Electronic identity in Finland: ID cards vs. bank IDs

Teemu Rissanen

Received: 22 October 2009 / Accepted: 18 February 2010 / Published online: 6 March 2010 © The Author(s) 2010. This article is published with open access at Springerlink.com

Abstract This chapter describes the introduction and diffusion of the Finnish Electronic Identity Card (FINEID card). FINEID establishes an electronic identity (eID), based on the civil registry and placed on an identity chip card issued by Finnish government to Finnish citizens and permanent residents from age 18 and older. It is a non-mandatory electronic identity card introduced in 1999 in order to replace the older citizen ID card. It serves as a travel document and is intended to facilitate access to eGovernment services as well as offering a possibility to sign electronically. Therefore the chip contains two certificates: one for authentication purposes, and one for qualified signatures. The eID function had to compete with the already existing PIN/TAN based TUPAS standard for online authentication for eBanking, eCommerce and eGovernment applications, and has lost this battle by reaching less than one percent of all online authentications. The history, actor constellation, time line and barriers will be described and a few communalities and differences to other countries under study in this special issue will be highlighted.

Keywords Bank ID · eID card · PIN/TAN authentication · Population register center · Social security identifier number · eGovernment · Electronic identity cards · Electronic passports · European interoperability of electronic identity cards · Finnish electronic identity · Identity management for citizens · Legal framework for electronic identities · Unique identifiers

Origins and context of electronic identities and ID cards

Finland was the first country in the world to introduce an electronic identity card in 1999. The non-mandatory Finnish Electronic Identity Card (FINEID card) was
introduced in 1999 in order to replace the older citizen ID card with a machine readable data zone and smartcard chip, after studies carried out from 1995 to 1997. The FINEID standard establishes an electronic identity (eID), based on the civil registry and placed on a chip card. The card is issued by the Finnish government to Finnish citizens and permanent residents from age 18 and older. It serves as a travel document and is intended to facilitate access to eGovernment services as well as offering a possibility to sign electronically. Therefore the chip contains two certificates: one for authentication purposes, and one for qualified signatures.\(^1\)

The FINEID is provided and administered by the Finnish Population Register Centre (PRC), running the Population Information System (Väestötietojärjestelmä), which includes a key set of authentic identity attributes for all Finnish citizens and permanent residents registered. All of the attributes stored in the authentication certificate of the eID card are obtained directly from the Population Information System, except for the cardholder email address which can be included if the user wishes so.

However, since the beginning, the FINEID card has been in competition with an already existing PIN/TAN paper based online authentication system called TUPAS provided by the Finnish banks. So far almost all adult Finnish citizens are registered to the TUPAS service, while only around 10% of the adult population owns a FINEID card. Regarding the share on all online transactions (eGovernment and eCommerce) TUPAS accounts for 99.9 %, FINEID for 0.1 %.\(^2\)

Identity cards and passports

In Finland there is no obligation of citizens to hold an identity card. A national identity card is offered, but has been rarely used as the driving licences and the compulsory social security cards have provided equal standing as proof of identity, with the advantage of offering domain-specific services. For border control the passport serves as a regular means for authentication. Social Security cards (KELA card) are issued to every person living permanently in Finland. All Finns and permanent residents are also assigned a unique Social Security Identifier Number (SSIN). The KELA cards provide proof of valid health insurance coverage and since 2004 the KELA social insurance information can be included on the FINEID card as well.

When the first machine readable ID card was introduced in 1999 its main purpose was to serve as a travel document at least within the Schengen area offering a value which the other permits and cards could not provide. But In 2006 new passports have been introduced with biometric data on a RFID chip. The e-passports of 2006 contain the holder’s facial image, machine readable data zones and the signature certificates in accordance with the provisions of EC Regulation 2252/2004. The second generation e-passport is issued since 2009. The electronic data is protected using ICAO the specified Extended Access Control mechanism, in compliance with EC 2252/2004 technical annex. The Passport Act 2006/671 was amended in 2009

---

\(^1\) Detailed information is available through the official FINEID website (http://www.fineid.fi); available in Finnish, Swedish and English).

\(^2\) See section “Diffusion of FINEID and barriers to its use” for details.
(Act 2009/456) to include, amongst others, the acquisition of passport holder fingerprint minutiae and the subsequent use of biometric data with the e-passport. The Population Register Centre is the e-passport CA for Finland, while the authority for the issuance of the e-passport has the Ministry of Interior.

Compared to the e-passports the eID card was considered only as a “secondary” travel document only within the Schengen area. But recently legislation was launched to include an additional RFID chip into the eID card, containing a digital image of fingerprints in compliance with the EU directives. So far the eIDC does not contain biometric data and the FINEID specifications do not specify biometric data for the eIDC. As travel document and as electronic ID, the FINEID card is compounded card where the PRC issues the eIDC, but where the Ministry of Interior defines physical and technical components required for a Machine Readable Travel Document (MRTD). As a consequence, the forthcoming next generation eIDC will contain two separate chips: one FINEID specified eID for certificates using the contact interface ($T=0$) and another contactless chip (ISO-14443) for biometric data. The Passport Act 671/2006 and its amendment in 2009 provide that the fingerprint minutiae are included in all MRTDs, including the eIDC.

The National Register, the national number and the social security number

Every Finnish citizen receives a unique social security identifier number at birth and permanent residents are assigned this identifier as they register themselves to the Population Information System. The unique identifier is generated by the Finnish Population Register Centre (PRC). In Finland population information has been recorded since the 16th century as maintenance of records of men fit for military service became established in the 1550’s. The population registers are fully computerised since 1971. The PRC maintains the Population Information System in cooperation with local register offices. The information in the system is collected from citizens and from various public authorities such as the police, tax, social security, military etc.

