Open Smart Card Infrastructure for Europe

v2

Volume 4: **Public Electronic Identity, Electronic Signature and PKI**

Part 1: **Electronic Identity Whitepaper**

Authors: **eESC TB1 Public Identity**

EDITED BY: ARTTIC

FOR LIST OF MAJOR CONTRIBUTORS SEE ANNEX C

Table of Contents

Introduction

About electronic identity (e-ID)

When citizens are travelling from their country to another, they carry a passport. The passport's purpose is to identify the citizen and his/her country of origin.

Now citizens can use Electronic Identity when moving from one country to another, city to city, or even from one house to another in the world of computer networks. In the future more and more citizens will use Electronic Identity while making transactions in the networks. This has become possible because Electronic Identity provides reliable identification, authentication and electronic signature to be used in a distributed network interaction.

The purpose of the Electronic Identity is to make easy and secure transactions possible in the information networks. We can make the same business e.g. on the Internet that we used to make face-to-face prior to Information Society. We can now also make business and trust our partners in a network environment where we meet each other for the first time as we enter into transactions over actually long distances.

Governments are changing the way they work. Now governments are offering citizens a complementary way to interact with administrations in computer networks. Electronic Identity is a convenient and secure way for everybody to have access to the information and services from government to citizen.

White Paper

The White Paper on Electronic Identity aims at bringing to the interested parties a set of useful information on issues that are vital when starting to plan and implement e-ID systems based on Public Key Infrastructure (PKI). It can help and shorten the long path within a world of complicated international standards without forgetting that every country has a legislation of its own.

Besides semi-technical issues and international standards the White Paper is taking full notice of the Directive 1999/93/EC for electronic signatures. As the European Union has an advanced regulatory framework for data protection which determines the implementation of e-ID in the Member States, legal issues in relation to the use of e-ID are covered in the White Paper.

Technology is ripe and ready for use, but the practices and references are fragmented. It is necessary to bring together and distribute **minimum requirements** of e-ID because this will help to implement cross border interoperable solutions.

Although the minimum requirements given in the White Paper are independent from a specific e-ID scheme, background information on current practices in establishing identity in EU member states and on the status of e-ID card implementations is given to provide the reader with a more complete picture.

Furthermore some important aspects related to the implementation of e-ID systems are introduced, such as privacy, the use of biometrics and the technical framework proposed by the eEurope Smart Card Charter to support cross-border interoperability of national e-ID systems.

Applicability

The White Paper on Electronic Identity is applicable to Electronic Public Identity for which it presents requirements and specifications. The White Paper targets people and organisations concerned by e-ID related matters, for example Certification Authorities

(CA), Software vendors, Policy makers, Governments, or e-ID service providers. Specifications have been addressed to the third party (the public officials or other organisations), which have legal authorization by law of the issuing Member State to grant Electronic Identity cards/certificates for natural person.

Status of version 0.6

This present issue of the White Paper should not be considered as a final version, its content is open for discussion. E-ID deployment is still in an early stage: there are only a few member states that have actually introduced e-ID card schemes, feedback from deployment projects and interoperability pilots (such as the IST project eEpoch) needs to be taken into account and the White Paper updated accordingly to ensure that it is suitable for adoption by the different EU member states as regards their local specificities.

Relation with eEurope 2002

The White Paper is the result of the work carried out in the framework of eEurope Smart Cards by Trailblazer 1 "Public Identity".

The primary objective of Trailblazer 1 is to establish minimum requirements for e-ID which provides identification, authentication and electronic signature to be used in a distributed network interaction.

The benefits of the establishment of such minimum requirements will be

- an important step towards e-government in the European member states

- increased trust and confidence via enhanced data security

- promotion of European commerce and online transactions

The goals are:

- To establish minimum requirements for electronic identity. On the basis of these requirements participating member states can recognize the electronic identity issued in other member states.

- The aim is to bring out recommendation on how this should be done.

- To build a starting point for interoperable Electronic Identity.

The Electronic Identity token is not so much a replacement of the physical document as an addition. It is a token for an electronic environment as opposed to the traditional document for the physical environment.

The Electronic Identity Token is defined as an identity token accepted by public authorities in the country where it is issued. The compliant token should be accepted in all countries that issue similar tokens.
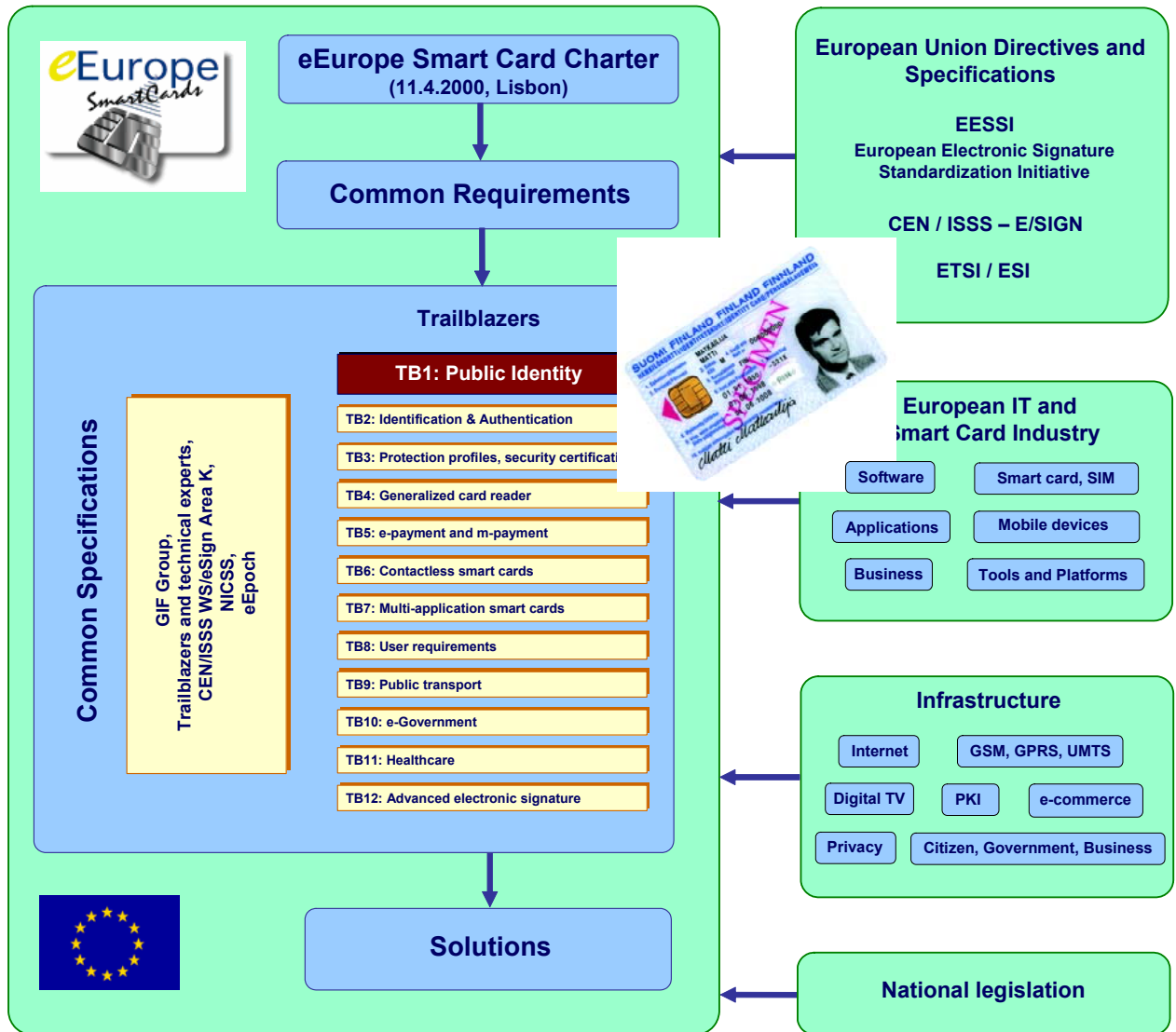
Overview of current activities of Electronic Signature Directive Implementation –

the role of Smart Cards in Public Identity

Part I:

Minimum requirements for a European Electronic Identity

- The Smart Card as an Electronic Identity Token

- Requirements for the Issuing of e-ID Cards

- Requirements on the Supporting PKI

- The Data Content of Certificates

1. Part I: Minimum requirements for a European Electronic Identity

1.1 The Smart Card as an Electronic Identity Token

1.1.1 Smart Cards and PKI – natural choice

Within the context of the eEurope Smart Card Charter, a natural choice for the platform of the Electronic Identity Token is the smart card, although other platforms can be envisaged for the future. Furthermore, in order to provide the required services, another natural choice is to base the Electronic Identity Token concept on the use of asymmetric cryptography and Public Key Infrastructure (PKI).

The primary function of the smart card as an Electronic Identity Token is to contain sufficient number (two or more) of private keys for the card holder and to protect these keys against misuse of others. This is achieved by the hardware and software security features of the smart card, and the requirement for entering an authentication code (PIN and/or biometrics) before allowing the use of the private key(s).

The identification of the card holder is achieved with the use of PKI-based electronic certificates which bound the corresponding public key(s) with personal data or other information (e.g. a 'pseudonym') which can be used to identify (directly or indirectly) his/her identity. The certificate is thus the actual digital counterpart of the visual identity document. For authentication purposes, the smart card just enables the card holder to prove that he/she is the person whose identity is stated in the certificate, since the smart card contains the private key corresponding to the unique public key of the certificate, and this private key only can be used by the card holder. Before the certification process, the identity of the card holder, and thus the one-to-one correspondence between the card holder and his/her public key, has visually been checked by CA (or RA). The certificate can be compared to a visual identity document, where the card holder proves his identity by showing that his face corresponds to the photo on the visual identity document.

For qualified electronic signatures, where a non-repudiation service is required, the signature can be verified using the public key of the certificate. Since the corresponding private key is held in the smart card under the sole control of the card holder, the card holder will not be able to repudiate his signature, even after the expiration of its certificates (long-time validation), especially if some supplementary measures have been taken (e.g. a timestamp or a notary/storage service).

For practical purposes, the certificates corresponding to the private keys are also stored in the smart card, although this is not in theory required. However, it enables applications to retrieve and distribute the corresponding certificates easily.

1.1.2 Definition of the Electronic Identity Card

In the context of this document, we are therefore defining the term Electronic Identity Card as follows:

Electronic Identity Card (e-ID-card): A smart card based token, containing private keys and corresponding public key certificates. Optionally, the card may also incorporate a visual identity document.

The purpose is to define a set of common requirements, for a PKI-based Electronic Identity token, based on a Smart Card and digital certificates (e-ID-card) that is accepted by authorities in the country where it is issued or could be of use for others to follow.

The e-ID-card can be used by a citizen

- for electronic identification and authentication to public and private on-line services

- for qualified electronic signatures conforming to the EU directive

- optionally for confidentiality services, enabling encryption of data transmitted over a network

- optionally as an official travel document within the EU. However, this requires that the smart card based Electronic Identity token also contains a visual identity document. (Note: although not further developed hereafter, because not within the focus of this White Paper, a requirements specification dedicated to "visual ID used as travel document on smart card" has been produced. It can be found on the e-ID website www.electronic-identity.org or the eESC documentation, available on the eESC CD Rom).

The e-ID-Card could be used for many different fields of application, like health insurance, social security, public transport, or financial transactions. Additional data or applications may be stored in the on-board memory of the card. These data or applications may support international interoperability like travel document or be country-specific or they may be chosen by the card holder (citizen).

1.2 Requirements for the Issuing of e-ID-Cards

1.2.1 Organization issuing e-ID-cards

The e-ID-card consists of a smart card, and contains private keys and certificates, issued by a Certificate Authority (CA). In the case of the e-ID-card, the "card issuer" and the CA can be different (outsourced) organization. It is especially important to observe if the e-ID-card also contains a visual identity document on its surface. The visual identity information and the certificate identity information must not be in conflict with each other. To carry out this the "card issuer" and the CA (Certificate Authority), SHOULD be supported by a common RA (Registration Authority) who should be responsible for identifying the card holder before the issuing of the card and the certificates (according to GIF the 'ultimate' responsibility is with the Card issuer who may subcontract CA and RA functionality). The liabilities of and between different parties should be defined according to the national legislation of the MS (Member State).

1.2.2 E-ID-cards and Qualified Certificates

One basic requirement for Issuers of e-ID-cards is that the certificate(s) supporting the 'qualified electronic signature' (non-repudiation) created within/by each e-ID-card must be issued as Qualified Certificates in the sense of the EU directive. This in turn means that the Issuer MUST comply with the ETSI Qualified Certificate Policy "QCP public + SSCD" (Secure Signature-Creation Device, specified in ETSI document TS 101 456) which is a certificate policy for qualified certificates issued to the public, requiring use of SSCD. For this reason the issued smart card SHOULD be evaluated and certified as a secure signature-creation device in the sense of the EU directive.

ETSI TS 101 456 contains all the requirements for an issuer of qualified certificates, defined in a technology-neutral way, regardless of the implementation platform. The rest of this chapter therefore only repeats some of these requirements, and details them further where needed for the specific case of using an e-ID-card.

ETSI TS 101 456 contains all the requirements for an issuer of qualified certificates, defined in a technology-neutral way, regardless of the implementation platform. The rest of this chapter therefore only repeats some of these requirements, and details them further where needed for the specific case of using an e-ID-card.

1.2.3 Registration procedures

The Registration Authority (RA) is responsible for identifying the candidate card holder before it commands the issuing of the card and of the certificates.

The RA shall verify by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person directly.

1.2.4 Information content of a certificate

The certificates used in e-ID-cards contain the name of the Certification Authority issuing the certificate, the name of the certificate holder, the unique identifier of the certificate holder, the period of validity of the certificate, the serial number of the certificate, information on the certificate policy used, the purpose of the certificate and other technical information necessary for the use of the certificates. The information on the certificates and their correctness is confirmed with the digital signature of the Certificate Authority.

A detailed definition of minimum certificate data content can be found in chapter 4 "The data content of certificates".

