eID Interoperability for PEGS

NATIONAL PROFILE FINLAND

November 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Jos Dumortier - Hans Graux, time.lex

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°3

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6484/5938

Executive summary

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable Pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with several different proposals how to build interoperability without affecting member states' own existing infrastructures.

This document describes the current situation regarding the use of electronic authentication means in Finnish eGovernment applications.

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf
[RD5]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf
[RD6]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- *Authentication*[1]: the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

2.2 Acronyms

A2A ..... Administration to Administration

A2B ..... Administration to Businesses

A2C ..... Administration to Citizens

CA ..... Certification Authority

CRL ..... Certificate Revocation Lists

CSP ..... Certificate Service Provider

eID ..... Electronic Identity

eIDM ..... Electronic Identity Management

IAM ..... Identity and Authentication Management

IDM ..... Identity Management

OCSP ..... Online Certificate Status Protocol

OTP ..... One-Time Password

PKCS ..... Public-Key Cryptography Standards

PKI ..... Public Key Infrastructure

SA ..... Supervision Authority

SOAP ..... Simple Object Access Protocol

SCVP ..... Server-based Certificate Validation Protocol

SSCD ..... Secure Signature Creation Device

USB ..... Universal Serial Bus

TTP ..... Trusted Third Party

XAdES ..... XML Advanced Electronic Signature

XML ..... eXtensible Markup Language

XML-DSIG ..... XML Digital Signature

3 Introduction

3.1 General status and most significant eIDM systems

The Finnish eIDM system is based on two frameworks: the national eID card framework (FINEID) and the Finnish Banker's Association paper token framework (TUPAS). Even though the national eID is regarded as the universal authentication system, the most significant eIDM system is based on the TUPAS.

The FINEID card is not mandatory and its use for online authentication is very limited or non-existent, depending on the service. Detailed information on the FINEID is available in English through the official Population Register Centre websites[3]. The card contains a chip holding two certificates: one for authentication and encryption purposes, and one for qualified signatures.

The FINEID system is run by the Finnish Population Register Centre (later PRC, *Väestörekisterikeskus* in Finnish), which is the Certificate Authority for the national eID. The data content of the authentication certificate of the eID card is obtained directly from the Population Register service.

The alternative token to the FINEID is the paper based banking ID token, which are issued by Finnish banks that belong to the Finnish Bankers' Association authentication service. The paper token scheme is called TUPAS and it is proprietary standard created first in the late 1980's. Although TUPAS credentials are available for only majors (over 18 years old) and holders of a banking account with activated online banking service, this eIDM system is the most widely accepted and used authentication system in Finland.

There are two unique identifier schemes available for linking user authentication with the PRC Population Information System: the FINEID based unique electronic identifier (FINUID) and the Social Security Number (SSN), which is used in non-FINEID based authentication. The FINUID is derived from the SSN, but it does not contain privacy sensitive information like the SSN does: unlike the SSN, the FINUID code has no use in physical world service, thus it is a strong protection against card-not-present identity fraud. The FINUID number is included as a serial number on the certificates of the eID card, and as part of the certificate CN field (following the holder name).

Identification information of legal persons is stored in the Population Information System, which is one of the basic register services provided by the Finnish Population Register Centre. Businesses and entrepreneurs are identified from the Business Information System (BIS), which is a joint service for businesses and organisations that are clients of the Finnish Tax Administration, Trade Register or Register of Foundations[4]. An organisation in the BIS system is identified by their VAT number.

---

[3] General info: http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/index_eng

Technical info: http://www.fineid.fi/vrk/fineid/home.nsf/pages/index_eng

[4] http://www.ytj.fi/english/default.asp?path=605

Two public online authentication services are available in Finland. The first VETUMA system is a Citizen-to-Government service, which offers identification and authentication to National and Local eGovernment services using FINEID, TUPAS, user names and passwords. The main access portal to the VETUMA authentication is the www.suomi.fi portal. The second KATSO service is a Business-to-Government service, which offers identification services using FINEID and TUPAS, and authentication and user self-provisioning services using service owned paper token credentials. Registered organisations eventually use only KATSO credentials and tokens for authentication. The main access portal to KATSO authentication is the www.tunnistus.fi portal. [5]

All of these systems will be discussed in greater detail below.

From a practical perspective, usage and uptake of the different eIDM systems can be summarised as follows:

eIDM system	Potential user base	Actual penetration	Actual use
National eID card (FINEID, including Mobile)	Estimated at 4 million (around 80% of the population)	Estimated at 150 000[6] (less than 3% of the population)	Less than 0,1% of online authentication transactions
Banker's Association paper token (TUPAS)	Estimated at 4 million (requires bank account in at least one of the Finnish Banker's Association member banks)	Estimated at over 3 million (nearly all of the potential user base)	99,9% of online authentication transactions

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

Finland is a republic with an explicitly parliamentary constitution and unitary state structure. The administration is sensibly decentralized as municipalities enjoy considerable independence, which is safeguarded by the Constitution. Ministries are also relatively independent as each minister is individually responsible to parliament.

[5] 'Suomi' stands for Finland and 'tunnistus' for authentication in Finnish.

[6] Source: http://eid.belgium.be/nl/navigation/documents/37098.html

In Finland's central administration, a number of different actors share horizontal and vertical coordination responsibilities in the use of eIDM systems in the context of eGovernment. During the last three years, several eGovernment applications have been developed at the national level. From the surface eGovernment services in Finland are only vertically integrated, i.e. within the same area of competence, since each service is focused on particular area. Although below the surface most of these services are integrated through the Population Information System, which is directly accessed and cross-checked by various government services such as tax, social security and labour. Nevertheless horizontal integration level is not very high and complex sharing of data across the administration (national or local) is not possible.

