Privacy and Security Risks when Authenticating on the Internet with European eID Cards

enisa
European Network and Information Security Agency

www.enisa.europa.eu

V1.0.1 | Date: 2009-11-26

ENISA position papers represent expert opinion on important NIS topics. They are produced by a group selected for their expertise in a particular area. The content of this paper was discussed from April to October 2009 via e-mails and through personal communications. It was edited by ENISA and the final version has been reviewed by the persons listed below.

Editor:

Ingo Naumann, European Network and Information Security Agency (ENISA), EU
E-Mail: eid@enisa.europa.eu

Contributors:

Herbert Leitold, Zentrum für sichere Informationstechnologie (A-SIT), Austria
John Velissarios, Accenture, UK
Jens Bender, Federal Office for Information Security (BSI), Germany
Gregory Henwood, Home Office, UK
Andre Vasconcelos, Agency for Public Services Reform, Portugal
Giles Hogben, European Network and Information Security Agency (ENISA), EU
Jaan Priisalu, Swedbank, Estonia
Marc Stern, Approach Belgium, Belgium
Henning Daum, Giesecke & Devrient, Germany
Lorenzo Gaston, Gemalto, France
Arie Schilp, Rabobank, the Netherlands
Frank Zimmermann, Hewlett-Packard, Switzerland
Raul Sanchez-Reillo, Universidad Carlos III de Madrid, Spain

Contents

Introduction

Whenever we use internet services, the first steps we take are usually identification (we input our names) and authentication (we prove that it is us). How we actually identify and authenticate ourselves depends on the security level of the application. The means used can vary from a simple combination of username and password, through a secret PIN, to a PIN generated by some external device or a smart card using cryptography.

Smart cards are being used increasingly for authentication purposes. Many European identity cards now contain a smart-card chip, equipped with functionalities for online authentication [1]. They are usually called 'electronic identity cards' (eID cards). This report focuses on authentication using smart cards and compares this approach with other common means of authentication.

The requirements for differing online applications exhibit a wide variety; whereas for some services a high level of security is required, in other areas the protection of the card holder's privacy is the first priority. The main purpose of this paper is to help define a comprehensive list of requirements for national ID cards in order to ensure that they are as flexible and as multi-purpose as possible.

In the last section of this report we will draw several conclusions which were reached with the help of a thorough risk assessment of smart-card based authentication on the basis of two use-cases: *online banking* and *social networking*[1]. We will define the assets for these two use-cases, identify the vulnerabilities, and derive threats and risks in order to draw conclusions. This risk assessment will follow the methodologies of the ENISA 'Emerging and Future Risk' (EFR) Framework.

The main conclusions of our discussion are:

- Electronic identity cards offer secure, reliable electronic authentication to internet services

and

- a *privacy-protecting universally applicable eID card* is technologically feasible.

---

[1] *Please note that the goal of this report is not to promote the use of electronic identity cards (eID cards) for online banking or social networking but rather to report on on-going discussions on this issue within the technical community. In some EU countries, national ID cards are in their infancy and are currently being introduced and the likelihood that reliance on them for online banking, or even social networking, will be a reality in the short-term is limited.*

1 Use-cases and applications

Bearing in mind the desired outcome of this report - defining requirements for electronic national ID cards - it seemed practical to choose two use-cases that are very different in terms of:

- privacy requirements
- security levels
- their existence in combination with smart cards.

The use-cases 'online banking' and 'social networking' differ significantly in all these respects and therefore qualify as representative examples. Please note that we will not go further into the details of how to introduce the use of ID cards for certain scenarios[2].

1.1 Use-case 1: Online banking

Online banking has become one of the most widely-used electronic services by European consumers. It is a strategic service for financial institutions and users find it extremely convenient because it offers service availability 24 hours a day, usually without any extra costs; indeed online banking may even offer reduced costs compared to traditional banking processes. It is therefore now widely accepted by users and for this reason a very large number of banks are offering their clients the advantages of online banking.

However, online banking fraud is also on the rise [17][19]. Thus, for online banking applications, privacy is usually of lesser importance, whereas security is a major concern. For this reason, some banks deploy smart-card based solutions for online banking but several other mechanisms are also in use (see chapter 2.1 Authentication and out-of-band mechanisms).

It is very important to distinguish between two different kinds of use-cases: a) enrolment of a new client (eg, opening a bank account), and b) when an existing client carries out a transaction (eg, transferring money or obtaining an account statement). The main difference is that in the latter case, which is much more wide-spread, the customer

[2] *Since national ID cards are typically introduced over a period of five or ten years, the establishment of commercial and governmental use-cases might be facilitated (a) either by looking at a closed user group that gets an eID over the same or a shorter time period, eg, everybody reaching the age of 16 or 18, or (b) by supporting two means of equally strong authentication in parallel (a legacy method for everyone without electronic ID cards and the owners of new eIDs as they receive them over a period of five or ten years).*

already has bank credentials which may have been issued after face-to-face verification of a traditional, government-issued ID card or passport. The government-issued document is not required after enrolment, the use of a bank-issued card (or other credentials) being sufficient.

We derive the enrolment case from traditional office-based banking. This facilitates the transition from traditional to electronic procedures for the bank ('integration complexity') as well as for the user ('user experience').

Therefore, we describe first the traditional procedure:

Traditional procedure - Opening a bank account (enrolment)

Actors:

Customer, Bank

Scenario:

- The customer enters the bank office and thereby identifies the bank.
- The customer identifies himself to the bank, usually using an ID card or a passport. If necessary, the bank files a photocopy of the ID card and requests a handwritten signature which may be compared with the signature on the ID card[3] and is usually stored in the files of the bank for future reference.
- After the customer has identified himself, the bank might check the financial standing of the customer. The customer can then be linked to one or more account numbers.
- The customer and the bank negotiate a transaction (eg, opening an account or obtaining a loan).
- The customer and (conditionally) the bank clerk sign the transaction.
- The customer receives his or her bank credentials (eg, card, passwords) at a later time.

[3] *In the UK there is a heavy reliance on the names and addresses on the electoral roll as a means of identity or authentication for the enrolment process.*

From this description of the traditional procedure we can arrive at the following electronic procedure:

Use-Case 1A - Opening a bank account (enrolment)

Actors:

Customer, Bank

Scenario:

- The customer navigates to the bank's website (SSL connection) and verifies the bank's certificate (eg, the customer makes sure that the browser indicates a secure session (green URL bar)).
- The customer connects the eID card with the PC (or the PC is already connected to the card); please note that this eID card is unknown to the bank.
- The customer types in the PIN of the card in order to allow access to the data and the authentication functionality on it.
- The customer logs into the bank's website and the server initiates a user session.
- The customer identifies him or herself on the bank's website: name, address, date of birth (which could also be done by reading the respective data from the card).
- The server verifies the trustworthiness of the customer's card[4]; the ID card must contain a certificate signed by a certification authority (CA) known to the bank (eg, a government CA) and be able to authenticate all information required by the bank to open a bank account.
- The customer follows instructions in order to open a bank account[5].
- The customer electronically approves or authorises a transaction[6] or a contract with the bank.
- The customer receives his or her bank credentials (eg, username, passwords).
- The customer logs off.

This use-case might become an important driver for the use of national eID cards in the

[4] The identification of the customer is often covered by money-laundering or similar laws and therefore has to meet regulatory conditions on strength, etc.

[5] If a copy of a handwritten signature needs to be stored in the bank's files, an additional process needs to be defined as to how this can be transferred to the bank and verified by the customer as a valid template.

[6] Note that 'approving or authorising' a transaction does not necessarily require a qualified electronic signature (QES); the service provider might as well accept a weaker mechanism.

banking sector. Banks which do most of their business online rely on an identification agent (eg, post officials in Austria, Germany and Switzerland [39]) to do the initial identification at registration. A national eID card would open opportunities to eliminate the agent from the process and therefore facilitate online banking. For the customer the advantage is obvious: besides not having to carry two different cards, the customer would not have to appear in person at any office in order to open a new business relationship with a bank[7].

There is significant interest from banks in enabling citizens of one European country to open accounts with banks in other European countries. Of course, this entails the issue of the cross-border interoperability of eID cards, electronic signatures and procedures. As cross-country interoperability is a general problem when it comes to eID cards we will not deal with it in this paper. More details can be found in [8].