1.2.5   Liability of the Certificate Authority

The CA has to ensure that the certificates have been created by using the procedures required by regulatory authority (DIRECTIVE 1999/93/EC on a Community framework for electronic signatures, item 11) and defined in the certificate policy and presented in its certification practice statement, and the card issuer that the e-ID-card has been prepared and personalized according to specifications. The CA is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate. Liabilities concerning the optional visual identity document on the e-ID-card shall be set according to the national legislation of the MS.

1.2.6   Responsibility for protecting the e-ID-card

The card holder has to take care of his e-ID-card in accordance with the Terms of Use stipulated in the contract between the card holder and the Issuer. The e-ID-card has to be protected so that it does not fall into the hands of outsiders, it is not altered or that it is not used without permission.

The e-ID-card and the PIN codes relating to it shall be stored by the card holder or according to national legislation. The card holder should store his e-ID-card and the PIN codes relating to it so that they are not disclosed to outsiders. The personal PIN codes should not be stored in the same place as the e-ID-card.

1.2.7   Other applications on an e-ID-card

Upon the request of the card holder, applications or information relating to different purposes of use may be stored in the vacant memory space of the card, if it is allowed by the issuer. Downloading and storage of additional applications should be protected by a PIN (and/or biometrics) code. It is recommended to use separate PIN for different applications. Placing of additional applications on an e-ID-card and the termination of the use of the applications is something between the card holder and the service provider, which is not within the scope of this document.

1.2.8   Renewal of an e-ID-card

The e-ID-card and the certificates it contains must have a certain validity period defined by the issuer. It is strongly recommended that the validity period of the card and its certificates are the same. Renewal of the certificates is accomplished according to the national legislation.

The e-ID-card shall be renewed by a proper and secure procedure. If there are other applications on an e-ID-card, the applicant himself is responsible for moving the other applications onto the new card when a card is renewed.

1.2.9   Prevention of the use of an e-ID-card and its certificates

Primarily the card holder himself decides how and when he wants to prevent the use of the card, e.g. if the card is lost, or prior to the termination of its validity. The use of an e-ID-card and its certificates can be prevented upon notification by the card holder. The certificates on e-ID-card can be entered in the revocation list so that the use of certificates relating to electronic communication and granted by the issuer is prevented.

1.2.10   Cancellation of an e-ID-card

Cancellation of an e-ID-card shall result in revocation of all known certificates. The card itself is NOT necessarily cancelled.

1.3 The requirements on the supporting PKI

The purpose of the e-ID-card is to provide a mechanism for public administrations and private entities to identify and authenticate the card holder in electronic communication. The entity relying on a certificate for such purposes is usually called a "relying party".

In order for the relying party to be able to trust and rely on the certificate, two areas have to be considered:

- The relying party must be able to judge the trustworthiness of the certificate issuer. This is covered by the requirements on the issuance of certificates and e-ID-cards in chapter 2.2.

- The relying party must be able to obtain all the information needed for the validation of the certificate and any information based on the certificate, such as an electronic signature. This is provided by the supporting PKI, and the subject of the present chapter.

Guidance for relying parties for the verification of electronic signatures can be found in CWA 14171: "Procedures for electronic signature verification". This chapter takes a somewhat reversed perspective, and tries to state the requirements from relying party on the supporting PKI provided by the Issuer of the e-ID-card and other components.

1.3.1 Obtaining and reading the certificate

In order to verify a certificate, it must of course first be obtained. Application of the card must therefore be able to read out the certificate from the e-ID-card and submit it to the relying party as part of the transmission protocol or data format.

The relying party software must then be able to read and interpret from the certificate all fields that are defined in "The data contents of certificates" in chapter 2.4 of this document.

1.3.2 Obtaining and protecting the CA certificate

The first step of certificate validation is to validate the certificate using the public key of the CA. In order to do this in a reliable way, the CA must provide a secure channel for distributing its CA and Root certificates to relying parties. It should be possible to verify the hash value of the root certificate at a secure web site of the CA.

The relying party software must also have a secure storage for the CA/Root certificates, protecting its integrity.

1.3.3 Obtaining certificate status information

The next step of certificate validation is to ensure that the certificate has not been revoked. It is therefore mandatory for the CA to provide a reliable and easily accessible service for obtaining or checking the status of certificates. The CA may issue CRL at regular intervals, or it may provide an OCSP service, providing on-line certificate status information.

1.4   The data content of certificates

In order to ensure interoperability between different issuers of e-ID-cards and their relying parties, it is imperative that issued certificates are harmonized to a certain extent. It is not necessary that all certificates contain the same information content. However, minimum data content needs to be defined, which MUST be followed by all complying issuers, and which MUST be supported by all complying applications.

The minimum data content defined below is based on PKIX RFC 3280 and RFC 3039. Furthermore, several national and international proposed certificate profiles have been taken into account.

1.4.1   Mandatory fields in the signature certificate (non repudiation)

Field	Criticality	Type/Value	Description
Certificate*			
signatureAlgorithm algorithmIdentifier		OID** (1.2.840.113549.1.1.5)	This field contains the identifier for the cryptographic algorithm used by the CA to sign the certificate. This field MUST contain the same algorithm identifier as the signature field.
signatureValue		BIT STRING	This field contains a digital signature computed upon the tbsCertificate. The tbsCertificate is used as the input to the signature function.
tbsCertificate		SEQUENCE	
TBSCertificate			
version		INTEGER	Only version 3 certificates shall be used, integer value is "2".
serialNumber		INTEGER	All certificates issued by one CA must have a unique serial number.
signature		OID (1.2.840.113549.1.1.5)	Contains the algorithm identifier for the algorithm used by the CA to sign the certificate.
issuer		Name (RDNSequences)	The issuer field identifies the entity that has signed and issued the certificate. RDNSequence consists of attribute type (OID) and value (String).
countryName		OID (2.5.4.6)*** Printable String	Country where the CA is operating.
organizationName		OID (2.5.4.10) UTF8String****	An informative unique name of the issuing organization.
commonName		OID (2.5.4.3)	An informative unique (inside organization) name of the CA. Useful if the CA issues

		UTF8String	certificates for different purposes (citizens, employees etc.).
validity notBefore notAfter		YYMMDDhhmmssZ (UTCTime)	The field is represented as a sequence of two dates: the date on which the certificate validity period begins (notBefore) and the date on which the certificate validity period ends (notAfter). Both notBefore and notAfter may be encoded as UTCTime or GeneralizedTime. CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime.
subject		Name (RDNSequences)	The subject field identifies the entity associated with the public key stored in the subject public key field. The subject field SHALL contain an appropriate subset of the following attributes:
countryName		OID (2.5.4.6) PrintableString	This **mandatory** field specifies a general context in which other attributes are to be understood. The country does not necessarily indicate the subject's country of citizenship or country of residence, nor does it have to indicate the country of issuance.
serialNumber		OID (2.5.4.5) UTF8String	The **mandatory** serialNumber field is used to differentiate between names where the subject field would otherwise be identical. It may contain a number or code assigned by the CA or an identifier assigned by a government or civil authority. It is the CA's responsibility to ensure that the serialNumber is sufficient to resolve any subject name collisions.
			Additionally, the subject field SHALL include at least commonName field or givenName field, or optionally both.
commonName		OID (2.5.4.3) UTF8String	A common name is a (possibly ambiguous) name by which the object is commonly know in some limited scope and conforms to the naming conventions of the country or culture with which it is associated.
givenName		OID (2.5.4.42) UTF8String	Contains the registered given name of the subject, in accordance with the laws under which the CA prepares the certificate.
			Other attributes may be present in the subject field.

subjectPublicKeyInfo
 	
  algorithm
 	
  subjectPublicKey
		OID
		
		BIT STRING
			Contains the public key and identifies the algorithm with which the key is used.

Extensions:			
keyUsage	C	BIT STRING	This extension defines the purpose (non repudiation) and the permitted uses of the key contained in the certificate.

certificatePolicies
 	
  policyIdentifier
 	
  policyQualifiers
	NC	BIT STRING
		
		OID
		
		URL
			This field lists certificate policies, recognized by the issuing CA, that apply to the certificate, together with mandary qualifier information containing a URL to the CPS.

authorityKeyIdentifier	NC	BIT STRING	This extension contains the Key Identifier of the issuing CA.
subjectKeyIdentifier	NC	BIT STRING	This extension contains the Key Identifier, which provides a means for identifying certificates containing the particular public key used in an application.
			Additionally, the extensions field SHALL include cRLDistributionPoints extension or authorityInfoAccess extension, or optionally both.
cRLDistributionPoints distributionPoint	NC	BIT STRING URI	This extension identifies how CRL information is obtained. Contains a uniform resource identifier (URI) pointing to the appropriate CRL for this certificate.

authorityInfoAccess
 	
  accessMethod
 	
  accessLocation
	NC	OID
		
		GeneralName
			This extension indicates how to access CA information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and CA policy data. (The location of CRLs is not specified in this extension; that information is provided by the cRLDistributionPoints extension.)

			Optionally, the extensions field MAY include qcStatements extension, and it is RECOMMENDED to be used, if applicable to the issuing CA.
qcStatements statementId	NC	OID	This field defines an extension for inclusion of defined statements related to Qualified Certificates. A typical statement suitable for inclusion in this extension MAY be a statement by the issuer that the certificate is issued as a Qualified Certificate in accordance with a particular legal system.

* For further details about certificate data content read RFC 3280 and RFC 3039.

** Further information about algorithm identifiers:
http://www.alvestrand.no/objectid/1.2.840.113549.1.1.html

*** Further information about X.500 attribute types:
http://www.alvestrand.no/objectid/2.5.4.html

**** According to RFC 3280 the UTF8String encoding is the preferred encoding, and all certificates issued after December 31, 2003 MUST use the UTF8String encoding of DirectoryString.

1.4.2   Mandatory fields in other end user certificates

The data content of other end user certificates is otherwise the same excluding these exceptions:

- The keyUsage MUST NOT be nonRepudiation

- The qcStatements extension MUST NOT be used.

It is also recommended to include the commonName attribute in the subject field, at least in the authentication certificate, because many client implementations presuppose the presence of the commonName attribute value in the subject field and use this value to display the subject's name regardless of present givenName or surname attribute values.

1.4.3   Keys and certificates

The e-ID-card must contain at least two separate keys and certificates, where one key pair is used for authentication and, possibly, for encipherment, and a second separate key pair only for the creation of 'qualified electronic signatures' (non repudiation). However, a three key pair e-ID-card (where the third key pair is used exclusively for encipherment) is also perfectly valid, and complying applications shall be able to handle such cards. The key length for end user keys is 1024 bits, though this may change in near future.

Certificate and key number	Certificate label (example)	X.509 key usage
1	'authentication [and encipherment certificate]'	digitalSignature + [keyEncipherment + dataEncipherment]
2	'signature certificate'	nonRepudiation

The "signature certificate" (non repudiation) shall be a 'qualified certificate'.

In addition, a CA certificate and a Root certificate (key lengths 2048 bit) may be stored on the e-ID-card. They can be used as a starting point of trust for the card holder.

Part II:

Current Practices in Establishing Identity

- Establishing Identity

- Documents used for Identification

- Identification when applying for an ID Document

- Identification when the ID Document is delivered

- National Legislation on ID Documents

- National Data Protection legislation

- The Present PKI-based e-ID Situation in the European Union

2. Part II: Current Practices in Establishing Identity

2.1 Introduction

This section consists of results of enquiries made on identity in member states; establishment of identity, how the identification is done on applying and on delivery for an ID document, national legislation on ID documents and data protection.

Establishing identity is quite comparable in all countries. It is done through registering government or municipal authorities. The practices vary slightly from one country to another. In only few countries there is a single ID number established that is used in identification documents. Applying for an ID document and its delivery vary and it is done in municipality and other authorities offices.

The enquiries from 16 January 2001 and 16 March 2001 have been supplemented by information taken out from the following documents:

- "e-ID of citizens and organisations in the European Union: State of Affairs", A report drawn up by Dr Jean-Michel Eymeri, Senior Lecturer at European Institute of Public Administration, Maastricht (NL) for the 37th Meeting of the Directors-General of the Public Service of the Member States of the European Union Bruges, 26 and 27 November 2001
- "IPSE-SG Final Report 1", A report drawn up by Initiative for Privacy Standardization in Europe (IPSE) and issued on 13 February 2002
- "eESCC TB2 Pre-Inventory", A report drawn up by TB2 of Smart Card Charter and issued in November 2001
- "Survey of Smart card-PKI projects", A report drawn up by EDS and Smart is Marketing for IDA and TB10 "e-government", issued on 10 July 2002; the review done by TB10 is completing this document.

No information on laws on digital signature has been provided in this document since comprehensive studies already exist and are broadly available on the web such as:

- Digital Signature Law Survey by Simone van der Hof from the Tilburg University in the Netherlands at http://rechten.kub.nl/simone/ds-lawsu.htm

2.1.1 Establishing identity

What are the practices in establishing identity (e.g. registration of a newborn child)?

Austria

The identity of the child is based on:

- Personal appearance of parents and

- Hierarchical deduction from the parents' birth certificate.

Identity, e.g. of a new child, is established at the Register Office of the district.

There is no ID number, but every person working in Austria has a social security number. There is however a project running for establishing a Central Register with a single ID number.

Belgium

The identity of the child is based on:

- The birth certificate of the child

- Submitted physically by one of the parents together with identity card of both parents.

Identity, e.g. of a new child, is established at the Population office of the municipality. The municipality registers all relevant data in the master database of the National Register and - when accepted - copies this information into its own population register.

There is a general single ID number allocated at registration phase by the National register to all persons residing in Belgium.

Denmark

The Danish Civil Registration System (CPS) is managed by the Ministry of Interior Affairs and Health's Central Office of Civil Registration (the CPR-Office), in cooperation with the municipalities.

There is a single ID number, the civil registry number, allocated by the Ministry of Interior to all persons born in Denmark as well as to persons who have their tax affairs handled in Denmark.

Finland

When a child is born it is appraised to District Register Office or directly entered into Population Information System. Then a new identity number and the relation information to parents are established. Given names must be appraised latest in two months. Foreigners residing in Finland have to report personally to District Register Office and present authentic identification documents.

France

For establishing the identity of a child, a certificate of birth must be presented at the municipality office, together with an ID and a wedding-book.