The so-called "authentic source" principle is well adopted in government basic register services but a lot of efforts are invested in developing the use of authentic source data in a more distributed way and on a on-demand basis, such as for pre-filled forms in different public and private services.

EGovernment, in particular horizontal integration, is driven by the following services:

- *National eGovernment*

  The Ministry of Finance (MoF) plays the most important role in the horizontal coordination of eGovernment actions. eGovernment strategy implementation is carried out by the State IT Management Unit (VALT-IT) in the ministry of Finance. The Unit started its functions in April 2005. It is headed by the State IT-director (CIO), who is responsible for running the State IT-management unit and reforming the government IT-functions in accordance with the Government IT-strategy[7].

  State IT Management Unit homepage:

  http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/04_valtion_tietohallinnon_ohjaus/index.jsp

  Information Society Programme information pages:

  http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/

  The KATSO authentication service is a horizontal identification, authentication and authorisation established by the ministries of labour and finances (tax service) and the Social Insurance Institution of Finland, KELA.

- *Regional and local eGovernment*

[7] The National Knowledge Society Strategy 2007-2015: http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/76222690188788831/default/Strategia_englanti_181006final.pdf

The Ministry of the Interior (MoI) is responsible for information management for regional administration and local authorities. It plays an important coordinating role at the local level. The MoI is responsible of the vertical coordination of eGovernment services. It ensures the diffusion and exchange of standards, good practices and approaches at the regional and local levels through its Municipal Information Management Unit (MunIT). The ministry also supervises inter-ministerial and interagency coordinating groups on electronic services. eGovernment implementation responsibility if delegated to the national level State IT Management Unit. The National Population Registry (VRK) works under the MoI administration.

The VETUMA system (online identification and payment) was launched in at the initiative of the capital-region municipalities in spring 2004. The central government participates in the service by refunding the authentication service costs to the municipalities, thus all costs due to the use of public registers for commercial use, the TUPAS authentication service, as well as online payment transaction services are covered by the State until 31. December 2007.[8]

The VETUMA authentication service for citizens is integrated into different communal websites in order to users to access eServices. VETUMA system verifies the user's credentials through an LDAP framework offered by either PRC or the users' bank service. Upon successful authentication by either of the services, the end user can access the local service.

A total of 60 municipalities are involved in the VETUMA project and the capital area cities are the first to offer secured connections via the VETUMA system. VETUMA integration follows a process, where the municipality has to sign contracts with different registry owners (PRC and the banks) and the VETUMA service provider (Fujitsu Services Finland), after which the municipality has to integrate and test the VETUMA interface implemented in the eService, and has to comply with the service licence requirements, including technical security requirements. Interface integration is done using Fujitsu's Software Development Kit (SDK exists in .NET and Java) or using an open source SDK developed at the University of Helsinki (in Perl). Links to all service descriptions, requirements and tools can be found at:

https://tunnistus.suomi.fi/info/index_en.html

3.2.2 -National eGovernment cooperation and coordination

The Finnish government has identified the need for integrated cooperation between different state and local government eServices. The cooperation has taken shape in form of a set of top priority projects defined in the national IT strategy[9]. The government strategy includes both national and local government projects, where VETUMA authentication service (for citizens) is shared by all services (state and local) and it is accessed through the Finland-portal service www.suomi.fi. The KATSO service is a national government service since it includes only the tax, labour and social

[8] Description of the VETUMA system: https://tunnistus.suomi.fi/info/index_en.html

[9] Government IT Strategy top priority project chart: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/2007_krkihankkeet.pdf

security services, which are national. KATSO authentication serves mainly enterprises for declaring salary and pension's costs, but there are some citizen cervices as well such seeking for work from the MoL database.

Among the different top priority projects are also the definition and the setting up of a common eServices platform[10]. The design and definition of the platform (legal framework and interoperability framework) are still under work. According to official statements, the government is less likely to define technical standards or legal requirements than to establish best practice cases in order to facilitate the use of existing eIDM systems in new eServices. In the area of electronic signatures, no strict format or content requirements are envisaged at the moment that would clear some of the existing interoperability challenges.

The interoperability of government IT infrastructures and services has been set up as a priority since 2006 when a cross-administration interoperability working group started its work under the Ministry of Finance Sate IT Management Unit. The interoperability programme is devised in three phases: design and definition project (2006-2007), eGovernment architecture implementation and dissemination (2008-2009), and eGovernment architecture consolidation (2010-2011).[11] As the design and definition project is still under work, no concrete results or specific guidelines are yet available on the eGovernment interoperability framework. Concerning the interoperability framework for eIDM systems, the use of the FINEID card in public administration is strongly supported in the preliminary report on civil servant authentication and identity management[12].

As far as eIDM standards are concerned, ongoing efforts are currently focused on the adoption of internationally accepted standards and protocols, including LDAP, SAML2 and WS-Federation (Kerberos). The technology choices are not government dictated as different existing authentication services already rely on different standards. Even if there is an urge to adhere to published and accepted standards with regards to eIDM, there is little guidance on how these standards are implemented and how well the different solutions are integrated with each other.[13]

3.2.3 Traditional identity resources

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 1550s. Census lists exist since 1634 and originally they served as tax registers, and later became an administrative tool for determining the place of residence and military recruitment, and acted as electoral registers and tax rolls. In Finland the church also keeps population register records (since 1628) and is responsible for collecting and

[10] State IT list of top priority eServices: http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/05_sahkoinen_asiointi/01_hankkeet/index.jsp

[11] http://www.hare.vn.fi/mHankePerusSelaus.asp?h_iID=11940&tVNo=1&sTyp=Selaus

[12] http://www.hare.vn.fi/mHankePerusSelaus.asp?h_iId=12297

[13] A good example is the KATSO authentication service, which creates additional KATSO paper tokens for organization users as FINEID or TUPAS tokens are too limited to the SAML2 standard implementation used in the service. This creates a multi-password environment that is difficult to see as an integrated eIDM system.

keeping of birth, marriage and death certificate records. Finland's earliest population statistics date back to 1750.