A more well-known online-banking use-case, transferring money from an already existing account to another person's account, is described below:

Use-Case 1B - Transferring money from a bank account

Actors:

Customer, Bank

Scenario:

- The customer navigates to the bank's website and verifies the bank's certificate (eg, the customer makes sure that the browser indicates a secure session (green URL bar)).
- The customer connects the eID card (or banking card) with the PC (or the PC is already connected to the card); the bank knows the client and his or her eID card (or bank card).
- The customer types in the PIN of the card in order to allow access to the data and authentication functionality on it.
- The customer logs in to the bank's website; the server authenticates the customer's card and initiates a user session.
- The customer performs a transaction (or several) as part of this user session[8].
- The customer logs off.

[7] In some countries legislation also allows combinations of the two approaches. For example, the user enters the website and decides to become a customer. Then he or she fills in an electronic form with all the information required, and the bank generates the documents to be signed by the customer's hand and sent to the bank together with a photocopy of an ID card or passport. Once the bank has received the documents it verifies their authenticity and the enrolment has been completed.

[8] If a bank requires an (advanced or qualified) electronic signature and if the national eID carries an electronic signature, even electronically signed transactions can be implemented.

1.2 Use-case 2: Social networking (and other web services)

Social networks qualify as mainstream identity management (IDM) applications. However until recently there was a big difference between the openness of the architecture of social networks and state-of-the-art IDM systems.

Keeping personal data in one central location under the control of one large corporate provider tends to alienate users who, understandably, perceive such systems as 'Big Brotherish' [11]. Users do not necessarily want to and should not be forced to use their real identity in a social networking site.

Recent incidents on social networking sites have highlighted the need for stricter control and raised awareness of privacy issues. Therefore, the need for a privacy-friendly authentication method is much higher in social networking than is the case in online banking, whilst security requirements in social networking are much lower.

The use of ID-card based authentication, however, might bring some advantages:

- **Anonymous age verification:** users may prove that they are of a certain age (eg, older than 18), provided this form of authentication is supported by the eID scheme, without disclosing their names or even their exact dates of birth. Support by the eID scheme could also make other forms of **anonymous attribute verification** possible, such as whether a person is female or male, a youth, or from a particular region, which would allow the formation of closed female / male / young / local user groups.
- **Anonymous revocation of access:** some service providers might wish to exclude a particular person from a service but without necessarily knowing who that person actually is. For example, a social networking site might require *all users* to log in using a government-issued electronic identity card. During the login procedure only the card would be identified[9], and the user could still decide which personal data he wants to disclose. Should the service provider want, at some point in time, to exclude someone from the service (eg, because of misbehaviour or unpaid bills[10]), he could just revoke the access rights for that person's card.
- **Pseudonymous authentication:** physical tokens can also offer support for pseudonymous authentication, ie, where the user does not log in using their real name but instead uses a pseudonym. Where a service provider wants to exclude multiple virtual instances of the same person, individual smart cards could offer unique, but nevertheless domain-specific or service provider-specific, identifiers. A necessary condition would be that the user cannot easily obtain and use two or more of these cards.

---

[9] *Strictly speaking, it is only necessary that the card proves to the service provider that the card owner has the necessary access rights and that they have not been revoked.*

[10] *This would, of course, entail the need for some kind of pseudonymous payment mechanism which goes beyond the scope of this paper. In any case, a pseudonymous payment scheme does not necessarily have to be based on eID cards or the authentication method used for the service.*

For social networking applications and virtual worlds, the use of electronic ID cards is clearly an emerging technology and plays the role of a rather academic example.

Electronic ID cards are not yet being applied in these contexts. However, there are many discussions on this subject within developer communities [3][7].

The fact that usually *all* users of the web service would have to log in using an eID card, in order to fulfil the requirements of the system, is considered to be the main obstacle to successful uptake and makes it a very difficult business case to justify. However, age-verification or pseudonymous authentication may be required in future social networks or virtual worlds and smart-card based authentication could offer the required mechanisms.

The procedure of smart-card based authentication to a social networking site could look like the following:

Use-Case 2 - Social Networking Site

Actors:

Customer, Service Provider

Scenario:

- The customer navigates to the service provider's website.
- The customer connects the eID card with the PC (or the PC is already connected to the card).
- Optional: the customer types in the PIN of the card in order to allow access to the data on it.
- The customer logs in to his or her personal page; service provider checks access rights of customer and revocation lists (different mechanisms possible); for the user this is a single sign-on action if the card is permanently connected to the computer[11].
- The customer performs actions such as blog entries, photo upload, and messaging.
- The customer logs off.

The optional step 'customer types in the PIN of the card' might constitute a problem for a universal card specification. On the one hand, gaining access using an identity card which contains personal information that can be used for online banking should be restricted with a mechanism such as a PIN; on the other hand, for an application such as social networking, an additional step, typing in an additional number (which you often forget), might be a big obstacle for the take-up of this technology.

[11] *This is probably not feasible if the smart card is a national eID card.*

Compromises, such as protecting only certain data or functionalities with a PIN and leaving other parts 'open', are possible. Or, more restrictively, certain data or functionalities on the card could be protected with a PIN *and* a certificate-based access control[12], while other parts are protected with only a certificate-based access control. In both these cases, the service provider is required to possess a certificate which is signed by a certification authority (CA) and accepted by the card. Therefore everybody who has access to the data is identified and (at least implicitly) authorised.

However, developing complex access policies usually entails long discussions among different stakeholders, in particular between service providers and data protection authorities.

[12] *Card-verifiable certificates (CV certificates) [12], not X.509 certificates.*

2 Technology overview

This chapter provides a brief overview of the technologies we will consider for risk assessment as well as some additional remarks that are important for our purpose. The intention, of course, is not to describe them in detail but rather to provide a list of references.

2.1 Authentication and out-of-band mechanisms

Authentication mechanisms can be as simple as a password a user has to type when logging in to a website or as complex as cryptography-based authentication using a hardware token.

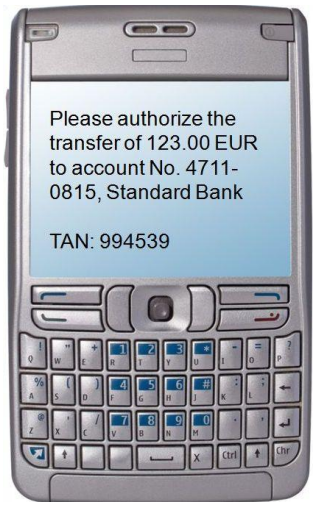

Figure 1: Transaction-based TAN on mobile device

Out–of–band mechanisms generally refer to additional actions taken beyond the technology boundaries of a typical transaction; eg, in an online banking scenario, these would be any actions taken outside the browser-bank server connection.

The following authentication technologies (ATs) will be addressed:

AT1. Password, PIN (typed in or using drop-down menus).

AT2. One-time passwords (OTPs), such as transaction authentication numbers (TANs), valid for one transaction or all transactions in one session (paper list); after being released (typed in), TANs are only valid for a short period of time (a few minutes).

AT3. iTAN ('indexed TAN', paper list); the server requests one particular TAN from a numbered list [2]. In this case, the knowledge of a single TAN is not sufficient for authentication; the claimant (or the attacker) must have access to the entire TAN list[13].

AT4. mTAN: ('mobile TAN'): TAN sent to a mobile device (or, less frequently used, to an e-mail account).

AT5. Transaction-based TAN/OTP: a mobile TAN that is communicated to the user together with information about the transaction for which it will be used (see example in

AT6. Figure 1). If the user refuses the TAN when the information about the transaction is incorrect, this mechanism can prevent attacks where the user's computer is comprised (and the mobile device is not). Note that there is a privacy

[13] *Or at least to a relevant portion of it. If an attacker phishes 10% of the list (about 10 TANs – not completely unreasonable) he can fake a transaction with 10% probability which poses a reasonable threat.*

threat in this concept: transaction details are sent via the out-of-band channel. In order to mitigate this threat, it is possible to send just partial information (eg, the first four digits of the account number) or encrypt the communication. The latter might be necessary anyway in order to mitigate the threat that an attacker simply transfers the victim's phone number onto another phone, as recently happened in Australia [21].