The municipality registers all relevant data in its municipal database, and then proceeds with the update of the wedding book after signature of official registry of birth.

There is an ID number allocated at birth to all persons born in France by the National Institute for Statistics and Economic Studies. De facto, it is however only used in the social security field and is not on the national identity card.

Germany

When a child is born, the responsible hospital certifies the birth (no official document). When the child is born at the parents' home, the responsible doctor certifies the birth.

The parents present this document at the civil registry office where the official birth certificate is issued and the family register ("Stammbuch") is updated.

There is no single ID number and it is even prohibited for an administration to allocate an ID number which could facilitate putting together personal data from different registers.

Greece

There is no single ID number, but many sector-related ones. There is an intention to unify them, but no detailed plans yet.

The identity card is issued by the Ministry of Public Order (Police Offices) to all citizens over the age of 12.

Ireland

A birth is registered by personal attendance of a qualified informant at the office of the registrar. The registrar enters the relevant particulars in manuscript in his/her register and both the informant and the registrar sign the entry.

There is no single ID number. However, the plans are to introduce the Personal Public Service Number (PPSN) for facilitating exchange of information with the administration. A new civil registration system is under development.

Israel

Each child's details (including given name, if it is known at this stage) are registered on a special form supplied to all hospitals by the Ministry of the Interior.

Each form has a unique number, which then becomes the Identification (ID) number of that person, a number that will be "attached" to him for the rest of his life.

The identity is established through the child's parents.

Italy

There is a single ID number allocated by the municipality to all residents and managed by the Ministry of Finance.

Luxembourg

There is a single ID number allocated by the State Information Technology Centre to each resident in Luxembourg. This Centre also manages the data of the general directory.

Netherlands

One of the parents goes to the Municipality of the town where the parent lives and declares that he has a newborn. In a later stage the Municipality checks with the hospital if the event did occurred.

There are two national ID numbers: the administration number (A-number) and the social-fiscal number (SOFI number).

The A-number is allocated by the municipality to all persons born in the Netherlands, if their parents are registered in the GBA (Municipal Personal Record Database), and the people who have immigrate in the Netherlands. The municipalities manage their own database.

The SOFI number is allocated to all people liable to pay tax in the Netherlands and people insured under the social security system. It is automatically allocated upon registration in the database of the tax authorities (birth, entry into the country, commencement of tax liability).

Norway

The hospital reports the birth to the Population Register, located at the Tax Office, which issues a temporary public ID and sends it to the hospital. A final and lifelong ID is issued to the child approximately one month after the birth (see http://www.uib.no/mfr/hjorne.html English section). The Public ID is an 11-digit number, unique for each citizen, and contains information about date of birth and sex.

Portugal

There is no single ID number, but several and amongst which the one allocated by the Ministry of Justice to all Portuguese citizens at birth, irrespective of their place of birth, and naturalised citizens. The Institute for Information Technology in Justice (ITIJ) is managing the database.

Spain

A birth is registered in the National Civil Register with an ad hoc form filled out by the child representative (e.g. parents) and by the doctor that attended the childbirth.

There is a single ID number allocated by the Ministry of Interior (Police department) when issuing the first National Identity card (DNI). This can be done at parent request, but becomes compulsory over the age of 14.

Foreign citizens living in Spain are given a foreign ID number (NIE).

Sweden

A single ID number is given by the National Tax Board - which is responsible for the population register – at birth to all children of residents and migrant workers after their first year of residence in Sweden.

The same authority handles the numbers for immigrants.

United Kingdom

The parent(s) of a newborn child have a legal obligation to register their child within 6 weeks of the birth. The details are presented to the local District Registrar of births, marriages and deaths. The Registrar records the child's name, gender, place, date and time of birth, parent's details etc. and a certificate is presented to the parent(s). No identity number is allocated. No documentary evidence is required to be submitted by parents.

There is no single ID number, but a variety of them, whose the most important one is the National Insurance Number used for benefit and taxation purpose. The national health insurance card where the number is mentioned is not an identity card.

2.1.2   Documents used for identification

What are the documents used for identification purposes?

Austria

The documents in use are
- The paper birth certificate (for governmental usage),
- The passport or identity cards (for common usage).

Applying for and using a passport is entirely up to the citizen. Applying for and using an electronic signature will also be entirely up to the citizen.

Belgium

The documents in use are
- The identity cards or the passport
- The driving licence
- The social identity card (SIS) which includes the personal ID number

Applying for and using a passport is entirely up to the citizen.

The electronic signature function of the ID card will automatically be delivered to the citizens by the delivery of a new Electronic Identity Card (under pilot phase with 11 municipalities in 2003).

Denmark

The documents in use are

- The identity cards introduced in 1968, mainly as a document providing the personal number, the identity card has become obsolete years ago and cannot be used as identification since address and name are not updated on a current basis. The name 'personal identity card' was even abolished in August 1995. The citizen will still be notified in writing by the CRS of any new identification number (naming infants, immigration and change of identification number (in case of error in sex and/or date of birth)).

- The passport and the driving licence issued by the police

- The health insurance card issued by the 14 Danish Counties includes also the personal ID number

At the moment, there are no plans regarding public electronic identity.

Finland

The ID documents issued by the Police, i.e.

- ID card,

- Passport,

- Driving licence.

The social security card with a photo is also considered as a valid ID.

France

Two official documents which are considered valid ID documents are

- The national Passport

- The national ID card.

For foreigners residing in France, the stay/working permit (similar to National ID) is considered as the valid ID document.

At the moment, there are no plans regarding public electronic identity.

Germany

Any official document, but the most popular document is the identity card.

At the moment, there are no plans regarding public electronic identity, even if there are projects for introducing the electronic signature and appropriate certification infrastructure. This should allow identification on a voluntary basis.

Greece

The main document in use both in public and private sphere is the identity card.

At the moment, there are no plans regarding public electronic identity.

Ireland

Birth certificate, passport, driver licence.

At the moment, there are no plans regarding identity card and public electronic identity. There is however plans for issuing smart cards for facilitating electronic exchange of information with the administration.

Israel

ID card, National Passport, special ID for foreign workers

Italy

The main official documents are

- The national ID card
- The national Passport

There are pilot projects for a multi-functional electronic identity card.

Luxembourg

At the moment, there are no concrete plans regarding public electronic identity, but studies are ongoing in this respect.

Netherlands

The documents in use are

- Travel documents (Passport and ID-card (NIK))
- Documents for aliens according to the "Vreemdelingenwet"

There are projects for electronic identity cards to be used as a travel document and for authentication and electronic signature.

Norway

The ID documents issued by the Police (all these have a photo), i.e.

- Passport,
- Driving licence, if issued after spring 1989,
- Military ID card
- Travel documents for refugees and ID card for asylum seekers
- Bankcard (with a photo)
- Postal Service ID card.

Not approved ID-documents, but widely used for some purposes:

- Student card and secondary school ID card
- Compulsory military service ID document
- Buss and train companies ID card

Portugal

The documents in use are

- The national identity cards or the passport

There is an action plan under preparation, leading to a "Common Citizen Electronic Card".

Spain

Two official documents are issued by the Police

- The national ID card (travel document between the European countries),
- The national Passport.

There are also other administrative non-general documents such as health services, social security etc.

There is a project for electronic identity cards to be used as a travel document and for authentication and electronic signature.

Sweden

The main official documents are

- Paper based certificate from the Taxation authority

- Some official documents which include the civil number (passport, driver license, voluntary ID Card and Electronic ID Card based on the Swedish SIS standard).

Electronic identity cards are already in use on a voluntary basis. There are however no plans to introduce an official identity card in the near future.

United Kingdom

The two most frequently used forms of identity (in the absence of an official ID card) are the:

- Passport (issued by the UK Passport Service (UKPS)) to UK nationals

- Driving licence (issued by the Driver and Vehicle Licensing Agency (DVLA) to anyone who can meet the minimum age and health requirements, regardless of nationality).

There are many other forms of identity used including birth certificates, students' cards, pension books, pensioners' bus passes but these are not considered to be as secure as driving licences and passports.

The UK government is currently running a public consultation on identity cards (referred to as entitlement cards). Views are sought on whether:

- The UK should introduce a form of identity card;

- It should be voluntary or compulsory;

- It should be a smart card;

- Biometrics should be used to prove unique identity.

The consultation document can be viewed at:

http://www.homeoffice.gov.uk/dob/ecu.htm

Digital certificates can be obtained on a voluntary basis for administrative electronic transactions through the Government Gateway but these are not widely used at present.

2.1.3   Identification when applying for an ID document

How will a person be identified when he/she applies for an ID document?

Austria

Application for an ID document is made at the Register Office of the district.

Personal appearance and previously issued documents are required.

Belgium

The municipality is inviting the person to replace/renew his/her old Identity card. Request for replacing a lost identity card is also made at the municipality of residence.

The person has to physically apply for an ID document from the Population office of the municipality. The basis for obtaining a new ID document or replacing an old one is an existing other ID document.

Denmark

No ID cards are in use

Finland

According to Finnish law ID can be issued if identity has been authentically discovered. If it is ID card with certificate the applicant must be physically present.

France

The delivery of the ID document is managed by the municipality.

The basis for obtaining a new ID document or replacing an old one is an existing other ID document, complemented with copies of "certificate of birth" of the person and the "wedding book" of his/her parents.

Germany

When applying for the identity card, the citizen has to present the official register and the birth certificate.

He is allowed to sign his application for himself, i.e. his parents do not have to sign.

Greece

No information provided

Ireland

When applying for a passport,

- A birth certificate must be supplied with the required documentation and
- A set of photographs which must be countersigned, in the presence of the person making the application, by a member of the police force.

Israel

An identifying document with a picture must be presented.

Italy

No information provided

Luxembourg

No information provided

Netherlands

An ID-document will be issued when a person exchanges his/her old ID-document, or when he/she has no ID-document, e.g. because the identity is being established. This is done with a check in the GBA.

Norway

The application for passport and driving licence is made personally at a local police office (normally in the municipality you live).

Drivers licence are requested at the Public road administration, Military ID card at the Military authorities, Bank card with photo, at the local bank (a "de facto" Norwegian standard), Postal Service ID card at the local post office, Travel documents for refugees and ID card for asylum seekers at their respective government agency.

Portugal

No information provided

Spain

The delivery of the ID document is managed by the Police.

The basis for obtaining a new ID document is the copy of the person's birth certificate and the "wedding book" of their parents.

Sweden

When applying for the ID document

- The paper based certificate from Taxation authority,

- A photo,

- An handwritten signature and physical appearance

There are additional needs for people applying first time.

United Kingdom

Passports. Most applications are made via the post direct to passport offices but personal applications are accepted at local offices. Some choose to make the applications at a post office that operates an application checking service. Passports are issued upon production of evidence of identity and nationality such as a birth certificate and a photograph, which is countersigned by a responsible person (such as doctor, magistrate etc.) who must have known the person for at least two years.

Driving licences. Most applications via the post but some choose to route their applications via a post office or a DVLA local office that will check the documentary evidence submitted (passport etc). If an applicant holds a passport, this can be submitted as proof of identity without further checks. If no passport is held, DVLA follows the same procedure as UKPS – birth certificate and countersigned photograph.

2.1.4 Identification when the ID document is delivered

How a person is identified when he/she has received the ID document?

Austria

Physical presence for verifying personal appearance and submission of documents.

Belgium

Physical presence for verifying personal appearance and submission of the document delivered for acknowledging the "application for ID documents".

Denmark

No ID cards are in use.

Finland

If it is ID card with certificate the applicant must be physically present to receive the ID card.

France

With another ID document.

Germany

No information provided.

Greece

No information provided.

Ireland

No information provided.

Israel

An ID document is delivered on the same day when applied.

Italy

No information provided.

Luxembourg

No information provided.

Netherlands

Physical presence for verifying the person with the data on the ID-document is obligatory. The verification process is being done by a civil servant of the municipality the applicant lives in.

Norway

In general, physical presence for verifying personal appearance and submission of the document delivered for acknowledging the "application for ID documents". Passport, Bankcard and Postal Service ID card however are sent by surface (registered) mail.

Portugal

No information provided.

Spain

A person must collect the ID card personally, presenting the slip which had been issued as a provisional receipt when the person applied for the ID card.

In the new ID project, the document is delivered on the same day.

Sweden

Visual control by appointed personnel employed by the issuing organisation.

United Kingdom

The majority of passports and driving licences are delivered through the post to the home address of the applicant.

As part of the proposals for an entitlement (identity) card, the government is looking at tightening the issuing process for identity documents, including driving licences and passports if entitlement cards are not introduced.

2.1.5 National legislation on ID documents

What are the main national laws and legislation on establishing identity and issuing ID documents?

Austria

No information provided.

Belgium

- The law of 8 August 1983 organising the National Register of the natural persons.
- The decree of 3 April 1984 relayed to the content of the ID number
- The law of 19 July 1991 related to the population register and identity cards.

Web address of the National Register: www.nationalregister.fgov.be

Denmark

- The Danish Act on the Civil Registration System (Act no. 426 of 31 May 2000)

Web address of the Central Office of Civil Registration: www.cpr.dk

Finland

- The Act for identification card. Implemented on 1. December 1999.
- Population Information Act
- The Population Information Decree.
- The Act on Electronic Service in the Administration.
- The Identity Card Act.

France

No information provided.

Germany

- The law on passport and identity card ("Gesetz über Personalausweise" from 21st April 1986, BGBl. p. 1182)

- The regulations for German passports are recorded in the "Passgesetz" of 19th April 1986 (BGBl. I p.537).

- The German identity card is accepted in numerous other countries as entry permit, for example the regulation of the passenger traffic between the European countries (BGBl II 1959 p. 389, and BGBl II 1996, p. 274 of 23rd January 1996).

Greece

No information provided.

Ireland

- None

Israel

- Parliament laws and regulations of the use and the structure of the ID card

Italy

No information provided.

Luxembourg

- Law of 30 March 1979 on the electronic identification of natural and legal persons

Netherlands

- WID ("Wet op de Identificatieplicht") (Identification Law)
- "Paspoort wet" (Passport Law)

Norway

- "Loven om pass" (passport law, June 1997)
- "Lov om elektronisk signatur" (electronic signature law, July 2001)
- "Vegtrafikklov" (Traffic/road law, June 1965)

According to Section 13 of this Act, all companies issuing qualified electronic certificates (i.e. "trusted third party" companies) are responsible for proper routines on verifying identities before issuing a certificate.