The population registers are fully computerised since 1971. The Population Register Centre maintains the Population Information System in cooperation with local register offices. On the basis of the statutory duty to provide information, information is received from citizens and from various public authorities such as the police, tax, social security, military etc. 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.[14] The system is at core of all existing authentic source -based online services in Finland (national, regional, private).

The PRC alone maintains a population register, which includes nationals and non-nationals. Persons registered in the population register are issued an identity card only if applied, and since 1999 the only available identity card has been the electronic FINEID card. The card is not mandatory, thus only a few people own one. Instead passports are more common as travel documents and drivers licence are more common as identity paper. The social security KELA-card is issued to every person permanently living in Finland and it is issued to all age groups (from birth until death). The KELA card is not electronic even though KELA card content can be printed on an eID card, which would create a merged KELA/FINEID card. All the identity cards, except for the passport are issued to both nationals and non-nationals, provided the non-national is permanently living in Finland.

The Population Information System contains population personal data and also information about buildings, construction projects, residences and real estate. The personal data recorded in the system includes name, personal identity code or social security number, address, citizenship and native language, family relations and date of birth and death (if applicable). The building data registered includes the building code, location, owner, area, facilities and network connections, intended use and year of construction. Real estate data registered includes the real estate unit identifier, owner's name and address, and buildings located on the property.

Information regarding legal entities is registered in the Business Information System (BIS). The system is jointly maintained by the National Board of Patents and Registration of Finland and the Finnish Tax Administration. The system enables businesses and organisations to report their information in one single notification to both authorities. The BIS includes businesses and organisations entered in the Trade Register, Register of Foundations, VAT register, Prepayment Register, Employer Register or the Client Register of the Tax Administration. The BIS also contains businesses and organisations that have filed a start-up notification, but have not yet been entered in the registers mentioned above. All businesses and organisations that are included in the BIS are given a Business Identity Code[15].

All these registers are fully computerised and online.

---

[14] http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/C06B93B4C73B0447C2257244002D3488?opendocument

[15] Non-profit associations also have a Business ID if it has been reported to the Register of Associations, to the Trade Register or to the Tax Administration.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

The FINEID card

The FINEID was created in order to replace the traditional citizen ID card. The roll-out of the electronic citizen ID card started on 1 December 1999 following studies undertaken from 1995 to 1997.

Since the beginning, the government has used its certification standard and infrastructure to develop an identity card for civil servants, which is used in ministries and agencies as well as municipalities and joint municipal boards for personnel authentication. The card has the dimensions of a bank card (ISO 7816), and contains user identity data such as full name, social security number, date and place of birth, gender, nationality, and card validity data. The printed data is also stored electronically on the chip. The card holder's address is neither printed nor stored electronically on the card since actual address information is readily accessible from the PRC information system through the online authentication services. 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 and the use of a qualified electronic signature. The authentication certificate is also used for encryption[16]. There is no key-escrow for encryption certificates (nor for any other) therefore once encrypted data can only be decrypted as long as the card remains functional and at hand.

In order to improve government efficiency electronic authentication allows the government to automatically retrieve card holder data that it already has, thus reducing data redundancy and unnecessary form filling (the so called "authentic source" principle). The data is retrieved from the Population Information System[17], which is computerised register containing basic information on citizens and foreign nationals residing permanently in Finland. The system also includes information about buildings, construction projects, residences and real estate. The Population Information System is the most-used basic register in Finland and it is also used by private enterprises that need accurate address information for billing etc. The registry service is not dependent of the FINEID card or certificates and its information service is also accessed by the Finnish Bankers' Association TUPAS system.

[16] An email address can be included in the certificate when applying a certificate. The email address cannot be changed afterwards and the address owner is not verified. Email signing is not performed using the qualified signature certificate.

[17] See English introduction at: http://www.vaestorekisterikeskus.fi/vrk/home.nsf/www/populationinformationsystem

Only the signature certificate is considered to be qualified while the authentication certificate has not been given this label. The Finnish Act on Digital Signatures[18] does not impose same requirements for the authentication certificate as for the qualified signature certificate. The FINEID specification of the PKI application prevents any confusion or misuse of the different certificate types.

The Finnish Banker' Association paper token TUPAS

The TUPAS authentication service is a bank service that supports a one-time-password authentication method defined and standardised by the Finnish Banker' Association. TUPAS authentication can be used by individual customers with a Web banking agreement without any separate measures.

The TUPAS authentication service is commercial service offered for all types of organisations that need to identify their online users. The service is implemented with the signing of agreements with the banks whose customer the service provider wants to reach[19]. The TUPAS service does not require any separate hardware or software as it is based on One-Time-Passwords (OTPs) printed on paper. The user is given one to two pass-code lists (depending on the bank), a static user name and a static private password. The pass-code lists may have two functions: as a list of single-use pass-codes and/or random verification pass-code list. The methodology varies between different banks.

The service deals with user authentication executed by the bank on behalf of a service provider and by the customer's order. In the TUPAS service, the customer can authenticate himself using the same means as for the banks' Web services. The service can be accessed at all terminals equipped with an Internet browser. For authentication, the bank and the service provider are not in direct contact with each other, but it is the user that controls the transmission of data between the service provider and the bank. The user forwards the service provider's request to the bank and approves the transmission of the bank-provided identifier to the service provider. The communications between the customer and the bank and between the user and the service provider are encrypted using SSL. User identity is authenticated against the user social security number, which also serves as a unique identifier. The authentication procedure is a cookie based and the user SSN is stored in the cookie, which later will be stored in the service provider authentication server. As storing of the SSN requires additional privacy protection features from the service provider, centralised authentication services have emerged in the market.