AT7. Impersonal cryptographic token [30]: in a nutshell, the service provider requests an impersonal token which has a serial number but which anyone can buy in a local shop. The impersonal token requests the server to authenticate. This prevents man-in-the-middle (MITM) scenarios because the victim's token would not establish a connection to the attacker.

AT8. Independent counters, timers, one-time-password generators, and hand-held pass-code generators [25].

AT9. Personalized cryptographic tokens or smart cards, with contactless or contact interfaces; these require an additional reader for the user's PC; PIN codes might be typed in using a keypad on the reader (if available).

AT10. SSL connection to banking server (using trusted server certificates verified by the user), plus probably additional end-to-end encryption into the database[14]; note that we refer here to only one element of the authentication process (the SSL connection).

AT11. SSL connection (using trusted server and client certificates), plus probably additional end-to-end encryption into the database.

AT12. Call-back (voice) verification.

AT13. Biometric authentication, either in a centralized system or using distributed storage via personal tokens[15].

[14] *After a successful authentication, a secured (end-to-end) session context needs to be established – which is not provided by the rather stateless HTTP protocol. The main weakness, however, of SSL-certificates is the issuing procedure, which does not properly check the identity of the claimant.*

[15] *Biometric-based web authentication is a controversial topic. A general problem is that the user (or the attacker) sits alone at home, controls all devices and somehow would always be able to perfom a replay of biometric credentials. Even though usability and reliability might be increased there has not yet been a good solution to this weakness. One possibility to address this problem would be to impose certified, tamperproof sensors, which apart from the fact that they do not yet exist, would be very expensive. Therefore, we list this technology only for the sake of completeness but do not consider it further in the remainder of this paper.*

2.2 Privacy features of electronic ID cards

To address privacy requirements when using smart-card based authentication, a number of privacy features (PFs) have been defined (see [1]), including in particular:

PF1. **Access control mechanisms**: the card carries the data as plain text but the service provider or card reader can only access the data after successful authentication of the service provider and/or the cardholder (proof-of-possession and/or proof-of-knowledge). A successful authentication usually consists of proving knowledge of a PIN or possession of a private key. An authentication is called 'mutual' if the card authenticates to the service and at the same time the service proves its trustworthiness to the card, ie to the holder.

PF2. **Privacy-respecting use of unique identifiers (UIDs)**: unique identifiers are strings which allow applications to distinguish between individual citizens (citizen-specific UID) or their identity cards (card-specific UID). A card-specific UID changes when a new card is issued to the citizen. Identifiers have to be used very carefully in order to avoid risks to privacy. A well-designed UID scheme might offer more privacy than, for example, using a social security number or a combination of name and date of birth as the UID. In general, the more a UID is linkable to usage in other transactions (using the card or otherwise), the less privacy it offers. It is important to note that individual static data on the card, such as a public key or even an encrypted data block, has all the attributes of a UID if the data is unique.

PF3. **Domain-specific UIDs (or sector-specific UIDs or sector-specific personal identifiers)**: Different identifiers are used for different applications, domains or sectors, while the identifier is unique and static with one domain. The UIDs of other domains cannot be determined (eg, by access control). In this way domain-specific UIDs help to prevent the merging of databases. Domain-specific identifiers can be derived from (secret) identifiers held by a trusted central issuer.

PF4. **Selective Disclosure**: a commonly accepted privacy principle is that any data disclosed should be the minimum required for the stated purpose. This is an axiom of EU data protection laws. In order to respect this principle, the card should not disclose more information than has been approved by the user. For example, if the requesting application only requires the name of the card holder, the card should not give access to the user's address.

PF5. **Verify-only mode**: a special case of selective disclosure is verify-only mode where, instead of disclosing the actual value of a field, a yes-no answer is provided to satisfy a query; eg, whether age is greater than a certain value. In this case, the card should not return the user's date of birth but only the Boolean result of the query. Several other useful cases are conceivable, such as proving driving credentials or European citizenship.

PF6. **Pseudonymous authentication:** several techniques are described in the literature [1][7][12][16][25]. For example, a user might be able to use a handful of pseudonyms, a different one for each service. Revocation issues usually become more difficult when pseudonyms are allowed. If the user requests revocation but doesn't know the pseudonyms, there is a need for some kind of co-ordinating

entity. With regards to ID cards, there is another obstacle: it is quite difficult to convince citizens that the use of a government-issued ID card could be pseudonymous (or even anonymous).

PF7. **Secure communication between the card, the middleware and the server**: once data is released by the card, it is vulnerable to eavesdropping when it is in transit between the card and the middleware interfacing with the card and, further on down the chain, in transit between the middleware and the destination service. Therefore, in order to respect the privacy of the card holder, the data should be encrypted between these three entities, ideally in the form of an end-to-end encryption between card and (application or database) server.

2.3 Additional remarks

Digital signatures using smart cards

A *digital signature*[16] (or *electronic signature*) is a chunk of data which can be appended to any kind of message or contract, claiming that the signer has written the message or has approved (signed) the contract. The basic idea is that the signature can only be created by the signer but it can be verified by anyone.

For verification, the message or contract and the signer's public key (which might be stored in a public-key directory) is required; to sign the message or contract, the corresponding private key is required. Should the private key be compromised, all corresponding signatures become invalid[17].

In order to protect the private key (and also to prevent it being repudiated by the owner) it is often stored on a smart card because even inexpensive smart cards can have secure memories and cryptographic functionalities. It is very difficult, even for highly sophisticated and well-funded attackers using physical means, to retrieve the secret keys stored on a card.

The communication between a card and an application usually takes place via a card reader using either electrical contacts (as defined in ISO/IEC 7816) or a contactless radio frequency (RF) interface (ISO/IEC 14443 or other).

---

[16] *In some countries this term is used for a picture of the handwritten signature. We will not distunguish between digital and electronic signature in this report.*

[17] *If a trusted time-stamping service is used and the time when the key was compromised is known, all signatures from before that time may still remain valid.*

EMV

The EMV (Europay, MasterCard and Visa) specification addresses interoperability issues between smart cards and terminals equipped with readers that enable debit card and credit card transactions. EMV at its simplest is a replacement for the traditional magnetic strip card.

EMV provides card authentication, cardholder verification and transaction certification.

It comes in three different versions

- Static Data Authentication (SDA) where the card contains some 'static' data signed by the card issuer (the CA of the payment scheme) which verifies the PIN;
- Dynamic Data Authentication (DDA) which amends SDA with authentication of the card using a private/public key pair; and
- Combined Data Authentication (CDA).

The CDA specifications address the security risks of the earlier versions [28], but it has not yet been widely deployed.

Technical specifications also exist for online banking based on EMV. The Chip Authentication Program (CAP) specifies the use of EMV bank cards for authenticating users and transactions in online banking. Other names for CAP (used by MasterCard) are 3D-Secure and Dynamic Passcode Authentication (DPA, used by VISA).The EMV specifications are publicly available [22]. The CAP specifications are not public but have been partly re-engineered [20].

Challenges to be overcome: SSL connections and end-to-end security

After a successful strong authentication, a secure (end-to-end) connection needs to be established that is robust enough to work over the rather stateless HTTP protocol. The SSL protocol, including client and server authentication, can be used for this purpose.

However there are multiple software components along the session chain which is typically established between the smart card (via middleware, browser and internet) and the web server. An application server needs to provide assurance that the session context for every transaction performed on the database to which the authentication grants access will be secure.

Because of this complexity in end-to-end session handling, which increases the probability of flawed implementations, a multi-layered security concept is highly recommended. A situation that has to be avoided is one in which a user enters another user's session just because of dubious buffer overflows or similar software bugs. Controlling a smart card from the browser while maintaining end-to-end encryption is a challenging task.

For the client side, there are two common approaches:

- Using the smart card's certificate for client authentication in the SSL communication, or
- Signing transactions using the smart card, eg, using qualified electronic signatures.

In the first case, using SSL client certificates on the smart card, assurance of the client's identity is bound to the SSL connection, but this connection terminates at the web-server[18]. This is another reason why having user authentication bound to the SSL/TLS session is so important, not only from a client side - but also from the server side. If end-to-end session management needs to be assured, ie, into a customer database, it is highly recommended that a second layer of session handling, interlinked with the SSL/TLS session between the client's user credentials and the customer data base, be implemented.

