyber-fraud, thanks to the introduction of the authentication mechanisms.

The questions about the estimations of improvements achieved are of two kinds:

- Qualitative, i.e. comparing the current situation with respect to the previous one (without the authentication mechanism)
- Quantitative, i.e. providing a range of values of economic losses per user, number and time of take down of incidents.

In order to get the maximum number of contributions to the survey, the questions do not permit knowledge of the total loss of the institution, and the identity of the participant in the survey is completely anonymous, so a disclaimer will recall that the requested information should not be considered confidential. In addition, ENISA has the mandate of the Commission to collect information about data breaches and network and information security incidents in critical infrastructures, with the commitment to keep this information fully confidential, and not to publish the information in a way that could be associated to any particular stakeholder, industry or organisation.

The disclaimer concluded saying that: "Nonetheless, if there is any internal policy that prevents to disclose some information of the organisation related to the quantitative questions, it is always possible to skip those questions of the survey."

2 Types of operations and transactions in eFinance and ePayment services

e-Finance and e-Payment applications allow users to perform different kinds of transactions that can be categorized according to different factors. In this work, ENISA recognises four types of operations, each corresponding to a different risk level, partly following eID federation practices, and Data Protection Authority (DPA) recommendations for data breach criticality evaluation, which should be considered when assessing the suitability of an eIDA method to authorize an operation.

Thus, one of the aims of this project is to identify:

- How many levels of risk, i.e. types of operation are implemented in the e-Finance applications, and
- Which authentication mechanisms are used for each type of operation.

The four types of operations identified are the following, sorted from the lower to the highest risk:

1. **General customer Information (not financial)**, low risk operation, which, allows only read access to basic account information, i.e. personal data of medium sensitivity level, like:
   a. Personal data of the customer.
   b. Account number(s) only.
2. **Account Information (read only)**, low risk operation, which, allows only read access to personal and financial data, i.e. personal data of high sensitivity level, like:
   a. Personal data of the customer.
   b. Account number(s) only.
   c. Balance.
   d. Transaction History.
   e. Account statements.
3. **ePayments to known destinations,** medium risk operations are those that fulfil the requirements expressed in KC 7.1 of the ECB report “Recommendations for security of Internet Payments”: i) outgoing payments to trusted beneficiaries included in previously established white lists for that customer; ii) transactions between two accounts of the same customer held at the same PSP (Payment Service Provider); iii) transfers within the same PSP justified by a transaction risk analysis; iv) low-value payments, as referred to in the Payment Services Directive.

   Examples of known destinations could be:
   a. Utility / Supplier payments.
   b. Some Card Payments.
   c. e-Government payments.
   d. e-Merchant payments (some well-known ones).
4. **Transactions (modify data),** high risk operation, which, allows payments to “untrusted” destinations.
   a. Transfers to any destination
   b. Card payments / Access credit
   c. Insurance polices
   d. Managing personal data
   e. Investment instruments
   f. e-Merchant payments (not-registered ones)

Participants were asked to indicate the operation and transaction type of higher risk that is authorised by the authentication mechanism that is used. It is assumed that:

- Mechanisms allowing type 2 are assumed to allow also type 1, and to be a pre-requisite of the methods required for the other operations (1st step of authentication chain).
- Mechanisms allowing to launch operations of type 4 are assumed to allow also all the lower levels of risk types (last step of the authentication chain), i.e. all kinds of transactions.

As mentioned above (see 1.1), the new PSD[25] doesn't recognise so many types of operations, and requires strong authentication for any kind of transaction. As a result, the new directive will force the usage of so-called "strong customer authentication" for any remote payment transaction. Article 4 defines "strong customer authentication" in the following way: "*'strong customer authentication' means a procedure for the validation of the identification of a natural or legal person based on the use of two or more elements categorised as knowledge, possession and inherence that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data.*".

[25] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013PC0547:EN:NOT

3 Authentication mechanisms used in eFinance and ePayment services

The process that allows an entity to establish the identity of another entity is known as authentication. Current eIDA methods are based on some combination of something that you know, something that you have, and something that you are. When two or more of the aforementioned elements are combined, this procedure is known as strong authentication (two-factor or multi-factor authentication).
In the following section, the initial set of the eIDA methods used in this work is introduced, towards analysing the most common and strong customer authentication implementations used in current e-banking systems.

3.1 eIDA methods used in e-financial and e-banking systems

In the following sections a short description of each authentication mechanism suitable for e-banking and e-financial systems are introduced. These eIDA methods have been included in the survey, and are categorized according to their type of credentials, as they were shown in the survey.

3.1.1 Password/PIN

An eIDA method based on what you know, and consisting of a combination of a valid and unique identifier (username) and a secret pass-phrase (password/PIN), where end-users are requested to enter a private pass-phrase in order to be authenticated. Additionally, two important *security enhancements* might be implemented:

- Virtual Keyboard - consists of a software based keyboard displayed on the screen (to prevent keyloggers), and
- Partial password (Figure 1), the user is asked to enter only some of the digits or characters from the PIN/password, a common partial password approach requests different positions for each session.

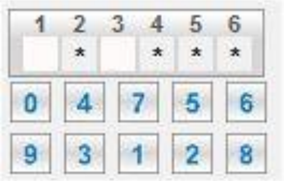


Figure 1 Partial password: the user is asked to introduce only 2 of the 6 digits of the PIN (Virtual Keyboard)

3.1.2 Biometrics

An eIDA method based on what you are, i.e. end-users are authenticated through their characteristics such as body biometry or behavioural biometry (recognition of fingerprint, voice, face, hand geometry) or behavioural biometry (keystroke dynamics, handwritten signature). Herein follow some explanations of the most commonly used techniques:

3.1.2.1 Behavioural biometry

Analyses how the user behaves, interacting with the computer:

3.1.2.1.1 Keystroke dynamics

Also known as typing biometrics, this authentication mechanism uses typing patterns (elapsed time between pairs of keystrokes) in order to authenticate a user.

3.1.2.1.2 Handwritten Signature

A graphical image of a handwritten signature, or the analysis of the speed of the strokes used to generate it, is used to authenticate the user.

3.1.2.2 Body biometry

Analyses how the user "is", i.e. some characteristics of his/her body, that can't be changed easily:

3.1.2.2.1 Fingerprint recognition

The user's fingerprint is scanned for the authentication process.

3.1.2.2.2 Voice recognition

This mechanism processes (spectral analysis) the user's voice in order to verify the identity of the speaking user.

3.1.2.2.3 Facial recognition

The biometric system scans user's face and analyses specific facial features/pattern in order to authenticate her.

3.1.2.2.4 Hand geometry

The geometric shape of the user's hand is used for verifying his/her identity.

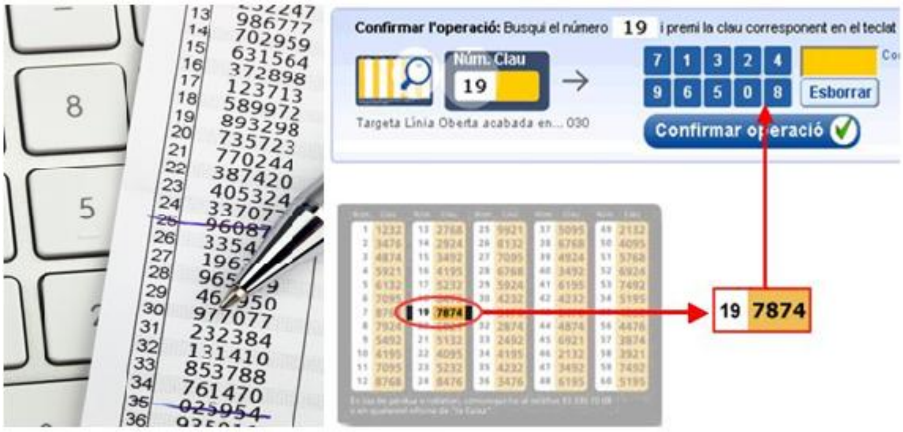
3.1.3 One Time Password (OTP)

This eIDA method is usually based on what you have, and it consists of generating a different, and essentially random password, known as a One Time Password or OTP that is only valid for one session or transaction, and it is also referred as dynamic authentication. A typical OTP implementation is based on one of the following algorithms: event-based OTP, time-based OTP, or challenge-response OTP. Additionally, OTPs can be delivered in several ways, providing different benefits in terms of usability, security and costs. Static OTP approaches are commonly based on TAN[26] code lists, while Dynamic OTP approaches include SMS-based OTP, Hardware Token, Software Token and QR-codes (Quick Response two-dimensional bar code, see section 3.1.3.3.4).

3.1.3.1 TAN code list or coordinates card

The user has a physical document with the list of codes (OTPs) s/he has to use to reply the challenge from the web banking application, just as shown in Figure 2. The challenges are generated randomly, and so the corresponding reply looks also random.

[26] Transaction Authentication Number



Confirmar l'operació: Busqui el número 19 i premi la clau corresponent en el teclat

Targeta Línia Oberta acabada en... 030

Figure 2 TAN Code List & Coordinates Card

3.1.3.2 Mobile SMS based

A different random OTP is sent to the user via SMS message to the registered phone number of the user, each time a transaction requires authentication.

3.1.3.3 Specific Token device

The user has a physical electronic device, which generates a specific Password (OTP) each time the user requests it. There are different types of devices that may be used for this purpose:

3.1.3.3.1 Hardware (special Token – time based OTP)

The user has a dedicated/special physical electronic device that generates a specific Password (OTP) each time the user requests it. The generated OTP in this case is a unique value, e.g. a six-digit number that changes at fixed intervals (for example every minute).

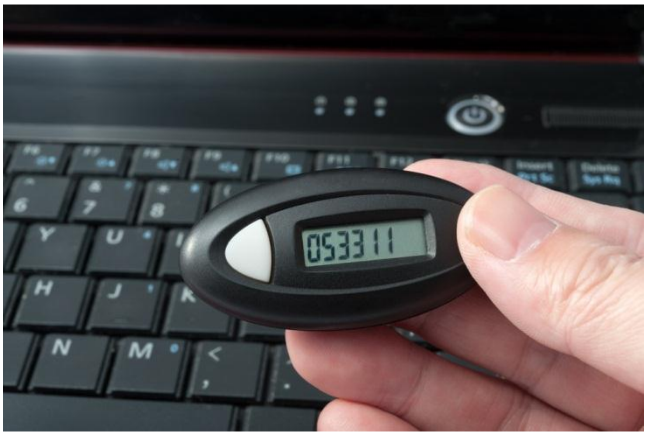


Figure 3 Hardware Token (time based OTP).

In this example the OTP is based only on the calendar time and a private key stored in the device.

3.1.3.3.2 Hardware (special Token – challenge/response OTP)

The user has a dedicated/special physical electronic device that generates a specific Password (OTP) each time the user requests it. In this case, a challenge-response protocol is used: at first, the web banking application generates a challenge (e.g. a random number); this challenge has to be typed in the token, in order to get the correct response for that time; finally, the response is sent back to the web banking application that will authenticate the user based on the response.

3.1.3.3.3 Mobile OTP Application (Token)

The user has a software application installed on his/her mobile telephone handset that generates a specific password (OTP) each time the user requests it. The user may need to type in a challenge code displayed on the computer by the e-Banking application website. Note that, in mobile-based solutions the registration of the mobile device is highly recommended in order to reduce the associated security risks that are inherent in mobile devices.

3.1.3.3.4 QR codes

The user scans a two-dimensional bar code of the challenge that is displayed on the screen of the e-Banking application (as shown in Figure 4), with the mobile phone handset application, which generates a specific Password (OTP) based on that challenge. This avoids the user having to re-type the challenge. It is worth mentioning that the security strength of the token highly depends on the way it is implemented. In QR codes, the mobile app/mobile device should be authenticated (i.e. registration to link it to a specific user) to avoid the QR code to be scanned from any malicious mobile app/device.

Figure 4 QR Code scanner application

3.1.4 e-Signature Certificate

This eIDA method is based on what you have, where end-users are authenticated through e-Signatures. The user's private key can be stored in: Computer stored key, Mobile phone, USB memory card, and Crypto-card

3.1.4.1 Local / Computer store of Key

The e-Signature is made using the private key of the user that is stored at his/her computer Hard Disk.

3.1.4.2 Device stored key

3.1.4.2.1 Memory Token (USB, memory card)

The e-Signature is made using the private key of the user that is stored in a USB or a memory card (removable memory storage).

3.1.4.2.2 Chip card token (e-Identity card)

The e-Signature is made using the private key of the user stored in the chip of his/er e-Identity card or specific smart card (with cryptographic embedded functions).

3.1.4.2.3 Mobile phone

The e-Signature is made using the mobile phone of the user, where the user's private key is stored.

3.1.5 Device Authentication

If the user accesses the e-Banking service through previously registered/used devices and platforms or through a specific mobile application for that service, then some authentication steps may be avoided.

3.1.5.1 Device Registration

The user identity is reinforced through registration of the device(s) that user has used before. Attempting to access the e-Banking application from a new device, platform or browser will cause a warming and/or require additional authentication mechanism.

3.1.5.2 Mobile e-Banking Application

The user accesses the e-Banking service from an application, specific for that Service, running on the mobile telephone handset.

3.2 Context authentication mechanisms used in eFinance and ePayment services

In this section we provide short explanations for the additional context authentication mechanisms which are hidden to the customer. They improve the level of confidence of the service provider on the identity of the customer independently of the user credentials that the customer may have or know. These mechanisms are normally implemented on the server side, in order to check the authenticity of the customer, based on the behaviour, location or device used and other parameters of the operations performed by the user during the interactive session with the service. The users do not easily recognise these mechanisms during the interaction with the service, so they normally are not aware that those authentication mechanisms are protecting them from being victims of fraud or from being impersonated.