Portugal

No information provided.

Spain

- The Royal Decree 196/1976 of February 6 regulates the DNI (National Identity Card).

- It has been partially modified by Royal Decree 1189/1978, 2002/1979, 2091/1982, 1245/1985.

- Minister of Interior orders of July 12, 1990 and April 26, 1996.

- Organic Law 1/1992, of protection of city life.

- Organic Law 15/1999, of protection of data of personal character.

Sweden

No information provided.

United Kingdom

- Passports are not covered by statute but are issued by Royal prerogative.
- Driving licences are issued in accordance with The Road Traffic Act 1988.

Should the UK government introduce an entitlement card, new enabling legislation would be introduced.

2.1.6   National data protection legislation

The information in this section has been extracted from the document "Initiative for Privacy Standardization in Europe (IPSE) Final Report", with reference: IPSE-SG#11, Doc. n°7 of 28 February 2002.

What is the national data protection legislation and individual privacy that applies on issuing ID documents?

Austria

The Directive has been implemented by the Federal Act Concerning the Protection of Personal Data (Data Protection Act 2000 – DSG 2000) that entered into force on 1 January 2000.

Web: http://www.bka.gv.at/datenschutz/

Belgium

A law to implement the Directive was passed by the Parliament and published in the Official Journal of 3 February 1999. It entered into force in September 2001 following adoption of secondary legislation in February 2001.

An unofficial English translation of the Belgian law is available free on line at www.law.kuleuven.ac.be .

Web: www.privacy.fgov.be

Denmark

The Directive has been implemented by the Act on Processing of Personal Data (Act No. 429 of 31 May 2000) that entered into force on 1 July 2000.

An unofficial translation of the Danish Act is available from the website of the Danish Data Protection Agency.

Web: http://www.datatilsynet.dk

Finland

- Personal Data Act (523/1999) Act on the Protection of Privacy
- Data Security in Telecommunications 22.4.1999/565

France

The French law on Data Processing, Data Files and Individual Liberties became fully operational in 1980. It covers automated and manual records and provides for a central registration system. The right of access in French law was extended to legal persons by an administrative decision of the French data protection authority, the CNIL (Comité National d'Informatique et de Liberté) in July 1984.

A report on implementation of the Directive was issued in March 1998. In August 1999 the Prime Minister announced that the Directive would be implemented by amending the current law. This was followed by further consultation and the outline of a bill was set out by the Ministry of Justice in October 1999. The Government consulted the CNIL on the pre-draft of the bill in July 2000.

A bill implementing the Directive has yet to be enacted. The legislation which still governs this area is the Data Processing, Data Files and Individual Liberties Act 78-17 enacted on the 6 January 1978.

Web: www.cnil.fr

Germany

The national measures implementing the Directive have been adopted on 18 May 2001 and published in the Official Journal (Bundesgesetzblatt) of 22 May 2001.

Each Land also has obligations to supervise elements of the federal law. Six Länder have adopted new data protection legislation pursuant to the Directive covering the private sector as well as some public sector matters. These laws are supervised by the Länder data protection authorities.

For the addresses of the Länder data protection authorities
see   http://www.datenschutz-berlin.de/

Greece

A law implementing the Directive was passed on 10 April 1997. The Act, entitled the Protection of the Individual with Respect to the Processing of Personal Data, covers computerised and manual personal data and applies to both the public and private sector. Under the Act the registration system is run by an independent data protection authority, the Authority for the Protection of Personal Data ("the Authority").

Web: www.dpa.gr

Ireland

A draft bill to implement the Directive was submitted to the government in 1998 but a bill has not yet gone to Parliament. Publication of a bill is still awaited.

The legislation currently in force is the Data Protection Act 1988 ("the Act"). The law covers automated data only and only applies to a limited range of data users.

Israel

Data protection law

Italy

The Directive has been implemented by the Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act (no. 675) of 31 December 1996. This Act came into force on 8 May 2000.

Web: www.privacy.it

Luxembourg

The Directive has not yet been implemented by Luxembourg. A new data protection law implementing the Directive was submitted to Parliament at the beginning of October 2000. This law has not yet been enacted. The legislation which currently governs this area is the Regulating the Use of Nominal Data in Data Processing Act of 31 March 1979.

Netherlands

On 6 July 2000 the Senate for the Netherlands approved the Personal Data Protection Act (Wet bescherming persoonsgegevens), ("the Act"). The Act implements the Directive and entered into force on 1 September 2001.

Web: http://www.persoonsgegevens.nl

Norway

"Personopplysningsloven" (Law on general personal privacy, effective January 2001)

The Norwegian Data Inspectorate ("Datatilsynet") has issued an English translation of this Act on their Web pages: http://www.datatilsynet.no

This Act is based on the EU directive 95/46/EF.

Portugal

The Directive was implemented by Act 67/98 on the Protection of Personal Data on 26 October 1998, which came into force on 27 October 1998. An English translation of the Act is available from the website of the Comissão Nacional de Protecção de Dados (CNPD), listed below.

Web: http://www.cnpd.pt

Spain

The Directive was implemented by the Organic Law 15/1999 of 13 December "Protección de datos de Carácter Personal". This Act was passed on 13 December 1999 and came into force on 14 January 2000.

Sweden

A law to implement the directive was issued on 29 April 1998, entitled the Personal Data Act (1998:204). The Swedish Government also issued supplementary regulations concerning the processing of personal data in the Personal Data Ordinance (1998:1191) on 3 September 1998. Both the Act and the Regulations came into force on 24 October 1998, and repealed the Data Act (1973:289).

The Act applies to processing of personal data that is wholly or partly automated. It also applies to other processing of personal data, if the data is included in or is intended to form part of a structured collection of personal data that is available for searching or compilation according to specific criteria. The Supervisory Authority under the Act is the Data Inspection Board.

United Kingdom

Directive 95/46/EC has been implemented by the Data Protection Act 1998 which was given Royal Assent on 16 July 1998. The Act came into force on 1 March 2000. The legislation covers England, Scotland, Wales and Northern Ireland but does not cover the Channel Islands (Jersey, Guernsey) or the Isle of Man which have their own data protection legislation.

Web: http://www.dataprotection.gov.uk

2.2 The present PKI-based e-ID situation in the European Union

The present situation in projects is miscellaneous. Many countries are running pilots and projects but only few have a working system available for citizens. Sometimes the different authorities are running pilots of their own instead of cooperating with other similar projects on a different administrative branch. Finland, Sweden, Italy and Belgium are the most advanced.

The present situation of PKI-based e-ID projects fulfilling level 5.1 of the directive on electronic signatures:

- **Does a certificate exist?**

- **What are its specifications?**

- **How is the issuance and management of certificates performed?**

Austria

- A citizens' card project "Bürgerkarte" would be an extension of social security cards, currently under development. It will be a smart card and will offer electronic signature services. It is planned to subdivide the smart card into "compartments" (e.g. health care administration, student card).

- Project specifications still under discussion

- There are few Certification Authorities as well as a central control instance.

Belgium

- The below projects are one of the key elements of the Belgian e-Government strategy:

  - FedPKI aims at creating a PKI infrastructure and deploying cards e-ID for civil servants with IAS services

  - BelPIC aims at creating the infrastructure required for linking the municipalities and the National Register for the purpose of the deployment of the electronic ID card for the citizens

  - EIC aims at launching a pilot for electronic ID card for the citizens with IAS services (60 000 cards) on 11 municipalities and then the full deployment, under the condition of a positive decision from the government. This card will replace the current ID card mentioned under question 2 above.

- The card will include 3 certificates (root, authentication and electronic signature), all compliant with X509 version 3.

- In the EIC project,

  - The Card Issuer is the National Register, similarly as with the existing ID card,

  - Municipalities will act as Registration Authority, using the database from the National register and be in charge of distributing smart cards, similarly as with the existing ID card,

  - The Certificate Provider function will be subcontracted similarly as the personalisation and initialisation of the card.

Denmark

None have been found which might be relevant for the purpose of this document.

Finland

Several projects in progress.

- Working systems:

    - Notice of removal service / The Finnish Population Register Centre and Finland Post

    - Banking service / OKO Bank Group

    - Childminding application / The Municipality of Tuusula / The City of Riihimäki

    - City municipal public services / Espoo/Vantaa/Pori/Oulu.

    - Submission of an application for an educational institute / National Board of Education.

    - Insurance services / Fennia Group.

    - Employment administration services / Ministry of Labor.

    - Electronic transaction with municipalities / The Cities of Lappenranta, Tampere and Vantaa

    - Company electronic declarations National Technology Agency: Funding application

- Existing Certificate

    The electronic identification card is issued by the local police department. The Finnish Population Register Centre supplies the on-board certificates which are used in electronic identification. In addition to the card, a card reader is needed for on-line use. In the future, identification can be done from a mobile device such as a cellular phone equipped with a special chip.

- Issuance of certificate

    Issued by the local police department. Applicant must be personally present as applying it at local police department. Must be personally present also when the ID card is delivered.

- Management of certificate

    The Finnish Population Register Centre controls subcontractors who take care of the administration and management of the certificate i.e. Revocation list and directory service.

France

Three major projects are:

- The TITRE FONDATEUR project is centred on a common identification system to be the basis for the issuance of various identity cards with or without ability to electronically sign, with elected representatives and civil servants as priority users. This project is a key element of the French e-Government strategy.

    In the TITRE FONDATEUR, which is still at a preliminary stage, only a very reduced set of information will appear printed on the card, while extra info recorded in the card will be available only to accredited authorised persons (under the control of their own professional card).

For the TITRE FONDATEUR
- the French Administration will manage the master registry, which identifies and authenticates each person. It is based on the book maintained in each municipality;
- the municipalities will continue being the first access point similarly with the current ID card.

- The CPS card and the SESAM-VITALE card are designed to work together in the domain of healthcare and social insurance; the first one is reserved to health professionals, supports electronic signature for administrative purpose and protection of sensitive information, while the second one is only used to identify the insured person and to carry a few information on his/her rights.

- The Ministry of the Interior in France has decided to start in 2003 a trial for the Citizen Electronic Card, CEC, in 15 sites. The city of Issy-les-Moulineaux is candidate to be one of the trial sites.

An experimental standard has been defined by AFNOR with the participation of the Ministry of the Interior and various industrialists. An experimental demonstration platform has been designed and a presentation is ready. The CEC will provide three types of functions:
- Proof of identity with means of control including biometrics.
- Travel document in the European Union area, with means of control including biometrics.
- E-administration, or accessing to administrative procedures through Internet with authentication and electronic signature functions where needed. The CEC will be considered as the safe for personal data of each citizen.

This project integrates the European dimension and intends to be interoperable with the rest of the EU. The AFNOR standard is based on the existing European standards and it defines the French conditions of use.

Germany

- Two very different projects were examined in Germany:
    - The LAND OF BADEN-WÜRTTEMBERG is experimenting smart cards for several usages such as car registration, requests for agricultural funding, applications in the department of Justice, the users being civil servants, citizens or enterprises.
    - The BESCHAFFUNGSAMT (procurement agency) of the Federal Ministry of Home Affairs aims at implementing qualified electronic signature throughout the whole life cycle of contractual relationship between administrations and providers.

- There are several other projects:
    - The e-Administration "BundOnline 2005"
    - Banking projects / Deutsche Bank and HypoVereinsbank
    - Technical University Berlin multi-functional card
    - Bremen online service / City of Bremen
    - EISter, electronic tax declaration
    - FASME project (Facilitating administrative Services for Mobile Europeans)

- The pilot project of the LAND OF BADEN-WÜRTTEMBERG is aimed at providing IA services with a multi-functional card. It uses the IDENT-procedure of their provider SignTrust (Deutsche Post) for the smart card personalisation and delivery process and for the registration process.

Greece

A White Paper of the Greek government entitled "Greece in the Information Society" was published in February 1999 and an Operational Programme for the Information Society (OPIS) has been adopted in the framework of the EU's 2000–2006 Structural Funds Framework in order to promote the use of the electronic signature in a coherent and integrated way.

Ireland

None have been found which might be relevant for the purpose of this document.

Israel

In the national ID system, the introduction of smart card based ID cards is on the way. The eEpoch pilot is part of the overall puzzle, and allows for testing the PKI and "Public Identity" applications before the national roll-out. It is planned to introduce an employee card for government employees. A tender was already published and the vendor chosen. It is expected to distribute 150 000 cards in the long run, and 10 000 – 40 000 cards in the short run. The cards will be multi-functional, providing physical access to parking and government buildings, recording time attendance, providing a login and digital signature. The approach corresponds to the Finnish example, having not much data on the card and an important certificate. B2B applications in government (procurement) are being tested, as well as the interoperability of card readers and cards from different vendors. A registration computer data base as basis for implementation is available, but the certificate authority has not yet been chosen. Standardization recommendations, laser engrossing and optical features are open questions.

Italy

- The Italian electronic ID card (IEIC) project provides IAS services to various sectoral administrative applications and network access control. It is currently mainly used in the public administration for electronically signing documents.

- Certificates are X509 version 3 compliant

- The electronic cards are requested through delivered by the municipalities which act as an interface between the citizens and a central Registration Authority. The CT-RUPA "Centro Tecnico per la Rete Unitaria per la Pubblica Amministrazione" technically supports the whole process. The IEIC project has its own CA.

Luxembourg

None have been found which might be relevant for the purpose of this document.

Netherlands

Providing high level electronic services and transactions is an important goal for the Dutch government. A well-developed, thorough approach to electronic service provision requires a reliable system for identification and authentication that offers the same guarantees currently standard in non-automated services.

- In "PKI overheid", certificates are X509 version 3 compliant. The specifications are put down in the "programma van eisen PKI Overheid" or Statement of Requirements. This can be found at http://www.pkioverheid.nl

- The Dutch PKI will be hierarchically designed and will be aimed at achieving maximum interoperability. There will be a central government policy authority (PA) and three domain PAs (for government to government communication, government to business communication and government to citizens communication). The certification authority (CA) function and the registering authority (RA) function will be separate roles within a Certification Service Provider (CSP). Within this scheme, it will be up to the central

government to provide the necessary framework for implementing a general PKI and to lay down the rules and regulations which all participating organisations will have to comply with. An independent body will audit the CSPs. The CA function will be performed by TTP.NL (Trusted Third Party Netherlands).