Binding the authentication-channel and the SSL-channel is not easy, technically speaking, but it is feasible and is widely applied by several online banks. Solutions include the use of signed applets and specific middleware. These are, however, usually developed specifically for a certain application or eID card. The lack of standards for smart card integration to browser hinders a broader take-up.

[18] *Approaches to bind the SSL session to upper layer protocols and thus the application exist, such as RFC5056 'On the Use of Channel Bindings to Secure Channels'.*

3 Risk assessment

3.1 Definitions

In an information technology context, assets are the targets to be protected in a risk analysis [1]. The *assets of an organization* are 'anything that has value to the organization'; the term *vulnerability* is applied to a weakness in a system which allows an attacker to violate the integrity of that system; and we define a *threat* as 'the potential cause of an incident that may result in harm to a system or organization'.

According to these definitions, a *risk* is 'the potential that a given threat will exploit the vulnerabilities of an asset or group of assets and thereby cause harm to the organization'. It is measured in terms of a combination of the probability of an event and its consequences [13].

3.2 Scenarios

For the purposes of risk analysis we will consider all kinds of authentication on the internet using smart cards. When we evaluate the risks, we will take into account the two specific use-cases, online banking and social networking.

3.3 Assets

Assets are the targets for protection in a risk analysis. In order to facilitate discussion, we can make a distinction between primary and secondary assets.

Primary assets are:

- **Money,** of the card holder, of a relying party, or corporate income
- **Personal data,** the 'electronic identity'
- **Reputation,** of the relying party or the card holder[19] – **Customer trust**
- **Intellectual property**
- **Privacy,** 'the right to be left alone'

[19] *This does not refer to reputation in the sense of social networks but in relation to all non-monetary assets. For example, the reputation of a bank may be harmed if someone breaks into my account without causing actual monetary harm.*

Secondary assets are everything that must be protected in order to enable the primary assets to be protected. They include:

- Knowledge: passwords, PINs, secret questions (and answers), secret keys
- Ownership: physical tokens (smart cards), TAN-lists
- Transitory secrets: session keys, transaction-dependent OTPs

3.4 Vulnerabilities

For the discussion, we categorize vulnerabilities (Vs) into distinct groups and, in some cases, give specific examples:

V1. **Flaws in smart card design** such as, for example:
   a. Flaws that allow an attacker (or the user) to obtain a secret key
   b. Flaws that allow an attacker to clone a card
   c. Flaws that allow an attacker (or the user) to change the data on the card
   d. Flaws that allow an attacker to obtain the secret PIN of a stolen or delegated card.

   These issues are outside the scope of this report. The interested reader is referred to [16] as a starting point.

V2. **Weak or flawed cryptography, flawed authentication protocols** (but not including weaknesses in the concepts of these protocols, see below (V4)), or **flawed implementation,** which results in compromised keys such as, for example:
   a. Key lengths that are too short or passwords that do not contain enough entropy
   b. Broken cryptographic algorithms
   c. Protocols that enable replay attacks[20] or that do not provide forward secrecy[21]
   d. Flawed implementation of these protocols.

   A wealth of scientific literature exists on these issues which are outside the scope of this report. The interested reader is referred to [16] as a starting point.

V3. **Vulnerabilities of the user's PC**; we will not classify in detail these vulnerabilities, but only list them according to their implications. These are vulnerabilities that enable:
   a. Trojans
   b. Illegitimate browser-plug-ins, downloaded from a website
   c. Software or process flaws which lead to the acceptance of illegitimate SSL certificates.

---

[20] *A form of attack in which a valid data transmission is recorded and maliciously repeated at a later time [16].*

[21] *The property that an ephemeral key derived from the communicating parties' public and private keys will not be compromised if one of the private keys is compromised in the future.*

V4. **Weaknesses in authentication *architecture and protocols* that enable certain attacks, such as:**

a. Lack of mutual authentication: if only the user is authenticated by the server, or only the server is authenticated by the user, this might result in a susceptibility to certain attacks, depending on the use-case.
b. Physical token not required for authentication: in general, if no physical token is required for authentication, one of the two factors, the 'something you have', is missing[22]. This should only be permitted in low-security applications.
c. Credentials do not expire: if credentials used for a transaction expire within a short period of time, eg, within a few minutes, an attacker is forced to perform the attack in real time.
d. Lack of out-of-band authentication in general
e. Lack of out-of-band authentication that contains information about the transaction (a sub-cased of d): in this case, out-of-band authentication exists but there is no direct link to the transaction in a way that would prevent the user from providing the credentials for a rogue transaction (see AT5).
f. Authentication transmits more (personal) data than required: the authentication itself should only assert the user's identity or eligibility for a certain service. It should not disclose additional personal information, such as date of birth or address. Even the use of a challenge-response protocol for authentication (basically the use of digital signatures for this purpose) can be considered an infringement of privacy because of hidden semantics in the challenge [1][12].
g. Passwords or other credentials are too short, do not have enough entropy or attempts are not throttled; sometimes there is a connection between password length and retry counters which also has to be considered.

V5. **Weaknesses of the infrastructure**; we will not describe these vulnerabilities in detail, but only classify them according to the attacks they enable. These are vulnerabilities that enable:

a. DNS spoofing or poisoning
b. Attacks targeting availability (eg, DDoS attacks).

V6. **User behaviour or lack of awareness**, for example:

a. User clicks on links contained in phishing mails and enters credentials.
b. User presses the 'ok' button when asked to accept an illegitimate certificate[23] (see also [32]).

---

[22] Three-factor authentication: something you know (eg, a password), something you have (eg, a smart card) and something you are (biometrics)

[23] This vulnerability could also be seen as a conceptual weakness: 'User can accept new certificates without browser update.'

c. User does not close the session and leaves the computer unprotected.
d. User gives the card (or other credential) to another user; this could be for a completely different purpose or in order to delegate a task and allow the other person to authenticate as the user.
e. User discloses credentials via telephone.
f. Usability is too complex and off-putting or is perceived to invade the user's privacy and so the stronger authentication option is not used[24].

V7. Card theft

We note that the vulnerabilities listed in V1 to V3 are usually unexpected flaws that emerge when systems are already in place. Category V4, on the other hand, contains conceptual vulnerabilities which, in many cases, are deliberately taken into account during the design phase. In the remainder of this report, we will focus on these items because proper risk assessment is particularly important for this group of vulnerabilities.

3.5 Threat agents

For our scenarios, we can identify the following threat agents (TAs):

TA1. **Malicious attacker**: an attacker who intercepts and manipulates the communication between the user and the service provider in order to carry out illegitimate financial transactions. In the worst case, this attacker belongs to a criminal organization, is highly motivated, has a lot of expertise and resources and runs large-scale attacks, eg, by using botnets, against a high number of users. There are many articles in the media that can confirm these assumptions (see, for example, [24]).

TA2. **Service provider**: with regard to infringements of privacy, the service provider itself is usually the threat agent. Personal information is collected and used for marketing or other purposes and sometimes sold. The databases of several providers may be merged in order to profile users and increase the value of the information.

TA3. **User**: in theory, even the user might attack the system by falsifying data or credentials stored on the card.

Insiders working for service providers are not considered relevant as threat agents for the types of threats considered in this report.

[24] *Or, they just do not use the service, which would fall into the category of business risks.*

3.6 Threats

We will apply a similar categorization to threats (Ts) as we did in the previous section to vulnerabilities. We will assign short names to all categories which will be used later when evaluating the risks.

For the sake of completeness, we will begin with (groups of) threats that directly relate to V1 and V2 and are not further discussed here.

T1. **(Short name: Card)** Attacks directed against a smart card (involves V1)
T2. **(Short name: Crypto)** Cryptographic attacks (involves V2)

These threats are interesting from an academic point of view but are not very relevant in practical terms.

Reverse-engineering smart cards can take a lot of time and money because the levels of physical tamper-resistance available from the best vendors have improved significantly over the last few years. It does, however, depend critically on the right choice of products and their use [16]. Certification schemes such as the Common Criteria standard (ISO/IEC 15408) may provide a certain degree of assurance about the processes of specification, implementation and evaluation of a product.

We will not consider these two threats in the remainder of this report.