The Finnish eID contains a unique identifier (FINUID) generated by the Finnish Population Register Centre (PRC). The personal data recorded in the population information system includes name, social security identifier number or personal identity code (for those without an SSIN, such as temporarily resident aliens), address, citizenship and native language, family relations and date of birth and death (if applicable). The system also includes the FINUID for those who have been issued an eID card and / or born after 2002.

The Finnish Population Information System serves a variety of societal functions including election arrangements, taxation, judicial administration, administrative decision-making and planning, compilation of statistics, and research. Businesses and other organisations also have access to data collected in the Population Information System. The system is at core of all existing authentic source-based online services in Finland (national, regional, private).

The Social Security Identifier Number (SSIN) is formed using the date of birth, a gender code and a check sum. It is easy to remember and it is widely used as verification means for several applications. As the SSIN includes the
date of birth and gender it may be used only by special permission. Providers of eID applications are only allowed to use the SSIN in cases authorised by the Privacy Ombudsman and in compliance with the provisions of the Personal Data Act (523/1999). Service providers qualify for using the SSIN if they fulfil the legal obligations set by this Act. The liberal and uncontrolled use of the SSIN has been seen as a major privacy problem and the FINUID has been developed to mitigate the privacy concerns.

The FINUID is not an original personal identity number as in other European countries, but it is generated from the SSIN for privacy reasons. The PRC creates the FINUID from the SSIN using a mathematical formula that both avoids collision and is irreversible. It is therefore both secure and useful for identification purposes. But unfortunately the FINUID has not been widely implemented in practice as a more privacy enhancing alternative to the SSIN.

Bank ID’s and the VETUMA service

In the field of eCommerce nearly all sites rely solely on the PIN/TAN based bank ID TUPAS for both authentication and online payment (international credit card and PayPal payments offer the other alternative). Online payment transactions have an important role in electronic services. A payment transaction is regarded as equivalent to authentication and can therefore also substitute an electronic signature in the meaning of a “record of legal act”.

The bank PIN/TAN based TUPAS identity scheme is not certificate based. It is a proprietary “shared secret” identification solution using a combination of a username and password with one-time transaction authentication numbers (TAN) that are printed on a paper slip. Osuuspankkki bank offered also until 2009 an EMV payment card that could contain a citizen certificate if the customer so wanted. The solution was not popular since it lacked the travel document value and offered very little other services than just access to online banking.

The bank TUPAS account is linked to a user, which can be natural or legal person. The citizen certificate on the other hand is only issued to a natural person; hence the eIDC may not be used by companies to manage their online bank services. As no authorisation services are available the citizen certificate holder cannot delegate the use of the certificate to a legal person.

The banks offer a relatively uniform interface for accepting online payments using TUPAS and therefore eCommerce sites have widely adopted this technology. The TUPAS services require that the user is a customer of a TUPAS scheme participating bank and it also requires that the service provider signs bilateral service contracts with each bank participating in the scheme. This results into that not all online services or eCommerce sites accept TUPAS authentication from all the banks and not all users are able to access the services (namely customers of smaller banks).

There are also liability issues that create other limitations to the use of TUPAS and these are all reasons why the eIDC was initially developed. Unfortunately due to very modest take-up of the eIDC, the TUPAS scheme has proven to be the winning
solution and all eGovernment applications support TUPAS via the national portal VETUMA as the primary solution for authentication as well.\textsuperscript{4} A latest sign of this disenfranchising was OKO Bank’s decision to stop the eIDC support for online banking access in September 2009 due to low usage.

**Characteristics of the finnish eIDMS FINEID**

The FINEID specification that defines and describes the eIDC does not specify the physical layout or other card surface and body material elements, which are part of the Ministry of Interior’s police and permit department’s competence area for all official ID documents.

The FINEID card

The Finnish citizen eID card\textsuperscript{5} (Fig. 1) is a polycarbonate ISO 7816 form factor type smartcard with several physical security features, including laser engraving, Guilloche and rainbow-colour printing, amongst others. The card details are given in Finnish, Swedish and English, as the card also serves a travel document. For this reason the machine readable data set is also provided on the back of the card. The card front contains user identity data such as full name, social security number (SSIN), date and place of birth, gender, nationality, and card validity data. The printed data is partly stored electronically on the chip, except for the SSIN. The cardholder’s address is neither printed nor stored electronically on the card since actual address information is readily accessible from the Population Information System. Possible disclosure of address information is considered to present privacy risks and the need to have this information on the card has not emerged in practice.

The chip contains two user certificates, allowing the authentication of the citizen via the unique identifier FINUID and the use of a qualified electronic signature. The FINUID is included in the FINEID citizen certificate in two areas: as part of the certificate holder’s Distinguished Name (DN) and as Serial Number (SN). The authentication certificate is also used for encryption. There is no key-escrow for encryption keys or for any other keys as all eIDC keys are generated on board. Therefore once encrypted data can only be decrypted as long as the card remains functional and at hand. Optionally the card holder may request to include her email address in the certificate.

The eID card has a serial number, but this is not used by eGovernment applications. The eIDC is distributed by the police and its price was initially 40 €, today 48 €. The eIDC is valid for 5 years after which a new card is issued upon application.

Compared to the four southern and western European countries under study in this special issue, the FINEID and eID card do not correspond directly to any of

\textsuperscript{4} For more details on VETUMA see Ministry of Finance (2008).

\textsuperscript{5} There are also sector-specific ID cards issued by the PRC such as the organisation certificate smartcards for professional use.
these cases (Table 1). It comes closest to the German case, where the ID card is not mandatory if a passport is held. But in Germany there is no unique identifier, there already is a RFID chip, qualifying the card as a travel document for the future.