Most people use TUPAS for authentication and even for signatures, when applicable. From a practical perspective, a user can authenticate oneself using the paper token in a number of applications that are integrated into either the VETUMA or KATSO service, using a two-factor authentication. Where interoperability is concerned, the paper token is particularly interesting as it serves to obtain access to secured online public and commercial services, such as online shops. The payment capability (direct connection to user debit account) is also featured in some of the local government VETUMA-authenticated services such as payments for tuition or other communal fees.

[18] Translated version of the original Act *Laki sähköisistä allekirjoituksista* (14/2003):

http://www.finlex.fi/en/laki/kaannokset/2003/en20030014.pdf

[19] Customers of the Nordea, Osuuspankki, Sampo, Tapiola, Säästöpankki, Handelsbanken and Ålanlandsbanken

However, the TUPAS token also presents certain limitations, specifically with regard to the user group (which only covers natural persons who possess a bank account). As a result, for users outside of this group the system is presently not accessible. Furthermore, security could be a concern when using the token, since no physical identification of the requesting party is made. Another privacy related problem is that the token is not private, as it legally belongs to the bank, from which it is issued from. In this regards, the TUPAS token cannot proof true non-repudiation as there is no mechanism to testify on the uniqueness of the TUPAS credentials.

It seems likely that, given the slow take up of the national eID cards, the TUPAS token will be used as primary eIDM system for the public for years to come. Nevertheless in the near future the TUPAS token might change its media from paper to a one-time-password generator token, but this change will not fundamentally change the password dependence of the system.

The Multiplatform FINEID (Mobile Certificate Card)

The FINEID certificate can also be issued to the Subscriber Identity Module (SIM) used in mobile telephones. A PKI enhanced SIM is also called a SIM Wireless Identity Module or SWIM. The mobile FINEID specifications are the same as for the standard card, only separate Certificate Policies are published for the mobile use. Mobile FINEID based authentication and digital signature is achieved through SMS and WAP services and wireless telecommunications service providers have established a global roaming service which enables the use of the FINEID across carriers. Two standards are applied in the implementation of the mobile FINEID: the GSM standards based SIM Application Toolkit and WAP-standards. The difference in the standards does not affect the end-user experience.[20]

Other systems

The FINEID card was merged with the national social security and insurance card (KELA-card[21]) on the 1st of June 2004. All citizens and foreigner living permanently in Finland are covered by the national social security (KELA) system. The card is used for attesting of insurance coverage and patients need to present their KELA-card each time when using public healthcare services or when purchasing KELA-reimbursable prescription medication. The electronic KELA-card is in fact the same national eID card, but enhanced with a code bar signalling the user's insurance reference number. The code bar and other possible insurance data are printed on the back side of the card. Users can apply for the electronic KELA-card while they apply their national eID card and there is no separate from or FINEID -independent electronic KELA-card scheme.

[20] PRC Mobile certificates information pages in English: http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/FE039B4246B8FED9C22572450036E7E6?opendocument

[21] http://www.kela.fi/in/internet/suomi.nsf/NET/080801145040EH?openDocument

VeTuMa authentication at www.suomi.fi

The VETUMA system is a citizen identification and payment service. The service is the responsibility of the Ministry of Finance and it is provided by Fujitsu Services Oy. The service has been developed in the VETUMA Project (Online identification and payment project), which was launched at the initiative of the capital-region municipalities in spring 2004. Also the central government has participated in the development of the service. By using the service, users can identify themselves to the online services of public administration and to make payments to the authorities. Depending on the online service, users can be identified with TUPAS bank identifiers, a FINEID certificate card or a simple username and password. Payments can be made from the user's bank account or using a credit card.

KATSO authentication

KATSO system is an identity management, authorization and authentication platform for organizations. KATSO system is maintained by government organizations, currently National Board of Taxes and the Social Insurance Institution of Finland. KATSO system was designed to replace an authentication the TYVI system. It is an identity management, authorization and authentication framework for organizations. The system design started in early 2005 and development started August 2005. KATSO went in production in February 2006. KATSO is based on Ubilogin[22] IDM framework.

KATSO and the associated authentication infrastructure implement international standards in authentication and attribute distribution. KATSO implements Oasis SAML 2.0 and Liberty ID-WSF 2.0 standards in user authentication and attribute queries. According to service provider, the KATSO system serves around 120 000 businesses. It enables businesses to file and interact with the Board of Tax, it acts as the identity provider, and provides a standard interface to a range of e-services. KATSO also provides authorization services, where business can authorize his bookkeeping company to do income tax declaration on his behalf. Bookkeepers must accept the authorization before it is valid. In addition, the solution utilizes Web service interfaces so businesses and citizens can do the e-filing straight from their payroll system without accessing any of the Board of Tax portals, simplifying and shortening the filing process. [23]

The KATSO system creates KATSO credentials and paper tokens for registered users so that the user can define user account provisioning and authorisation independently of the other eIDM systems, which are used only for identification purposes.[24]

[22] www.ubisecure.com

[23] http://ubisecure.com/content/files/Katso_-_a_Nation_Wide_Outsourced_Identity_Management_System.pdf

[24] It was once said that KATSO is an eID application for avoiding the use of an eID.