We continue with some threats that are quite easy to mitigate (short names again given in parenthesis):

T3. **(Passwd)** Attacker can guess the password (or there is none) and just logs in and impersonates the user. Basically this is the weakest of all possible threats (and nowadays quite theoretical). It can be seen as a justification for having a password in a low-security system or, taking it one step further, as a justification for *strong* passwords.
T4. **(Keylog)** Attacker installs key-logger and sends credentials by mail (not real-time).

More relevant in practice are different types of man-in-the-middle attacks [15]. In the online banking scenario, for example, the man in the middle just lets a user type in his valid PIN (and TANs) but changes the amount and receiving account details for a transaction.

T5. **(MITM)** 'Regular' (not real-time) man-in-the-middle attacks executed in order to obtain private information or credentials (V6.a, V6.b)
T6. **(Real-time)** Real-Time man-in-the-middle attacks (V3.c,V6.a,V6.b,V4.e)
T7. **(Browser)** Real-time browser-in-the-middle attacks[25] [31] (V3.a, V3.b, V4.e)

Also very relevant and closely connected are so-called 'social engineering' attacks:

T8. **(Phishing)** Different kinds of 'phishing', where the user is requested by e-mail to connect to a rogue website and enter credentials; the rogue server then acts as a man-in-the-middle to the real banking site and uses the user's credentials (V6.a).
T9. **(Low-tech)** 'Low-tech attacks', eg, 'social engineering by telephone' (V6.e) [23]

From the perspective of privacy, there are other risks:

T10. **(Data greed)** Service provider obtains access to personal data on the physical token (other than as required).
T11. **(Merge)** Service provider and other companies merge their data bases and generate user profiles.
T12. **(Eve)** A third party intercepts personal information transmitted to the service provider (without being 'between' the communicating parties).
T13. **(Reputation)** In social networking, compromised and misused credentials of one user may have negative effects on other user's reputation.

There are some purely user-awareness related threats:

T14. **(Coffee break)** Attacker uses an open session in an unobserved computer in order to perform illicit actions.
T15. **(Delegation)** Attacker uses delegated credentials (password, hardware credential, PIN, TAN) to perform illicit actions[26] (V6.d).

At a higher level of abstraction, these threats all lead to three types of negative consequences:

---

[25] *Also called 'man-in-the-browser attacks'*

[26] *Obviously, if all credentials are given to the attacker then no security mechanism, other than biometrics, can mitigate the risks. The use of biometric information in online scenarios is, however, very limited due to a missing 'control agent' who can guarantee that the real user is voluntarily authenticating to the system.*

RT1. **Theft:** illegitimate money transfer from user's bank account[27]; unjustified charge to credit card
RT2. **Privacy Infringement:** disclosure of personal information, user profiling and subsequent misuses of these data
RT3. **Fraud:** cloning or forgery of government-issued ID card and subsequent misuse

Another term which is quite often used in this context is 'identity theft'. Identity theft is a disputed term, just as (electronic) identity itself has no universally accepted definition. We will therefore refrain from using it in the remainder of this paper but rather provide references to the specific threats we are addressing.

3.7 Risks

The assessment of risk level is expressed using two parameters: *probability* (of the threat, ie, the probability that the attack will occur) and *impact* (which the attack would have). To both parameters we assign five levels, represented by five different colours (further details and a very well-elaborated example can be found in [4]).

Please note that we are looking at the risks from a user perspective, ie, risks for the evaluation of the business case (eg, liability issues) or for society (eg, document fraud) are not considered.

Low	Low to Medium	Medium	Medium to High	High
1	2	3	4	5

Figure 2: Colour Scale "Probabilities/Impact"

Depending on the risk management methodology, a risk level can be derived from the probability and the impact in many different ways [5].

[27] *This opens the question of where the money actually is transferred to. Usually, online banking applications do not allow clients (and therefore not the attackers) to transfer money to countries where anonymous accounts are allowed or are easy to set up. Various mechanisms exist by which an attacker may launder this money [16] but they are outside the scope of this paper.*

A *security risk*, roughly speaking, is the potential that a given threat will exploit a system's vulnerabilities. It is measured by the impact multiplied by the probability of the threat [6]. Thus, we will use the following colour scale for the evaluation of risks:

Low	Low to Medium	Medium	Medium to High	High
1	4	9	16	25

Figure 3: Colour Scale "Risk"

The following table contains an evaluation of the threats in terms of probability and impact. The last column shows the corresponding risk level.

In assigning probabilities, we have assumed that state-of-the-art technology and, of course, smart-card based authentication are being used.

Threat	Probability	Impact	Risk Level (Scale from 1 to 25)
T1 Card	Low - Attacker has to get hold of the card (plus other credentials) and be able to crack it	High - Illegitimate money transfer (RT1)	5 - Low to Medium
T2 Crypto	Low - Practical attacks on cryptographic algorithms are very rarely feasible	High - Illegitimate money transfer (RT1)	5 - Low to Medium
T3 Passwd	Low - There are always proper mechanisms in place that prevent this threat	High - Illegitimate money transfer (RT1)	5 - Low to Medium
T4 Keylog	*Online banking*: Low to medium - credentials usually expire *Social networking*: Medium to high - a valid attack	*Online banking*: High - illegitimate money transfer (RT1) *Social networking*: Medium - possible impersonation	*Online banking:* 10 - Medium *Social networking:* 12 - Medium

T5 (T8)[28] MITM	*Online banking*: Low to Medium - credentials usually expire *Social networking*: Medium	*Online banking*: High - illegitimate money transfer (RT1) *Social networking*: Medium - possible impersonation	*Online banking:* 10 - Medium *Social networking:* 9 - Medium
T6 (T8) Real-time	*Online banking*: Medium *Social networking*: Low - too much effort for the attacker	*Online banking*: High - illegitimate money transfer (RT1) *Social Networking*: Medium - possible impersonation	*Online banking:* 15 - Medium to high *Social networking:* 3 - Low to medium
T7 (T8) Browser	*Online banking*: Medium *Social networking*: Low - too much effort for the attacker	*Online banking*: High - illegitimate money transfer (RT1) *Social networking*: Medium - possible impersonation	*Online banking:* 15 - Medium to high *Social Networking:* 3 - Low to medium

T9 Low-tech	*Online banking*: Medium *Social networking*: Low - too much effort for the attacker	*Online banking*: High - illegitimate money transfer (RT1) *Social networking*: Medium - possible impersonation	*Online banking:* 15 - Medium to high *Social networking:* 3 - Low to medium
T10 Data greed	*Online banking*: Low - service provider usually knows all data on the card or requires access in any case (except facial image, if	Low to Medium - privacy infringement (loss of some personal data)	*Online banking:* 2 - Low *Social networking:*

[28] *The relevant threat here is the man-in-the-middle attack (T5), which might be initiated via phishing (T8).*

	applicable) *Social networking*: Medium to high		8 - Medium
T11 Merge	Medium to high	Low to medium - privacy infringement (loss of some personal data)	8 - Medium
T12 Eve	*Online banking:* Low - communication is encrypted *Social networking:* Low - too much effort for the attacker	*Online banking*: High - illegitimate money transfer (RT1) *Social networking*: Medium - possible impersonation	*Online banking:* 5 - Low to medium *Social networking:* 3 - Low to medium
T13 Reputation	*Online banking:* Not applicable *Social networking:* High	Low to medium - implicit negative effect on reputation	*Online banking:* Not applicable *Social networking:* 10 - medium
T14 Coffee break	*Online banking:* Low - sessions close after a few minutes and users are usually aware *Social networking:* High	*Online banking*: High - illegitimate money transfer (RT1) *Social networking*: Medium - possible impersonation	*Online banking:* 5 - Low to medium *Social networking:* 15 - Medium to high
T15 Delegation	*Online banking:* Low - users are usually aware *Social networking:* Medium	*Online banking*: High - illegitimate money transfer (RT1) *Social networking*: Medium - possible impersonation	*Online banking:* 5 - Low to medium *Social networking:* 9 - Medium

As a general observation we note that all risk levels range between 'Low' and 'Medium to High', ie, there are no threats with high probability *and* high impact.

The use of smart cards in online banking systems is fairly safe and the infringement of personal information when using social networking sites is usually not considered to be critical. However, there are some security and privacy issues which need some attention.

We will derive requirements for the two use-cases in the following chapter and provide recommendations in the final part of this report. The recommendations and conclusions should be seen as the result of the discussions of the working group and not as being solely derived from the assessment of risk.