Digital functions and their applications areas

The eIDC may be used for authenticating online, digitally signing documents, encrypt data and for signing and encrypting email messages, provided the card holder has applied for the optional email certificate extension to be included. The eIDC does not contain address, role or other information that would be used with different applications. All eIDC relying party applications fetch the needed information from the Population Information System, after the user identity has been established by mapping the FINUID with the corresponding SSIN.

Table 1 Comparison of European eID card characteristics

|                          | AUT | BEL | GER | ESP | FI |
|--------------------------|-----|-----|-----|-----|----|
| **Carrier card**         |     |     |     |     |    |
| identical with national ID-card | –   | X   | X   | X   | X  |
| **Card issuance**        |     |     |     |     |    |
| obligatory               | no  | yes | no  | yes | no |
| From age >               | –   | > 12 | >16 | >14 | > 18 |
| **Card function**        |     |     |     |     |    |
| Authentication (online)  | X   | X   | X   | X   | X  |
| Authentication (visual)  | Xc  | X   | X   | X   | X  |
| e-signature              | X   | Xb  | X   | X   | X  |
| national register number | –   | X   | –   | X   | (x)d |
| **Card attribute**       |     |     |     |     |    |
| visual data:             |     |     |     |     |    |
| · address                | Xc  | –   | X   | X   | –  |
| · owners photograph      | Xc  | contact | X | X | X |
| contact/contactless chip |     | contact | RFID | contact | contact |
| PIN-protected identity data | X   | X   | X   | X   | X  |
| Biometrics face fingerprints | –   | –   | X   | X   | Planned on a second chip |

a opt out b opt in c depending of used card d FINUID derived from SSIN
The authentication and signature PIN codes are individual and of different length. Both are initially random and the user may change both PIN codes. The user receives the PIN1, PIN2 and PUK codes in a sealed PIN envelope via mail and the user is requested to change the PIN values and keep the PUK code. In case the user forgets her PIN codes and does not have the PUK code, PIN unblocking is done at the police station, which is the local Registration Authority.

The use of electronic signatures is defined in sector specific legislation. There are no formal requirements for electronic signatures in Finland. With regard to the use of electronic signatures by public administrations to issue signed documents to citizens or businesses, this is not yet done in appreciable levels in Finland. The Finnish approach to eGovernment revolves largely around web services and around establishing trusted relationships between public administrations and partnering private sector organisations for the direct exchange of authentic information. Signed electronic documents are generally not used. Thus, when information needs to be exchanged, typically this will be done through these trusted networks rather than by requiring the creation of a specific electronic document.

With regard to the eIDC application areas, the Online Authentication and Payment VETUMA service is a national portal for authenticating towards eGovernment applications and services. The portal supports the use of the eIDC besides the above mentioned TUPAS. Thus eGovernment applications that rely on the VETUMA service, have the possibility to authenticate users with their eIDC, but as mentioned, this option is chosen in less than one percent of all transactions. The VETUMA service will be further developed during 2010 and it is not clear whether how the eIDC will be supported in the future. It is highly probable that the service providers will stop accepting the eIDC for economic reasons.

The authentication process

For authentication to eGovernment services via the VETUMA service using the eIDC, the following process steps are usually taken:

- User accesses an online service that requires authentication and selects the eIDC authentication option which is symbolised in all FINEID accepting services using the following “Etu” (=benefit in Finnish) symbol:

  ![Etu](image)

- The Vetuma authentication page is displayed and the user is advised to enter her eIDC in the card reader
- The user is then prompted by the client side CSP middleware to provide her corresponding PIN code
  - In some cases the user may be asked to select the appropriate certificate in case several certificates are stored in her computer
  - The CSP middleware may ask for either PIN1 or PIN2 depending on whether the transaction calls for the authentication or signature certificate
In the backend the user’s identity is mapped to the user registry using the FINUID code provided in the certificate. Usually the mapping is done towards the population information system, which provides the user’s SSIN or other population information to the website that accepts FINEID.

The certificate validity is also verified in the backend using the Certificate Revocation List (CRL) provided by the PRC. The CRL address or distribution point is discovered from the certificate or in some cases the authentication service provider may store the CRL in the system.

In case the user PIN is correct and the validity verification is also successful, the user is automatically redirected to the original web site. In the return sequence usually a cookie or HTTP POST message is used to deliver the authentication data payload, which may contain the SSIN and other information requested by the website.

When the VETUMA service is not used, the data fetching process from the PRC is nevertheless identical.

The legal framework

The eID cards issued by the Population Register Centre (PRC) and the use of the eID are governed by following acts:

- Identity Card Act (829/1999),6
- Population Information Act (507/1993),7
- most recently by the Act on the Population Information System and on the Population Centre Certificate Services (661/2009), which will enter into force 1st March 2010,
- the European Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures was transposed into Finnish legislation through the Act on Strong Electronic Authentication and Electronic Signatures (617/2009). The Act contains provisions on electronic signatures created by means of a qualified certificate. The Act obsoletes the previous Electronic Signature Act 14/2003.
- The Regulation on the Requirements for Reliability and Information Security in the Operation of Certification Authorities Providing Qualified Certificates (8/2003M)8, which came into force on 1 February 2003 and remain valid until 31 January 2008.
- Regulation of FICORA (Communication Regulatory Authority) on CA’s notification obligations.