Norway

There are available commercially qualified certificates to the general population. It is the Norwegian Post and Telecommunication Authority (a government agency) that registers vendors of qualified certificates. So far only ZebSign AS has been approved by the agency.

Specification: National law on digital certificates, based on the EU-directive.

Some examples of current projects:

- National Lottery electronic ID card with an electronic purse (use the "ZebSign ID" policy)

- Local municipality (use the "ZebSign ID" policy)

- Telenor employee electronic ID card

- Telenor Mobile: PKI on SIM cards in mobile phones (use the "ZebSign ID" policy) used for both authentication and electronic signatures. Used especially for SmartPAY (mobile payment solution with a full PKI infrastructure)

- Social security services begin pilots on medical certificates and sickness leave from the first of January. PKI vendor will be chosen the 17th of December 2002.

Portugal

Some sectorally-based pilot projects are already underway (Ministry of Justice, Ministry of Agriculture) for introducing electronic signatures for the authentication of electronic exchanges within the public administrations or between them.

Spain

- The "Fabrica Nacional de Moneda y Timbre" (MINT) provides smart cards with PKI based certificates for identification and authentication and for electronic signature to several administrations. Presently, the two major users are

    - The "Agencia Estatal de Administración Tributaria" (for tax declaration)

    - The "Seguridad Social" (Social Security).

- In addition, there is a starting project for the creation of a national electronic ID card issued by the Police. Work is in progress to establish a single universal certificate for all administrative transactions. The current certificate is regulated in the Technical Annex of Royal Decree 1290/1999.

- In the MINT project

    - There are two mandatory certificates and one optional for administrations, for Class 1 certificates. Certificates are X509 version 3 compliant.

    - The registration process is made of two steps: issuance of a certificate request and face-to-face appearance to the RA. The issuance of the certificate is insourced.

    - The "Consejo Superior de Informática" act as Policy Board

Sweden

- Posten AB provides a multi-function ID card for three basic services: identification, signing and coding.

- The Posten AB card issued by the Swedish Post and Telia to the public

    - Includes 2 certificates, X509 version 3 compliant

    - The card is based on a Swedish standard (based on PKCS#15) and a policy produce by an interest group called SEIS (now taken over by the GEA organisation). The security level is well above the ETSI standard requirements for QCs.

- The Certificate provider function is outsourced.

United Kingdom

- The Southampton project aims at developing local services based on multi-function smart cards. That project is the first pilot of the "Smartcities" initiative that joins several towns throughout Europe with many partners as providers.

- Tentative explorations have been made in the direction of a migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive. There is however no plans yet to roll out qualified certificates

- The card issuance is currently carried out by both Southampton City Council (SCC) and the University of Southampton. The issuance policy/authentication framework has been created by SCC and endorsed by the wider consortium. The service providers are and will be a mix of private and public organisations. They also act as access provides, managing the infrastructure aspects.

The current consultation on entitlement cards invites comments on whether the card should be smart and, if so, whether it should include a government issued PKI-based digital certificate for citizens.

Part III:

Aspects Related to e-ID Evolution and Implementation

- Legal Issues in Relation to the Use of Electronic Identity

- Technical Requirements for Interoperability of e-ID Card Systems

- Privacy-enhancing Requirements

3. Part III: Aspects Related to e-ID Evolution and Implementation

3.1 Legal issues in relation to the use of electronic identity

In the implementation of e-ID systems it is necessary to ensure that the processing of personal data and the protection of privacy is taken into account according to the related European regulations.

A study on the impact of the EU regulations for e-ID was made. The conclusions from this study are listed. For the detailed report please refer to the e-ID website (www.electronic-identity.org) or the eESC documentation (available on the eESC CD Rom).

3.1.1 Data protection regulations in the EU and relevance for e-ID concept

The European Union has an advanced regulatory framework as regards protection of personal data:

- The European Directive relating directly to the data protection is the Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data.[1]

- The European Commission has adopted a Decision 01/497/EC setting out standard contractual clauses ensuring adequate safeguards for personal data transferred from the EU to countries outside the Union.[2]

- Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.[3]

- The European Parliament and the Council of Ministers have adopted the Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Directive 01/45/EC.[4]

- The European Parliament and the Council of Ministers have adopted the Directive 99/93/EC of 13th December 1999 on a Community Framework for Electronic Signatures.[5]

- The European Parliament and the Council of Ministers have adopted the Directive on a Legal Framework for Electronic Commerce 00/31/EC, which was adopted on 8th June 2000.[6]

Some directives relate directly to the protection of personal data, i.e. the Directive 95/46/EC, the Directive 97/66/EC, the Directive 01/45/EC and the decision 01/497/EC, whereas the other Directives refer to the regulation of different topics but refer to the data protection directives, especially to the Directive 95/46/EC.

---

[1] Official Journal L 281, 23/11/1995 P. 0031 - 0050

[2] Official Journal L 181, 4/7/2001 P. 0019 - 0031

[3] Official Journal L L 024 , 30/01/1998 P. 0001 - 0008

[4] Official Journal L 008, 12/01/2001, P. 0001 - 0022

[5] Official Journal L 13, 19/01/2000, P. 0012 - 0020

[6] Official Journal L 178, 17/07/2000, P. 0001 - 0016

3.1.2   Conclusions for e-ID

General conclusions

1. The e-ID aims to build a universally recognized electronic ID token for identifying citizens in multiple use case scenarios. The e-ID will make it possible to pass the identity, once issued from one legal entity into other existing infrastructures of applications, may it be in the private sector, may it be in the public sector. In addition the e-ID will use certification service providers, most probably in the different national legislations. This proposal takes into account different functionalities and builds on various processes. From that perspective it is justified not to speak of the e-ID but rather of the "e-ID concept".

2. In most cases the roles of the different sectors are clearly defined in their specific areas of national regulations and thus the legal requirements follow the specific national legislation and the existing national legal organisational framework; e.g. the various European Member States have national data protection legislation and a matching national organisation. Although the European Directive 95/46/EC aims for harmonisation in European data protection, the differences in the various national data protection laws might be significant, e.g. the use of codes of conducts are in some Member States accepted, in some Member States they are not accepted. This leads to a more complex legal assessment.

3. The legal assessment becomes more complex if, in addition to the various national areas of regulation, other geographical areas like e.g. the US or Japan have to be implemented in the e-ID concept. The European Union clearly has the most regulated environment as regards data protection and electronic signatures. US regulation tends to be more pragmatic than EU regulation and hence more flexible. Other regions of the world do not reach the level of US/European regulations.

4. The European Union has an advanced regulatory framework as regards protection of personal data. The European Directive relating directly to the data protection is the Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data. In addition to the Directive 95/46/EC the European Commission has adopted a Decision 2001/497/EC setting out standard contractual clauses ensuring adequate safeguards for personal data transferred from the EU to countries outside the Union.

5. From a data protection perspective the Directive 95/46/EC has to be identified as the main reference regulation for the e-ID concept. In addition to that Directive the Decision of the Commission 01/497/EC on standard contractual clauses has to be closely linked to that perspective as this Decision ensures adequate safeguards for personal data transferred from the EU to countries outside the Union. As the e-ID concept will include electronic signatures based on PKI the data protection provisions in the Directive 99/93/EC on electronic signatures have to be taken into account as well.

6. The Directive on e-commerce does not have any specific data protection provision. However, the Directive builds especially on the Directive 95/46/EC as a general legal basis. The e-ID concept has therefore – as far as the Directive on e-commerce is applicable – taken due regard to the principles and provisions of the Data Protection Directive.

Conclusions as regards data protection and e-ID

1. The e-ID concept will lead to a processing of personal data by automatic means, whereby data are either processed on the e-ID card itself or will be closely linked to the automatic processing of personal data outside the e-ID card using various

databases. In any case the e-ID card will be connected to the processing of personal data by automatic means.

2. Independent of the decision, who is determining the purposes and means of the processing of personal data it has to be noted for the e-ID concept, that independent of the establishment of the data controller within the European Union, the same level of data protection pursuant to the Directive has to be implemented by the member states. This principle is of some practical importance and has to be taken into account as regards the organisational issues of the data controller. If the data controller is one entity or organisation the national data protection laws have to be applied, where this data controller has its establishment. If the e-ID concept plans to have several distributed data controllers the concept has to take into account that several national implementations of the Directive have to be in place.

3. To issue the e-ID it will be necessary to collect, store and process personal data on various levels or steps: identification and registration of the card holder, provision of applications to the card holder and provision of services (content) to the card holder. The e-ID token may carry additional information or personal data on the card itself. Personal data will be either processed on the e-ID card itself or will be closely linked to the automatic processing of personal data outside the e-ID card using various databases.

4. Within the e-ID concept it has to be discussed whether the processing of personal data takes place on the card itself or outside the card; this may have some effect on the definition and accordingly on the responsibility for the various data protection provisions which are imposed on the data controller. In this context it has to be discussed furthermore what roles the various parties within the e-ID concept will have from a data protection perspective.

5. The description of functionalities from a smart card point of view are not sufficient from a data protection point of view. The e-ID concept has to take into account that it is not possible to nominate one single data controller, but it has to recognize that several possible data controllers are at stake: the card issuer, the application provider and the content or the service provider. It is therefore recommended to include at least the "content or service provider" in any data protection provision within the e-ID concept. In addition to the above discussed roles of the "data subject" and the "data controller" the Directive 95/46/EC identifies the roles of the "processor", the "third party" and the "recipient". It is also recommended to add these roles to the data protection provision within the e-ID concept.

6. Confidentiality of the personal data while processed and security of the processing itself are a "must" when protecting the personal data of a data subject. Using a smartcard within the data processing with its many technical options is a challenge for these principles and, at the same time, an opportunity to provide a technical viable solution for safeguarding confidentiality and security of the processing of personal data. The e-ID concept has to watch these principles very carefully. Any threat for unwanted disclosure of personal data on the smartcard or from a database will question the reliability of the card itself and thus reducing acceptance of the technology with the data subject.

7. It is recommended for the e-ID concept to have one overall security concept which would implement in general terms the required security features and thus would contribute to a harmonized approach for the e-ID concept. The GIF model should cover this issue.

8. The "magna charta" of any data protection regulation are the rights of the data subject. These rights enable the data subject to have transparency on the processing of personal data, they enable the data subject to judge the purposes of any processing of his personal data, to view stored personal data and to reject unlawful processing. At the same time the correct execution of these rights put the obligation on the data

controller to inform the data subject on any processing step. This information is the basis for the trust relationship between the data subject and the data controller.

9. The necessary information to the data subject has to be provided either by the card issuer, the application provider and/or the content or service provider. Within the e-ID concept this situation could end in a multiple information exercise, which is possibly leading rather to confusion with the data subject than to transparency. It would be recommendable to concentrate the required information on one specific data controller, which could be the card issuer. As long as the intended processing of personal data is known, this "combined information" to the data subject is a reasonable way of handling the required information. Nevertheless this simplification will not relief any other content or service provider who is added later on to the e-ID framework from his obligation on information.

10. The e-ID concept has to enable the execution of the rights to access, rectification, blocking, or deletion of personal data without any constraint and without excessive delay or expense. The use of the e-ID card for accessing this information online is more appropriate than a written procedure.

11. For cases where data is transferred to non-EU countries, the Directive includes provisions to prevent the EU rules from being circumvented in Article 25 and Article 26. The basic rule is that the data should only be transferred to a non-EU country if it will be adequately protected there, although a practical system of exemptions and special conditions also applies (such as for data where the subject has given consent or which is necessary for performance of a contract with the person concerned, to defend legal claims or to protect vital interests (e.g. health) of the person concerned).

12. An "E-ID Model Contract on transfer of personal data to non-EU countries" could help to ensure the acceptance of the transfer of data to non-EU countries. The e-ID concept may establish safeguards that make them less dependent on the good will of the legislators of a given country. Even in the best case scenario, a number of non-EU countries are likely to fall short of an "adequate" level of protection, and individuals may be reluctant to give their consent to the transfer to such countries of their personal data. In addition this "e-ID Model Contract" would speed up the process with multiple private companies and/or public agencies. This standard "e-ID Model Contract" could be an integral or an annexed part of the Privacy Code of Conduct (to be found in the Common Specifications , Chapter User requirements, TB 8)

13. The certification-service provider within the e-ID concept has to follow the specific data protection regulation pursuant to Article 8 of the Directive on electronic signatures by focussing the personal data which may be collected and processed by the certification-service provider strictly to the purposes of issuing and maintaining the certificate. By this the personal data processed will be very limited, except the data subject explicitly consents to the processing for other purposes. It is recommended that this specific provision is taken into account in the Code of Conduct.

14. Any processing of personal data within the e-ID concept must be lawful and fair to the data subjects. In particular data within the e-ID concept must be adequate, relevant and not excessive in relation to the purposes for which they are processed; the purposes must be explicit and legitimate and must be determined at the time of collection of the data; the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified.

15. It is recommended that the major principles on data quality are mentioned explicitly in the Code of Conduct. It is the responsibility of each data controller to safeguard the data quality. Moreover the issue of identification of the data subject has to be addressed in the Code of Conduct.

16. It is mandatory that the collection, the storage and any other processing of personal data are in line with the requirements of the Directive 95/46/EC. In addition to the

principles for data quality in Article 6 the Directive uses accepted principles to provide legitimacy to data processing, especially the informed consent of the Data subject. It is recommended that the different use cases, the sectors affected and the personal data necessary for processing are discussed in more detail as soon as use cases are defined.

17. The e-ID concept may lead to some kind of an identification number, e.g. by using a certificate, a pseudonym or any other identifier. This universal number would have to face severe fears of the data subjects as it would possibly allow cumulating of personal data around the unique identifier, from various databases and eventually end in a personal profile. The Directive addresses this issue in Article 8 Paragraph 7, however leaves the question up to the Member States to determine the conditions under which a national identification number or any other identifier of general application may be processed.