Even though the evaluation of threats, in particular the assignment of probabilities to the threats, is rather rough, performing a risk assessment in a standardised manner turned out to be very useful for this purpose.

4 Security requirements

A security requirement is a documented need of what a particular service should do about security issues. Security requirements are different from general requirements such as interoperability or usability, and they might even stand in contradiction to other requirements.

In this paper, the identification of security requirements should help us define general recommendations for the target audience of this paper. We will do so, using a classical engineering approach, in which sets of requirements are used as inputs during the design stages of product development.

From the risk analysis we can derive a list of security requirements for the two use-cases:

4.1 Online banking

Online banking needs to be secure. The protection of the user's personal information (from the point of view of the bank) is clearly only a secondary consideration. The main concern for the bank is that the user can be clearly identified and that another user cannot impersonate him or her. The security requirements for online banking include:

- secure authentication mechanism for bank users and/or for all citizens during login
- highly secure authentication mechanism for performing bank transactions
- optional: an electronic signature functionality (if required for certain transactions, eg, opening a bank account online)

The distinction between 'secure' and 'highly secure' is taken from real-world systems, where for reasons of convenience, the level of security during login is lower than for performing bank transactions. Many banks, for example, allow users to see their account statements after they type in their usernames and passwords, whereas the transfer of money to another account requires additional credentials, such as a one-time password or the value of an external counter. The 'highly secure' authentication mechanism requires:

- protection against man-in-the-middle-attacks
- protection against browser-in-the-middle-attacks.

4.2 Social networking, online forums and virtual worlds

The security requirements for social networking sites are completely different from the requirements for online banking. First of all, an authentication procedure that is convenient to use is important. In addition an authentication of the user is required while, at the same time, the user's privacy has to be protected. This leads to a dilemma.

A good description of this dilemma is given by David Birch in his article about a hypothetical ID card called 'Psychic ID' [18]. Birch describes a phenomenon which he calls the 'Chat-room Paradox':

Parents will only allow their children to use chat-rooms if they know that the other people in the chat-rooms are not criminals. In order to make sure of this, a validation against a criminal register is required. However, should somebody else in the chat-room want the children's names and address to check them against a register, the parents would not want to give it to them.

This is the paradox: the user wants full disclosure from everybody else who wants to be part of the sub-group but will refuse any kind of disclosure on their side.

Bearing this paradox in mind, we can derive some requirements for user authentication on social networking sites from the use-case scenario:

- Age verification (eg, under 18 / over 18) without disclosing additional personal information [3]; this could be broader; for example, not only age but nationality, address (area), membership or school affiliation could be verified in this way. This is particularly interesting for web services addressed to minors, as lurking risks are different to this category of users than to adults. For details, please refer to [9].
- Similar actions, eg, the verification of a user's real name without disclosing any additional personal information
- Various features of pseudonymous authentication, for example:
    - ability to block users without access to any user's personal information, eg, their real name
    - ability to edit blog comments entered 'anonymously'
- Pseudonymous payment
- Anonymous verification of reputation scores; this person is seen to have x, y, and z attributes by x, y, and z people.
- Non-existence of persistent proofs, ie, if an authentication has been performed, the service provider cannot provide proof about it to a third party; this implies that electronic signatures have to avoided, even in challenge-response protocols [1].

5 Addressing the requirements

In this chapter we will investigate existing technologies regarding the requirements we have identified.

Threats with regard to security:

The following table describes the suitability of the authentication technologies for mitigating the identified risks.

Mechanism→ Threat↓	AT1 PIN	AT2 TAN	AT3 iTAN	AT4 mTAN	AT5 tbTAN	AT7 Imp T	AT8 Timer	AT9 Card	AT10 SSL	AT11 SSL m.a.	AT12 Call-back
T3 Passwd	**X**	**X**	**X**	**X**	**X**		**X**	**X**		**X**	**X**
T4 Keylog		**X**	**X**	**X**	**X**		**X**	**X**		**X**	**X**
T5 (T8)[29] MITM			**X**	**X**	**X**	**X**	**X**	**X**	+	+	**X**
T6 (T8) Real-time					+	**X**		**X**	+	+	**X**
T7 (T8) Browser					+						
T9 Low-tech					+		**X**	**X**			+
T14 Coffee break		+	+	+	+		+	+			**X**

Legend: **X**: can prevent threat +: can mitigate threat tbTAN: Transaction-based TAN
Imp T.: Impersonal token
m.a.: Mutual authentication

Please note that the entries in the table only indicate whether a mechanism *can* prevent or mitigate a threat, ie, whether it has the *potential* to do so. Of course, this does not necessarily have to be the case if, for example, implementation is flawed.

The mitigation of man-in-the-middle (MITM) attacks requires, generally speaking, proper server authentication. In the worst case scenario, the MITM controls the user's browser (browser-in-the-middle attack) and its interface to the user which makes it impossible for the user to notice the attack should no additional security measures be applied.

[29] *The relevant threat here is the man-in-the-middle attack (T5), which might be initiated via phishing (T8).*

Threats with regard to privacy:

The following table describes the suitability of the privacy features for mitigating the identified privacy risks on the assumption that a hardware token is used for authentication.

Mechanism→ Threat↓	PF1 Access control	PF2 no UID	PF3 spec. UID	PF4 select	PF5 verify	PF6 pseudo	PF7/AT 10/AT11 SSL
T10 Data greed	**X**			**X**	**X**		
T11 Merge		**+**	**X**			**+**	
T12 Eve						**X**	**X**

Legend: **X**: can prevent threat +: can mitigate threat

Some of these technologies are already incorporated in existing European eID cards [1].

Remark *(Portugal)* Regarding online banking and other e-services, the Portuguese citizen card [36] provides certificates for user authentication and signature (online). Besides X509 certificates, the Portuguese citizen card chip has an EMV application for generating OTPs according to CAP specifications. Since bank cards also comply with the EMV norm, citizens can use the same reader for reading bank cards (issued by banks) and national ID cards (issued by the government).

Remark *(Austria)* The Austrian citizen card [34] is based on qualified electronic signatures and sector-specific (or domain-specific) identifiers derived from the central residents register. The scheme is open to both the public and private sectors. Thus, several banks have enabled the use of the citizen card for authentication to their online banking applications using qualified electronic signatures. Some of these banks allow accounts to be opened and for registration to take place without the need for a personal appearance, as the authentication and qualified signature functions provide sufficient assurance of identity.
Every bank card and several credit cards have been prepared for qualified electronic signatures and can be activated as an Austrian citizen card. Other citizen cards are the health insurance card and student service cards which can also be used for online banking once the citizen card option is offered by the bank.

Remark *(Estonia)* In Estonia, the national PKI infrastructure is based on the Estonian eID card and is operated by the company SK which is owned by two banks and two telecommunication services providers. A signature hardware device is implemented on the national ID card and on mobile phones. Several banks are involved in the issuing process of ID cards, and the mobile phone operator is issuing 'mobile IDs'. The Estonian

government owns the ID cards and governs the PKI framework.
The electronic signature is legally binding.
A citizen portal exists from where most available services can be accessed which increases their acceptance. However, many institutions are operating their own services which make use of eID cards. All government services are available online, except for the ID card issuance itself. Even elections have taken place over the internet. It is also possible to establish an Estonian company solely via the internet.
A degree of cross-border interoperability with the Finnish national eID card, the Belgian national eID card, the Portuguese national eID card and the Lithuanian 'Mobile ID' exists [37]. Estonian internet banks use the national PKI with both eID cards and mobile ID. The authentication function is used for the initiation of online sessions whereas the digital signature is used to for sustainable proofs of payment orders and contracts. Password cards and PIN calculators can also be used as means of authentication.
An Estonian company, OpenID.ee [29] enables national PKI certificate holders to federate authentication and also anonymise themselves for service providers.

Remark *(United Kingdom)* In the UK, the national ID card scheme is still in its infancy relative to other European states. Reliance on national ID cards for opening new accounts or transacting online has not been observed as of yet. Banks in the UK tend to own their own client relationships and seldom outsource this function and associated risk to third parties. In addition, the manner in which legislation enforces compliance with associated KYC and AML rules currently restricts the amount of non-paper based transactions (such as account opening) which can be performed exclusively online.