In these Acts the PRC is mandated to act as Certification Authority to the Finnish government. The requirements of the Act on Electronic Signatures, the Act itself and the Act on Electronic Services and Communication in the Public Sector (13/2003)9

---

6 Henkilökorttilaki (829/1999): http://www.finlex.fi/fi/laki/ajantasa/1999/19990829 Not translated into English.
7 Väestötietolaki (507/1993): http://www.finlex.fi/fi/laki/ajantasa/1993/19930507 Not translated into English.
8 http://www.ficora.fi/englanti/document/FICORA082003M.pdf
9 Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): http://www.finlex.fi/en/laki/kaannokset/2003/en20030013.pdf (Unofficial translation).
apply to the PRC. In accordance with the Act on Electronic Communication within Administration, qualified certificates may always be used within administration. These Acts set out the legal guidelines for personal identification and for the production of electronic signatures and services.

The powers of the PRC are governed by:

- The Act on Register Administration (166/1996),\(^\text{10}\)
- The corresponding Decree (248/1996),\(^\text{11}\)
- The Act on the Population Information System and on the Population Centre Certificate Services 661/2009 (will enter into force 1st March 2010).\(^\text{12}\)

Depending on the authentication method (FINEID or TUPAS), eGovernment applications use either the FINUID or the SSIN as unique identifier. When using FINEID/FINUID authentication, there are no privacy related obligations for service providers. But this is the case when using TUPAS/SSIN authentication, where the handling and storing of the user SSIN by the service provider is regulated by the Personal Data File Act (523/1999)\(^\text{13}\). The Act does not constitute a compliance framework to which service providers can certify to, but in case of privacy data breach (disclosure of user SSIN), the service provider can be held responsible for negligence.

The PRC has interpreted the Personal Data File Act so that it has a monopoly to generate and issue FINUIDs. This interpretation has been contested in many occasions and the Act on the Population Register and the PRC CA Activities 661/2009 (enters into force 1st of March 2010), stipulates that the PRC has no monopoly in the issuance of the FINUID and that other CAs established in Finland will have the right to issue this identifier to their certificate users. The Finnish Communications Regulatory Agency (FICORA) will define the requirements which CA service providers will need to comply with in order to be able to issue FINUIDs.

The use of the FINUID has remained very limited and the use of the SSIN is the norm, even though this requires the above mentioned extra privacy protection measures for the service provider defined in the Personal Data Act. The need to request user consent as well as the need to notify the Data Ombudsman’s office in case a user registry is created, are namely the main constraints for organisations using the SSIN as identifiers for their users. In practice also the use of the FINUID has not found its place in eGovernment applications since even though users would use their eID card to authenticate and sign, hence identifying one self with the FINUID, the service applications still rely on SSIN identification. As a result a FINUID is always referenced and mapped to the SSIN, which then is used by the application. Economically this solution is problematic since although the use of the eIDC is free of charge, querying the Population Information System for an SSIN is charged by the PRC, and consequently the eIDC relying application will need to pay for the authentication.

\(^\text{10}\) Rekisterihallintolaki (166/1996): http://www.finlex.fi/fi/laki/ajantasa/1996/19960166 Not translated.
\(^\text{11}\) Rekisterihallintoasetus (248/1996): http://www.finlex.fi/fi/laki/ajantasa/1996/19960248 Not translated.
\(^\text{12}\) Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009) http://www.finlex.fi/fi/laki/ajantasa/2009/20090661 Not translated.
\(^\text{13}\) Henkilötietolaki (523/1999): http://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf Unofficial translation.
Distribution, personalization and activation of FINEID

The FINEID card has to be requested and to be picked up at the local Police Station, but it is produced and personalized centrally by the Finnish Population Register Center (PRC). The cards are produced by Setec, a part of French Gemalto group (www.gemalto.com). After successful application, the user first receives the PIN1, PIN2 and PUK codes in a sealed PIN envelope via mail, after which the card can be retrieved from the local police in person. The certificates on the eIDC are readily included and the authentication function is activated by default. No separate request or activation is needed, nor is there any subsequent extra fee charged.

The PRC serves as the Certification Authority (CA) for the certificates, and also provides support for users via a central web-site, where a client software for offered for download, a FAQ page is published and customer support is offered via telephone and email. However the eID card reader has to be bought separately.

Main Actors and timeline of the eID/eIDC introduction process

Main actors

The man actors in the introduction process starting in 1999 were three ministries Table 2:

The Ministry of Finance (MOF) plays the most important role in the horizontal coordination of eGovernment actions. The ministry’s policy-making responsibilities range from general ICT policy and guidance for the state administration to horizontal coordination of eGovernment services. These functions are primarily carried out by the Information Management (IM) Unit of the Public Management Department (www.valtit.fi). Since 2008, the ministry also supervises the Finnish Population Register Centre (PRC, VRK in Finnish), which is the National Certification Authority (www.fineid.fi). The Ministry is also responsible for the future development of the eIDC for the Government and citizens.

Table 2 Main acting ministries

| Ministry of finance | Ministry of transport and communications | Ministry of interior |
|---------------------|------------------------------------------|---------------------|
| Information Management Unit Population Register Centre | FICORA UBI INFOSOC Board | Police and Permits |
| -Horizontal coordination of eGovernment actions | -Responsible for the development of the eGovernment initiatives related to digital signatures | -The police issues the eIDC (local Registration Authority) |
| -The PRC specifies, acquires and produces the eIDC | -The INFOSOC Board advises on the development of the eIDC and related initiatives | -The Ministry defines the eIDC travel document |
| -The Population Information System is the authoritative repository for Citizen Identity information | | |
The Ministry of Finance is also responsible for information management in regional administration and local authorities. It plays an important coordinating role at the local level. The MoF ensures of the diffusion and exchange of standards, good practices and approaches at the regional and local levels through its Information Management Unit. The ministry also supervises inter-ministerial and interagency coordinating groups on electronic services.\textsuperscript{14}

The Ministry of Transport and Communications (MinTC) is responsible for the development of the eGovernment initiatives related to digital signatures, including preparation of legislation. It also legislates the legal framework under which eIDC’s are issued and managed according to the relevant EU directives. In accordance with the Act on Strong Authentication and Electronic Signatures, qualified certification authorities are supervised by the Finnish Communications Regulatory Authority (FICORA), which is an agency under the administration of the MinTC.