The new proposed regulation on data protection (GDPR[27]) imposes some restrictions on the profiling of the users. It includes also a "ban on profiling", i.e. monitoring of customer transactions may be only possible with the prior consent of the customer - something which at least theoretically could affect the possibilities to monitor transaction on potential fraud, that may have an impact on the right to use these techniques. For this reason, maybe it will be necessary to set up legal notices advising the user about their implementation.

3.2.1 User behaviour analysis parameters

These parameters are used by the financial services to authenticate users by tracking their overall e-banking operation and transaction history when using/interacting with the service. Thus, through

[27] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

deviations from expected online behaviour, fraudulent activity can be detected and prevented. This category of authentication parameters includes:

3.2.1.1 Time between sessions

User's account/transaction operations may be rejected based on their frequency of access to the service within a time window.

3.2.1.2 Destination account filter

Based on the user's transaction history, transactions to account numbers other than those preferred or most used money transfer destinations for the current user are restricted.

3.2.1.3 Total amount in operations

Based on a user's profile, if the total amount in operations of this user within a period of time is above the threshold for that profile, the transaction is rejected.

3.2.1.4 Time of day

Each user interacts with ePayment services and makes transactions in a personalized way, e.g. some specific times during the day. Thus, the transactions and operations that do not take place within his/her usual times of the day may be rejected.

3.2.1.5 Keystroke dynamics

This authentication parameter uses typing patterns (elapsed time between pairs of keystrokes) in order to identify and authenticate a user.

3.2.2 Sessions analysis parameters

These parameters are used to authenticate the user by separately monitoring each of his/her session. This category of authentication parameters includes:

3.2.2.1 Amount filter

Amount transaction thresholds (bigger than, usual) are derived from the user's profile. The user's transactions that do not comply with these thresholds are rejected/restricted.

3.2.2.2 Blacklisted bank accounts

The financial institution may have a blacklist of bank accounts know to be associated with fraudulent activities.

3.2.2.3 Time between operations within one session

An average time between user's operations is compared with the normal value for his/her profile, which is used to detect abnormal or fraudulent activity. If a malicious program hijacks the identity of the user then the time between operations could be shorter.

3.2.3 Network analysis parameters

These parameters are used to authenticate users by analysing networking characteristics. This category of authentication parameters includes:

3.2.3.1 Whitelisted IP addresses

Current customer IP address is checked against whitelisted IP addresses.

3.2.3.2 Blacklisted IP addresses

The user's transactions/operations may be rejected because his/her IP address is blacklisted (commercial blacklists, lists with compromised computer, blacklisted IP addresses due to previous fraudulent activity, etc.).

3.2.3.3 Anonymous proxy

Transactions from anonymous proxies are rejected since their IP addresses are blacklisted.

3.2.3.4 High risk country classification

A transaction may be rejected if it is carried out from an IP address block that is allocated to a high risk country.

3.2.3.5 Time between sessions from one source IP address

The transaction/operation activity from a single IP address may be marked as fraudulent or suspicious if its frequency is high, or if it is used to access several customer accounts.

3.2.3.6 Geographical distance between operations

Current customer IP address geolocation is checked against the last recently used by that customer. Customer's transactions and operations may be rejected based on the geographical distance between them.

3.2.4 Device Authentication

If the user accesses the e-Payment service through a previously registered/used device, or platform, or browser, then some authentication steps may be avoided.

3.2.4.1 Platform identification

The user identity is reinforced through registration of the platform (mobile device, browser, operating systems, etc.) that the user has used before. Attempting to access the e-Banking application from a new device, platform or browser will cause a warning and/or require additional authentication mechanisms.

3.2.4.2 Storage of user key in a device

The device of the user (e.g. mobile or tablet) is authenticated in order to allow the user to make transactions and operations storing a security key in the device or mobile phone SIM card.

3.2.5 User Profiling

In this category of contextual analysis mechanisms, some parameters that characterise the interaction of the users with the service are profiled, and the user behaviour is analysed and compared against specific patterns of behaviour, i.e. profiles of user. We may have several approaches, depending on the type and amount of information stored by the server.

3.2.5.1 Single behaviour pattern

User behaviour is analysed only during the current session and it is compared against only one user profile in the whole system, resulting in users being profiled with a single pattern.

3.2.5.2 Multiple behaviour patterns

User behaviour is analysed only during the current session and it is compared against one of the several standard user profiles defined in the whole system. Thus, users are associated to one of those patterns or segments (e.g. company profile, end user profile, investor profile). If the behaviour of the user in the current session does not match with the profile associated to this user, then the operations are restricted.

3.2.5.3 Individual behaviour pattern

Users are profiled (their behaviour is analysed) in all sessions, in order to create an individual pattern for each customer. Thus, an individual user profile (history) is stored in the system and the user's current and historical sessions are compared.

3.3 eIDA method Evaluation and selection Factors

This section introduces the list of the proposed **selection criteria** based on real implementations, i.e. considered by security professionals, managers and decision makers in e-banking:

- **Strength**, Covered risk and Efficiency to resist potential attacks and the risk they represent and its sophistication.
- **Implementation difficulty** in terms of technical requirements to be fully deployed and functional.
- Absolute loss and Reduction of **Loss** per involved customer
- Yearly Frequency and Reduction of the number of security **incidents**, successful attacks per year, regardless of the number of customers affected by each of them.
- **Usability**: the authentication mechanism's quality of being user-friendly and closer to user needs and requirements.
- Implementation **cost**: the cost impact of the eIDA methods implementation effort.
- Adequacy to **user segment**: The eIDA method quality of being able to meet a user segment's needs and expectations. Categorizing user segments is an important task when assessing the suitability of an eIDA method implementation. Thus, in this section we propose a generic categorization that identifies different user segments. Note, that not all financial institutions might include all of the propose user segments; there exist those institutions aimed at only one of them.
  - **Retail**: personal banking or consumer banking, aimed at regular customers making low amount transactions.
  - **Private**: personal banking with special needs, i.e. customers making large amount transactions.
  - **Corporate/Business**: aimed at companies/enterprises.
  - **Investor**: aimed at users managing investment tools.

3.4 Survey questions

The survey was intended to be used on-line[28], where the participants were asked to select the authentication mechanisms that they use. The survey was addressed to two communities:

- **End user associations'** representatives and e-commerce Merchants, who were asked to answer questions only about the first set of authentication mechanisms described above.
- **e-Finance institutions** IT security professionals, who were asked to answer the survey split in two parts, one for the Transparent authentication mechanisms described above, and a second one for the Context authentication mechanisms, also described above. Then, for every one of the selected mechanisms, the participants were asked to reply some questions in order to provide their view about the strength, usability, efficiency and improvements achieved using those mechanisms.

Concerning the questions about the **estimations of improvements** achieved, they were of two kinds as stated in Section 1.4: **Qualitative and quantitative**.

The Annex II collects the screenshots of the survey, which show all the authentications mechanisms (Part I of the survey), as well as the additional **context authentication mechanisms** (Part II of the survey) for which, participants were asked to provide input. Participants should answer a set of related questions for each of the selected mechanisms.

[28] Survey Web site: https://www.enisa.europa.eu/surveys/professionals-survey

4 Threat analysis

This section introduces the Threat Landscape of the identified threats relevant to eIDA method as shown in Figure 5. The most relevant threats and attack scenarios concerning online banking authentication, especially those regarding its ICT infrastructure are then introduced in the following sections.

The report ETL[29] (ENISA Threat Landscape) collects a more complete analysis of cyber-threats, risks and threat agents, including general threats (e.g. botnets, IP spoofing) not described here to avoid duplications. This section collects only those threats directly related to authentication methods used by citizen in e-Finance applications.

4.1 Threat Categorization

A categorization of threats based on the component/asset attacked has been adopted from the approach that has been proposed by C. Dimitriadis [7].

4.1.1 Threats against end-users

a. **Physical observation/surveillance**: End-users may be subjected to shoulder surfing, filming of their keyboard or recording of keyboard acoustic and electromagnetic emanations. Thus, by being surveyed, the credentials of the end users can be captured or even stolen (e.g. theft of written down passwords).

b. **Social engineering**: through non-technical means, the user's credentials can be compromised, e.g. knowledge of personal details of the user, user impersonation and claimed identity during registration, phone calls, etc.

c. **Phishing:** end-users may be victims of traditional phishing email campaigns or highly targeted spear-phishing ones. Furthermore, given mostly the proliferation of mobile devices and social networks, phishing has evolved and heterogeneous phishing campaigns (text messages-SMiShing (SMS phishing), malicious links from online social networks, fake mobile applications - app-based phishing, voice phishing (vishing) have arisen.

4.1.2 Threats against end-users' devices

The below mentioned threats primarily target the devices of end users (e.g. PC, mobile device, tokens, etc.):

a. **Physical theft of token or device**: End-users may be victims of theft of their token device and their mobile device (or even the piece of paper with their passwords written down).

b. **Tampering (or replication) of token or device**: PIN brute force attacks, side channel attacks and hardware keyloggers are some attack examples of this threat.

c. **Malicious software (malware):** Malware authors increasingly target online banking. Malicious code with rootkit features, i.e. as Man-in-the-Browser (MitB), and mobile banking trojans which can hijack two-factor authentication, i.e. Man-in-the-Mobile (MitMo), are the most prominent threats for e-banking identity theft and fraud

[29] ETL 2013: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

4.1.3 Threats against communication networks

These threats target the communication channel between end users and the remote banking server.

a. **Pharming[30]:** Attackers may target the network infrastructure (specifically routers and DNS servers) and redirect end users to illegitimate websites, i.e. users are redirected to a malicious URL while having entered the correct one in the address bar.
b. **Eavesdropping/Interception/Hijacking[31]:** This threat category includes network-based and server-based man-in-the-middle attacks. Banking credentials, transaction data, OTPs and other sensitive data can be captured through erroneously trusted fake SSL certificates, passive traffic monitoring (sniffing), replay attacks, as well as active man-in-the-middle attacks.

4.1.4 Threats against remote banking services.

These threats target the ICT infrastructure of the bank that hosts the web banking service and the respective data stored.

a. **Web code injections against banking servers:** Attackers exploit vulnerabilities of the web-banking server through SQL injection, cross-site scripting, cross-site request forgery, redirection to a malicious URL and other web exploitation techniques. The adversaries placing such attacks try to extract data such as credentials.
b. **Denial of service attacks (DoS):** Brute force DoS attacks against online banking server do not pose a direct threat to the components of the end users' authentication process. Nevertheless, DoS attacks can be launched as a diversion as part of a larger attacks and can be reinforced by the misuse of open DNS resolvers.
c. **Bank data breaches:** bank internal or external threat agents as well as third parties can compromise sensitive information (e.g. end users' credentials, account information, social security numbers etc.)

4.2 Attack patterns

This section presents common attack scenarios implemented in real world attacks.

4.2.1 Attack scenarios

Typical attack scenarios and methodologies based on current malware trends for e-banking are introduced next.

4.2.1.1 Phishing attack scenario

As stated by Kaspersky[32], in 2012-2013, 37.3 million users suffered from phishing attacks, 20% of which targeted the banking and financial sector. Concerning the mobile platforms, Trend Micro reports that 75% of mobile phishing URLs were rogue versions of banking and financial services. Thus, given the large use of mobile devices and the growing threat of mobile e-banking phishing, we present below such an attack scenario:

[30] http://en.wikipedia.org/wiki/Pharming

[31] https://www.owasp.org/index.php/Network_Eavesdropping - - https://www.owasp.org/index.php/Session_hijacking_attack

[32] http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year

- First, the user receives the phishing email and since he has 24/7 connectivity with their mobile he opens his mailbox.
- The message sender is spoofed and pretends to be the e-banking service requesting the user to update his account information by providing a malicious link.
- Upon clicking the malicious link, the user accesses the legitimate-looking e-banking service and is lured to give his/her e-banking credentials and in some cases other sensitive information (e.g. email credentials, government-issued identity card, passport, etc.).

4.2.1.2 Man-in-the-Browser attack scenario

MitB attacks are of increasing sophistication, hard to detect and can be highly customized for a specific target financial institution. As stated by RSA[33], MitB attacks are conducted by many financial Trojan families (personified by Zeus and SpyEye, which are also available for mobile devices) and their prevalence is widespread. The latter is being reinforced by the existence of many infection vectors: malicious email attachments, drive-by downloads, online social networks, infected removable media, etc. In a Man-in-the-Browser attack:

- The malware is hosted in user's PC or mobile device and is waiting for the user to access the online banking server.
- When the user successfully logs in his online banking service, the malware exits stealth mode and hijacks the online session of the user.
- At this time, the malware can:
    a) simply log user's submitted credentials
    b) modify in real time transaction content (i.e. amount and destination account) or
    c) insert additional transactions to mule accounts.
- Finally, malware modified or added transactions are made invisible to the user and the online banking application.
    a) On the one hand, the user is deceived by means of social engineering techniques: by pretending unavailability of the e-banking service and by displaying the legitimate transaction (instead of the fraudulent one) or a fake account balance, etc.
    b) On the other hand, the online banking service cannot detect the aforementioned fraudulent transactions due to the fact that any activity seems to have been performed by the user's browser.

4.2.1.3 Man-in-the-Mobile attack scenario

Man-in-the-Mobile attacks are the natural evolution of Man-in-the-Browser ones, specifically targeting mobile devices browsers.

4.2.2 Real attack incidents

In this subsection, we present the attack methodology of two high impact real attack incidents targeting e-banking services that took place during 2012.

4.2.2.1 The High Roller attack scenario

The first stage of High Roller attack[34] [4] is a combination of phishing and man-in-the-browser scenarios.