Authentication policies

There is no official authentication policy in Finland that defines a strict hierarchy of the different authentication systems in use. However, there is a certain hierarchy deductible from the requirements of legally binding digital signatures, which functions as a theoretical model for assessing authentication requirements. With regard to natural persons, the following hierarchy can be drawn:

Level	Registration citizen identity	Authentication citizen identity	Applications
0	None	None	Public information and services
1	On line registration using address, GSM or SSN number as ID.	By assigned user number in combination with a password chosen by the user	Information/services of limited sensitivity
2	Level 1 + send-out of a confirmation e-mail with activation URL to an address indicated by the citizen, or SMS.	Level 1 + standard challenge-response authentication method	Information/services of average sensitivity
3	Physical identification at the bank for the acquisition of TUPAS credentials	TUPAS authentication certificate	Information/services of high sensitivity and requiring non-qualified electronic signature
4	Physical identification at the police station (LRA) for the acquisition of an eID	Authentication certificate on the eID + signature certificate on the eID + password per transaction	Services requiring a qualified electronic signature

Thus, there are four levels of authentication above public access: basic username/password, use of an SMS with challenge-response, use of the TUPAS authentication, and use of the FINEID card's signature and authentication.

The VETUMA authentication service is designed to support SMS challenge-response authentication (without certificates) but this is not used in any existing applications yet.

3.3.2 Legal framework

The Electronic ID Cards and the certificates issued by the Population Register Centre (PRC) are governed by the provisions of the:

- Identity Card Act (829/1999)[25]; and
- Population Information Act (507/1993)[26].

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)[27] 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.

Other acts with which the PRC has to comply with include:

- The Personal Data File Act (523/1999)[28]; and
- The Act on the Openness of Government Activities (621/1999)[29].

The powers of the PRC is governed by:

- The Act on Register Administration (166/1996)[30];
- The corresponding Decree (248/1996)[31].

Finland has no specific regulations with regard to the process of authentication in general. The e-Signatures law (14/2003) transposes the provisions of the e-Signatures Directive, but does not apply to authentication as such.

Depending on the authentication method (FINEID or TUPAS based), eGovernment applications use either the FINUID or the SSN as unique identifier. When using FINEID/FINUID authentication, there are no service provider side privacy concerns to overcome, thus no special regulations are directly involved. This is not the case when using TUPAS/SSN authentication, where the handling and

[25] Henkilökorttilaki (1999/829): http://www.finlex.fi/fi/laki/ajantasa/1999/19990829 Not translated.

[26] Väestötietolaki (993/507): http://www.finlex.fi/fi/laki/ajantasa/1993/19930507 Not translated.

[27] Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003):
http://www.finlex.fi/en/laki/kaannokset/2003/en20030013.pdf

[28] Henkilötietolaki (523/1999): http://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf

[29] Laki viranomaisten toiminnan julkisuudesta (1999/621)
http://www.finlex.fi/en/laki/kaannokset/1999/en19990621.pdf

[30] Rekisterihallintolaki (1996/166): http://www.finlex.fi/fi/laki/ajantasa/1996/19960166 Not translated.

[31] Rekisterihallintoasetus (1996/248):
http://www.finlex.fi/fi/laki/ajantasa/1996/19960248 Not translated.

storing of the user SSN by the service provider is regulated by the Personal Data File Act (523/1999). 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 SSN), the service provider can be held responsible for negligence.

3.3.3 Technical aspects

The FINEID card is based on PKI technology, and incorporates two certificates: one for authentication, and one for electronic signatures, with only the latter being considered as qualified. Each private key is protected by a PIN-code. Each card is issued at the level of the police districts (which function in this regard as a so called 'local registration authority' on behalf of the National Population Register, which provides the actual information to be included on the card), and has a validity of 5 years.

The certificates on the FINEID are issued by the National Population Register acting under the name of "Citizen CA" (there is no separate "Foreigners CA" service). The certificates follow the X509v3 standard. More details on the certificates and the CSP can be found on the CA's website:

http://www.fineid.fi/

The eID card is not the predominant identification token in Finland at this time. Bank onetime password authentication will continue to be the dominant authentication method in the foreseeable future unless the major banks shift strategy in order to combat more efficiently increasing phishing attacks on Nordic internet banking services.

The FINEID card is manufactured and personalised in Finland by Gemalto (Setec). The card is operated by a Java Open Platform card OS by Setec (SetCos 5.1.1B), which is invisible to card applications since the FINEID application emulates a native data and information structure. The FINEID profile complies with ISO/IEC 7816-15.

The FINEID card has 72 Kb (64 Kb stated) EEPROM memory, where only a part is allocated to additional certificates or data objects, and much of the memory space is left unused. According to the FINEID specifications, there are two PKI key pairs on the citizen qualified certificate card. The FINEID contains 4 certificates in total: two CA certificates and two user certificates. The VRK RootCA certificate is identical to all certificate cards issued by PRC. The second CA certificate is the VRK CA certificate, which is different depending on the certificate type (citizen certificate, organisation certificate, other). The CA certificate key lengths are RSA 2048 bit.

The two user certificates are for authentication and non-repudiation. The authentication certificate is used for both authentication and encryption. The non-repudiation/signature certificate is used for signing, but not for encryption. The user certificate key lengths are RSA 1024 bit.

The user certificates are protected by different PIN codes with different minimum lengths. The authentication certificate is protected by a 4 - 8 digit PIN code. The signature certificate is protected by a 6 - 8 digit PIN code. Both PIN codes can be managed and changed by the user and both are

blocked after three unsuccessful attempts. Unblocking of the card is performed at the LRA point (i.e. police station) for a cost of €10 (stamp duty included).