The Ministry of Interior (INTERMIN/PERMIT) prepares the laws relevant to travel documents (Passport Act) and assigns responsibilities to the PRC as to the issuance of the eIDC and signing of e-passports as the National ICAO CA.

Relevant for offering applications which need online authentication for eGovernment services are local governments. But they rely on the Authentication and Payment Gateway service VETUMA, which is a joint service initiative from the MoF and large municipalities.\textsuperscript{15} VETUMA offers a single gateway for supporting FINEID and TUPAS authentication in parallel. The application provider can chose which one he accepts. But as mentioned VETUMA is probably reconsidering support for the FINEID and therefore it is a powerful actor with regard to the future of the FINEID.

Other important actors on the operational level include:

The Population Register Centre (PRC), which issues the eIDC and is responsible for the population information system. It operates under the administration of the Ministry of Finance and its Government IT Department. The PRC is responsible also towards the Ministry of Interior which is responsible for permits and travel documents, including the e-passport and the eIDC. The PRC reports to the FICORA, the Data Ombudsman’s Office and the Parliament. The PRC uses the MININT network of police permit offices as Local Registration Authorities for the issuance of the eIDC.

FICORA is dependent of the Ministry of Communications and it is responsible for supervising CA’s in Finland. It also defines the regulatory requirements and controls that govern the issuance and management of Qualified Signature Certificates and service providers offering strong authentication solutions and services to the general public.

The Data Ombudsman is responsible for issuing recommendations on how to implement the provisions of the Personal Data Act and other relevant Acts that relate to privacy issues. The use of the SSIN and FINUID as well as certificate content is subject to review by the Ombudsman.

\textsuperscript{14} http://www.vm.fi/vm/en/13_public_management_reforms16746/02_hallintorakenteen_kehittaminen/01_aluehallinto/index.jsp
\textsuperscript{15} http://www.suomi.fi/suomifi/qualitytotheweb/eservices_and_forms/eservices/index.html
The unicameral Parliament ratifies EU directives and passes all legislation in Finland. The Government and the Parliament define the overall strategy for IT and the main objectives for the competent Ministries and Agencies.

The Porvoo Group is a discussion forum founded by the PRC in 2002 that has a vocation for promoting use of eIDC’s and international interoperability with different eID’s. The work of the Porvoo Group has had a significant role in the communication of different European, US and Asian eIDC projects, initiatives and good practices. It is notable that the US NIST has had a very active role in the working of the Group and this has partly influenced the development of the Federal PIV (Personal Identification and Verification) scheme towards closer interoperability with European eIDC schemes.

The Ubiquitous Information Society Advisory Board (UBI INFOSOC), which was established by the MINTC in 2007 to coordinate the national information society policy, is a Public-Private working group that provides analysis and advice on the development of the eIDC. The Board has a strong influence on the legislation, notably on the recent Act on Strong Authentication and Electronic Signatures 617/2009. The Finnish Financial Industry Federation FFIF and the Finnish Communication Industry Association FICOM have an active role in the UBI INFOSOC Board. In addition the FFIF has a stake in the KATVE Consortium, which is in charge of Identity Services for the Tax Services, the Social Security KELA and the Ministry of Labor (MOL).

The HST Group (HST is the Finnish acronym for the eIDC) has currently ceased its activities. It was a Public-Private interest group that thrived to promote wide adoption of the eIDC. In part, the UBI INFOSOC Board carries the work of the HST Group.

The technical specifications for the FINEID have been provided by Setec Oy, together with the PRC. Setec is the former Bank of Finland's banknote printer. Meanwhile Setec is owned by the international smart card vendor Gemalto. When Setec's banknote printing was ended, the company focussed on producing passports, smart cards, ID-cards and digital security products, e.g. Sweden's, Norway's, Denmark's and Singapore's passports as well as bank and SIM cards to Europe and Asia.

With regard to the power distribution between policy fields and actors in the Finnish case the field of interior/police, governed by the Ministry of Interior was most influential, followed by the field of Public Administration and eGovernment under the authority of the Ministry of Finance. Nevertheless Financial Services like the tax authority did not play an important role. Also eCommerce has not had a significant role. Social and Health issues did play a role in defining the eID and in employing the eID card as an additional token for the Social Security Card content. Compared to the four countries in the first comparison the pattern of influence comes closest to the case of Germany (Table 3).

Time line

The process of planning an eID card and an eID function in Finland can be divided in three phases (Fig. 2). It started in 1995 with government initiated studies and leading to eIDC Pilots in 1998. The first European eIDC was issued on 1.12.1999,
when the Identity Card Act came into force. The Civil servant ID chip card guidelines were issued 3.11.2000 and served as a blueprint for the development of FINEID specifications in 2002. In October 2002 the HST-Group was founded to boost usage of the eID card.

The second phase may be called the roll-out of the FINEID and its slow adoption. Key events were the Act on Electronic Signatures in 1.2.2003, the Act on Electronic Services and Communication in the Public Sector of 1.2.2003, a HST-Group business strategy paper from 12.5.2003, and the Ministry of Finance guidelines on identification in e-services 29.9.2003, which give equal standing to eIDC and TUPAS as authentication method for eServices. Important events were also the option of a combined eIDC and social security card since 1.6.2004, the launch of mobile wireless PKI services in 2005 and finally the State Auditor’s report 161/2008, which addressed the problems related to the FINEID eIDC and government services, and the Ubiquitous Information Society Advisory Board report published on 15.10.2008.