Remark *(Belgium)* Belgium has a national PKI owned by the government. Mandatory national eID cards [35] supporting this PKI are distributed to all citizens and will soon be distributed to foreign residents also (currently in the pilot phase). Electronic ID cards are used for authentication through a standard TLS authentication scheme or qualified signatures (two different keys). The card middleware is already included in some standard Linux distributions, as well as in Microsoft Windows updates. The most popular application is the on-line tax declaration which is currently used by several hundred thousand people.

Remark *(Germany)* The roll-out of the German eID card (elektronischer Personalausweis (ePA)) will start in November 2010. The design of the card itself, as well as the corresponding infrastructure, is nearly finalized.
The concept of the German eID card is based on the following main features:

- Card centric: for privacy reasons there is no central database of the data stored on the card. Furthermore all security mechanisms (such as access control or domain-specific UIDs) are based in the card itself.
- Mutual authentication: the authentication process using the eID card not only authenticates the owner of the card, but also the service provider. The proof of authenticity of the service provider is PKI-based, using 'access certificates', which not only identify the service provider but also define the maximum access rights of the provider to data on the card.
- Strong access control: accessing data stored on the card is only possible after entering the holder's secret PIN and authentication of the service provider. For every authentication the holder can precisely select which data are accessible to the service provider.

- Secure channel: part of the access control is the establishment of an encrypted and integrity-protected end-to-end channel between the card and the service provider.
- Verify-only and pseudonymous authentication: the card offers a mechanism for verify-only access (eg, age verification without disclosing the date of birth) as well as pseudonymous authentication.

Although the security mechanisms are based in the card itself, there are many other components to be considered. Examples are the middleware/reader, which has to provide the means to securely enter the secret PIN or to correctly display the access certificates of the service provider. A further essential part of the concept is the PKI used to certify the service providers.

Remark *(The Netherlands)* In the Netherlands the project 'PKI-overheid' has already been running for some considerable time. It offers reliable electronic communication with and within the Dutch government. At this moment however it is only in limited used within the government.
For reliable communication with the (local) government, citizens and companies can use DigiID. Identification and authorisation is based on an UID/password combination, with the addition of a one-time password delivered by SMS.
Banks are issuing EMV cards to their clients who can use them for internet banking. These cards can also be used as a strong authentication for generic applications.

Remark *(Norway)* In Norway, BankID is an electronic ID service that offers secure electronic identification and signatures on the internet. BankID has been developed and is maintained by the banks in Norway for use by private persons, authorities and other companies.

Remark *(Spain)* Spain has been issuing a compulsory national ID card, the Documento Nacional de Identidad (DNI), for decades. The cards are issued by the Ministry of Home Affairs, using national police facilities. The enrolment procedures are based on legal birth certificates and family relationships in order to capture all personal data. A government employee is present during enrolment.
Personal data collected during this process are name, date of birth, current address, parents' name, date of issue, date of expiry, document serial number, facial image, fingerprint information and an image of the holder’s handwritten signature. Each time the document is renewed, all biometric data are re-captured. If the citizen changes address, he or she has to provide legal proof of their new address and a new document is issued, following the same rules and free of charge.
The latest generation of the ID card is a smart card, the DNI electrónico (DNIe) [38], where the chip contains the following information:

- all personal data
- two electronic certificates for the citizen (one for authentication purposes and the other for signing documents)
- the public certificate of the issuer
- a photograph of the citizen, an image of the handwritten signature, and the ISO/IEC 19794-2 compact records with the minutiae of two fingerprints
- a PIN code for cardholder authentication, to enable access to personal data, user certificates and PKI functionalities to be granted.

Being the most known, accepted and relied upon means of identification, the Spanish

electronic DNI (DNIe) is being used to prove the identity not only at a physical level (eg, proving the identity of the credit card holder) but also at the electronic transaction level. Public administrations are supplying most of their services through the internet by using recognized certification schemes, the DNIe being one of them. Banks are also migrating their electronic banking systems to accept the DNIe as a mean to authenticate the customer and to sign electronic transactions.
Match-on-card technology using the fingerprint information is restricted to police services. Using this biometric authentication, the PIN can be changed (even if forgotten or blocked) and user certificates can be renewed.

6 Recommendations and conclusions

Because more and more internet applications that require some kind of authentication are gaining popularity, more standardized and harmonized approaches to user identification and authentication are needed. In Europe, several states have already rolled out electronic ID cards or have committed themselves to doing so and are in various stages of planning [1]. Most of these cards offer capabilities to electronically authenticate to an internet application. We expect that these technologies will, one way or another, be used for popular internet services such as online banking, tax declarations, even virtual worlds and gaming, and social networking.

In this report, we have analysed two fundamentally different use-cases in order to derive requirements for electronic ID cards which might serve as a universally applicable authentication token[30] for European citizens and internet users in the future. The underlying vision is that an electronic ID card should be easy to use and, from a business perspective, provide economies of scale, ie, offer cost advantages per unit as scale is increased.

The risk assessment process, as well as our discussions, have resulted in a set of recommendations and conclusions:

Conclusion *(Technical Feasibility)* The universally applicable eID card is technologically feasible. Requirements for online banking and internet applications such as social networking or virtual worlds could be combined using existing technologies. Proper procedures for lost cards will have to be defined, as the impact of a lost card depends on its universality.

Recommendation *(Reader Infrastructure)* It is advantageous for the business case if the reader infrastructure (including drivers and middleware) is largely rolled out in parallel or even before national eID cards are issued. Ideally, all new mobile and desktop devices would already be equipped with the required readers and software components, to allow immediate deployment and use of a national eID card without the need to install any additional software or hardware.

Recommendation *(Migration)* Since the roll-out of government documents usually takes many years, for certain web services there might be a need for a migration plan and the support of multiple means for secure authentication during this transition phase. Every citizen should be able to either receive an electronic ID card immediately or be enabled to employ another credential, which could be an industry-issued smart card, in order to use a web application.

---

[30] We refer to 'universally' here in terms of online authentication. Another question, though outside the scope of this paper, is whether the card contains other 'card applications' [26], such as a border control/ICAO application (Sweden, the Netherlands and planned in Germany [1]) or an ATM application (Portugal).

Electronic identity cards bring new opportunities to increase the security level of already existing internet applications. However, security and privacy issues which are important still remain to be considered. Mitigating these risks might, in some cases, require changes in legislation, eg, on privacy issues.

Recommendation *(Privacy Requirements)* European governments need to define privacy requirements for electronic identity cards. This is a particularly difficult task because the approaches to privacy in the Member States vary fundamentally and requirements vary between applications. Expert groups containing stakeholders from industry and academia and led by government representatives should produce specific guidelines to support legislative changes (eg, the adoption of domain-specific UIDs or a ban on entirely unprotected personal data on national eID cards).

Conclusion *(Revocation)* Sound revocation[31] mechanisms for ID cards and certificates are fundamental. In particular, when deploying new technologies, such as domain-specific UIDs or pseudonymous authentication, it is important 'to have revocation in mind' when designing the infrastructure. In the case of a universal eID card, revocation requires close co-operation between all institutions involved.

Recommendation *(Interoperability)* Cross-border interoperability of applications involving authentication (or 'electronic identity') is essential. Legal harmonisation as well as technical compatibility will be required in the near future. If new opportunities for cross-border services are to be enabled, a service provider in one country must be able to accept customers from another country on the basis that the electronic identity used for online transactions is effective and reliable. The continuous funding of European interoperability projects, such as STORK [40] and future activities (eg, ELSA), is necessary for a European-wide take-up of the new technologies.

Conclusion *(Privacy Concerns)* Under the assumption that the technology is applied in the right way, privacy concerns and the risk of identity theft are not necessarily higher in the case of a universally applicable eID card than in the case of several cards[32].

Conclusion *(Security of Banking Applications)* Electronic identity cards offer secure, reliable electronic authentication to internet services. In order to use national ID cards for banking purposes, co-operation between banks and governments is required and security requirements and guidelines have to be in place.

---

[31] Please note that, in the case of government-issued credentials, revocation is usually initiated by the cardholder due to a lost or stolen card or compromised credentials. In other cases, revocation might also be initiated by the card issuer.