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 at: http://www.fineid.fi/vrk/fineid/home.nsf/pages/0767597E406159C0C2256FFF00390405

Specific middleware applications intended to be used together with the card have been developed by several companies, including Setec/Gemalto, Nexus/ID2 and Fujitsu Services Finland. There is also an Open Source project (OpenSC) that supports the FINEID. The middleware applications have capabilities to interact not only with the FINEID card but also with several types of smartcards.

The source code for the various middleware applications have not been made public, except for OpenSC (for Linux). The SetWeb middleware developed by Setec/Gemalto serves as an example as it is available free of charge to all FINEID card holders. The SetWeb FINEID middleware, which constitutes the key interface for most eGovernment applications, is implemented into each specific application by providing a layer between the application itself and the device performing the cryptographic operations (the e-ID card, in conjunction with the compatible card readers).

SetWeb is a software package that provides Windows CryptoAPI integration using Advanced Setec SetCSP (SetCSP). Applications using PKCS#11 (e.g. Netscape Browser) can use Setec's PKCS#11 (v2.11 library) implementation called SetTokI (Setec Cryptographic token interface - Cryptoki). SetCSP is a Cryptographic Service Provider (CSP). CryptoAPI is an application programming interface for cryptographic operations in Windows environment. SetCSP enables applications to use smart cards to perform digital signatures, and to encrypt/decrypt files or messages using algorithms such as 3DES, SHA, MD5 and RSA.

For Microsoft® standard applications, a Cryptographic Service Provider (CSP) is created that implements the cryptographic operations from the smartcard. Application developers can use functions in the CryptoAPI without knowing anything about the underlying implementation. The CSP part of the middleware establishes the link between the abstract CryptoAPI and the underlying PKCS#11 interface. The developer will never call any of the functions of the CSP directly, but only through the CryptoAPI. In non-Microsoft applications, the PKCS#11 (v2.11) interface is used generally. Custom applications can also make use of this interface instead of the CryptoAPI interface. The PKCS#11 interface is also called Cryptoki. A detailed description of this interface can be found on the website of RSA Laboratories:

http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/.

The CSP is registered as PROV_RSA_FULL type CSP. SetWeb supports the following algorithms:

- RC2 CALC_RC2
- RC4 CALG_RC4
- DES CALG_DES
- 3DES CALG_3DES
- SHA CALG_SHA
- MD5 CALG_MD5
- MD2 CALG_MD2
- RSA CALG_RSA_SIGN

- RSA CALG_RSA_KEYX

During the authentication process, the underlying library itself will show a GUI to either ask the user to enter her PIN. The FINEID card currently uses one PIN for accessing the authentication and the signature key.

The description of the fields of the authentication certificate is contained in the table below[32]:

FINEID citizen Authentication Certificates					
Base Certificate	OID	Include	Critical	Value	
Certificate					
signatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1withRSAEncryption	Fixed
signatureValue		X			
TBSCertificate					
Version		X		3	
Serial Number		X		(unique nr / certificate)	Dynamic
Signature		X		Sha-1WithRSAEncryption	
Validity					
Not Before		X		Key Generation Process Date/Time	
Not After		X		Key Generation Process Date/Time set according to the certificate policy	
SubjectPublicKeyInfo		X		RSA 2048 (PKCS #1 v1.5)	
Issuer					
countryName	{ id-at-6 }	X		"FI"	Fixed
commonName	{ id-at-3 }	X		"VRK Gov. CA for Citizen Qualified Certificates"	Fixed
subject			Required		
countryName	{ id-at-6 }		YES	"FI"	Dynamic
commonName	{ id-at-3 }		YES	Combination of subject's surname givenName and serialNumber	Dynamic
surname	{ id-at-4 }		YES	Family name of subject	Dynamic
givenName	{ id-at-42 }		YES	One of the first names of subject	Dynamic
serialNumber	{ id-at-5 }		YES	Unique identifier of subject in Finland (FINUID) (8 digits + checksum character)	Dynamic
Standard Extensions	OID	Include	Critical	Value	

[32] See http://www.fineid.fi/vrk/fineid/files.nsf/files/24EA4C4CD4A1EAA0C2257054002A55BD/$file/S2v21.pdf

CertificatePolicies	{id-ce 32}	X	Non-critical	mandatory	
policyIdentifier	1.2.246.517.1.10.2	X		2.16.56.1.1.1.2.1	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt 1 }	X		CPS	Fixed
Qualifier		X		http://www.fineid.fi/vrk/fineid/home.nsf/Pages/8159D738E49D3251C2257054002D7EF4	Fixed
Qualified Certificate Statement					
qcStatement	{id-etsi-qcs 1 }	X	Non-critical	Mandatory, used in non-repudiation certificates id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }	
keyUsage	{id-ce 15}	X	critical	mandatory	
nonRepudiation				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	Non-critical	mandatory	
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	Non-critical	Mandatory	
distributionPoint					
FullName		X		http://proxy.fineid.fi/crl/vrktpc.crl	Fixed
NetscapeCertType		X	Non-critical	Usage of this extension in software products is discouraged.	
	2.16.840.1.113730.1.1			sMime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	Non-critical	Mandatory, OCSP-extension will be used in future when OCSP-services are available.	
accessMethod	{ id-ad-2 }	X		calssuers is currently only implemented extension.	
accessLocation		X		http://www.fineid.fi/vrk/fineid/home.nsf/suomi/ca-varmenteet – Points to RootSigned Governmen top root CA.	
accessMethod	{ id-ad-1 }	X			
accessLocation		X			

Technically the FINEID card has the capability to contain other applications which could be run within the card processor chip, e.g. for generating key pairs and using the private keys, but the FINEID specifications do not allow the use any additional applications. The FINEID card is thus “blocked” and even it is based on a multi-application Java platform, the FINEID applet performs only native card operations. No further multi-platform applications are being envisaged either and the FINEID card is not planned to be carrier of any other data. Only exception to this, are simple data objects permitting the use of some industry solutions for Windows login etc.