[33] http://viewer.media.bitpipe.com/1039183786_34/1295277188_16/MITB_WP_0510-RSA.pdf

[34] http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps

- Attackers used online reconnaissance in order to gather information and send specifically crafted and highly targeted emails to bank customers with high balance accounts.
- Then, using spear phishing as the attack vector, attackers managed to install their malicious code in victims' PCs.
- The malware was triggered when the user started an e-banking session and injected requests for additional authentication information (e.g. TAN used in two factor authentication schemes).
- While the user was waiting to be authenticated, the malware had already initiated a silent fraudulent transaction to a mule account[35].
- Finally, the malware had the ability to hide the fraudulent transactions (e.g. false account balance) from the logged-in user.

4.2.2.2 The Eurograbber attack scenario

A high impact attack of this kind was the Eurograbber incident which was made public during December 2012. As reported[36], 36 million Euros were stolen from more than 30,000 bank victim customers in Netherlands, Spain and Germany. The attackers targeted both PC and mobile devices of the users in order to hijack two-factor authentication (SMS-based OTP is commonly used in Europe) and make fraudulent transactions. The anatomy of the Eurograbber attack was the following [5]:

- Firstly, the user's PC is infected with a variation of Zeus Trojan malware through malicious email attachment or through a drive-by download.
- The malware hosted by the infected PC remains in stealth mode until the user accesses his banking website.
- Using social engineering techniques (i.e. bank security upgrade), the malware lures the user to give his/her mobile phone number.
- As soon as attackers receive the customer's mobile phone number, they send a SMS including a malicious link for downloading a mobile banking security application.
- Upon installation of this application, attackers have infected both PC and mobile device of the user.
- Thus, when the user logs in to his banking account, the PC-malware component initiates a fraudulent transaction to a mule account while the mobile-malware component receives the SMS authentication code and sends it to the attacker.

[35] An account to which fraudsters transfer funds from the compromised account
[36] https://www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf

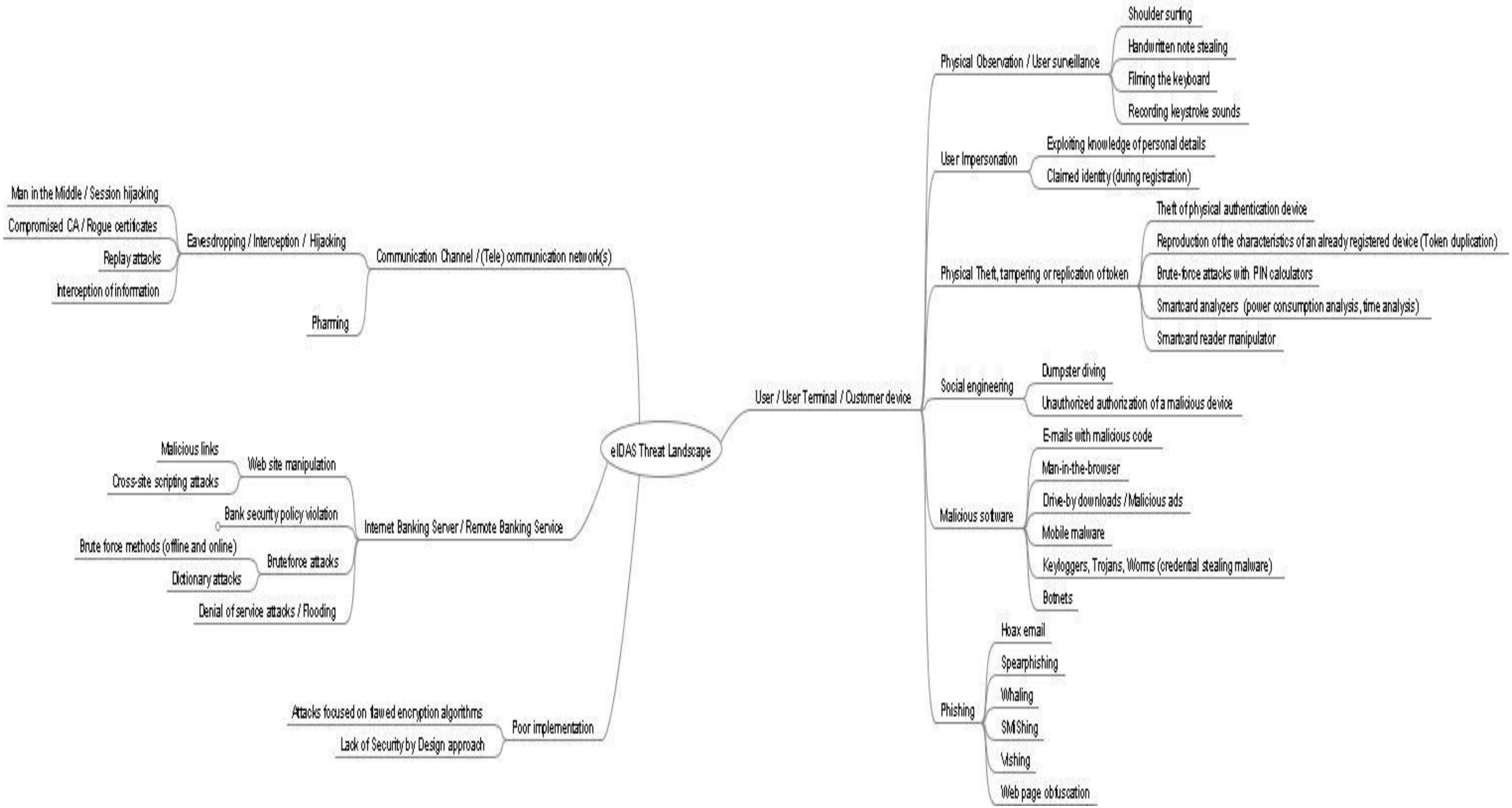

eIDAS Threat Landscape
Communication Channel / (Tele) communication network(s)
Eavesdropping / Interception / Hijacking
Man in the Middle / Session hijacking
Compromised CA / Rogue certificates
Replay attacks
Interception of information
Pharming
Internet Banking Server / Remote Banking Service
Web site manipulation
Malicious links
Cross-site scripting attacks
Bank security policy violation
Bruteforce attacks
Brute force methods (offline and online)
Dictionary attacks
Denial of service attacks / Flooding
Poor implementation
Attacks focused on flawed encryption algorithms
Lack of Security by Design approach
User / User Terminal / Customer device
Physical Observation / User surveillance
Shoulder surfing
Handwritten note stealing
Filming the keyboard
Recording keystroke sounds
User Impersonation
Exploiting knowledge of personal details
Claimed identity (during registration)
Physical Theft, tampering or replication of token
Theft of physical authentication device
Reproduction of the characteristics of an already registered device (Token duplication)
Brute-force attacks with PIN calculators
Smartcard analyzers (power consumption analysis, time analysis)
Smartcard reader manipulator
Social engineering
Dumpster diving
Unauthorized authorization of a malicious device
Malicious software
E-mails with malicious code
Man-in-the-browser
Drive-by downloads / Malicious ads
Mobile malware
Keyloggers, Trojans, Worms (credential stealing malware)
Botnets
Phishing
Hoax email
Spearphishing
Whaling
SMiShing
Vishing
Web page obfuscation

Figure 5 Threat Landscape

5 Survey analysis

The categorization of Operations, Authentication methods and Threats, described in Section 2, Section 1.1 and Section 4 respectively, has been proposed mainly to support the survey addressed to security professionals in the e-financial sector. The survey objectives were to identify the eIDA methods currently used in online banking services and identify: usability and costs for operation types and customer segments, perceived strength and qualitative information about measured risk parameters, and improvement achieved. As it has been previously remarked, the survey was distributed and conducted by ENISA, with participation of members of the APWG.EU, CaixaBank, and Merchant Risk Council (MRC), and distributed to security professionals of the financial sector through SecuRe Pay, EU FI-ISAC, ECB, and EPC, and users' representatives through the MRC and the FSUG.

5.1 Current practices

Amongst the above mentioned eIDA methods (Section3.1), only those shown in Figure 6 have been widely adopted. Figure 6, presents the most common eIDA methods implemented in e-banking and the type of operation (according to categories described in Section 2) associated with each method. As can be observed, the weakest methods on the left are mostly used for non-risk operations, and the safest ones to authorize risky transfers. Survey results show that in many cases the professionals that answered it, did not make considerable differences between operations types 1&2, and something similar happened with operation types 3&4.

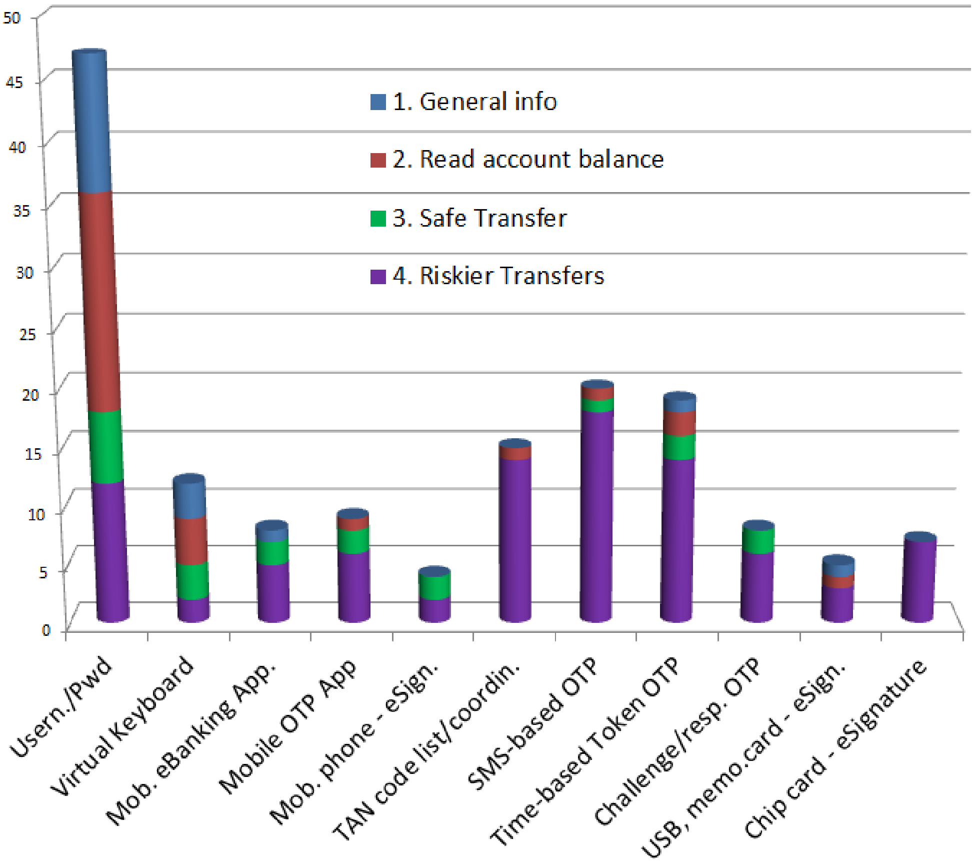


Figure 6 eIDA methods implementation for each operation type

5.2 Applicability of identified Threats to eIDA methods

Table 1 presents the applicability of the identified threats (according to categories described in Section 4.1) to the different eIDA methods. It has been assessed taking into account common practices in e-banking, recent literature [7], [11], and real world attack scenarios.

Authentication mechanisms	Threats										
(eIDA method)	**1a**	**1b**	**1c**	**2a**	**2b**	**2c**	**3a**	**3b**	**4a**	**4b**	**4c**
Username/password	5	5	5	3	3	5	5	5	5	5	5
TAN code list	4	3	5	5	5	5	5	5	5	4	5
SMS-based OTP	1	1	4	3	2	5	4	5	4	2	5
Time-based h/w OTP	1	1	3	5	3	5	3	5	4	3	5
Chal. Resp. h/w OTP	1	1	3	4	2	4	3	4	3	2	5
Mobile OTP App	1	2	3	3	3	5	3	5	3	3	5
Token e-Signature	1	1	1	4	2	4	1	3	2	1	3
Chip card e-Signature	1	1	1	3	1	4	1	3	2	1	3
Mobile phone e-Signature	1	1	1	3	2	4	1	3	2	1	3

Table 1 eIDA methods THREATS APPLICABILITY. Threats are described in section 4.1 above[37]. Applicability ranges from 1: Not Applicable to 5: Highly Applicable

The most noticeable points arising from Table 1 are:

- Most of the identified threats are highly applicable to the Username/password eIDA method.
- Moreover, only malicious code (i.e. threat 2c) and bank data breach (i.e. threat 4c) are applicable to all eIDA methods.
- Physical attacks against devices or tokens (i.e. threat 2a) are mostly applicable to the OTP and eSignature eIDA methods categories.
- Tampering of devices, (i.e. threat 2b) applicability depends on the robustness of the device.
- Finally, phishing (i.e. threat 1c) apart from being applicable to Username/password and TAN code list is also applicable to the OTP eIDA method category.

[37] Summary of Threat Categories described in 4.1:

1. **Threats against end-users.**
   a) Physical observation. b) Social engineering:. c) Phishing:
2. **Threats against end-users' devices.**
   a) Physical theft of token or device. b) Tampering (or replication) of token or device. c) Malicious software (malware)
3. **Threats against communication networks.**
   a) Pharming. b)Eavesdropping, Interception and Hijacking.
4. **Threats against remote banking services.**
   a) Web Code injections against banking server. b). Denial of Service (DoS). c) Bank data breach.

5.3 Perceived strength, usability and cost

Through the responses of the security professionals, we have identified quite clearly three groups of eIDA methods according to their strength, which suggests their suitability for the operation types (described in Section 2), i.e. the weakest methods are suitable for low risk operations and the stronger methods should be implemented to grant high risk operations. This perception of security professionals is summarised in Figure 7 Professional's perceived strength, usability and cost.