![Timeline of the introduction and rollout of the FINEID](image_url)

**Fig. 2** Timeline of the introduction and rollout of the FINEID
Today we are in a third phase, which could be called “renovation”. It includes an interim report on the future of CA services published by the Ministry of Finance 5.6.2009, the Act on Strong Authentication and Electronic Signatures 617/2009 in force since 1.9.2009 and the recent Act on Population Information System and PRC 661/2009 coming into force on 1.3.2010. But this phase is not finished yet and the result of this renovation is uncertain.

Consent and disputes

The technological options characterising the FINEID card represent a high degree of continuity and consensus guided by the following principles: the development and implementation of a Finnish Electronic Identity specification framework (FINEID) as basis of the National eIDC, strong alignment with international standards such as ITU, ISO-IEC, ETSI standards and the proprietary PKCS#15 standard, and compliance with the EU requirements for Secure Signature Creation Device (SSCD). Exceptions have been accepted with regard to the SSCD requirement e.g. for the Mobile FINEID using UICC/SIM technology and OKO Banking card using an EMV compliant IC platform. Nevertheless the FINEID eIDC is IC based and not software based as in Denmark or Sweden.

There have been only few disputes regarding the eIDC in general, except for the financial cost and the poor adoption rate which lead to a contentious political debate in May 2008 when the State Financial Auditor reported on the eIDC overall costs since its inception.\(^{16}\) The main disputes have concerned the Population Register Centre’s actions as a National CA that offers commercial CA services and also holds monopoly on the issuance of the citizen unique identifiers for electronic transactions, the FINUID. Other potential CAs have not had the possibility to issue FINUID identifiers to their certificate holders, preventing thus issuance of certificates whose holder identities could be easily matched with existing public data records.

The PRC has made it a policy to not allow other organisation to issue FINUIDs, but this decision has been more politically than legally motivated as neither the previous nor the current legislation on the matter does support this position. Nevertheless commercial CAs in the late 1990’s decided it was too big a financial risk to challenge PRC’s policy and thus did not dispute this question in courts. Later other potential commercial CAs, namely the three MNOs (Mobile Network Operators) Sonera, Elisa and DNA did neither try to challenge this policy.

The current law on electronic authentication and signatures of 1st of September 2009 (Act 617/2009) makes it explicitly clear that no Government actor has monopoly in the issuance of FINUID’s and that it is also acceptable to use the user’s privacy-sensitive SSIN (Social Security Identifier Number) as a unique identifier in a PKI scheme, provided that the number is not included in the public part of the certificate, is not published in a public directory and its use is protected by user consent (i.e. PIN).

\(^{16}\) Tunnistuspalveluiden kehittäminen ja käyttö julkisessa hallinnossa. Valtiontalouden tarkastusviraston toiminnantarkastuskertomus. Edita Prima Oy, Helsinki 2008. ("The development of authentication services in the public sector. A State Financial Audit Office report")
The Passport Act 671/2006 revision from 2009 included the acquisition and use of fingerprint minutiae from passport applicants for the new ICAO and EU norm compliant MRTD (Machine Readable Travel Document) with EAC (Extended Access Control) functionality. The privacy issues related to the MRTD EAC’s capability to safeguard fingerprint and other identity data was raised during the legislative process, which had to undergo additional review phases by the Constitutional Council. The Council is called to review law proposals only when concerns of the constitutionality of the proposed law are raised. As media attention on the MRTD BAC (Basic Access Control) mechanism was raised after a group of Dutch researchers successfully “skimmed” identity data from the Dutch e-passport, the privacy concerns were also very strong in the specialised public community. Finnish e-passports are technically the same as the Dutch (SDU Identification), but as the EAC was not concerned, the potential dispute between privacy advocates and the law makers quickly dried out.

Another privacy concern was related to the use of the collected fingerprint data. The police advocated for a positive use of the fingerprint data, which would have allowed fast and reliable on-the-spot identification of citizens by police officials. This system would have allowed the discharge of a number of permits and potentially the eIDC as well since the police would have been able to verify a person’s identity based on a one-to-many fingerprint matching, and verify the relevant data attached to the persons record (e.g. driving licence). This controversial issue was later taken out of the final text, but it remains present in the backdrop for future revisions of the Passport Act.

Biometry issues raised in the e-passport Act directly affect also the eIDC since the Ministry of Interior issued a public RFP in 2008 for the delivery of new citizen eIDCs with the same specifications as for the new EU MRTD, including fingerprints. The new eIDC was intended to be a dual-interface card with two separate IC components: one contactless chip for the EU and ICAO compliant biometric passport data, and one contact chip for authentication and digital signature certificates that is conformant with the EU SSCD requirements and FINEID. The RFP was later contested by one of the card vendors and the Ministry decided to put the whole project on hold, as there were also several other legislative projects under progress in parallel that had a direct effect on the eIDC in general. The current status of the new eIDC is still unknown to the public.

Stimulation of diffusion and innovation of application

In 2003 the HST-Group made several suggestions and business plans for accompanying measures to support the eIDC initiative, but the political will and interest from the commercial and notably the financial sector had already dried out then. There were political debates until 2006 on whether card readers or the eIDC should be distributed free of charge to everybody, or at a nominal cost.