Since 31 March 2003 the VRK CA model is based on a common Root CA model where only the Root Certificate is self signed and other VRK CAs are signed by the VRK Root CA. The VRK Gov. Root CA has certified the private keys of the CAs in the government domain including the FINEID Citizen CA.

The reference certificates used in the Finnish FINEID card certificate hierarchy are published at the FINEID web site[33]. The FINEID certificate card contains the RootCA and CA certificates of the issuer, thus enabling an offline certificate validation performed on card. The VRK RootCA certificates are not included by default in commonly used internet browsers. For the online validation of electronic signatures created by means of the FINEID, Certificate Revocation Lists (CRLs) have to be used. The CRL distribution point full name is: http://proxy.fineid.fi/crl/vrkcqcc.crl.

Online Certificate Status Protocol (OCSP) responder services are not in use nor available for online certificate validity status check-up. OCSP services are not under development yet as the number of revoked FINEID certificates remains relatively small and CRL lists are manageable.

The VRK CA FINEID Certificate Policies and Certificate Practice Statements are published at:

http://www.fineid.fi/vrk/fineid/home.nsf/pages/8159D738E49D3251C2257054002D7EF4.

The FINEID specifications are published at:

http://www.fineid.fi/vrk/fineid/home.nsf/pages/1ABAB7CCA8D192DB C2257054002D8811.

Procedures have been put in place to suspend or revoke certificates when the FINEID card is lost or destroyed. The Revocation Service operates all day every day when calling from Finland or from abroad. There is also a text phone service available for those with impaired hearing. Information on the revocation service is available at:

http://www.fineid.fi/vrk/fineid/home.nsf/en/certificateinfo.

3.3.4 Organisational aspects

In practice, authentication services using the eID card implement the specific FINEID middleware provided by the PRC. The user then authenticates using a standard interface prompting for certificate PIN code, using a generic PC and generic card readers. The four number PIN-code is initialised randomly when the card is first issued, but can be changed at choice by the bearer.

In 2004 the Finnish Ministry of Finance introduced quality criteria for public online services and set goals to the creation of tools development of online services. The starting points of the quality criteria

[33] http://ldap.fineid.fi and

http://www.fineid.fi/vrk/fineid/home.nsf/pages/04D9D9BD86DF1D64C2257075002B1B3F

have been usability, effectiveness and high impact. A key enabler for achieving the quality criteria is the adoption of an online authentication service, available for all users and all eGovernment services. A centralized service called VETUMA for citizens' electronic identification has been implemented starting from 2004. The service can be attached to any eService provided by municipalities or state agencies and it provides authentic source user information from the Population Information System. The service offers both FINEID and TUPAS identification and authentication methods and it is designed to support also other available schemes, such as challenge-response authentication using mobile phone. The VETUMA system is Citizen-to-Administration service and it is designed for authentication and payment, although payment functionality is linked to TUPAS authentication only.

Personal and address data contained in the Population Information System is used for checking legal capacity, in government decision-making, address service, academic research, statistics, updating of customer registers, market research, opinion polls, direct advertising and judicial administration. Everyone has a right to forbid the disclosure of his or her personal information by the Population Information System for purposes such as direct advertising, market research, opinion polls, address service, genealogical research or public registers. Using the authentication functionality of the FINEID card, the holder can verify which data of his is stored in the Population Information System using the *Check Your Registered Data* -service[34]. Users cannot modify registered data, but can manage the level and content of personal information that can be disclosed to thirds.

As for the electronic identification of the businesses Tax authorities have implemented a centralized Business Identification System for the whole government.

With regard to authorisation/mandate management, the KATSO service offers a generic infrastructure that is in place already. It remains to be seen if the KATSO service evolves as a generic self-service authorisation and user account provisioning solution for eGovernment services at large.

3.4 Interoperability

As stated in the introduction above, the FINEID card and TUPAS paper tokens are issued to Finnish nationals and permanent residents. As official eID token, the FINEID card is a universal authentication token, whereas the TUPAS credentials and paper tokens require a customer relationship contract with at least one of the Finnish banks that support TUPAS.

There have been noteworthy advances in the mutual acceptance of the FINEID with Estonian eIDs and Austrian eIDs. Interoperability initiatives have been taken within the *Porvoo Group*.

The Finnish Population Register Centre has taken an active role in establishing and running of the Porvoo Group, which is an international cooperative network whose primary goal is to promote a trans-national, interoperable electronic identity, based on PKI technology (Public Key Infrastructure) and electronic ID cards, in order to help ensure secure public and private sector e-transactions in Europe. The Group also promotes the introduction of interoperable certificates and technical

[34] http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/ 5E429BC9918D72F2C225724600539D96

specifications, the mutual, cross-border acceptance of authentication mechanisms, as well as cross-border, on-line access to administrative services.

The founding meeting of the group took place in Porvoo, Finland in spring of 2002 during the international conference held in conjunction with the Public Identity Project of the Smart Card Charter operating under the eEurope 2002 initiative and supported by the IST programme.

3.5 eIDM Applications

This section will provide a short overview of key applications for the eIDM systems.

3.5.1 FINEID card applications

The "Palkka.fi" (or Salary.fi) is a service portal for employers to calculate wages and other regulatory payments. This service is accessed through the KATSO authentication service. (http://www.palkka.fi)

The Ministry of Labour job search, vocational training applications, on-line CV service is also accessed through the KATSO authentication service. (http://www.mol.fi)

The National Social Security services, KELA offers online services for unemployed, those on sick leave, family, housing and student allocations, and also querying about personal data records and applications. The services are accessed through either the KATSO authentication service (with regards to enterprises submitting pensions data) or through KELA's own authentication service. (http://www.kela.fi)

The Suomi.asiointi.fi, formerly Lomake.fi (or Application.fi) offers an applications online service for citizens, civil society and private organisations.