The comparison of Figure 6 and Figure 7 confirms the well-known feeling that a common practice in the financial sector consists of giving priority to usability over other criteria. The eIDA methods considered more usable are also those financial institutions do implement more. The exception is the Mob. Phone e-Signature, because there were few responses of professionals reporting having used it, and for this reason, the statistical accuracy of that data is not very good. Nevertheless, we have kept it because it's an emerging authentication system well evaluated by the professionals that already have implemented it. Figure 7 also shows the tendency lines of implementation factors cheapness and strength, green and blue respectively. In general the weaker the eIDA methods are, the cheaper to implement, except in the e-signature based eIDA methods, which, being the stronger ones, are perceived as cheaper to implement than other weaker methods.

The usability restriction for implementing stronger eIDA method should be avoided through adequate training and awareness of customers. The adoption strategy and the "user experience" through adequate developments should also be improved.

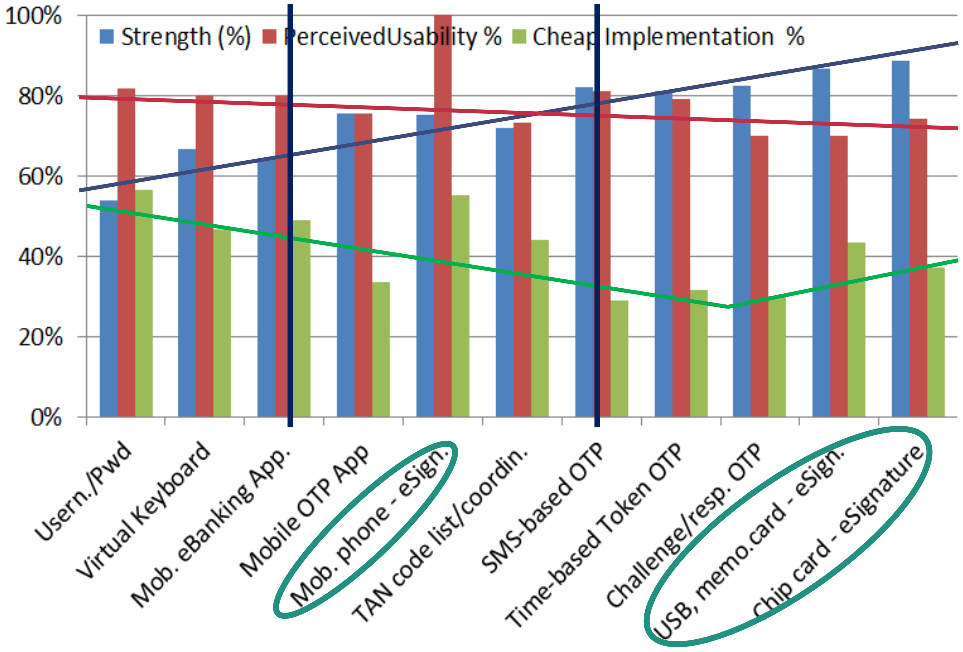


Figure 7 Professional's perceived strength, usability and cost

5.4 Adequacy of eIDA methods selection criteria

The survey asked the participants to indicate the criteria (several) that made them choose the implementation of one eIDA method in preference to others. The identified selection criteria were:

- Adequacy to one or several customer segment.
- Usability from the point of view of the customer, provided their skills and professional profile.

- Covered Risk, i.e. the capability of the eIDA method to prevent the success of known threats to the e-Banking authentication system.
- Efficiency of the investment, it is a more abstract concept, because combines both Risk reduction achieved by the eIDA method and the implementation Cost.
- Implementation cost, the answers reflect that the participants have taken into consideration the number of customers in the segment or profile to which the eIDA method is addressed.
- Implementation easiness, the survey shows that this is not a criterion to implement a eIDA method.

According to the set of criteria used to select the implementation of one eIDA method in a given environment, three groups of patterns have been identified. Figure 8 shows the relative relevance of the different selection criteria for implementing eIDA methods for the low, medium and high strength groups of operations respectively. In each group, the specific selection criteria for that group have been encircled in blue. In the group of medium strength, the criteria that show the difference with the low strength group of eIDA methods have been encircled in yellow, and those criteria become the most important to select the stronger eIDA methods. The user segment whose preferences attract more the attention for the selection of most of the authentication mechanisms is the “retail customers”.

For the authentication mechanisms most suitable for low and medium risk operations the adequacy to the retail customers and the usability are the dominant criteria. This means that the professionals participating in the survey declared that they implemented the authentication (eIDA) mechanism due to their feeling that it was more adequate to one or several customer segments, being the “retail” segment the one reported more times, as well as other parameters of the eIDA methods. Most of the participants indicated that several criteria were used to justify the implementation of one authentication mechanism, being the usability the parameter selected most times, but not the single one, e.g. the cost is also important in the selection of the eIDA method for the low risk operations (see Figure 8 below).

The mechanisms suitable for intermediate risk operations are implemented due to its usability and adequacy to the requirements of most of the users, and also by its efficiency and covered risk.

For the authentication mechanisms that look more adequate for riskier operations the covered risk replaces the usability as top selection criteria, and more attention is paid to the corporate and private bank customers.

All eIDA methods involving the use of hardware tokens are more suitable for corporate, private and investor customer segments (Section 3.3). Distribution costs and usability (another device to be carried) drawbacks are less relevant for those customer segments, because the number of customers is significantly lower (<1% of retail users), and they are more conscious of their transactional risk, thus, accepting stronger eIDA methods to be applied. New kinds of token devices are now emerging, able to improve usability, e.g. token in credit card format; however, the associated costs, are even higher, reducing the profile of the customers to which they could be offered.

Circled in blue, are the most relevant criteria for each strength group, and in yellow the criteria that show more changes, comparing the responses given to eIDA methods of each of the 3 groups. The fact that the eIDA methods with lower strength are selected principally because of their usability, and the stronger ones because of the covered risk, confirms the quality of the responses stating the perceived strength.

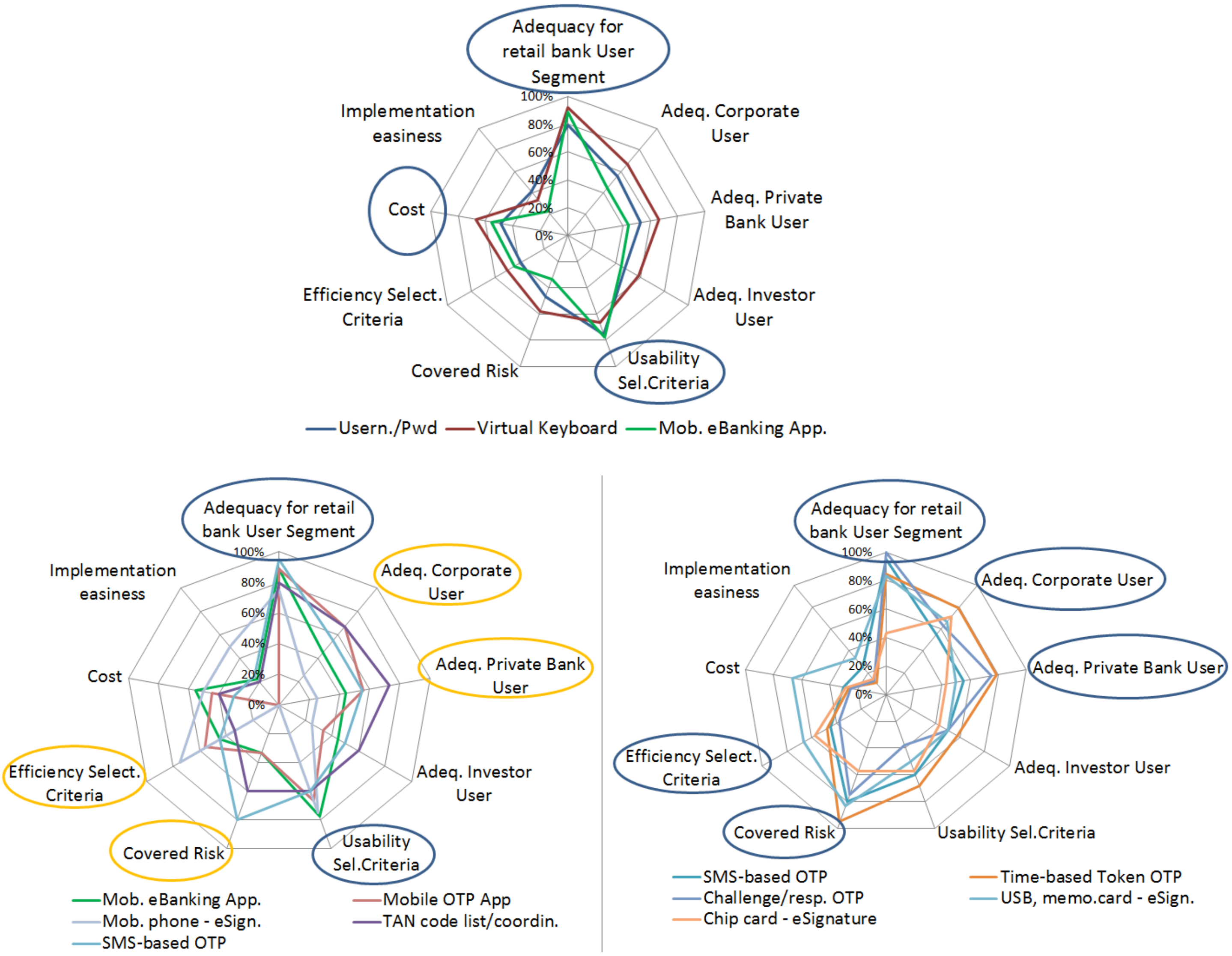


Figure 8 Comparison of criteria used to Select eIDA methods of Low (up), Medium (left) and High (right) Strength

The relationship between selection criteria and perceived strength is shown in Figure 9 below. This figure shows some aspects of the responses that are worthy of comment, highlighted with yellow ellipses:

- Mobile banking Application and Mobile OTP are selected for their Efficiency rather than for the covered Risk.
- TAN code list is considered quite well in terms of covered risk, whilst it gets the worst estimation of Efficiency.
- The discrepancy is even larger in all OTP eIDA methods, they are selected for the covered Risk and not for their efficiency, probably because of the relative high cost of adopting them. Those methods, together with the USB e-Signature, are considered the methods covering more Risks, and are selected for this reason.
- The e-Signature eIDA methods are those considered more efficient than any other did.

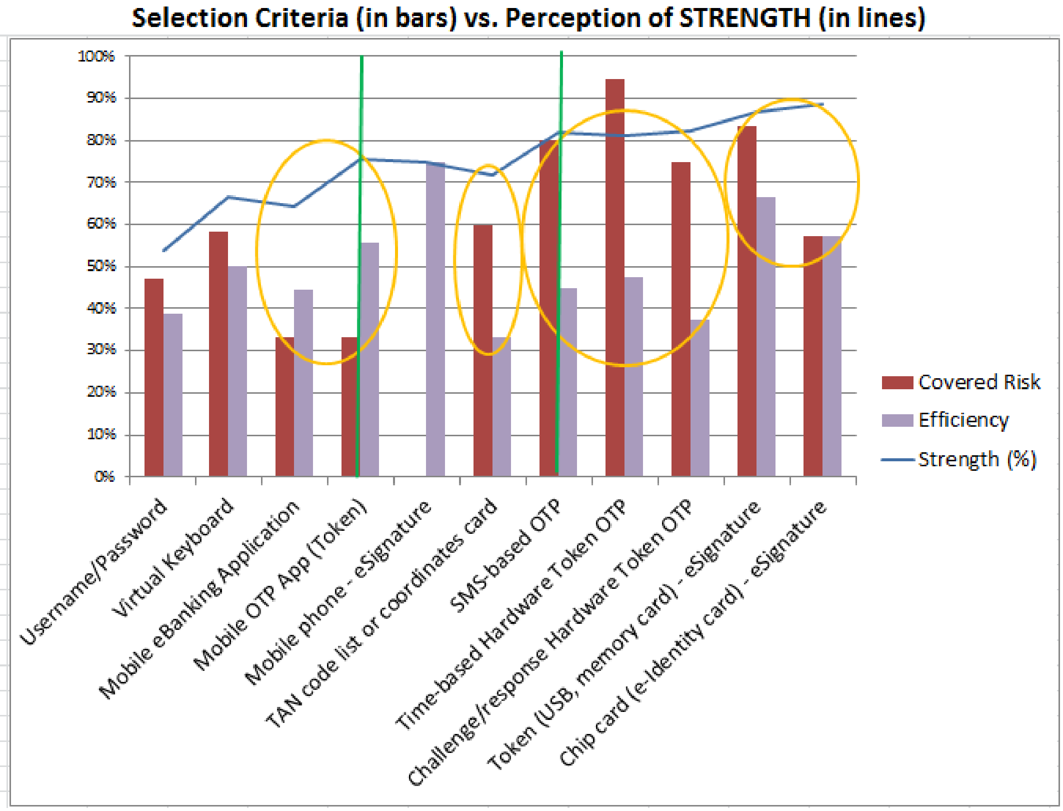


Figure 9 eIDA methods Selection criteria vs Perceived strength

5.5 eIDA methods Risk Reduction benefits

Figure 10 shows the summary of the survey participants reported loss and loss reduction per user and incident, and the number of incidents associated with each eIDA method.

The most frequently used eIDA methods have also the higher risk, because they attract the interest of criminals to research and develop more sophisticated attack patterns and tools, since they will be applicable to more customers.

It is worth highlighting that the absolute loss reduction figures are per user involved in an incident.