Conclusions as regards next steps

1. The Code of Conduct for e-ID related data protection is a valuable and accepted contribution from the Directive's point of view. In addition, it would help to overcome to a certain extent the need to match the e-ID concept not only to the Directive but also to the implementation of the data protection legislation in Member States. The Code of Conduct will be "soft law" and it has to be matched against all implementations of the Member State or the Member States. It does not replace the national legislation, but it would support initiating such kind of legislation in the Member States.

2. Decisions on Codes of Conduct on the Community level will have to take into account the data protection regulations by the Member States, i.e. the Working Party will have to match the proposed Code of Conduct to each Member State where it is intended to be applied. The EU Commission is authorised to publish the Code of Conduct, as soon as the Working Party has approved the Code of Conduct.

3. In relation to the "Rules of conduct for privacy and card integrity" it is recommended to match the rules to the national data protection rules pursuant of the Directive and to propose these rules to the Working Party according Article 29 by an appropriate industry association.

4. An "e-ID Model Contract on transfer of personal data to non-EU countries" could help to ensure the acceptance of the transfer of data to non-EU countries. This standard "e-ID Model Contract" could be an integral or an annexed part of the Code of Conduct.

3.2   Technical requirements for interoperability of e-ID card systems

The minimum requirements proposed in this White Paper address only the data (content and format), that an e-ID scheme should adopt to support cross-border interoperability. This level is independent from a specific implementation for a given e-ID scheme.

To achieve full interoperability an e-ID card scheme should rely on a standard implementation of smart card based IAS (Identification, Authentication and Electronic Signature) system. The corresponding requirements have been developed by eESC in the GIF (Global Interoperability Framework) and a standardisation initiative has been started. Although beyond the scope of the work carried out by TB1 and requirements addressed by this White Paper, and in order to provide the complete picture for the reader, the following section contains an overview on the GIF which will be validated in a pan-European pilot programme, the eEpoch project.

3.2.1   Global Interoperability Framework (GIF) for identification, authentication and electronic signature (IAS) with smart cards

Background: The Smart Card Charter [7]

This Framework for Identification, Authentication and Electronic Signature (IAS) is part of the eEurope Smart Card Charter Common Specifications. Its aim is to facilitate interoperability between the various IAS schemes using trusted electronic tokens emerging in Europe and more widely throughout the world. The Global Interoperability Framework makes extensive use of the following concepts:

- a Smart Card Community (SCC): all smart cards issued and managed by a given card issuer

- an e-service community: all smart cards recognized by a given service provider

- functional architecture: the 3-layer architectural model comprising six entities (IAS nucleus, platform, additional applications, connectivity, human interface, PKI) and four nucleus interfaces required for smart card information system to work (see Fig 5)

- the IOP adapter: the interface operating in the card and card reader connectivity level and enabling process interfaces between the IAS and application levels required for accessing/transferring data for the purpose of the front office application layer or the on-board card application

- the PKI adapter: the interface required for a relying party in a smart card community or e-service community following the GIF functional architecture to verify certificates issued by different PKI authorities

- on-us or not-on-us: mode of operation assigned to a component of the smart card management framework referring to use in its domestic community or in a host scheme respectively

- on-card and off-card: implementation distinction driven by optimization considerations based on business rules and technology parameters

---

[7]   See http://eeurope-smartcards.org/

Objectives

The framework provides smart card communities and e-service communities with the necessary concepts and guidance on the tools required for access to e-services and for security of transactions over the Internet where special "high-end" requirements must be fulfilled concerning identification, authentication (tokens and persons), non-repudiation (by electronic signature), encryption and integration with other applications. This guidance includes:

- **Preparing information systems for interoperating** i.e. providing the rules and standards which should be used within information systems in order to be able to guarantee IAS interoperability for internet transactions;

- **Organizing the operation of this IAS interoperability** i.e. the ability of an e-service community to verify the identification and the validity of the authentication and electronic signature of members from different smart card communities.

Scope of the Framework

The framework is restricted to the data, technology and process agreements required for IAS interoperability with smart cards. Its scope is the "interoperable nucleus" of Internet-based high-end services which are accessed and protected by smart cards. The hooking mechanism to these services is part of the framework, but the Internet-based services themselves are not. The Framework provides a minimal architectural nucleus for *e-ID*s within a general common conceptual model. It allows sufficient flexibility so as not to impede developments in smart cards technology and infrastructure and still support the forseeable pan-European and wider needs of the following stakeholders:

- Smart card users

- Large volume issuers of smart cards and smart card services

- Card management suppliers

- Providers of public and private key infrastructure schemes

- Application and service suppliers that are or will be connected in sessions using the common interoperable e-ID smart card token

- Suppliers of smart cards, system components and infrastructure.

The 4-part framework specifies requirements, technologies based on open standards, together with identified minimum logical functions and the agreed data for common use.

- **GIF Part 1: Contextual and conceptual modeling**
  an in-depth modelling of the smart card, its environment and interoperability issues with regards to identification, authentication and electronic signature

- **GIF Part 2: Requirements for IAS functional interoperability**
  a list of functional requirements and interoperability prerequisites taken into account when defining the operational and implementation models

- **GIF Part 3: Recommendation for IOP specifications**
  guidance for enabling, implementing and operating IAS interoperability

- **GIF Part 4: Deployment strategies for generic IAS**
  an overview of business plan elements, organization issues, and system development   processes for mass deployment strategies.

In this way, the Interoperability Framework has been designed to include the necessary specifications and, at the same time, be:

- **Focused** on the content required for "interoperability of IAS with smart cards"

- **Flexible** and, therefore, **as least constraining** as possible in order to support or participate in a broad development of the usage of smart cards in e-service communities

- **Comprehensive**, in the sense that at minimum it clearly identifies all issues which prevent two smart card-communities from fully inter-operating at IAS level. Notwithstanding this list, it is expected that some items will remain, for a certain period of time, only resolvable by bilateral agreement between two or more communities until more comprehensive standards are widely agreed and adopted.

While the framework addresses IOP at the level of smart cards, it also considers IOP essential at the levels of the information systems and data.

Smart card management framework

A Smart Card Management Framework (SCMF) is defined at conceptual level as a system constituted of a set of roles and corresponding entities which enable and make use of smart cards within a smart card information system. Three roles are critical from an IAS perspective: Card Issuer, e-Service Provider and Card Holder. GIF assigns the card issuer and service provider roles to distinct entities and thereby develops the concepts of a smart card community and an e-service community. The Card Issuer leads the smart card community, managing the identity data and the certificates of the Card Holders in the community. The e-service community is ruled by the Service Provider business rules and its members are the group of users authorised to use the service(s). This group may span more than one smart card community. A secondary distinction concerns the place i.e. on-card and off-card, where the business rules belonging to the e-community are positioned. The on-card application providers are a subcategory of the service providers, having a special relation with those smart card communities that allow downloading of applications to the cards in their smart card community.
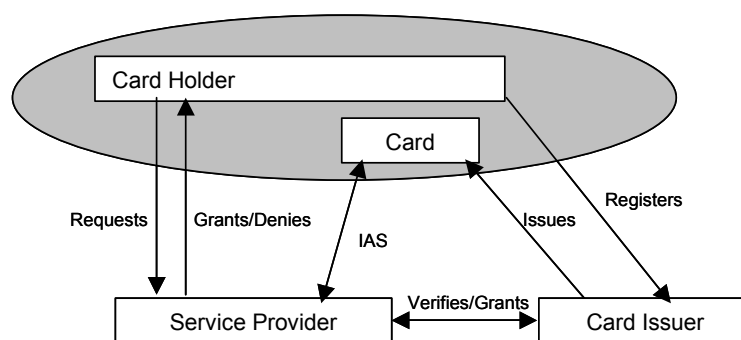

Figure 1: Basic roles model for a Smart Card Management Framework

This perspective enables a whole new generation of service providers using the smart card IAS functions without having to be on-card application providers and offering services to a larger audience beyond a particular Smart Card Community. The following IAS implementation scheme then applies:
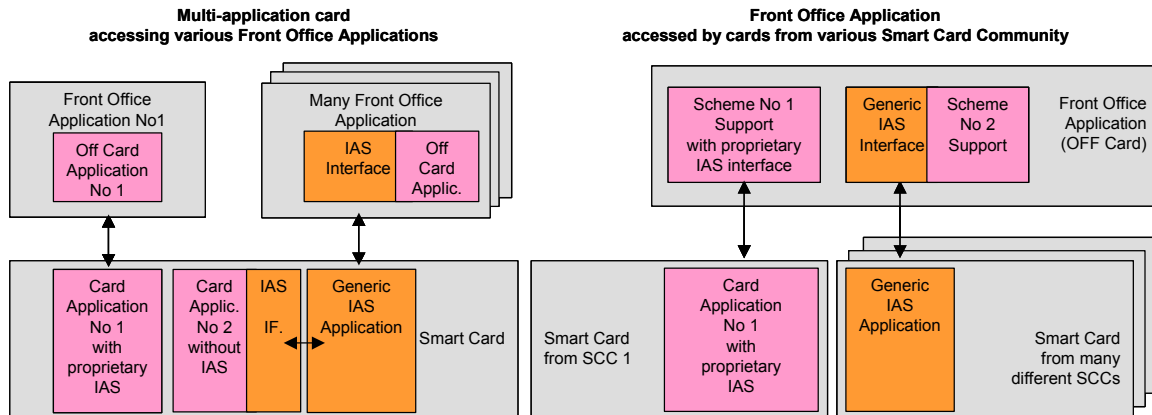
Multi-application card accessing various Front Office Applications

Front Office Application accessed by cards from various Smart Card Community

Figure 2: Implementing generic IAS

The general case of N card issuers and N service providers where groups of service providers agree to mutually recognize each others' cards independently of the card issuers involved can be achieved on a "one to one" basis between service providers or by the definition of a common scheme within a specific industry. This scheme typically enables *e*-service communities to span several distinct smart card communities as described below:
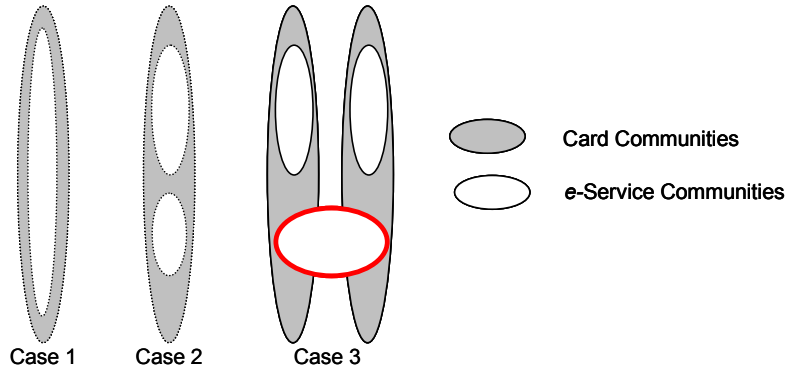

Figure 3: Offering service to cards from several card issuers

The roles and processes required for interoperability between smart card communities are shown in Figure 4: Interoperability relationships.
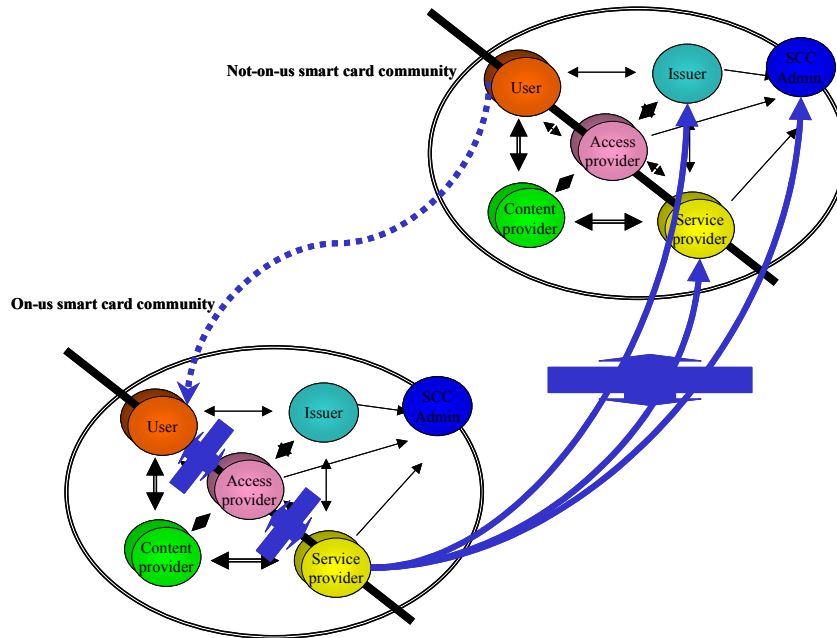

Figure 4: Interoperability relationships

Smart card information system

The smart card is one of the functional components of an information system. The Smart card information system is made up of three architectural layers, each with their own sets of specific building blocks as follows:

-   The **smart card layer**

-   The **infrastructure layer,** including card readers and other card interacting devices, remote servers and private or public telecommunication networks,

-   The front office **application layer** comprising

    -   The application which delivers a service to a user with a smart card

    -   An interface to the IAS generic application which needs to be integrated in the business application and connected to its counterpart on the card for IAS processes.