The first Matti Vanhanen Government was already in favour of not funding broadband initiatives and the same policy was applied to the eIDC by the Information Society Programme, led by the Prime Minister. Instead, in 2003 the Ministry of Finance issued guidance on the use of TUPAS for accessing eGovernment services, which made the use of the eIDC quite irrelevant to the general public.
Other legislation, namely the Electronic Signature Act 14/2003 also made it irrelevant to use a formally qualified signature certificate for signing electronically as any electronic token was deemed equally valid with the eIDC.

The applications delivered to the general public remained very marginal and most of the services were available in parallel via telephone (e.g. the change of address application). The government does not have the possibility to favour certain service delivery methods and discard others as it is bound by the provisions of the Act on the Openness of Government Activities (621/1999) and the Act on Electronic Services and Communication in the Public Sector (13/2003) which do not include any exceptions favouring the eIDC. Any favouritism towards one solution is deemed contradictory to higher principles of openness of public services.

Diffusion of FINEID and barriers to its use

Around 85% of the population (less than 5 million) are authorised to receive the eID card. According to the last published statistics from July 2009, close to 265 000 eIDCs were issued, from which 220 300 are valid. Half of the eIDCs include the optional Social Security data. The number represents around 5% of the population, but augments at an average rate of 5000 / month. There are no public statistics available on the usage of the eIDC in eGovernment services, but the State Financial Auditor has collected figures showing that less than 1% of all online authentications are conducted using the eIDC.

The card reader hardware has to be purchased by the card holder. The National Population Register evaluates card reader conformity and publishes a list of tested readers. In 2007 the PRC selected the Fujitsu’s mPollux DigiSign Client as the specific middleware software providing a layer between the application, the eIDC and the card reader. The PRC acquired a global license for the solution, which can be downloaded free of charge.

Other middleware applications have been developed by several companies, which have capabilities to interact not only with the FINEID card but also with other types of smartcards.

The DigiSign FINEID middleware implements the Cryptographic Service Provider and the Microsoft Crypto-API. It has to be installed manually and there are no easy-to-use accessible web services that would help non-technical users to install a reader and the middleware. In addition the middleware is designed to meet the criteria of technically oriented end-users as the menus and features are not usable via graphical symbols or pictures, which is the case in some of the more user-friendly middleware applications (e.g. the Belgian). Usability is unfortunately not prioritised and installing of certificates to the operating system and importing of email certificates to the email editor requires prior know–how on the matter. Manuals and guides are available in different languages, but these do not substantially change the overall problems related to usability.
Usability is also a problem for many of the eIDC application in the Internet. Certain service providers fail to support other Internet browsers than Microsoft IE. As a direct result of the low usage of the eIDC function, in many cases services might be down for a certain time before the problem is even noticed. An example from the private sector, already mentioned is OKO Bank which was the only bank offering support to the eIDC, but has terminated this service in September 2009 due to low usage.

Future perspectives for the eID/eIDC

The so called Ubiquitous Information Society Action Programme 2008–2011 delivered by the Committee carrying the same name and the Ministry of Transport and Communications, states that:

The use and development of electronic services requires reliable, secure and easy-to-use electronic identification methods suitable for different purposes. Secure electronic identification is particularly required for the use of public electronic services that contain sensitive personal data as well as for services that require payment. Citizens currently have the opportunity to identify themselves in electronic services with either bank identification codes according to the TUPAS standard or with a qualified certificate. In the private sector, use of electronic services is generally based on a user ID and password created by the users themselves. One objective of an efficient information society is for the same user to be able to identify him/herself in all, or at least nearly all, public and private sector services using one reliable method. Nevertheless, there may be a number of methods in use side by side. A further objective is to ensure the interoperability of different identification methods in Finland and to prepare for the requirements of internationally interoperable identification.

In June 2009 the Ministry of Finance made an interim report on the future of the National CA services. The report suggests two optional strategies:

1) the National CA provide services only for the public sector (all government services and agencies, public healthcare professional certificates, e-passport certificates),
2) the National CA provides services only for the public sector and citizens (in the form of Electronic Identity Documents).

In both scenarios the certificates would be issued to several optional platforms varying from smartcard to SIM and USB-dongle with secure chip. Also in both scenarios the State Treasury IT Service Centre’s role is augmented as the service providing entity for the cross-administration National CA solution.

In the first scenario the Ministry of Finance would supervise the services and the Treasury IT Service Centre (VIP) would acquire and manage the CA services for all administrations. The service provider market would be competitive as no single CA

20 Ubiquitous Information Society: Action Programme 2008–2011. ISBN 978-952-201-728-4 http://www.arjentietoyhteiskunta.fi
provider would dominate the government market. The PRC and VALVIRA (in charge of the healthcare professional CA services) would have equal standing as sector specific service providers, without independence from VIP.

In the second scenario, the role division between the PRC, FICORA and the Ministry of Transport and Communications were seen as similar to the current situation, with addition that the PRC and VALVIRA would have equal standing as CA’s. On top of the organisation, the Ministry of Finance would supervise the services and the Treasury IT Service Centre would acquire and manage the technical services for all administrations.

The new law on strong authentication and electronic signatures (Act 617/2009) does not redefine roles as envisioned in the interim report, but it includes provisions for ID service providers to comply with specific regulation when delivering strong authentication services to the general public. This definition singles out any customer-service provider specific or professional ID schemes, as well as services that do not claim to offer strong authentication. The law sets control and compliance requirements and payment fees to any service provider issuing strong authentication credentials and tokens, and digital signature certificates for the general public. A new paragraph also provides that the PRC does not withhold the right to use the FINUID for any service provider that fulfils the requirements of the Act. Additionally the liability issue that has discouraged private CA’s to issue qualified certificates in Finland has been amended to state that the CA is not liable for damages caused by user that are contrary to the respective certificate policy. The previous liability clause did not provide any limitations to damages to the CA, which was legally impossible to sustain for any limited liability company.