The methods that show higher reduction of loss are also those that have been identified as having higher loss per incident and user. This is because in general they are also considered stronger (OTP based methods) and for this reason used to authorise operations of high value, so if they are faked the loss for the user is high, but the graphic also shows that the number of incidents for the strongest eIDA methods is very low. A special case are the Username/Password and Virtual Keyboard, which are considered to introduce a surprisingly relative large loss reduction, but with relative high Loss per user and incident, and large number of incidents per year (12 and 17).

The opposite case is the Token (USB, memory card) e-Signature, with relatively large number of incidents and very low loss for each, because of the difficulty to use the token by other person rather than the owner, and because this method is also used for low risk operations, in many cases as first authentication method to log into the service.

In general, the results of the survey show that the lower number of incidents corresponds also to the less implemented methods; mostly those based on mobile handset token OTP or e-signature.

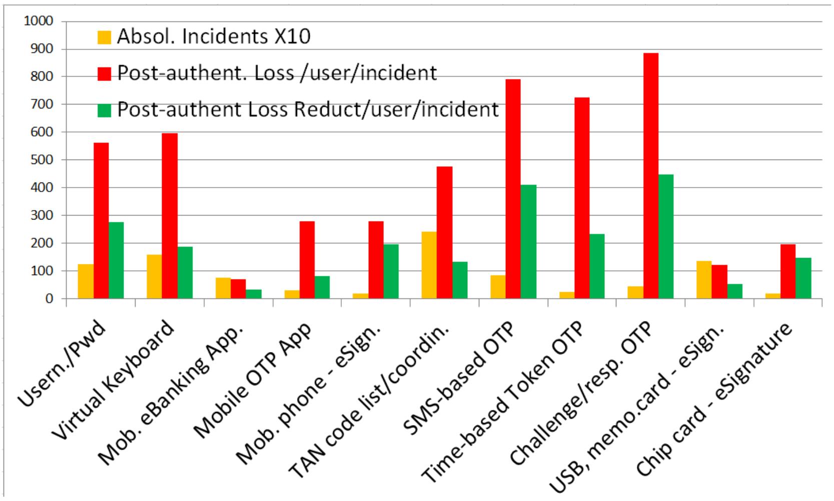


Figure 10 Reported incidents, loss and loss reduction

One factor that is not considered in this analysis is the customer skill. This is probably the reason why the TAN code method is the one with more incidents reported per year, which, added to the fact that, in some institutions it is used to grant access to riskiest transactions, it makes the actual loss per incident relatively large also, resulting in the large Risk already mentioned.

Another perspective of the answers given in the survey is shown in Figure 11, where it is possible to confirm that the riskiest eIDA methods are those used by a larger number of customers. They are also those providing a larger reduction of loss, about 10% (notice that the pre-authentication Risk is 10 times larger than shown in the bars, to make uniform the ranges of values of both data sets). The eIDA methods that provide more than 10% of loss reduction are:

- e-Signature (mainly phone and chip stored key)
- OTP (Challenge/Resp. token and SMS based)
- Username/Password, probably because of the estimation of potential loss that could be reached if the unsuccessful attempts to break the password would be successful.

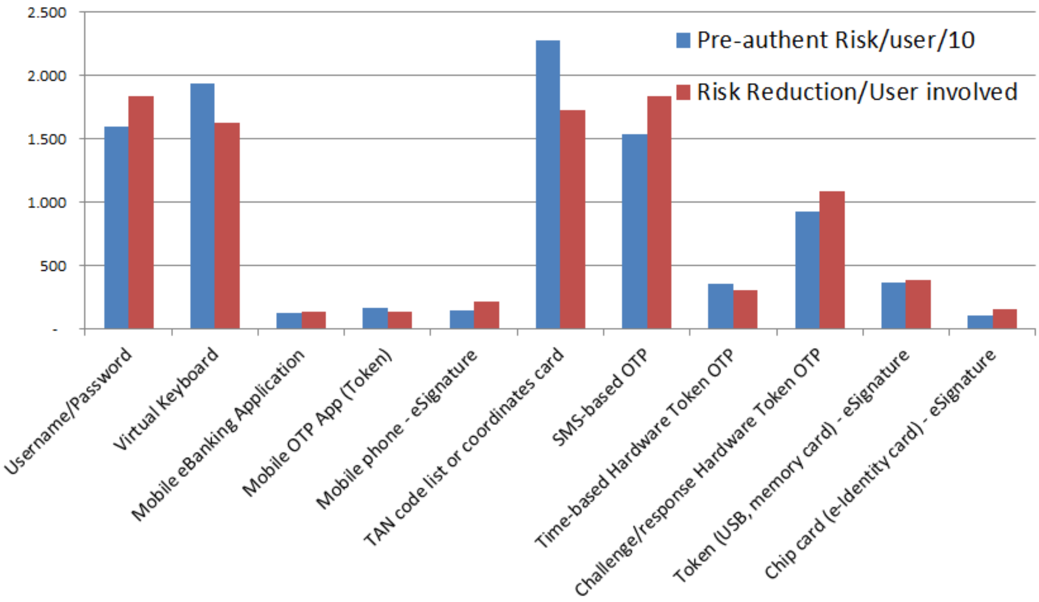


Figure 11 Risk reduction

6 Risk analysis guidelines

The threats introduced in Section 4.1 have a different impact on the target environment, also depending on the actor involved, e.g. a threat to the communication channel of a e-Banking service represents a greater impact than what can be achieved if the victim is a retail customer. Thus, an ad-hoc Risk Analysis of the target environment is recommended. Moreover, in terms of implementation, a definition of security aims - in accordance with the identified risk categories and the access rights granted to the customer- should be taken into consideration within the Risk Analysis. Considering that, when it comes to securing e-payments, there might be a difference concerning security aims depending on the perspective of the stakeholder. Whereas an individual bank would judge its security investments based on some business case considerations (i.e. comparing the cost of payment for damages with the cost of preventing fraud), while a payment system or a central bank, which is responsible for trust and security of the overall payment system may have a different view.

Therefore, in accordance with the current regulatory proposals[38] and with the aim to increase efficiency of payment systems, additional considerations on the security aims for the various transaction types should be taken into account. To give some examples:

- *for account information services relevant security aims could be to safeguard personal customer information from unauthorized access;*
- *for payments the security aim from a societal perspective would most likely be to support the 'finality of payment' (i.e. the payment is irrevocable and legally enforceable) and 'non-repudiation' (i.e. the payment cannot successfully be disputed afterwards by the originator) in order to withstand legal dispute.*

The result of the survey shows that the most frequently used selection criteria for the authentication mechanisms are the strength and the usability of a mechanism, with different weights depending on the number and profile of the users, and the risk associated to the operations normally performed by those users. However, given the above-mentioned regulation, which is coming into effect in the coming years, some financial institutions may shift the criteria to merely: "**comply with regulation",** therefore an analysis with a detailed judgement on what will comply and what will not can be of great benefit.

For this reason financial institutions should be encouraged to perform a quantitative risk analysis, based on the actual data of number of incidents, customers involved and average loss per customer in the organisation. Those fraud costs should be introduced in the calculation of the cost of non-implementing the authentication mechanisms, and compare that cost with the cost of implementing them. The results of the survey show that most of the security experts of the financial institutions have that information, but it is not taken into consideration in the decision process for the selection of eIDA methods.

One good practice to improve and guarantee the ROSI (Return of Security Investment) could be to make the risk analysis tailored to different customer profiles in the institution. This is important for two reasons:

1. Some threats like spear phishing are targeting customers with large balances on their accounts, so the impact of those attacks will be high on them. But application of countermeasures to customers with other profiles, not targeted by them, would be useless.

[38] European Directive on Payment Services , PSD: http://ec.europa.eu/internal_market/payments/framework/

2. The loss reduction and the number of incidents associated to an authentication mechanism are also linked to the profile of the customer using it. The most qualified customers are more likely to take care and appreciate the robustness of more sophisticated and stronger authentication mechanisms, whilst customers perceiving less risk of being victims of an attack or having losses in their accounts, would not take adequate care and may easily be victims of credential steal or replication. The cost of introducing those kinds of measures to unaware customers will be more expensive than introducing it to aware ones, because it should include the cost of launching adequate awareness campaigns. Moreover, the loss reduction will also be different, because the number of incidents per user and the loss per user and incident will be linked to the consciousness of the customers and the kind of operations they perform regularly through e-Banking applications.

All those considerations will result on different ROSI depending on the profile of the user (awareness, kind of transactions, account balance, etc.), and the number of customers of that profile in the financial institution. Another important aspect mentioned by some reviewers of this report is the Corporate Social Responsibility (CSR). So far, the policy of many institutions has been to recover customers' losses, at least partially. But the new regulation of Data Protection will oblige them to disclose threats if the number of victims or the impact on them is high, so it will not be so easy to avoid damages to the public image of the institution, and the benefit of covering the losses of the customers will not be so evident. Then the single way to preserve the image of the institution will be to prevent the success of the attacks, introducing the potential loss of qualified customers if the security mechanisms offered by the financial institution prove to be weak to protect the interests and assets of the customers. In addition, the national central banks are appealing to the CSR of the banks to protect the citizens and keep the fraud statistics in the country within "acceptable" boundaries, compared with other countries.

In the next two sections there are some analysis to specific emerging authentication mechanisms.

6.1 Biometrics adoption related risks

The results of the survey show that very few professionals incorporate biometrics as an eIDA method solution for e-banking. The rationale behind this phenomenon is that institutions must be able to comply with the GDPR. There exist legal issues when dealing with personal information (different legislation for every country). In Europe, a specific authorization from customers is required, which is a difficult task, since the majority of people do not feel comfortable with granting permission on the storage of their biometric information (i.e. personal body patterns). This, in general, is only manageable if a strong juridical base exists and the use is adequate, relevant and not abusive in correspondence with the goals and reasons for biometric data to be collected, used or saved, resulting in an important challenge to be addressed.

Moreover, there exist high associated risks, mainly due to the potential attacks to a centralised data base storage of biometrics parameters. The risk of compromise of the biometric information DB (even if it's encrypted, hashed, etc.) is real and non-acceptable for CISOs and directors of the e-banking sector. The sensitive nature of biometric information: data is compromised forever (i.e. it's not possible to change the hand print, Iris, fingerprints, etc.), resulting in both high risk, and great responsibility to be accepted, especially if other eIDA methods are suitable.

Another important factor is the usability, since current technologies do not provide 100% of accuracy at the first try. There are still open issues related to the False Rejection Rate (FRR) and the False Acceptance Rate (FAR), which remain open even in scientific experiments or proof of concepts.

In summary, because of the associated risks, the financial sector is still not prepared to use biometry neither as a unique authentication factor nor a second authentication factor.

Biometry is used in emerging countries, where there are no other means of unique identification of the persons, due to lack of governmentally supported credentials, and also in countries where Personal Data protection is not a priority, like it is in EU.

Specialists are working in finding a solution to the high risk associated to using the biometry, and one solution that is being analysed and starting to be implemented is the local storage of biometric identification profiles. This has three advantages: 1) the responsibility of the storage is transferred to the end user, 2) the chances of a successful threat to steal large amount of biometric information is low, because the threat should be successful on many devices and stores, 3) the biometric identification vector doesn't have to travel over the network.

6.2 Mobile phones related risks

Advances in mobile technology, currently allow the use of mobile devices in a wide range of services and applications. An important reason for involving mobile phones in authentication systems such as OTP systems, is that, most users already have one, and therefore, no extra hardware needs to be bought, deployed or supported. Moreover, since a mobile phone is considered a highly personal device, the number of incidents due to losing it are relatively low, especially compared with the hardware token devices.

The most common authentication solution involving mobile devices is the SMS-based OTP. A user willing to make an online transaction will receive an OTP from the server. The OTP will be delivered to the mobile device on an SMS. As it can be observed from this study the SMS-based OTP is one of the most implemented authentication methods by the financial sector, nevertheless, SMS-based OTP also convey clear disadvantages, which include, the associated costs, roaming, latency and more importantly the associated security risks, SMS-based OTPs are vulnerable to a different attacks, such as, the Man-in-the-middle (MITM) attacks. The “Eurograbber” incident (see 4.2.2.2) showed how two factor authentication based on SMS-OTP was circumvented, resulting in a 36 Million Euros loss. To avoid this threat customers and e-Banking applications should avoid displaying phone numbers associated to the bank account through Internet, whether displayed or modified, even with assumed secure communication channel. Adequate training on this sense has to be launched to both of them.

An alternative to the SMS-OTP is the Mobile phone e-Signature, which greatly reduces the possibility of a successful MITM attack since credentials are protected in the secure element (SE) of the mobile phone. However, the majority of SE implementations rely on a third party, which does not provide a suitable solution to stakeholders such as the financial institutions, as they would certainly like to have more autonomous and cost effective solutions for their mobile payments implementations. Moreover, the limited size of physical SE dramatically affects the number of applications that could be placed in those SE. Financial institutions should promote joint ventures with the organisations that manage the content of those SE, in order to improve the trustworthiness between them.

Another currently implemented solution is the mobile e-banking application, which is able to provide enhanced security if a private key is installed. However due to the nature of mobile devices, important security risks are also present, such as malware hosted on fake applications. Moreover, the development of applications is not always aligned with current security best practices. Best practices like “security by design”, secure storage and all actors involved in the process must guarantee delivery and integrity of applications: software developers, financial institutions and customers.

Following the same direction, an emerging solution is the mobileOTP, which consists on iinstalling the software tokens on the mobile phone. A key advantage of the mobile software token is that there are no new devices for customers, since customers already own the device, which they already carry everywhere. Another advantage regarding the mOTP solution is the ability for the software tokens to be distributed and updated immediately, and without logistical planning, since the mOTP token consists of an application that only need to be loaded on the mobile device. Thus, mOTP have become a more reliable deployment method than hardware tokens, nevertheless, as in mobile e-banking application, the software tokens also inherit the same security vulnerabilities from the mobile phone. In fact mOTP could be considered a particular case of mobile e-Banking application.