(http://www.suomi.fi/suomifi/suomi/asiointi_ja_lomakkeet/)

The Change of address notification service for citizens is offered by the PRC.

(http://www.muuttoilmoitus.fi)

The Työeläke.fi service offers personal data information service on work pensions to citizens. (http://www.tyoelake.fi)

The "Tarkista tietosi!", or "check your personal information" -service enables the verification and management of personal information collected by government officials into the Population Information System.

(http://www.vaestorekisterikeskus.fi)

Finnish private enterprises are eligible for research and development funding from TEKES, the Finnish Funding Agency for Technology and Innovation. (http://www.tekes.fi). TEKES provides the Tekes.fi service for the submission and handling of funding applications by using the FINEID card.

The National Board of Patents and Registration of Finland (http://www.prh.fi/en.html). The Patent registration service offers online services for applying for patents, verification of patents applications, trusted communications with patent officials and other information exchange. This eService is based on strong authentication (FINEID card) and is actually available only for contractual customers. The Company and Association registers use KATSO service because of large part of common company information is shared with the Tax Administration.

3.5.2 TUPAS paper token applications

As the TUPAS paper token is considered equal to the FINEID in terms of authentication, all the aforementioned services are equally accessible using TUPAS.

As indicated above, Finnish eGovernment services are strongly centred around TUPAS tokens, and FINEID cards remain either marginal or concentrated to only official use. The current eID cards could eventually become the standard for authentication services in Finnish eGovernment processes, but this could take a very long time and prior to that, the TUPAS tokens will most probably be changed into one-time-password generator tokens.

The Finnish government is looking at extending the use of the FINEID card, especially by encouraging the use of mobile phones with SIM-form factor platform, but until now the mobile FINEID has not been popular either, mainly because of a complex process when acquiring and costs.

3.6 Assessment

The Finnish approach has a number of advantages and disadvantages, which can be briefly summarised as follows.

3.6.1 Advantages:

- Government basic registers are comprehensive and widely used, which enables the effective use of authentic source information. The public administration is relatively well “connected” in terms of use of common and shared basic registers in their back-office processes. This is a strong advantage when building paperless processes to support public eServices.

- The FINUID electronic unique identifier mechanism is a very effective method for referencing identity information in electronic form without privacy risks that are of significant importance while using traditional SSN identifiers. The invention of the FINUID mechanism (sort of surrogate for the SSN) is an example of a good design at an early technology adoption phase, which has proven to be very mature.

- The popular TUPAS paper token eIDM system offers good capabilities for achieving reasonably well secured authentication and communication methods for both public and private services, with payment possibilities included. TUPAS system is very widely spread and accepted originating since about 15 years, thus bringing out a great number of potential eService users; almost 3 million in a population of 5 million.

- The VETUMA authentication service is available for all municipalities and until the end of 2007 it is fully financed by the State. As communal services are scattered into small service units, generic services for authentication bring true savings for the municipal eServices. Common services also enable higher interoperability between different organisations and systems.

- The KATSO service is a standard Liberty Alliance based identity management system that enables authorisation user self provisioning and de-provisioning functionalities. This is relatively new and advanced in eGovernment services and with time similar services will most likely be of use in all eGovernment applications.

3.6.2 Disadvantages:

- Non-existing use of FINEID cards. As identity card, the FINEID is not compulsory and replacing identifiers are abundant (driver's licence, passport). The historically well disseminated TUPAS bank ID tokens fulfil on their part the acute need to proof one's identity online. Besides authentication, TUPAS enables also payment functionality; all features that make TUPAS "too good" to be replaced by the FINEID card. Besides the card costs 40 euros and requires a card reader and some learning effort as to the installation and certificate usage.

- No decision to promote the FINEID. Only 150.000 FINEID cards have been issued since 1999 and no plans have been published on the promotion of the cards. Financially the qualified CA service running the FINEID is tremendously expensive if compared with the number of transactions conducted using FINEID. If online authentication service use grows using TUPAS only, the government will eventually pay more for not using the FINEID. The only way lower the per transaction price of the FINEID is to distribute cards to the population and start to promote the use of the cards, because it is the only transaction cost-free eIDM system for the government.

- Lack of attractive services. One can argue that FINEID services are not attractive, but in many cases most public services in general are relevant to the average citizen only once or twice a year. Some services are needed only once or twice in a lifetime. eServices would most probably benefit from an opening to service areas where authentic source information is needed but authentication or signatures are less. Trustworthy online transactions require strong authentication, but in many eCommerce or eHealth services strong anonymity is also

an advantage. The combination of reliable identification combined with anonymity could salvage a good number of eService scenarios for the FINEID.

Public acceptance for the FINEID is not strong and the government is not drawing all the conclusions, this implies with regards to trustworthy eServices based on universal authentication. The national knowledge society strategy focuses mainly on the promotion of easily acceptable and accessible eServices, not to complex or structural changes in the provision of the eServices. This means services where FINEID based strong authentication is not a priority ignoring also at the same time need for digital signatures. Meanwhile the FINEID system is a robust security mechanism that is difficult on reconcile with requirements for flexible and simple authentication techniques. Obviously both the public perception of service accessibility (i.e. ease of use) needs to evolve a little, but also the FINEID needs to be more at pace with actual needs and expectations. The FINEID security design is state-of-the art, but more flexibility could prove crucial for a wider acceptance, especially among SMEs and later among ordinary citizens.