Each of the three layers is communicating with the others through the connectivity "functional box" via a secure communication channel.
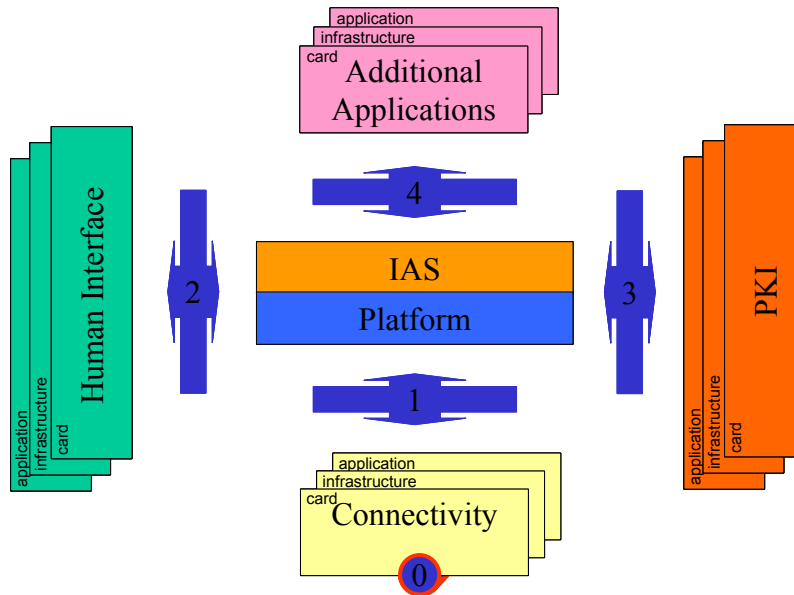
Figure 5: The basic functional architecture

The functional input/output interface between the central boxes and the peripheral boxes is labelled as the "IOP-interface" (interoperability interface). Four IOP-interfaces are defined:

- #1. From nucleus to (external) connections

- #2. From nucleus to human interface

- #3. From nucleus to PKI application

- #4. From nucleus to front office applications when IAS functionality is required.

For the purpose of modelling interoperability scenarios, a new attribute is assigned to each component of the SCMF (i.e. the members of a Smart Card Community as well as the technical components such as cards, certificates, reader). The attribute "**On-us**" or "**Not-on-us**" is assigned to each component of the SCMF depending on whether it is being used respectively in their domestic community (i.e. in the community for which they have been primarily produced - e.g. on-us card or certificate) or in a host scheme (i.e. in a community other than their domestic one - e.g. not-on-us card or certificate).

Keeping the Infrastructure Layer constant (i.e. "on-us") and assuming the certificate and card layers are at same level (either "on-us" or "Not-on-us"), four IOP scenarios are possible and defined in detail.

For each of these scenarios the required interfaces and connections are shown below.
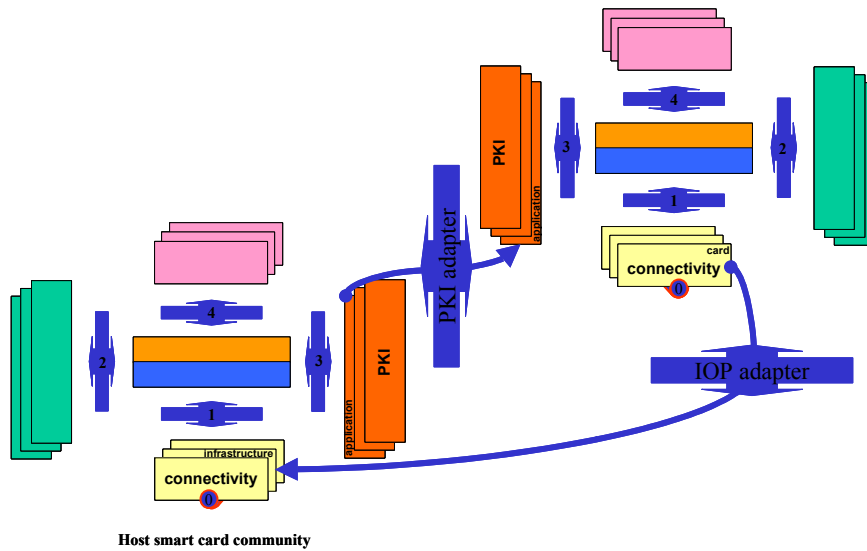
Figure 6: IOP and PKI Adapter Interfaces

As shown in the figure, two adapters are introduced to interface between two smart card communities: IOP Adapter and PKI Adapter.

IOP Adapter

The IOP adapter operates in the connectivity level and enables process interfaces between the IAS and application levels required for accessing/transferring data at card layer for the purpose of the front office application layer according to the following stipulations:

- At connectivity level, it may be implemented using a card reader with multiple card interfaces and supporting multiple card operating systems. It is located in the infrastructure layer of the smart card information system of the host smart card community and under the responsibility of the access provider's concerned.

- At IAS level, it includes all conditions on how to handle an IAS request from a "not-on-us" smart card community process. These conditions are extensions to the host ("on-us") smart card information system. These add-on conditions, modeled in the "IOP-adapter", include both the receiving and sending smart card community requests.

- At application layer, it includes all business rules applicable to the agreed interoperability between the two smart card communities.

When access is required by or from another smart card community, the connectivity mechanism triggers the IOP-adapter (see Fig 6: IAS Decision tree related to IOP) . This IOP-adapter translates the interaction with the (at least virtual) interfaces from the host infrastructure to the infrastructure of the requesting smart card community.

The PKI Adapter

The PKI adapter is the interface required for a relying party in a smart card community or e-service community following the GIF functional architecture to verify certificates issued by different PKI authorities. It enables:

- The verification of the validity of certificates delivered by a CA to be used by

    - The card holder/user for a trusted transaction with an Internet application,

    - The smart card community building blocks for securing the smart card information system.

- The establishment of a trusted relationship between the host smart card community and the "not-on-us" Certification Authority.

The PKI adapter, in technical terms, deals with the interface questions of accessing a Certificate Revocation List - or an OCSP responder or a Verification Authority - from the "not-on-us" Certification Authority. Solutions for the PKI verification process (e.g. cross-certification, hierarchical certification, community of interest, bridge validation) already exist on the marketplace.

The involvement of the PKI Adapter in connecting two smart card communities will be triggered by the IOP adapter as shown in the decision tree below. The PKI Adapter will be invoked as soon as the infrastructure layer or the front office application layer identifies that the certificate to be verified for authentication or electronic signature purposes has been issued by a Certification Authority from another smart card community. How this information is determined and verified is an internal matter.
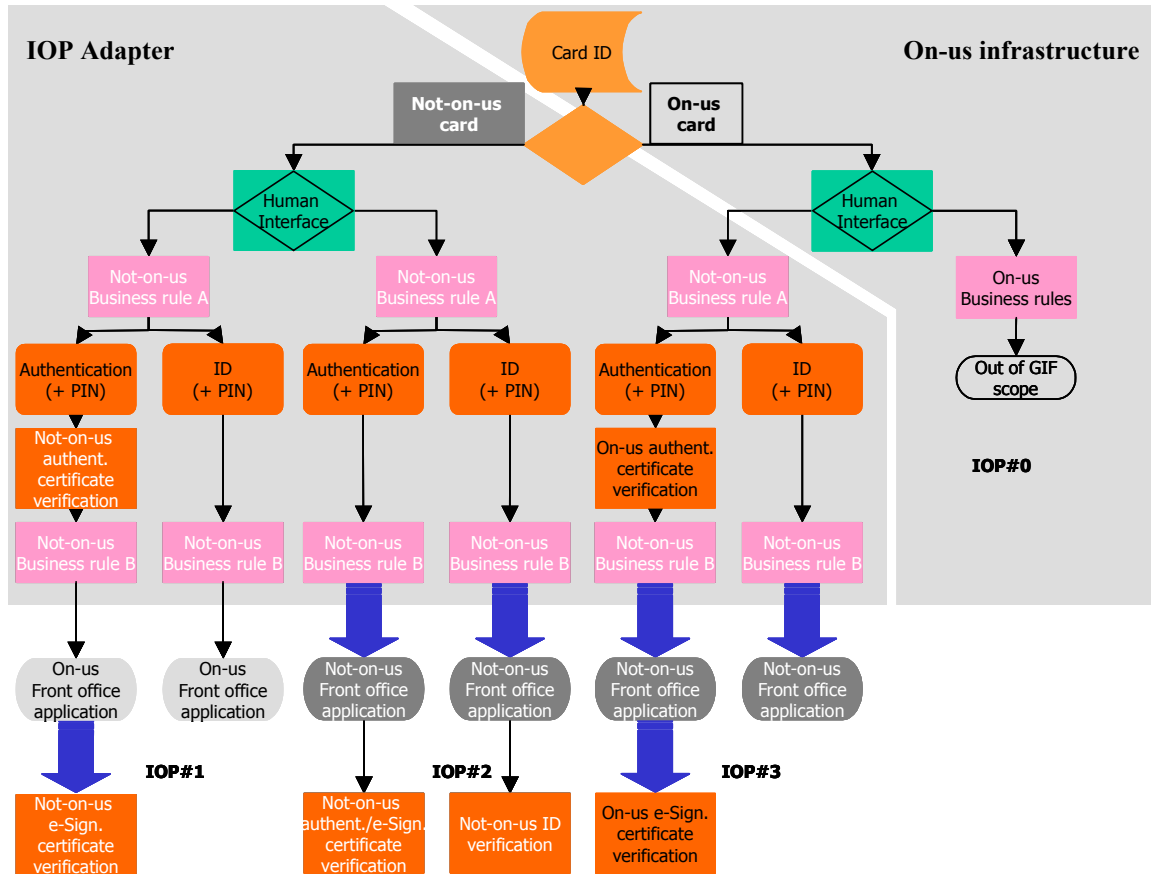
Figure 7: IAS decision tree related to IOP [8]

A service provider/relying party, especially when using a not-on-us card to render a service, must be able to verify the validity of an identity and an e-signature using the on-us infrastructure and services. To execute this routine the required interface will either be already on the card, or be downloaded at time of need via a URL pointer. This requires 'investments' by both the relying party and the PKI operator. In practice it is generally the card issuer who installs this interface on the card either pre or post issuance.

More information

The Framework for Identification, Authentication and Electronic Signature (IAS) is part of the Common Specifications. Its aim is to facilitate interoperability between the various IAS schemes emerging in Europe and more widely throughout the world. More information including the text of the GIF and the latest version of the Common Specifications is available from the eESC website http://eeurope-smartcards.org.

---

8   This drawing is applicable to both identification with authentication and identification without authentication.

3.3   Privacy-enhancing requirements[9]

3.3.1   Introduction

The enormous potential of communicating and transacting in cyberspace (including the Internet, e-mail, cable TV, and mobile networks such as GSM, and especially the new 2.5G and the coming 3G services) and in the physical world (by means of smartcards and handheld computers) can only be unlocked if the new communication and transaction mechanisms are adequately safeguarded. The business applications in this cyberspace, m-commerce, and the citizen services, e-Government, for example are totally dependent of the implemented strong security and trusted business procedures.

In order that e-commerce and electronic service delivering will be developed and accepted successfully, on different market segments from consumers to businesses, several underlying technologies, infrastructures and procedures should be specified and implemented with considerable care. This concerns, not only the technology and regulations, but for instance, the balance between risk management and security, as well as the growing importance of the privacy, too.

3.3.2   The power of digital certificates

Digital certificates are by far the most promising technique for safeguarding electronic communications and transactions. Just like passports, diplomas, driver's licenses, and other traditional certificates, these ID certificates can specify any kind of personal data.

Digital certificates are no more than cryptographically protected sequences of zeros and ones, and so they can be transferred electronically to any place on earth without notice-able loss in time or costly human intervention. Digital certificates offer unprecedented security because it is not practically feasible to compute the secret key used to protect a digital certificate.

Digital certificates have already taken off on the Internet, for the purpose of authenticating and encrypting e-mail and software. The Web browsers of all major software manufacturers have built-in capabilities for storing, sending, and verifying digital certificates. Digital certificates are also playing an increasingly important role in other telecommunication networks (such as GSM and GPRS) and in smartcard systems for public transport, electronic payment, for the citizen´s ID cards, and so on.

In the near future, digital certificates will be built into any device or piece of software that must be able to communicate securely with other devices or with individuals. This includes not only all sorts of computers that are clearly recognizable as such, but also televisions, cars, phones, access control to buildings, driver's licenses, ballots, door keys, electronic cash, etc.

3.3.3   The problem – privacy[10] dangers

While their prospects look bright and shiny, digital certificates have a dark side that has received surprisingly little attention thus far. If the current visions about the global PKI (i.e. the collection of all regional, national and international PKIs) turn into reality, then, unless the proper measures are taken, there will be a built-in potential for serious privacy dangers. Each digital certificate can be traced uniquely to the person to whom it has been

---

[9] *Note.* The earlier version of this memo has been sent and discussed also in ETSI m-commerce standardization project in September, 2000.

[10] *Privacy* is defined here the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

issued (or to the device in which it has been incorporated), and can be followed around instantaneously and automatically as it moves through the system.

Even digital certificates that do not specify the identity of their holder (anonymous certificates) can be traced in a trivial manner, because each certificate for security reasons must hold a unique identifier. Digital certificates in this respect are just like digitized fingerprints, Social Security numbers, or credit card numbers.

On the basis of these unique serial numbers, which will travel along whenever an individual engages in a communication or a transaction, organizations and even individuals can compile extremely detailed personal dossiers[11]. The dossiers can be compiled and linked without human intervention, can be dynamically updated in near real time, and will contain minute information about a person´s financial situation, medical history and constitution, habits, preferences, movements and other actions, life style, and so on. Any digital signatures made by certificate holders can be added to their dossiers, and as such, they form self-signed statements that cannot be repudiated. With the cost of digital storage space dropping almost by a hour, all dossiers will be stored potentially forever.

3.3.4   The solution – privacy-enhancing technologies

Privacy protection requires that each individual for him or herself has the power to decide how his or her personal data is collected and used, how it is modified, and to which extent it can be linked -- only this way can individuals remain in control over their personal data.

There are basic privacy-enhanced technologies available that are entirely feasible and secure for achieving these goals. In some of the technologies any user secret can only be computed with the consent of that user, when some technologies use the blinding technology only, or both. Some technologies use self-revocable unlinkability and untraceability, where certificate holders can prove been the originator of a showing protocol execution, can provide and can prove that they were not involved in certain transactions.

It can be constructed highly practical digital certificates that fully preserve privacy, without sacrificing security. These new certificates can be *called private credentials*.

The underlying theory behind the private credentials, discussed in this memo, is from Stefan Brands[12]. See also the White Paper[13].

Private credentials

While identity certificates are similar to passports and other paper-based identity documents, private credentials are more like coins, stamps, votes, gaming vouchers, public transport tickets, and other non-identity certificates (credentials may include as a special case also the ID certs and attribute certs).

Anyone can establish the validity of these certificates and the data they specify, but no more than just that. Furthermore, different actions by the same person cannot be linked.

---

[11] Dossier here means a bundle of documents or record of data with unique label.