Many organisations use mobile phones as support for the second authentication factor. Mobile phones may be considered “something the user possesses” for the purpose of implementation of two-factor authentication, from the technical perspective. However, from the legal perspective, mobile devices cannot necessarily be acceptable for attributing a specific transaction to its originator. For that purpose, e-signature tools have to be used, and they can be implemented in mobile devices or PCs. The mobile device on its own is not able to deliver evidence that a specific transaction could only have occurred with the approval of the legitimate owner of the mobile, it requires specific software and adequately installed private key to do so.

In summary, mobile device is an emerging authentication solution that can be seen as “something the user has”, when using it for identification purposes. Nevertheless, for attributing a specific operation to its originator, it’s not able to provide enough non-repudiation evidence that a specific operation has been performed by the owner of the device.

7 Recommendations / Best practices guidelines

This section introduces the main challenges found in our research, and, to overcome these challenges, a set of recommendations are proposed. The recommendations are grouped in Challenges, which express the main objectives to be achieved by the recommendations grouped there.

Those recommendations have been

7.1 Challenge: Promote Adequacy of eIDA method to Context

The selection of an eIDA method should be done considering the full context of the operation and, users segments.

7.1.1 Rec.1: eIDA method Selection proportionality

e-Finance Authentication mechanisms strength have to be proportional to the Risk associated to the operations they grant access.

When customers interact with the e-Banking service, they may perform operations of different level of risk (Section 2 above):

1. General information,
2. Read account balance,
3. E-Payments: Low-risk or low-value Transfers, as defined in the PSD.
4. Transactions: Transfers of funds not matching level 3 requirements.

Figure 6 shows the current practices in the sector.

7.1.2 Rec.2. Use Two Factor Authentication (2FA) for medium to high-risk transactions.

For medium and high risk operations, a strategy of using at least two authentication mechanisms that are mutually independent, where one is non-replicable and other non-reusable, exchanging credentials through different communication channels or devices should be implemented. Non-re-usability may be implemented by linking the authentication (e.g. OTP challenge) to the amount and payee of every transaction.

Many organisations use mobile phones as support for the second authentication factor. The adequacy of the authentication mechanisms for low, medium or high risky operations is described in section 5.4 above. It shows that the selection criteria used by the financial institutions already takes into consideration the different profiles of customers as well as the efficiency and strength of the eIDA method proposed. The aim of this recommendation is to shift the criteria to select the eIDA method used for medium level of strength: from its usability, to its covered risk and efficiency in protecting customers' assets.

Most banks already apply more than one authentication mechanism to grant access to different types of operations. Currently most used combinations are PWD, sometimes with additional security improvement methods like Virtual Keyboard, complemented with: SMS OTP (29%), TAN (25%), Hw. OTP (18%), MeBA (11%), Mob. OTP (9%), Chall.Hw OTP (8%), whilst other combinations are also reported. Figure 12 shows the relative weight of the different combinations of authentication mechanisms reported in the survey through the size of the circles.

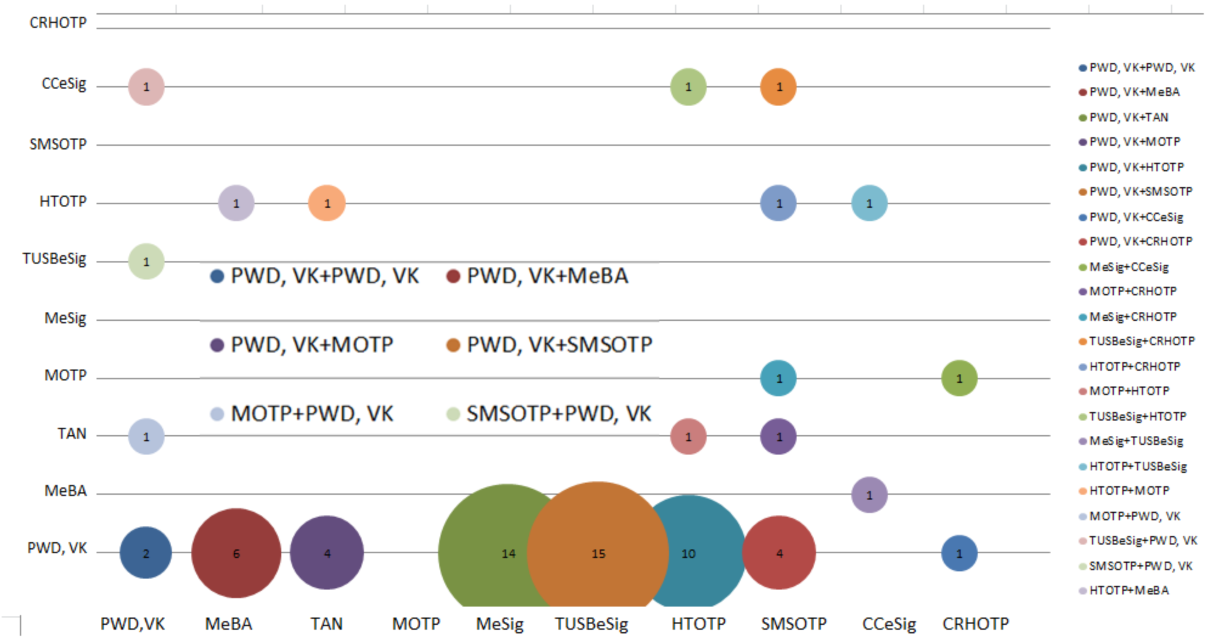


Figure 12 Combination of eIDA methods in authentication chains

1. From these observations, it's worth to highlight that: Accepted common practice for Read Access operations (not access to sensitive data[39]) is to use at least Password, Improved with some additional mechanism(s), e.g. virtual keyboard or Mobile e-Banking App (MeBA), depending on which kind of device is used by the customer for main (first) access.
2. The Recommendation for medium and high Risky Operations/Transactions is to Involve a 2nd device or something the user has[40], e.g.: mobile phone handset[41], TAN code list[42], eSign private key, hardware token OTP. The actual implemented method on each environment takes into consideration the perceived usability, mainly for the eIDA methods implemented for retail customer segment, but the stronger methods should have priority in the selection

[39] DPA have defined what is sensitive financial data

[40] This recommendation is shared with the ECB SecuRe Pay forum, which in their "Recommendations for the security of internet payments" (published on 31 January 2013 on http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf) states: "***Strong customer authentication*** *is a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. static password, code, personal identification number; ii) something only the user possesses (Strong authentication element), e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data".*

[41] It is considered a common feeling amongst experts that mobile devices are "something the customer has". Some people consider the mobile handset an object of more ownership than even a credit card, because it is less frequently left "unattended". Security of mobile phone devices has been analysed in section 6.2.

[42] Some experts consider questionable to qualify TAN code lists as ownership, because of its easiness to be replicated. The impact of this threat can be minimised with complementary security measures, like adequate user training against phishing, awareness about risks of replicating and leaving unattended the TAN code list, "secure delivery" to the customer, etc.

process. On top of this, the actual risk in the environment of the financial institution should be measured (see justification in section 6 Risk analysis guidelines and Recommendation in 7.3.1 Rec5. Environment risk analysis).

7.2 Challenge: Improve the knowledge and the behaviour of customers and professionals

7.2.1 Rec3. Professionals' training and awareness

Continuous training of professionals, to improve their perception of the actual risk associated to the e-Finance transactions, and the authentication mechanisms, keeping in mind the last threat patterns discovered by criminals. Professionals should also share their awareness with customers, to keep them continuously informed about incidents caused by common threats such as phishing or social engineering.

From the result of the survey, comparing the perceived strength, the reported number of incidents and average loss per incident, it looks like the professionals had a "feeling" that does not correspond with the data they report. E.g., Figure 9 shows that TAN code strength perception is at the same level as mobile phone signature or OTP, whilst TAN code is selected because of its covered Risk twice than the mobile-based methods. If professionals were aware of those figures of risk, awareness, costs, the eIDA method would be selected consequently with them. Therefore, it is worth to recommend the dissemination of actual Incident data amongst professionals of e-Banking applications, to improve the matching between their perception of strength and the actual reality.

7.2.2 Rec4. Enforcement of customer's eIDA method security & usability perception

The professionals of the e-Financial institutions should inform their customers about the usability and need of the safer authentication mechanisms required to have an adequate protection to their assets, in order to make them to feel comfortable enough using them.

The perceived strength of the authentication mechanisms by users and professionals is quite similar, but in most of the cases, the perception of usability by the professionals is much larger than for the users (see Figure 13).

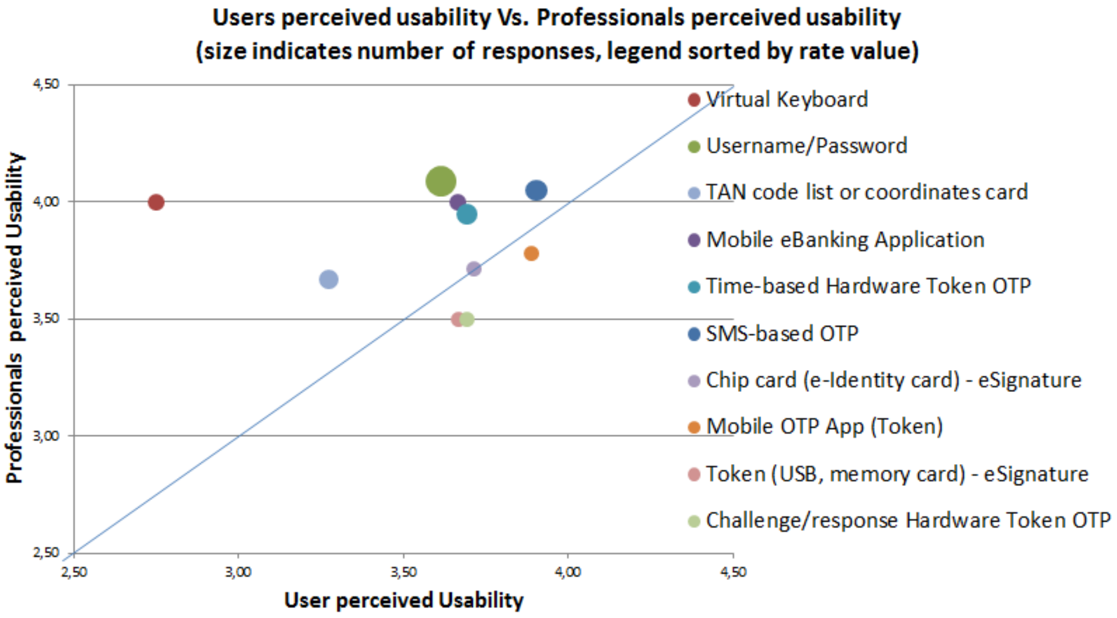


Figure 13: Perceived usability by users and professionals

Since usability is one of the most popular criteria for selecting authentication mechanisms in most of the e-banking applications, this difference of perception needs important attention and analysis. One extreme example worth mentioning is the virtual keyboard, perceived as easy to use by professionals (8/10) and un-usable by users (5.4/10), probably because nobody has explained them how to use it, its advantages to protect from keyloggers, or because the method is required to users accessing through devices un-suitable for it, like mobile handsets without touch-screen.

7.3 Challenge: Improve the security of the e-Finance environment

7.3.1 Rec5. Environment risk analysis

Financial organisations and e-commerce merchants must perform specific risk analysis for their environments, taking into consideration the actual loss, number of incidents, number and skills of customers involved, and actual vulnerabilities of the authentication methods available, in order to be able to choose the ones that most effectively reduce the number of incidents and loss, i.e. the risk to lose money.

The reduction of the risk (analysed in section 5.5) and the number of incidents should be one of the selection criteria, mainly for the secondary authentication mechanism (used to complement the first one for all operations, or to grant access to the most risky operations). The average figures of risk reduction in euros are shown in Figure 11 . But each organisation has to perform its own analysis, based on their number of customers of each segment, their readiness to accept some authentication mechanisms, the economic value (risk) of the transactions they perform, etc. (See section 5.5 above).

7.3.2 Rec6. Context based or continuous authentication

Customer authentication should be complemented with the implementation of a context-based authentication strategy, tailored to customer behaviour profile (e.g. transfer destination account), segment (e.g. total amount in operations) and the operation risk (e.g. destination country, black lists).

A more complete list of most commonly used context authentication and user behaviour parameters is as described in Section 3.2.

7.3.3 Rec7. User device security testing and evaluation

The security testing and evaluation of the device used to access the service has to be validated directly or indirectly by the PSP.

Mobile devices are becoming vulnerable to several security threats such as malware attacks (see section 6.2. Mobile phones related risks), where attackers abuse them for transactions without any interaction of the legitimate owner of the mobile phone, just as it has been possible in normal PCs since years ago. In June 2012, ENISA recommended financial institutions to "**Assume all PCs are infected**"[43]. Therefore, static security analysis of any device used by the customers to access e-Banking services should be performed, in order to estimate the degree of compromise of user's device. Some kind of analysis can be done remotely by the server accessed by the customer (e.g. browser version), but only customers can install and run anti-malware software on their devices, and

[43] High Roller ENISA's flash note: http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps

for this purpose have to be trained and convinced about their own interest on having their devices protected against infection.

7.3.4 Rec8. Device registration

The concept of "something the user has" can be extended to the platform used to access the service, and thus it is recommended to register any Device, Browser, or Mobile Application used by the customer. A real time validation of the authenticity of the device would be required.

This registration will prevent customers from being impersonated by somebody that has been able to replicate some credentials of the customer, using specific different credentials and process to authorise new devices for the user.

7.4 Challenge: Improve the security of e-Finance application development and distribution

7.4.1 Rec9. Secure e-banking application development

Technology providers must guarantee secure e-banking application development, taking into consideration actual threats to Operating Systems (e.g. mobile attack vectors).