The upcoming law on the Population Register and PRC CA services (Act 661/2009) will enter into force in March 2010, but this law does not redefine the PRC’s role, as was envisioned in the aforementioned interim report. It is possible that this law will be amended in case the government decides to implement the interim report’s recommendations to centralise CA services to the VIP.

**FINEID in comparison**

In the light of the generalizations, which have been derived by Kubicek and Noack in the comparative chapter in this issue we can confirm that many of them also apply to the Finnish case.

With regard to path dependency there is the principle of adopting international technical standards. But at the early time when the technical specifications for the FINEID were developed, there were no established standards for relevant cryptographic features. Therefore in the Finnish case the early development of the PKCS#15 cryptographic token format as part of the FINEID standard had marked a propriety national track in the deployment of the eIDC. The FINEID PKCS#15 standard was a technical innovation heavily influenced by Setec Oy, the national fiduciary and permit document printing company. Currently Setec is part of the French Gemalto Group, and it specialises in printing the Danish and Swedish passports among others. Due to the lack of widespread industry support and low take-up, FINEID did not establish a reference market for taking it to other countries.
The FINEID standard has remained a Finnish specificity, albeit based on the now commonly supported ISO/IEC 7816–15 standard.

On the organisational path similar to Austria there was a path creation concerning the main identifier. For privacy reasons the SSIN as the traditional identifier has not been continued to the eID but is translated into the newly created non-speaking FINUID. Planned changes regarding the inclusion of fingerprints in the eID card, which would have been a path fusion with the e-pass path, were postponed because of privacy and economic concerns. On the organisational path the PRC, responsible for citizens identity has been assigned not only responsibility for the eID but become a CA as well. Such a centralization of functions in one public agency did not happen in any other country under study here. Although the monopolistic position of PRC has been challenged and legislation has been changed to open the market for CAs, this probably will not change this strong position.

This confirms the generalizations concerning the relevance of the point in time for path related decisions on the technological path (G 4.3.) and the self enforcing power of newly established paths for the organizational path (G 4.4.).

The fact that there were little disputes concerning the technical, organizational and regulatory features of the FINEID Management System can be explained by the high degree of path continuity on the technical, organizational and institutional paths.

The rather strong privacy regulation in Finland has lead to the FINUID solution, and thereby removed a barrier that prevents the use of the eID for eCommerce in Belgium. Nevertheless the eCommerce industry showed little interest during the development processes, and banks did not support eID based authentication, except for one bank which also terminated support of this option because of low usage in 2009.

The eGovernment authentication gateway service VENTUMA supports both the FINEID and the historically dominant TUPAS based authentication and FINEID lost the battle with a 1 to 99% share also in the field of eGovernment services. This confirms the generalization drawn from all other cases: As long as previous modes of authentication are still offered there is no incentive for users to change to a more secure eID based option, as this requires additional investment and a change of habits. And FINEID is a good example of the vicious circle mentioned in G 10.4 : As long as existing methods of authentication are offered in parallel, there is no need to adopt eID-based authentication. Providers of frequently used e-government services cannot close other ways of authentication as long as not all potential users installed the equipment.

In Finland the eIDC take-up has been much lower than in the other countries that have adopted electronic ID cards. This is due to the fact that there is no other country with one single method for authentication in eGovernment and eCommerce with almost full national coverage.

However, with regard to eGovernment there is a remarkable difference in the Finnish case. In the other countries under study, the formal authority of national Ministries on e-government services on the regional and local level is limited or not existent at all. In Finland the Ministry of Finance has some legal authority in this respect, but did not employ it to support FINEID but on the contrary gave equal legal acknowledgement to the less secure TUPAS method. This demonstrates the challenges posed by a de facto monopoly of pre-existing ID solution and the need to
align government’s strategy on eID with the overall legal and policy level context which define the various eGovernment initiatives.

Open Access  This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

Ministry of Finance. Vetuma Service. Electronic authentication and payment services for citizens. PDF, download from. http://www.suomi.fi/suomifi/qualitytoweb/eservices_and_forms/eservices/vetuma_service/vetuma_service/VETUMA_service.pdf 2008.

Further Reading

IDABC. eID Interoperability for PEGS. National Profile Finland. European Communities, Brussels 2007 http://www.epractice.eu/files/media/media2064.pdf 2007.

Sähköisen tunnistamisen kehittämisryhmän 1. väliaraportti arjen tietoyhteiskunnan neuvottelukunnalle: sähköisen tunnistamisen nykytila Suomessa (15.1.2008) (Ubiquitous Information Society 1st interim report: current status on electronic authentication in Finland) http://www.arjentietoyhteiskunta.fi/files/36/Sahkoisen_tunnistamisen_nykytila_lopullinen_080115.pdf

Tunnistuspalveluiden kehittäminen ja käyttö julkisessa hallinnossa. Valtiontalouden tarkastusviraston toiminnantarkastuskertomus 161/2008, ISBN 978-952-499-039-4 (PDF) (“The development of authentication services in the public sector. A State Financial Audit Office report”). ISSN 1796-9514 (PDF); Edita Prima Oy, Helsinki 2008. English abstract at: http://www.vtv.fi/files/177/1612008_Identification_services.pdf

Valtion varmennetoiminnan uudelleenjärjestäminen, hankeryhmän väliaraportti (5.6.2009). (The reorganisation of governmental CA activities, project team interim report) http://www.hare.vn.fi/upload/Asiakirjat/14725/141239_Varmennetoiminnan_y%C3%A4liaraportti_050609.pdf