[32] The consequences of card theft or lost cards are an open issue, if the card gives access to many services. A lost card, of course, increases the risk of identity theft. On the other hand, users will be more careful with the PIN codes of a universally applicable card than with a bunch of cards which are used for a number of services. Many people carry all their cards in a single wallet anyway.

Conclusion *(Opening a bank account online)* National electronic ID cards enable online opening of bank accounts. This may become an important application for national eID cards in the banking sector. Banks which do most of their business online rely on an identification agent to do the initial identification at registration. A national eID card would therefore open opportunities to eliminate the agent from the process and facilitate online banking.

Conclusion *(Liability)* Only through intensive co-operation could banks and national ID card producers solve the problem of liability, ideally under the guidance of appropriate government institutions. Most banks still rely on credentials they themselves issue to authenticate customers and do not rely on another institution or agency which would effectively own the risk for management of the credential.

Conclusion *(Social Networking)* The introduction of physical authentication tokens for social networking applications and virtual worlds remains highly speculative. There are clear advantages in doing so, in particular with respect to anonymous age-verification, but to impose the use of any kind of physical credential constitutes a major obstacle for the uptake of the solution.

Recommendation *(User Awareness)* Even the best security mechanisms do not help if the users do not follow certain procedures (such as not accepting rogue certificates when banking online) or completely lack 'security common sense' (eg, leaving a computer with an open session unprotected). The procedures should obviously be as simple as possible but a certain amount of user awareness will in any case be crucial and needs to be fostered. ENISA issues reports on IT security user awareness on a regular base [9].

7 References

[1] ENISA Position Paper: *Privacy Features of European eID Card Specifications*, February 2009, http://www.enisa.europa.eu/act/it/eid/eid-cards-en
[2] ENISA Position Paper: *Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID)*, November 2008, http://www.enisa.europa.eu/act/it/eid/mobile-eid
[3] ENISA Position Paper: *Virtual Worlds, Real Money*, November 2008, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_security_privacy_virtualworlds.pdf
[4] ENISA Report: *Being Diabetic in 2011, EFR Pilot, Identifying Emerging and Future Risks in Remote Health Monitoring and Treatment*, March 2009, http://www.enisa.europa.eu/media/press-releases/remote-health-monitoring-scenario ,
[5] *ENISA Inventory of Risk Management/Risk Assessment Methods and Tools,* http://www.enisa.europa.eu/act/rm/files/deliverables/inventory-of-risk-assessment-and-risk-management-methods
[6] ENISA in co-operation with Hilton, Jeremy; Burnap Pete; Tawileh, Anas: *Methods for the Identification of Emerging and Future Risks*, November 2007,
[7] ENISA Position Paper: *Security Issues and Recommendations for Online Social Networks*, http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks
[8] ENISA Report: *Report on the State of Pan-European eIDM Initiatives*, http://www.enisa.europa.eu/act/it/eid/eidm-report
[9] ENISA Report: *Children on Virtual Worlds*, http://www.enisa.europa.eu/act/ar/deliverables/2008/children-on-virtual-worlds
[10] ENISA: *Awareness Raising*, http://www.enisa.europa.eu/act/ar
[11] Hogben, Giles: *Security Issues in the Future of Social Networking*, http://www.w3.org/2008/09/msnws/papers/Future_of_SN_Giles_Hogben_ENISA.pdf
[12] Germany Federal Office for Information Security (BSI): *Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 2.01* https://www.bsi.bund.de/cae/servlet/contentblob/532066/publicationFile/27971/TR-03110_v201_pdf.pdf
[13] ISO/IEC 13335-1, Information technology — Security techniques — *Management of information and communications technology security, Part 1: Concepts and models for information and communications technology security management*, International Standard
[14] RFC 3631: *Security Mechanisms for the Internet*, http://www.rfc-editor.org/rfc/rfc3631.txt
[15] RFC 4949: *Internet Security Glossary*, Version 2, http://www.rfc-editor.org/rfc/rfc4949.txt
[16] Anderson, Ross: *Security Engineering*, Second Edition, 2008, Wiley Publishing, Inc., ISBN 978-0-470-06852-6
[17] BBC: *Big jump in online banking fraud*, 19 March 2009,

http://news.bbc.co.uk/2/hi/business/7952598.stm
[18] Birch, David G W: *Psychic ID A blueprint for a modern national identity scheme*, Identity in the Information Society, April 2009, Springer, ISSN 1876-0678, DOI 10.1007/s12394-009-0014-6, http://www.springerlink.com/content/hk1p8r133867x402/
[19] cnet: *Online banking is booming,* 16 June 2009, http://news.cnet.com/8301-1001_3-10265409-92.html
[20] Drimer, Saar; Murdoch, Steven J.; Anderson, Ross: *Optimised to Fail: Card Readers for Online Banking*, Computer Laboratory, University of Cambridge (UK), http://www.cl.cam.ac.uk/~sjm217/papers/fc09optimised.pdf
[21] Ducklin, Paul, *Elvis is alive, and is in the building!* , http://www.sophos.com/blogs/duck/g/2009/10/13/elvis-alive-building/ , blog entry, 13 Oct 2009, captured 14 Oct 2009
[22] EMVCo, http://www.emvco.com/
[23] Washington Post: Krebs, Brian: *High Crimes Using Low-Tech Attacks*, 7 July 2009, http://voices.washingtonpost.com/securityfix/2009/07/high_crimes_using_low-tech_att.html
[24] Washington Post: Krebs, Brian: *The Growing Threat to Business Banking Online*, 20 July 2009, http://voices.washingtonpost.com/securityfix/2009/07/the_pitfalls_of_business_banki.html
[25] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A.: *Handbook of Applied Cryptography*, CRC Press, ISBN 0-8493-8523-7
[26] Rankl, Wolfgang; Effing, Wolfgang: *Handbuch der Chipkarten*, Carl Hanser Verlag, ISBN: 3-446-22036-4; (English translation available: *Smart Card Handbook*, John Wiley & Sons, ISBN: 0-470-85668-8)
[27] Hiltgen, Alain; Kramp, Thorsten; Weigold, Thomas: *Secure Internet Banking Authentication*, http://www.zurich.ibm.com/pdf/csc/SecureInternetBankingAuthentication.pdf
[28] Murdoch, Steven J.: *Defending against wedge attacks in Chip & PIN,* http://www.lightbluetouchpaper.org/2009/08/25/defending-against-wedge-attacks/, blog entry, 25 Aug 2009, captured 16 Sep 2009
[29] OpenID.ee, https://openid.ee/
[30] Oppliger, Rolf; Hauser, Ralf; Basin, David: *SSL/TLS Session-Aware User Authentication - Or How to Effectively Thwart the Man-in-the-Middle*, http://www.inf.ethz.ch/personal/basin/pubs/mitm-cc.pdf
[31] Stone-Gross, Brett; Cova, Marco; Cavallaro, Lorenzo; Gilbert, Bob; Szydlowski, Martin; Kemmerer, Richard; Kruegel, Chris; Vigna, Giovanni: *Your Botnet is My Botnet: Analysis of a Botnet Takeover*, http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf
[32] Sunshine, Joshua; Egelman, Serge; Almuhimedi, Hazim; Atri, Neha; Cranor, Lorrie Faith: *Crying Wolf - An Empirical Study of SSL Warning Effectiveness*, 17th USENIX Security Symposium, August 10-14, 2009, Montral, Canada, http://lorrie.cranor.org/pubs/sslwarnings.pdf
[33] Tuliani, Jonathan: *The Future of Phishing*, Computer Fraud & Security, Volume 2004, Issue 4, Apr 2004, Page 11, http://www.eb2bcom.com/knowledgebase/articles/Phishing.pdf
[34] The Austrian eID Card 'Bürgerkarte', http://www.buergerkarte.at/

[35]The Belgian eID Card, http://eid.belgium.be/
[36]The Portuguese eID Card, http://www.cartaodecidadao.pt/
[37]e-äriregister (Estonia), RIK Centre of Register and Information Systems, Company Registration Portal, https://ettevotjaportaal.rik.ee/index.py?chlang=eng, captured 13 Oct 2009
[38]The Spanish eID Card, http://www.dnielectronico.es/
[39]Wikipedia (German), Identitätsfeststellung, http://de.wikipedia.org/wiki/Identit%C3%A4tsfeststellung, captured 22 Aug 2009
[40]The STORK project, http://www.eid-stork.eu/