Special emphasis has to be given to managing personal data, for which purpose specific data security analysis (persistency, access control) have to be implemented during the development phases.

Another security issue that may have strong impact on the adoption of strong eIDA methods is the implementation process and tools, for two reasons:

- **eIDA method incorrectly implemented may have security back doors or vulnerabilities**
- **eIDA method with inadequate or too complex implementation tools will not be accepted by customers.**

In the case of mobile phone applications, it is also recommended to develop applications to be executed within Secure Execution Environment, using available secure elements that will make them more robust against emerging threats, before those threats become reality.

7.4.2 Rec10. E-Banking applications distribution

Distribution of e-Banking applications has to be made through trusted channels, reputable sites that guarantee that applications have been tested for security.

It is very difficult for customers to validate the authenticity of e-Banking applications on their own, because criminals have demonstrated their ability to sign fake applications with trustworthy software signing certificates that can overcome the normal installation filters in many devices.

For this reason the use of software distribution platforms (software marketplaces or e-Banking websites) that guarantee that they have performed security tests on the applications is very important for the security of the device on which the application is installed and to guarantee that the application will be executed as expected by the developers.

8 Conclusions

Those recommendations are intended to improve the security of eIDA methods in the landscape of the eFinance sector shown up by the results of the survey launched by ENISA and replied by users and professionals. Their implementation will be responsibility of the e-Finance and e-Payment institutions, in some cases because they are guidelines to achieve their responsibility to preserve the security of the assets of their customers, and in others, because they are mandatory to fulfil security requirements expressed in the PSD.

The recommendations also: a) reinforce those made by ECB to implement Internet payments and customer authentication[44], and b) help financial institutions and payment service providers to implement the new Payment Service Directive (PSD2).

[44] "Recommendations for the security of internet payments" published on 31 January 2013 on the ECB's website http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

9 References

[1] comScore Data Gem, "http://ww.comscoredatamine.com/," 2012. [Online]. Available: 1 in 4 Internet Users Access Banking Sites Globally. [Accessed July 2013].

[2] N. Bhas, "Juniper Research," 2013. [Online]. Available: http://www.juniperresearch.com/viewpressrelease.php?pr=356. [Accessed July 2013].

[3] Division of Consumer and Community, "Consumers and Mobile Financial," Board of Governors of the Federal Reserve System, 2013.

[4] D. Marcus and R. Sherstobitoff, "Dissecting Operation High Roller," McAfee, 2012.

[5] D. B. Eran Kalige, "A Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware," Versafe (White paper), 2012.

[6] M. R. Nami, "E-Banking: Issues and Challenges," in *10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing*, 2009.

[7] C. K. Dimitriadis, "Analyzing the Security of Internet Banking Authentication Mechanisms," *Information Systems Control Journal ,* 2007.

[8] L. Peotta, M. D. Holtz, B. M. David, F. G. Deus and R. T. d. S. Jr, "A Formal Classification of Internet Banking Attacks and Vulnerabilities," *International Journal of Computer Science & Information Technology,* pp. 186-196, 2011.

[9] A. Fatima, "E-Banking Security Issues – Is There A Solution in Biometrics?," *Journal of Internet Banking and Commerce, August 2011, vol. 16, no.2,* vol. 16, no. 2, 2011.

[10] A. Hiltgen, T. Krampand and T. Weigold, "Secure Internet Banking Authentication," *IEEE Security & Privacy,* 2006.

[11] R. Chouhan and V. S. Rathore, "e-Banking Security and Authentication Issues," *International Referred Research Journal,* 2011.

[12] J. Choubey and B. Choubey, "Secure User Authentication in Internet Banking: A Qualitative Survey," *International Journal of Innovation, Management and Technology,* vol. 4, no. 2, 2013.

[13] A. Y. Lindell. [Online]. Available: http://www3.safenet-inc.com/blog/pdf/Time_vs_Event_Based_OTP.pdf. [Accessed 21 July 2013].

10 Annex I: Abbreviations

2FA	2 Factor Authentication
APWG	Anti-Phishing Working Group
BP	Best Practice
CISO	Chief Information Security Officer
COM	European Commission
Chall.	Challenge
CNP	Card Not Present
CSR+A47	Corporate Social Responsibility
DG	Directorate General
DNS	Domain Name System
DoS	Denial of Service
DPA	Data Protection Authority
EBA	European Banking Authority
EC	European Commission
ECB	European Central Bank
EDPS	European Data Protection Service
eID	Electronic Identification
eIDA	electronic Identification and Authentication
EMD	E-Money Directive
ENISA	European Union Agency for Network and Information Security
EPC	European Payments Council
eSign	electronic Signature
ETL	ENISA Threat Landscape
EU	European Union
FAR	False Acceptance Rate
FI-ISAC	B48Financial Services Information Sharing and Analysis Center
FRR	False Rejection Rate
FSUG	Financial Services User Group,
GA	Governance authority (of a payment scheme)
GBP	Great Britain Pound
GDPR	General Data Protection Regulation
H3	Unit H3: Retail financial services and consumer policy
Hw	Hardware
ICT	Information and Communication Technologies
IP	Internet Protocol
IT	Information Technology
KC	Key Considerations
LEA	Law Enforcement Autority
MeBA	Mobile e-Banking Application

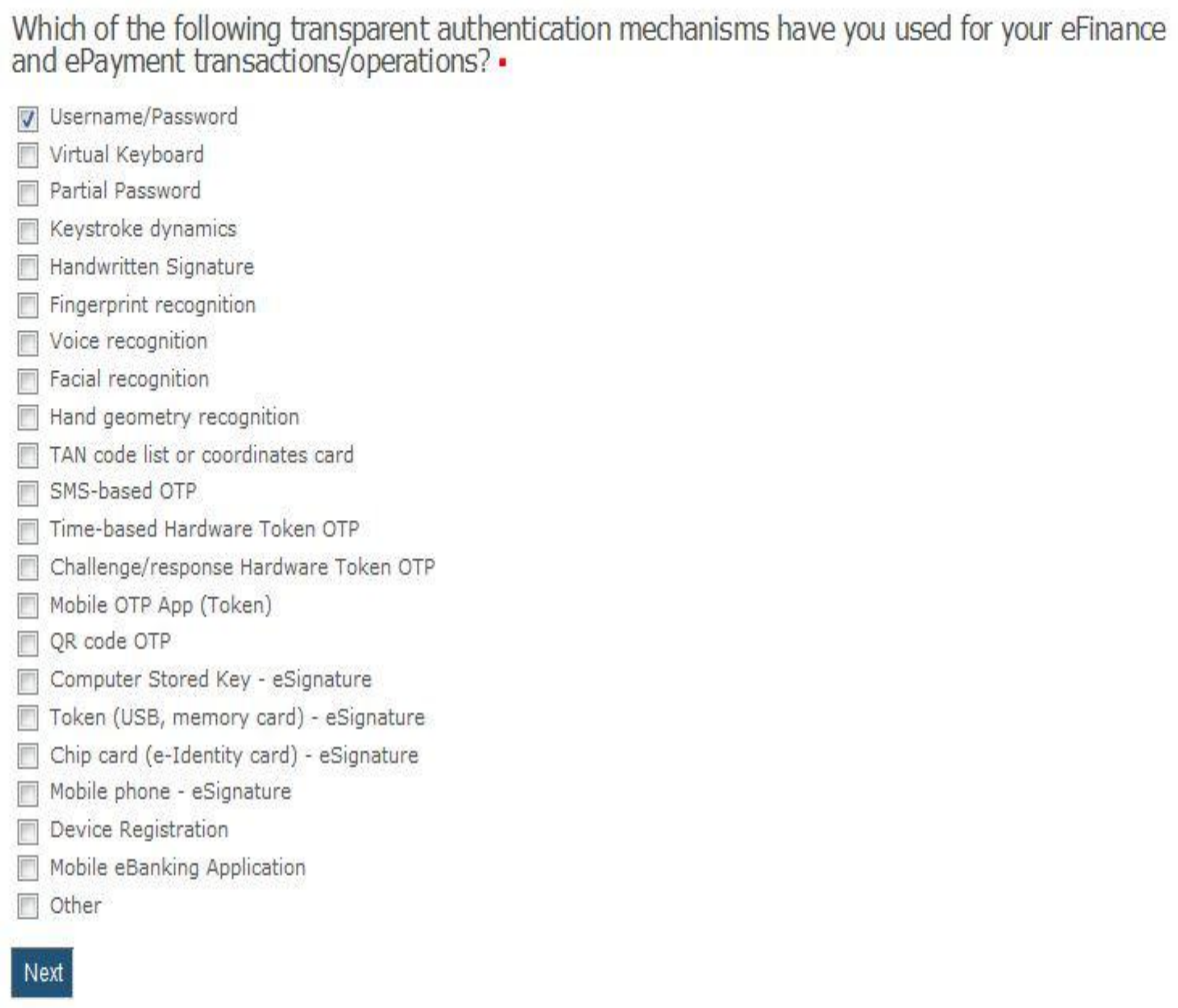
MitB	Man in the Browser
MITM	Man in the Middle
MitMo	Man in the Mobile
Mob.	Mobile
MRC	Merchant Risk Council
MS	Member State
NIS	Network and Information Security
NRA	National Regulator Authorities
OTP	One Time Password
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
PSD	Payment Services Directive 2007/64/EC
PSD2	Payment Services Directive COM/2013/0547 final - 2013/0264 (COD)
PSP	Payment Service Provider
PWD	Password
QR	Quick Response
ROSI	Return of Security Investment
RSA	Rivest, Shamir y Adleman
SE	Secure Element
SecuRePay	Secure Retail Payments
SMS	Short Message Service
SP	Service Provider
SQL	Structure Query Language
STORK	Secure *IdenTity* AcroSs BoRders LinKed project+B27
TAN	Transaction Authentication Number
TP	Third-party service provider
UK	United Kingdom
URL	Uniform Resource Locator
USB	Universal Serial Bus
USD	United States Dollar
WG	Working Group
WP	Work Programme
WPK	Work Package

11 Annex II: Survey questions

The following screenshots show both parts of the survey Part I authentication mechanisms and Part II context authentication mechanisms for which participants were asked to provide their input. Additional questions were available, once an authentication mechanisms had been selected

11.1 Authentication mechanisms

The participant is asked to select all of the authentication mechanisms that are used, as shown in the figure below. There is also a help page, containing most of the information of this document, in case more information about these authentication mechanisms is need

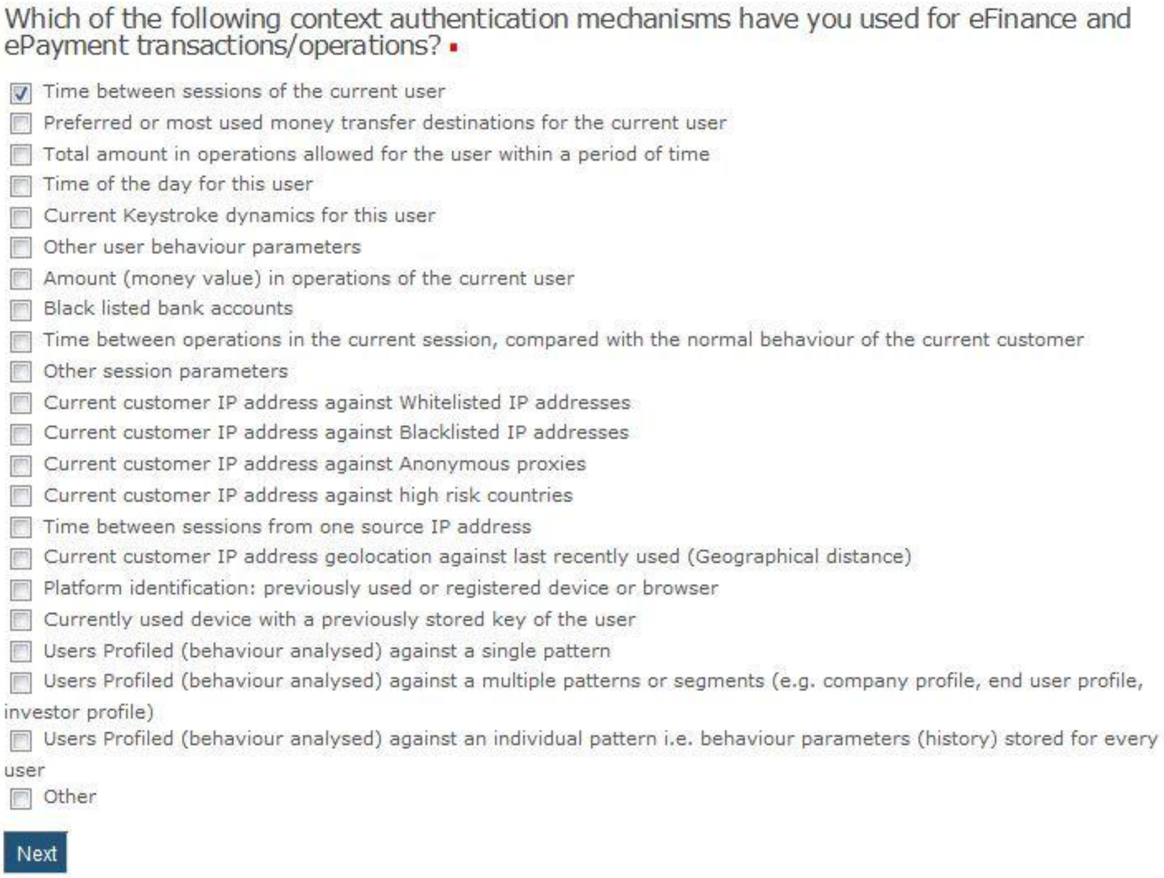


Which of the following transparent authentication mechanisms have you used for your eFinance and ePayment transactions/operations? ▪

- ☑ Username/Password
- □ Virtual Keyboard
- □ Partial Password
- □ Keystroke dynamics
- □ Handwritten Signature
- □ Fingerprint recognition
- □ Voice recognition
- □ Facial recognition
- □ Hand geometry recognition
- □ TAN code list or coordinates card
- □ SMS-based OTP
- □ Time-based Hardware Token OTP
- □ Challenge/response Hardware Token OTP
- □ Mobile OTP App (Token)
- □ QR code OTP
- □ Computer Stored Key - eSignature
- □ Token (USB, memory card) - eSignature
- □ Chip card (e-Identity card) - eSignature
- □ Mobile phone - eSignature
- □ Device Registration
- □ Mobile eBanking Application
- □ Other

Figure 14: Transparent Authentication mechanisms

In the second part of the survey addressed to professionals, the participant is asked to select all of the additional context authentication mechanisms that are used (see figure below). There is also a help page for this second part of the survey.