[12] Stefan A. Brands, Rethinking Public Key Infrastructures and Digital Certificates, Building in Privacy, The MIT Press, Cambridge, Massachusetts, 2000 (Dissertation).

[13] The White Paper, A Technical Overview of Digital Credentials, Dr. Stefan Brands, Credentica, Feb. 2002.

Private credentials are not only more secure and efficient than their paper-based counterparts, but more powerful too. For instance, a certificate holder can decide for him or herself which part of the data, encoded into a certificate, he or she wishes to disclose.

A certificate can also be presented in such a manner that the verifier of the certificate is left with no evidence at all (much like waving passport when passing customs) or only with evidence of a part of the disclosed property (much like presenting a paper-based certificate with crossed-out data fields so that a photocopy can be made).

The credential technologies are not yet, however, commercially available in a large scale. The development and implementation needs cooperation between various parties from standardization to device manufacturers and from consumers to governments and businesses.

3.3.5   Privacy standardization

Privacy is not yet technically standardized issue. W3C, the body standardizing Internet Web issues, has defined the P3P platform for enhancing the privacy in Web environment. Electronic Identity, based on smart cards and PKI, for example, is very important for the services and applications where true identity is required. But also, the new type of identity, based on such new technology as private credentials, for example, is important for those applications where the true privacy should be negotiable. These types of solutions and technologies should be studied in organizations, like ETSI, from the technical, political and user requirements point of view, as well as from the generic environment and procedures for privacy needs, point of view, too.

Because privacy has a very important role in EU regulations and programs, the new type of privacy enhancing technologies also should play an important role in EU standardization.

Annex A
Glossary

A.1 Acronyms

CA	Certification/Certificate Authority
CI	Card Issuer
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Service Provider
CWA	CEN Workshop Agreements
DS	Digital Signature
e-ID	Electronic ID
ETSI	European Telecommunication Standard Institute
G2B	Government to business
G2C	Government to citizen
G2G	Government to government
GPRS	General Packet Radio Service
GSM	Groupe Systèmes Mobiles or Global System for Mobile communications
HTTP	Hypertext Transport Protocol
INPS	Istituto Nazionale della Previdenza Sociale
ISO	International Organization for Standardization (http://www.iso.ch)
MOC	Match-on-cards
MS	Member State
OCSP	Online Certificate Status Protocol (RFC2560)
OID	Object Identifier
P3P	Platform for Privacy Preferences Project
PIN	Personal Identification Number
PKCS	Public-Key Cryptographic Standard/Public key cryptosystem

PKI	Public Key Infrastructure
POS	Point Of Sales (terminal)
PRC	Population Register Centre
QC	Qualified Certificate
QCP	Qualified Certificate Policy
RA	Registration Authority
RFC	Request For Comments
SEIS	Secure Electronic Information in Society (http://www.seis.se)
SHA-1	Secure Hash Function 1
SIS	Swedish Institute of Standards (http://www.sis.se)
SSCD	Secure Signature Creation Device
TBS	To be signed
TTP	Trusted Third Party
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
W3C	World Wide Web consortium

A.2 Terms

Term	Description
Asymmetric Cryptosystem	Synonym for Public Key Cryptosystem
Authentication	The process whereby a card or a terminal verifies that the other party´s identity is genuine.
Automated Teller Machine (ATM)	A machine which can handle many of the functions of a bank teller, including the dispensing of cash.
Biometrics	Determining a countable, weighable or measurable feature of a living organism, based on a physical or behavioural characteristic. For example a fingerprint or a voice pattern.
CA Certificate	The public self-certified key of the Certification Authority relating to the CA key.
CA Key	An enciphered key used by the Certification Authority to sign certificates and revocation lists.

Card Issuer	The entity responsible for issuing cards and obliged to pay or redeem transactions or balances presented to it. Issuer is usually, but not necessarily, a financial institution or a group of financial institutions.
Card Reader	Equipment that can electronically read the information from one or many types of cards.
Card Holder	Generally the person to whom a nominative card is issued. For financial transaction cards, the card holder is usually the customer associated with the primary account number recorded on the card.
Certificate	Proof that the requirements of certification have been met.
Certificate Holder (Customer)	A person, role person or computer system whose public key has been certified by an enciphered key of a CA and with whose personalised data the certificate is equipped with.
Certificate Label	The label is purely for display purposes (man-machine interface), for example when a user has several certificates (e.g. "signature certificate", "authentication certificate", etc.)
Certificate Revocation List (CRL)	A list of certificates cancelled before their periods of validity have expired. A certificate which has been placed on the revocation list cannot be re-activated for use.
Certificate Provider	The role of the certificate provider (also known as CSP) is to issue: - IAS certificates and attribute certificates related to the card holder - Any other certificates used for the functioning of the smart card information system.
Certification Authority	A body able to certify the identity of one or more parties in an exchange (an essential function in Public Key Cryptosystems).
Clearing	The process of transmitting, reconciling and, in some cases, confirming financial transactions between financial institutions prior to settlement, possibly including netting of instructions and the establishment of final positions of settlement. Sometimes the term is used (imprecisely) to include settlement.
Contact	A point of electrical connection between an integrated circuit card and its external interface device. ISO standard IC cards have eight contacts (the contact plate is commonly called a module).
Cryptography	The science of transforming confidential information to make it unreadable to non-authorised parties (see also Public Key, Private Key, DES, RSA).
Customer	The certificate holder, certificate owner.
Digital Certificate	A public key directory entry that has been signed or validated by a certification authority. Digital certificates are used to verify digital signatures.
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and

	integrity of the data unit and protect against forgery, e.g. by the recipient. Digital signature is a special case of a more general electronic signature.
Electronic Identification Card	An identification card issued by the police in which a FINEID application has been stored in the technical section.
Electronic Signature	Data in the electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data
Encryption	A means of scrambling data so that it can only be understood by the party that has the key to changing it back to its original format. In the plastic card world, the encryption of data is performed using either a private key cryptographic system such as DES or a public key cryptographic system such as RSA.
Encipherment	The process of converting plain text into ciphertext using a sipher and a key
End User	A person, role person or computer system that is a FINEID certificate holder or user but not a certification authority or a local registration authority.
European Telecommunication Standard Institute (ETSI)	The EU organisation in charge of defining European telecommunications standards. The most well known European telecom standard is GSM. ETSI has been very active in the Smartcard field in building European standards where there are holes in the ISO standards. All ETSI card standards work is based on ISO standards where published.
Global System for Mobile communications (GSM)	Global System for Mobile Communications, a European standard for digital cellular telephones that has now been widely adopted throughout the world. Under the ETSI standard, GSM telephones contain a SIM smartcard that identifies the individual subscriber.
Identification	Determination of the identity of a person or a good.
International Standards Organisation (ISO)	ISO has published standards for a variety of cards and work continues on smartcards (contact and contactless), optical memory cards and others. For smartcards, the central standard is ISO 7816. ISO 7816-1 Physical Characteristics of IC cards ISO 7816-2 Position of Module and Contacts on IC cards ISO 7816-3 Exchange protocol with IC cards (i.e., communication between readers and cards) ISO 7816-4 Command set for microprocessor cards
Interoperability	The ability of several systems or system components to work together actively. More specifically for the OIC a tuning of chip card application systems and system components in such a way that more than one application of different application providers can be combined on one card (co-branding), or so that a cardholder can purchase several services from different service providers through a CAD of one of these service providers.

Key	A value that is used with a cryptographic algorithm to encrypt, decrypt or sign data. Secret Key Cryptosystems use only one secret key. Public Key Cryptosystems used a public key to encrypt data and a private key to decrypt it.
Key Length	The number of bits forming a key. The longer the key, the more secure the encryption. Government regulations limit the length of cryptographic keys in a number of countries.
On line	This refers to any system where individual components are connected via telecommunications lines either directly to each or indirectly via a switching centre. In the card area, it is used to refer to a system where both the cards and the operations which are carried out with them are authorised by a central processor.
Personal Identification Number (PIN)	Secret code entered into a terminal (ATM, POS) to identify the card holder.
Private Key	Secret part of an asymmetric key pair e.g. signature creation data as specified in the EU directive for electronic signatures.
Protocol	A set of rules and procedures governing interchange of information between a smartcard and a reader. The ISO defines several protocols, including T=0, T=1 and T=14.
Public Key (PK)	Public Key Cryptosystems are based on trapdoor one way functions. Forward direction: encryption, Inverse direction: decryption.
Public Key Infrastructure (PKI)	Data Transmission Infrastructure which considers security, confidentiality, integrity, availability, authentication, non repudiation and certification aspects
Qualified certificate	Certificate which meets the requirements laid down in annex I (of the Directive) and is provided by a certification-service-provider who fulfils the requirements laid down in annex II (of the Directive 1999/93/EC).
Registration Authority (RA)	Authority in a PKI which verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it.
Revocation List Service Provider	A provider receiving revocation list requests and transmitting them into the certificate system.
Root Certificate	A self-signed certification authority (CA) certificate that identifies a CA. The root CA must sign its own CA certificate because by definition there is no higher certifying authority to sign its CA certificate.
Secret Key	Value used in an algorithm to enable authentication or communication ciphering.
Smartcard	This term is used in CCITT for plastic cards of ISO standard dimensions with a chip embedded towards the middle of the left-hand side. It should maybe be noted that a vast majority of such cards in circulation today are not "smart" in the true sense at all, but are simple prepaid cards without a microprocessor. Under this definition, there are three basic types of smartcards. These are prepaid or stored value cards either of the throwaway or

	reloadable type, simple wired logic cards able to handle multiple functions and microprocessor equipped cards able to perform functions on the information stored in them. The latter contain a CPU for data processing and security functions, RAM for storing interim calculations, ROM for storing programs and operating instructions and either EPROM or EEPROM for storing specific information about the individual card. Smartcards of all three types may be of the contact or contactless variety.
Smartcard Community	A Smart Card Community is made up of all smart cards issued and managed by a given card issuer
TBS Certificate	The field contains the names of the subject and issuer, a public key associated with the subject, a validity period, and other associated information (RFC 3280).
X509	CCITT recommendation for authentication of users of directory services.

Annex B
Bibliography

Part I: Minimum requirements for a European Electronic Identity

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

IETF PKIX RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

IETF PKIX RFC 3039 - Internet X.509 Public Key Infrastructure Qualified Certificates Profile

FINEID S4-1 (Finnish Electronic ID Application)

SEIS (Secured Electronic Information in Society)

ETSI TS 101 456 v. 1.2.1, Policy requirements for certification authorities issuing qualified certificates

Part II: Current Practices in Establishing Identity

The enquiries from 16 January 2001 and 16 March 2001 supplemented by information from the following documents:

e-ID of citizens and organisations in the European Union: State of Affairs, A report drawn up by Dr Jean-Michel Eymeri, Senior Lecturer at European Institute of Public Administration, Maastricht (NL) for the 37th Meeting of the Directors-General of the Public Service of the Member States of the European Union Bruges, 26 and 27 November 2001

IPSE-SG Final Report 1, A report drawn up by Initiative for Privacy Standardization in Europe (IPSE) and issued on 13 February 2002

eESCC TB2 Pre-Inventory, A report drawn up by TB2 of Smart Card Charter and issued in November 2001

Survey of smart card-PKI-projects, A report drawn up by EDS and Smart is Marketing for IDA and TB10 (e-government), issued on 10 July 2002; the review done by TB 10 is completing this document.

Digital Signature Law Survey by Simone van der Hof from the Tilburg University in the Netherlands at http://rechten.kub.nl/simone/ds-lawsu.htm

Part III: Aspects Related to e-ID Evolution and Implementation

EU directives and decisions on data protection and privacy:

Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the Protection of indivduals with regard to the processing of personal data and on the free movement of such data; Official Journal L 281, 23/11/1995 P. 0031 - 0050

Decision of the European Commission 01/497/EC setting out standard contractual clauses ensuring adequate safeguards for personal data transferred from the EU to countries outside the Union; Official Journal L 181, 4/7/2001 P. 0019 - 0031

Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector; Official Journal L L 024 , 30/01/1998 P. 0001 - 0008

Directive 01/45/EC of the European Parliament and the Council of Ministers on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; Official Journal L 008, 12/01/2001, P. 0001 - 0022

Directive 99/93/EC of the European Parliament and the Council of Ministers on a Community Framework for Electronic Signatures; Official Journal L 13, 19.1.2000, P. 0012 - 0020

Directive 00/31/EC of the European Parliament and the Council of Ministers on a Legal Framework for Electronic Commerce; Official Journal L 178, 17/07/2000, P. 0001 – 0016

National data protection legislation:

http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.html

Annex C
Contributors

This White Paper has been prepared with contributions from:

Tapio	Aaltonen	Finnish Population Register Centre	tapio.aaltonen@vrk.intermin.fi
Jan	van Arkel	e-Europe Smart Card Charter	arkel@cardlife.nl
Stefan	Engel-Flechsig	Radicchio	stefan.engel-flechsig@radicchio.org
Arno	Hollosi	Chief Information Office Austria · Operative Unit	arno.hollosi@cio.gv.at
Esa	Kerttula	Prof-Tel Oy	esa.kerttula@proftel.pp.fi
Voitto	Kiviharju	Finnish Population Register Centre	voitto.kiviharju@vrk.intermin.fi
Marc	Lange	Build in Europe	Marc.Lange@Build-in-Europe.be
Robert	Müller	Giesecke & Devrient	ex-Robert.Mueller@de.gi-de.com
Hans	Nilsson	Hans Nilsson Consulting	hans.nilsson@nilsson.com
Mika	Pohjolainen	Finnish Population Register Centre	mika.pohjolainen@vrk.intermin.fi
Dirk	Scheuermann	Fraunhofer – Institut für Sichere Telekooperation	dirk.scheuermann@sit.fraunhofer.de
Vicente	Sebastián	ETRA I+D	vsebastian.etra-id@grupoetra.com
Christos	Sioulis	Athens Bar Association	csioulis@dsa.gr
Theo	van Sprundel	SchlumbergerSema	Theo.Vansprundel@bull.nl
Bruno	Struif	Fraunhofer – Institut für Sichere Telekooperation	struif@sit.fraunhofer.de