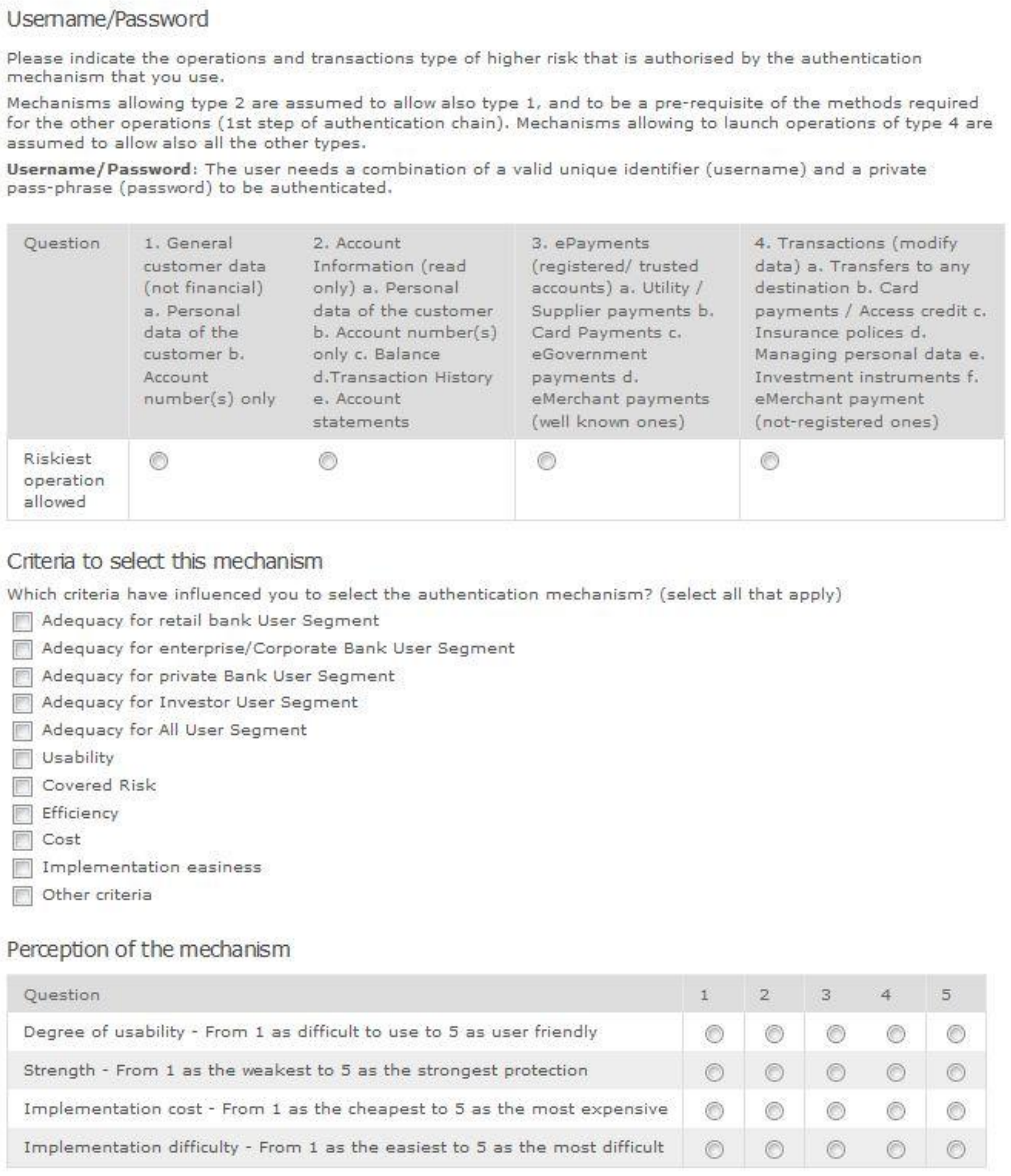
Which of the following context authentication mechanisms have you used for eFinance and ePayment transactions/operations? ▪

☑ Time between sessions of the current user
□ Preferred or most used money transfer destinations for the current user
□ Total amount in operations allowed for the user within a period of time
□ Time of the day for this user
□ Current Keystroke dynamics for this user
□ Other user behaviour parameters
□ Amount (money value) in operations of the current user
□ Black listed bank accounts
□ Time between operations in the current session, compared with the normal behaviour of the current customer
□ Other session parameters
□ Current customer IP address against Whitelisted IP addresses
□ Current customer IP address against Blacklisted IP addresses
□ Current customer IP address against Anonymous proxies
□ Current customer IP address against high risk countries
□ Time between sessions from one source IP address
□ Current customer IP address geolocation against last recently used (Geographical distance)
□ Platform identification: previously used or registered device or browser
□ Currently used device with a previously stored key of the user
□ Users Profiled (behaviour analysed) against a single pattern
□ Users Profiled (behaviour analysed) against a multiple patterns or segments (e.g. company profile, end user profile, investor profile)
□ Users Profiled (behaviour analysed) against an individual pattern i.e. behaviour parameters (history) stored for every user
□ Other

Figure 15: Context authentication mechanisms

11.2 Questions for each authentication mechanism

Professionals are asked to reply the following set of questions for every of both Transparent and Context authentication mechanisms selected in the introductory question. The following figures show those questions, as well as some instructions to reply them.



Username/Password

Please indicate the operations and transactions type of higher risk that is authorised by the authentication mechanism that you use.

Mechanisms allowing type 2 are assumed to allow also type 1, and to be a pre-requisite of the methods required for the other operations (1st step of authentication chain). Mechanisms allowing to launch operations of type 4 are assumed to allow also all the other types.

Username/Password: The user needs a combination of a valid unique identifier (username) and a private pass-phrase (password) to be authenticated.

Question	1. General customer data (not financial) a. Personal data of the customer b. Account number(s) only	2. Account Information (read only) a. Personal data of the customer b. Account number(s) only c. Balance d.Transaction History e. Account statements	3. ePayments (registered/ trusted accounts) a. Utility / Supplier payments b. Card Payments c. eGovernment payments d. eMerchant payments (well known ones)	4. Transactions (modify data) a. Transfers to any destination b. Card payments / Access credit c. Insurance polices d. Managing personal data e. Investment instruments f. eMerchant payment (not-registered ones)
Riskiest operation allowed	○	○	○	○

Criteria to select this mechanism

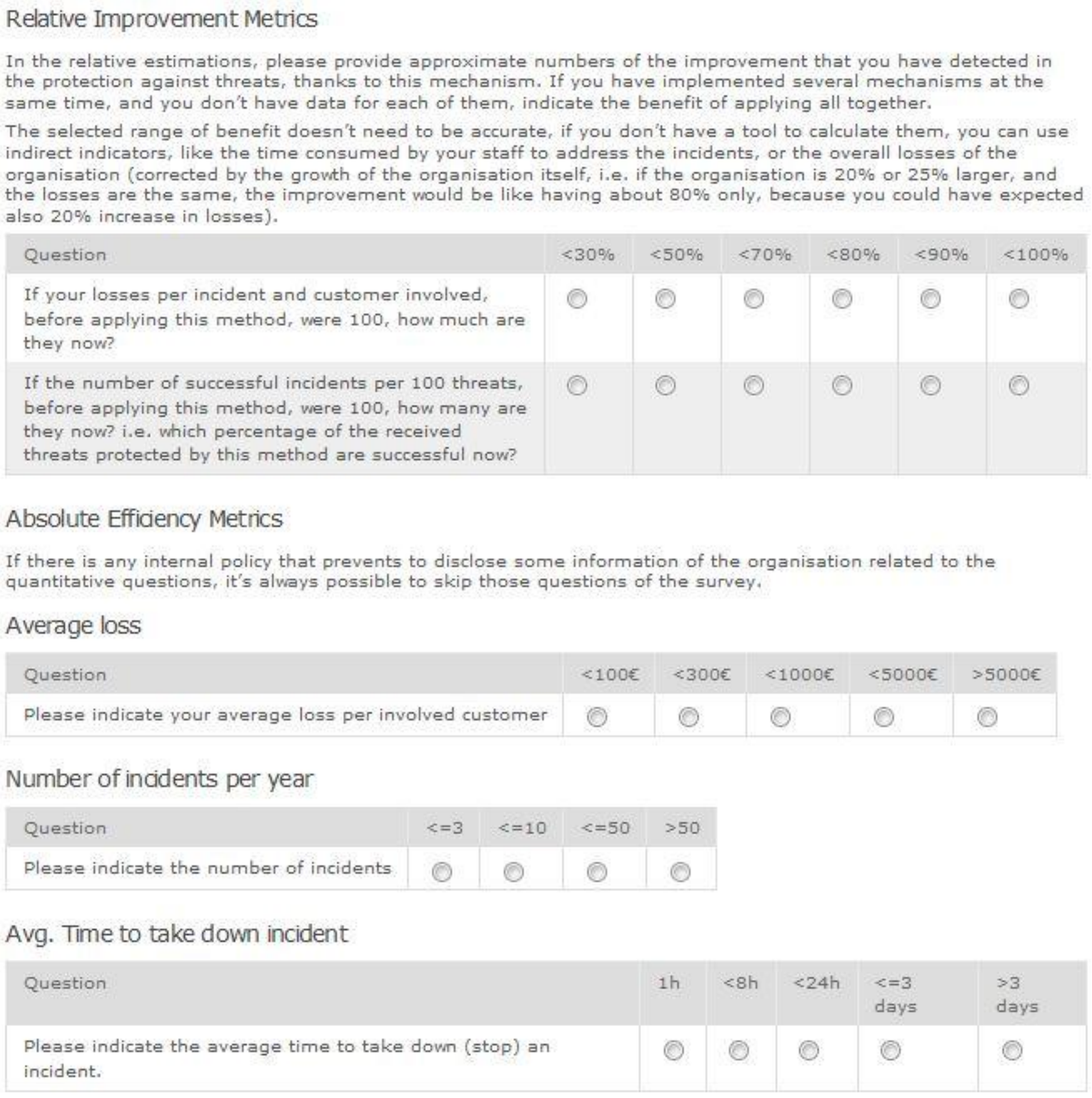
Which criteria have influenced you to select the authentication mechanism? (select all that apply)

□ Adequacy for retail bank User Segment
□ Adequacy for enterprise/Corporate Bank User Segment
□ Adequacy for private Bank User Segment
□ Adequacy for Investor User Segment
□ Adequacy for All User Segment
□ Usability
□ Covered Risk
□ Efficiency
□ Cost
□ Implementation easiness
□ Other criteria

Perception of the mechanism

Question	1	2	3	4	5
Degree of usability - From 1 as difficult to use to 5 as user friendly	○	○	○	○	○
Strength - From 1 as the weakest to 5 as the strongest protection	○	○	○	○	○
Implementation cost - From 1 as the cheapest to 5 as the most expensive	○	○	○	○	○
Implementation difficulty - From 1 as the easiest to 5 as the most difficult	○	○	○	○	○

Figure 16: First part of the questions asked for each selected authentication mechanism.



Relative Improvement Metrics

In the relative estimations, please provide approximate numbers of the improvement that you have detected in the protection against threats, thanks to this mechanism. If you have implemented several mechanisms at the same time, and you don't have data for each of them, indicate the benefit of applying all together.

The selected range of benefit doesn't need to be accurate, if you don't have a tool to calculate them, you can use indirect indicators, like the time consumed by your staff to address the incidents, or the overall losses of the organisation (corrected by the growth of the organisation itself, i.e. if the organisation is 20% or 25% larger, and the losses are the same, the improvement would be like having about 80% only, because you could have expected also 20% increase in losses).

Question	<30%	<50%	<70%	<80%	<90%	<100%
If your losses per incident and customer involved, before applying this method, were 100, how much are they now?	○	○	○	○	○	○
If the number of successful incidents per 100 threats, before applying this method, were 100, how many are they now? i.e. which percentage of the received threats protected by this method are successful now?	○	○	○	○	○	○

Absolute Efficiency Metrics

If there is any internal policy that prevents to disclose some information of the organisation related to the quantitative questions, it's always possible to skip those questions of the survey.

Average loss

Question	<100€	<300€	<1000€	<5000€	>5000€
Please indicate your average loss per involved customer	○	○	○	○	○

Number of incidents per year

Question	<=3	<=10	<=50	>50
Please indicate the number of incidents	○	○	○	○

Avg. Time to take down incident

Question	1h	<8h	<24h	<=3 days	>3 days
Please indicate the average time to take down (stop) an incident.	○	○	○	○	○

Figure 17: Second part of the questions asked for each selected authentication mechanism.

Catalogue Number: TP-04-13-115-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN 978-92-9204-077-2
9 789292 040772
doi: 10.2824/27272

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu