ETSI TR 102 438 V1.1.1 (2006-03)

Technical Report

Electronic Signatures and Infrastructures (ESI); Application of Electronic Signature Standards in Europe

Reference

DTR/ESI-000044

Keywords

IP, electronic signature, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

1 Scope

A number of initiatives were started in Europe, funded by the European Commission, in order to provide support to the Directives that apply electronic signatures and have their roots in Directive 1999/93/EC [1], among which Directive 2001/115/EC [2] addressing invoicing in respect of value added tax.

These initiatives regard, or regarded, the following subjects: e-invoicing, e-procurement, e-authentication. They also address electronic storage and have furtherance on development of CWA 14890 Smart Card. Electronic registered email is also being developed inside and outside Europe.

All these subjects are impacted by, and may benefit from, the documents on electronic signature that were developed by ETSI TC ESI, along with the CEN Workshop El-sign. ETSI has launched an STF to harmonize the above mentioned initiatives to the existing ETSI Technical Specification (TS), in order to optimize interoperability.

The present document presents the results of this work to assist in the harmonization of the use of election signature standards across Europe. Where other bodies activities were already closed when STF 288 was launched, or closed during the STF 288 performing time, reports are attached as annexes summarizing, through abstracts and extracts, the documents issued by the such bodies.

2 References

For the purposes of this Technical Report (TR), the following references apply:

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

NOTE: The above is referred to as "the Directive" in the present document.

[2] Directive 2001/115/EC Council Directive of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax.

[3] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[4] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[5] ETSI TS 101 862: "Qualified certificate profile".

[6] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[7] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

[8] ETSI TS 102 280: "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

[9] CWA 15264-01: "Architecture for a European interoperable eID system within a smart card infrastructure".

[10] CWA 15264-02: "Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services".

[11] CWA 15264-03: "User Requirements for a European interoperable eID system within a smart card infrastructure".

[12] ISO/IEC 10536-1 (2000): "Identification cards - Contactless integrated circuit(s) cards - Close-coupled cards - Part 1: Physical characteristic".

[13] ISO/IEC 10536-2 (1995): "Identification cards - Contactless integrated circuit(s) cards - Part 2: Dimensions and location of coupling areas".

[14] ISO/IEC 10536-3 (1996): "Identification cards - Contactless integrated circuit(s) cards - Part 3: Electronic signals and reset procedures".

[15] ISO/IEC 14443-1 (2000): "Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1: Physical characteristics".

[16] ISO/IEC 14443-2 (2001): "Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 2: Radio frequency power and signal interface".

[17] ISO/IEC 14443-3 (2001): "Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anticollision".

[18] ISO/IEC 14443-4 (2001): "Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol".

[19] ISO/IEC 15693-1 (2000): "Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 1: Physical characteristics".

[20] ISO/IEC 15693-2 (2000): "Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 2: Air interface and initialization".

[21] ISO/IEC 15693-3 (2001): "Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 3: Anticollision and transmission protocol".

[22] Sixth council directive of 17 May 1977 on the harmonization of the laws of the Member States relating to turnover taxes - Common system of value added tax: uniform basis of assessment (77/388/EEC).

[23] Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects of electronic data interchange.

[24] Commission decision of 14 July 2003 on the publication of reference numbers of generally recognized standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council.

[25] CWA 14890-1: "Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements".

[26] CWA 14890-2: "Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services".

[27] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[28] CEN EN 1332-4: "Identification Card Systems - Man-Machine Interface - Part 4 : Coding of user requirements for people with special needs".

[29] CWA 13987-1: "Smart Card Systems: Interoperable Citizen Services: Extended User Related Information - Part 1: Definition of User Related Information and Implementation".

[30] CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".

[31] CWA 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)".

[32] CWA 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)".

[33] CWA 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP".

[34] CWA 14169: "Secure Signature-creation devices "EAL 4+"".

[35] CWA 14170: "Security requirements for signature creation applications".

[36] CWA 14355: "Guidelines for the implementation of Secure Signature-Creation Devices".

[37] CWA 14890-1: "Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements".

[38] CWA 14890-2: "Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services".

[39] ISO/IEC 14443: "Identification cards - Contactless integrated circuit(s) cards - Proximity cards".

[40] ISO/IEC 15693: "Identification cards - Contactless integrated circuit(s) cards - Vicinity cards".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

advanced electronic signature: electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

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

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable (see Directive 1999/93/EC).

certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

NOTE: See ITU-T Recommendation X.509.

certification authority: authority trusted by one or more users to create and assign certificates

NOTE 1: See ITU-T Recommendation X.509.

NOTE 2: A certification authority is a certification-service-provider issuing certificates.

certificate policy: named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

NOTE: See ITU-T Recommendation X.509.

certification practice statement: statement of the practices which a certification authority employs in issuing certificates

NOTE: See RFC 3647 [27].

Certification-Service-Provider (CSP): entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

NOTE 1: See Directive 1999/93/EC [1].

NOTE 2: The present document is concerned with certification service providers issuing qualified certificates (or component services for issuing qualified certificates. The present document is not concerned with other types of CSP functions such as time-stamping and key escrow.

EDIFACT - Electronic data interchange for administration, commerce and transport: ISO standard providing a set of ten Application level syntax rules addressing EDI communications

Electronic Business using eXtensible Markup Language - ebXML: a modular suite of specifications that enables enterprises of any size and in any geographical location to conduct business over the Internet

NOTE: From the ebXML site http://www.ebxml.org/geninfo.htm.

Electronic Data Interchange: transfer of commercial, administrative and business information between computer systems, using data formats which have been mutually agreed by the parties (94/820/EC: Commission Recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange)

Electronic Invoice: invoices sent by electronic means

electronic signature: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data

NOTE: See Directive 1999/93/EC [1].

Porvoo Group: international cooperative network whose primary goal is to promote a trans-national, interoperable electronic identity, based on PKI technology (Public Key Infrastructure) and electronic ID cards, in order to help ensure secure public and private sector e-transactions in Europe

NOTE: From the Porvoo Group web site: http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/20710B02C6C5B894C2256D1A0048E290/.

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)

Qualified Certificate Policy (QCP): certificate policy which incorporates the requirements laid down in annex I and annex II of the Directive 1999/93/EC

qualified electronic signature: advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device, as defined in article 5.1 of the Directive 1999/93/EC

secure-signature-creation device: signature-creation device which meets the requirements laid down in annex III of Directive 1999/93/EC

signature-creation data: unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

NOTE 1: See Directive 1999/93/EC [1].

NOTE 2: In qualified certificates based on public key cryptography, as covered by the present document, the signature-creation data is, for example, a private key. Hence, within the present document the term private key is used for the signature-creation data.

signature-creation device: configured software or hardware used to implement the signature-creation data

NOTE: See Directive 1999/93/EC [1].

UN/CEFACT - United Nations Centre for Trade Facilitation and Electronic Business: a United Nations body. It encourages close collaboration between governments and private business to secure the interoperability for the exchange of information between the public and private sector. It has develop (UNECE - United Nations Economic Commission for Europe web site).

Value Added Network: provider of EDI focused network services

X-12: one of the three major sets of EDI standards, along with UN/EDIFACT and the Uniform Communication Standard (UCS); it is developed and managed by ANSI ASC.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AdES	Advanced Electronic Signature
ASP	Application Service Provider
CA	Certification Authority
CAdES	CMS Advanced Electronic Signatures
CEN	Comité Européen de Normalisation
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
EbXML	Electronic business using eXtensible Markup Language
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
EESSI	European Electronic Signature Standardisation Initiative
ERP	Enterprise Resource Planning
ESI	Electronic Signatures and Infrastructures
HSM	Hardware Security Module
IAS	identity, authentication, electronic signature
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	On-line Certificate Status Protocol
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
PP	Protection Profile
SCA	Signature Creation Application
SSCD	Secure Signature Creation Device
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
VAN	Value Added Network
XAdES	XML Advanced Electronic Signatures (XAdES)

4 Monitored Bodies and Workshops

Particular considerations were given to the activities of the following bodies and their deliverables in considering the application of the electronic signature standards with the aim of harmonizing their use.

1. e-Invoicing (see clause 5):

   a) CEN/ISSS e-Invoicing Focus Group on Standards and Developments on electronic invoicing relating to VAT Directive 2001/115/EC [2] - see clause 5.1; an abstract of its final deliverable is attached as annex A;

   b) CEN/ISSS eInvoicing Workshop on "Interoperability of Electronic Invoices in the European Union" - a report on its ongoing activities is in clause 5.2.

2. e-Procurement: CEN/ISSS Workshop on eProcurement (see clause 6);

3. e-Registered mail: (see clause 7) - Universal Postal Union - Electronic PostMark;

4. CEN/ISSS Workshop on e-Authentication (clause 8):

   a) Part 1: Architecture for a European interoperable eID system within a smart card infrastructure;

   b) Part 2: Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services;

   c) Part 3: User Requirements for a European interoperable eID system within a smart card infrastructure;

   d) Towards an electronic ID for the European Citizen, a strategic vision:

   Abstracts of the previous documents are in annex B.

5. CEN/TC 224 Machine Readable Cards, related device interfaces and operations - Transformation of some CWAs into ENs (clause 9).

5 e-Invoicing

5.1 CEN/ISSS e-Invoicing Focus Group

To implement the goals of Council Directive 2001/115/EC [2], the European Commission requested CEN/ISSS to prepare an overview on standardization issues relating to electronic invoicing. CEN/ISSS set up an open "e-invoicing Focus Group", and issued a report analysing requirements on standardization issues relating to electronic invoicing resulting from the new VAT legal framework.

The CEN/ISSS e-Invoicing Focus Group final report, issued in the last months of year 2003, examines the standards relevant issues related to e-Invoicing and VAT in relation to the Council Directive 2001/115/EC [2] that details the conditions "*for invoicing in respect of value added tax*", in particular regarding requirements on taxable persons and their service providers.

A summarization of this final report is presented in annex A.

5.2 CEN/ISSS Workshop on "Interoperability of Electronic Invoices in the European Union"

5.2.1 Workshop purpose

This CEN Workshop acts upon Mandate M339 from DG Enterprise and concerns standardization in the domain of electronic invoices in the European Union, in order to support the implementation of the Council Directive 2001/115/EC [2].

The Workshop builds upon "the Report and Recommendations of CEN/ISSS e-Invoicing Focus Group on Standards and Developments on electronic invoicing relating to VAT Directive 2001/115/EC [2]", published in 2003.

The Workshop objective [from the Workshop Business plan] refers in particular to intra-EU transmission, storage of electronic invoices, and their mandatory information rather than their content. Further, since the primary role of an invoice is as a request for payment, the Workshop shall also take due account of requirements concerning payment requests as appropriate. The Workshop may also make recommendations concerning standardization of commercial invoicing issues.

The output of this Workshop will be one CEN Workshop Agreement to be released in mid 2006.

5.2.2 Workshop organization

The WS had its operational kick off meeting on 9 February 2005, where its activities were defined and the WS participants were appointed. The WS addresses the following four subjects:

1) EDI;

2) Electronic signature;

3) Storage;

4) Modelling.

The WS is planned to make documents available for public comment publish the in early 2006, finalize its operations in mid 2006.

The WS is organized in 3 main tasks, addressing:

1) EDI and Business standards;

2) Electronic Signature for eInvoices;

3) Overall work items.

The Workshop specific main purposes follow (texts extracted from the WS Work Plan). For each of them one Task has been set up.

Task 1 - EDI and Business standards

1. To prepare a draft new version of Directive 1994/820/EC including a generic and open definition of the term EDI ("EDI definition").

2. To produce the list of invoice content details expressed as UN/CEFACT Core Components ("Invoice core components").

3. Recommendation to allow identifiers as an alternative to the current unstructured clear text identifications ("Identifiers").

4. To prepare a standardized set of codes with definitions to replace plain text in invoice messages ("Code sets").

5. To collect from each Member State the ways data elements are applied. Revise the existing list from the Focus group. Group, and propose a harmonized approach ("Data elements").

Task 2 - Electronic Signature for eInvoices

1. To produce guidelines specifying how to apply digital signatures to companies; define exactly which certificates are necessary to use and the merits of a hardware solution such as HSM or a soft-token based solution for implementation ("Companies signatures").

2. To produce guidelines specifying how to apply digital signatures to multi-tier communications used by this "trusted third party" [intermediary service provider] to sign the electronic invoices on behalf of the supplier, that is authorized by the VAT authority and accepted by biller and receiver of electronic invoices ("AES").

   NOTE: Under evaluation to change it to "AdES", to avoid confusion with the symmetric algorithm and consistently with the ETSI acronym used in TS 101 903 [7].

3. To detail standardization objectives of authentication ("Authentication").

Task 3 - Overall work items

1. To prepare recommended archiving guidelines focused on rules and guidelines for inspection. This includes also the kind of data, and the traceability of commercial operations ("Archiving Guidelines").

2. To contact relevant authorities in E.U. (to establish a number of common arrangements governing the use of electronic invoicing) ("Authorities").

3. To describe rules and guidelines for service providers, such as ASP and VAN, to facilitate interoperability between customers, service providers and payment institutions as well as between different service providers, especially in an international environment (cross-border, invoicing and payment).A secondary objective is to get tax authorities" buy in, especially in questions relating to data integrity and data storage ("Service Providers").

Task 4 - To define an e-Invoicing model ("Model")

The latest meeting was held in Brussels on 10/11/2005, and the next will be held in Brussels on 26 January2006. In the meantime a number of meetings, both in person and virtual (i.e. conference calls) are being held by members of the various Tasks and subtasks. Further meetings are envisaged until mid 2006, to discuss and resolve comments public coming and to finalize the documents.

5.2.3 Applicability of existing ESI standards and potential additional requirements on ESI standards

A formal liaison was established between ETSI TC ESI and the CEN WS and the ETSI ESI representative has been included in the Team regarding Task 2.1, addressing companies signatures (please see above), as clearly specified among the Task 2.1 Milestones in the mentioned Work programme:" … *Discuss with ETSI/ESI and any future CE e-signature activity*".

TS 101 903 [7] and TS 101 733 [6] will be addressed in an annex of the CWA as signature formats that may be used for signatures on invoices (for further details see below). This CEN WS and the new ETSI STF on signature format profiles would mutually benefit from jointly defining the relevant requirements and the relative profiles suitable for the eInvoices.

5.2.4 Report on electronic signature related matters

5.2.4.1 Introduction

Directive 2001/115/EC [2] regarding eInvoicing makes explicit reference to advanced electronic signatures as one means to ensure authenticity and integrity to electronic invoices. The second specified method is EDI, "*when the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data*". As a third option Member states can accept other electronic means. This item is being widely discussed by the WS Task 2.

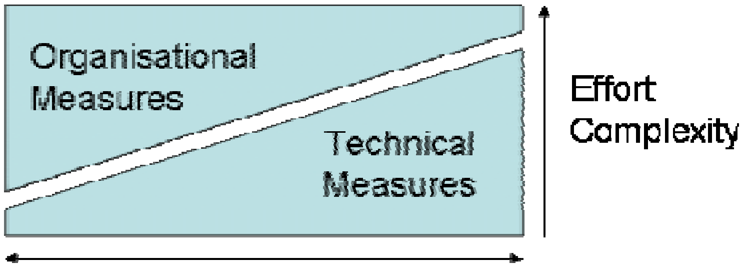
A strict interaction has been found between Task 2 and the Task 3 subtask related to eInvoices storage, that is explicitly and widely addressed by the Directive. Invoices are to be kept, depending on the applicable law) from a minimum of four years to 10 years.

5.2.4.2 ETSI relevant CEN WS matters

The CWA issued by the WS will be structured in various parts, the first of which will specify all common definitions and assumptions.

Among the other CWA parts, one will regard electronic signatures and another the eInvoices storage.

It has been agreed that the security measures to be applied to electronic signatures in order to ensure them a suitably long life are inversely related to the reliability of the organization in charge of their storage: the more reliable this organization (and consequently the greater their commitment to security and the more specific their organizational measures), the simpler the electronic signature format can be, as sketched in the following figure (from the CWA that will be published).



The basic requirements for electronic signatures types will be defined in the main document body, as per the previous remark. Depending on the assumed organizational measures, it will be specified which signature features apply, for example: where a simple ES is enough, where a time stamp token is necessary and sufficient, where complete certificate and revocation references, etc.

The XAdES formats specified in TS 101 903 [7], as well as the CAdES ones specified in TS 101 733 [6], that provide the above mentioned features, will be referenced in an annex, but the current CEN WS position is not to recommend usage of TS 101 903 [7] or TS 101 733 [6] formats, despite their having been developed by a standardization body on the basis of European Commission Mandates, because they are deemed too complicated by the eInvoice users" community. Where other electronic signature formats will be brought to the Task 2 attentions that provide analogous reliability levelssimilar annexes will be added.

5.2.4.3 EDI vs. electronic signatures

There are different viewpoints between supporters of electronic signatures and of EDI.

A possible solution has been proposed, and also endorsed by some of the WS participants, based on the following clarification.

On the one hand an electronic signature per se, where correctly carried out, is capable to provide suitable security features compliant with the Directive 2001/115/EC [2] that can ensure the signature itself the life span required by the invoices relevant applicable laws.

On the other hand, EDI requires agreements between parties on the exchanged document format. In this regard, Directive 2001/115/EC [2] specifies: "*when the agreement relating to the exchange* ***provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data***". One possible way to provide this guarantee can be the usage of suitably structured advanced electronic signature.

5.2.4.4 eInvoices storage vs. electronic signatures

As previously hinted to, where a suitably reliable organization takes care of storing the eInvoices and of safely keeping the storage media for the required time lapse, there is no need for a fully fledged ES-A like format. Conversely, where no such organization exists, a signature format intrinsically capable to withstand a long storage period (like ES-A) should be used.

The CEN WS will evaluate if this concept is to be elaborated to the point to produce recommendations.

5.2.5 Any recommendations

A specific attention has been given to Task 2 activities, particularly to the possible technical decisions by the Workshop regarding Advanced Electronic Signatures and corporate/organizational signatures.

Given the close relationship between Task 3.3 on authentication and the recently closed CEN Workshop on eAuthentication, a particular attention has also been given to this sub task to, where possible, achieve the best harmonization also in this field.

It has been brought to the CEN WS attention that when involved parties can agree that one audit log may be taken as a reference, then Time-Stamping can be replaced by Time-Marking. However, in case where the information from that third party is challenged, ways to demonstrate that the information really comes from that audit log may not be that simple and may be more costly and time-consuming than time-stamping techniques.

6 e-Procurement

6.1 Context

The issue of electronic procurement has been identified by the CEN/ISSS e-Business Focus Group, as being one of a number of key topics requiring more coherent standardization activity over the 2003-2005 timeframe. There has been other support for a dedicated activity from other CEN/ISSS groups and other stakeholders. EDI was and is still used where there is a regular exchange between buyer and seller, but there was no recent overviews of procurement requirements, in the context that procurers are moving towards e-procurement in a more general way, with the use of the Internet, or use of electronic auctions or a fully-electronic tendering process.

On 14 October 2003, a kick-off meeting for a Workshop was launched by CEN/ISSS on eProcurement, with the aim to promote and facilitate the use of inter-operable private and public eProcurement solutions in Europe, based on internationally recognized solutions and standards.

The Workshop appointed a team of experts in December 2003. The Workshop issued several drafts for comments and the final draft was released for public review, with comments awaited until 29 November 2004. The fourth and last meeting was held on 16 December 2004 and dealt with the comments received.

A disposition of comments was issued on 15 December 2004 (ePRO 039). Based on this disposition of comments the draft was subsequently revised and a revised draft was published on 22 December 2004 (ePRO 040).

The revised draft was made available for voting until 20 January 2005 and then approved as:

- **CWA 15236:** "Analysis of standardization requirements and standardization gaps for eProcurement in Europe".

The workshop was closed on 21 February 2005.

The web page of this workshop is:
http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/about_isss/wsepro.asp

Further information about WS/ePRO is available from the Workshop pages, hosted by the Workshop Secretariat held by NEN. See http://www.nen.nl/wseprocurement/.

6.2 Outcome of the workshop

The workshop has approved and published the following document:

- **CWA 15236:** "Analysis of standardization requirements and standardization gaps for eProcurement in Europe".

The conclusions and recommendations of this report must be considered as a starting point.

The 95 pages document is directly downloadable from:
ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eProc/cwa15236-00-2005-Feb.pdf

This CEN copyrighted CWA is available for downloading provided on the condition that it may not be modified, re-distributed, sold or repackaged in any form without the prior consent of CEN, and are only for the use of the person downloading them. For additional copyright information, please refer to the statements on the cover pages of the CWAs concerned.

6.3 Main content of CWA 15236

"Procurement" covers a very wide range of different standards issues in different groups. At one end of the chain are the principles of e-cataloguing and product classification, then moving into issues related to the business transaction process - seeking bidding document/offer/selection of bidders/transaction/delivery/invoicing, etc.

6.3.1 The main phases of e-Procurement

The four main phases of e-Procurement identified in this report are the following.

6.3.1.1 e-Tendering

This is the phase where an invitation to tender from the buying party is usually sent to parties known to them or their advising consultants.

6.3.1.2 e-Ordering

This is the phase where the buying party places an order to a winning tender.

6.3.1.3 e-Despatching

The despatch advice transaction provides information to the customer/consignee on the goods that have been shipped. The level of detail and accuracy of the information in the despatch advice transaction and the timeliness of the exchanges render this message extremely important in logistics and supply chain management in most industry sectors.

6.3.1.4 e-Invoicing

The commercial invoice is an accounting document, exchanged between trading partners. In addition to its commercial value, the invoice it has legal implications to both transacting parties, and it is the basis for accounting, VAT declaration and reclamation, for import, export and transit declaration of goods in the European community.

Because the legal status of an electronic invoice is only now being cleared and the VAT requirements laid down in the VAT Directive 2001/115/EC [2], private companies have often limited the implementation of the electronic invoice to inter company accounting, and have maintained the invoice paper process for VAT and legal requirements.

In response to a standardization mandate from the European Commission, CEN/ISSS has established a Workshop on Electronic Invoicing (WS/eINV). This Workshop follows up the report of a CEN/ISSS Focus Group assessing standards requirements. Details of the Workshop are to be found at http://comelec.afnor.fr/cen/wsei. A report on these CEN Worskhops activities can be found in clause 5.

6.3.2 The relationship with the EESSI work

The importance of the work done under the EESSI is acknowledged in clauses 1.3.4.6.1-6 which are copied below:

1.3.4.6.1 Non-repudiation

In electronic procurement the non-repudiation of transactions is a mandated requirement. Non-repudiation is addressed in Directive 1999/93/EC on a Community framework on electronic signatures (article 5.2). Pursuant to Directive 1999/93/EC, technical standards have been promulgated within ETSI ESI and CEN/ISSS e-Sign WS.

Among these standards the most prominent in the area of non-repudiation is ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates. However due to the approach adopted in the Directive with regard to non-repudiation the ETSI ESI standards are not the only way to meet the requirements set out in the Directive on electronic signatures. Confirmation that the various non-repudiation standards meet the requirements of public electronic procurement is a possible further step that can be addressed through best practices.

1.3.4.6.2 Authentication

In electronic procurement means of communication and electronic signatures provide for the authentication of data exchanged by parties involved in a transaction including sender and recipient. Authentication has assumed legal content pursuant to article 5.1 of Directive 1999/93/EC on a Community framework on electronic signatures. Pursuant to Directive 1999/93/EC, a number of technical standards have been promulgated in the context of ETSI ESI.

Among these standards the most prominent in the area of authentication is TS 102 042 Policy requirements for certification authorities issuing public key certificates. Authentication is also foreseen as requirement in the Directive on electronic invoices (00/115/EC). The Report of the CEN/ISSS eInvoicing Focus Group provides valuable insight in this regard. The CEN/ISSS WS on eInvoicing will produce additional input and standards in the area of authentication by means of electronic signatures. The CEN/ISSS WS on eAuthentication that aims at addressing requirements for public identity in the context of smart cards is yet another source of standards in electronic authentication. Confirmation that authentication standards meet the requirements of public electronic procurement is a possible further step that can be addressed through technical standards.

1.3.4.6.3 Time stamping

Time stamping is a requirement for the non-repudiation of a transaction. Pursuant to Directive 1999/93 on electronic signatures requirements for time stamping have already been addressed in standards that include ETSI TS 102 023 Policy requirements for time-stamping authorities. Coordinated efforts are further needed to address time stamping requirements in specific stages of an electronic public procurement process where that is mandated. In electronic public procurement the mandated requirement is those incoming tenders are time-stamped and locked until the specified time and date set for opening. Additionally all handling and manipulation of data concerned should be traceable. Therefore time-stamping standards have to be reviewed in the context of electronic public procurement by means of best practices.

1.3.4.6.4 Role attributes

*Certificate management allows for the attribution of specific features that include authorization to **act under a role**, or the award of an attribute. While ETSI TS 101 158 Policy requirements for attribute authorities sets out a general standardization framework for the use of attributes, it is necessary to further specify this framework with regard to electronic public procurement.*

Currently attributes and attribute certificates present an appropriate way to manage privileges.

Attributes have to be reviewed, however, in connection with DRM as well as any other technical solution aiming at controlling access and privileges within an eProcurement system. Best practices developed by stakeholders emerge as an appropriate way to address this issue.

1.3.4.6.5 Signature policies for public authorities

In article 6, Directive 1999/93/EC states that: "Member States and Commission (shall) work together to promote development and use of signature verification devices, in the light of the recommendations in Annex IV and in the interest of the consumer". In the broad context of its application, the Directive mandates the usage of all support elements for electronic signatures that can be useful to the end-user of a service. As such a signature policy can be seen as a mechanism that enhances the level of trust and support the verification of the identity of a signatory in a transaction.

Signature policy is a set of rules to create and validate electronic signatures, under which an electronic signature can be determined to be valid in a particular transactions context.

Standardization within ETSI ESI has already resulted in technical specifications and technical reports on signature policies. A signature policy may be written using a formal notation like ASN.1 or in an informal free text form provided the rules of the policy are clearly identified. When two or more parties transact in an electronic business environment they may need to define the conditions under which a particular electronic signature can be used. A signature policy describes the scope and the usage of such an electronic signature with a view to address the conditions of a given transaction context. In eProcurement there is often a need that several parties have to sign the same document. Verifying that a transaction bears the right number of electronic signatures from designated is a matter that has yet to be addressed.

In electronic public procurement it is necessary to identify the requirements for a signature policy that meets the requirements of contracting authorities. Signature policies must additionally include rules regarding the use and validation of timestamps together with electronic signatures.

Technical standards must be leveraged to develop signature policies for contracting authorities that allow for single as well as multiple signatories and relying parties and thus safeguard tenders from unauthorized access or use.

1.3.4.6.6 XML signatures

One goal for eProcurement systems is to enable XForms by supporting browser that produces XML-digital signatures. A framework is required to enable WYSIWYS ("What You See Is What You Sign") for XML documents. It is necessary to create XML Signatures according to ETSI TS 101 903 standard XML Advanced Electronic Signatures (XAdES). In addition ETSI has carried out a number of plug tests based on ETSI XadES.

The ETSI XadES standard extends the IETF/W3CXML-Signature Syntax and processing specification [XMLDSIG] into the area of non-repudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and meet the requirements of the European Directive on electronic signatures. Further standardization work through best practices is required, however, to ensure that the ETSI XadES standard is properly implemented in eProcurement.

The importance of the work done under the EESSI is also acknowledged for legal aspects in clause 2.3.1: "European Electronic Signatures Standardization initiative".

"The deliverables of the EESSI have held a pivotal position in the effort to deploy interoperable electronic signatures in the EU. Since its inception in 1999 EESSI has focused on electronic signatures in relation to Directive 99/93/EC. The EESSI deliverables have widely been acknowledged for being generic, flexible and applicable in a multitude of transactions."

6.3.3 The recommendations

The most important clause is clause 2.3.7 "Standardization recommendations for electronic public procurement" and particularly the statements related to **electronic signatures** and **signature policies** which are copied below.

Electronic signatures

Electronic signatures can benefit from additional standardization in the following areas:

- *Providing harmonized and widely published evaluation and approval criteria regarding the trust service providers. Potential benefits of a profile of the above TSL standard should be investigated in order to facilitate and speed up implementation and deployment for eProcurement.*

- *Specifying the requirements for CSPs issuing certificates to issuers of qualified certificates for the end user.*

- *Authentication with emphasis on trust status lists and consideration for identity management at large in order to lay out the requirements pertaining to electronic public procurement.*

- *Delegating electronic signatures and applying multiple signatures in a single document."*

Signature policy

In electronic public procurement it is necessary to identify the requirements for a coordinated signature policy that meets the requirements of contracting authorities in terms of e.g. the number of signatures that have to be applied.

Some other recommendations are present outside this section. For example:" in eProcurement there is often a need that several parties have to sign the same document. Verifying that a transaction bears the right number of electronic signatures from designated is a matter that has yet to be addressed".

6.4 Opinion on the outcome of the workshop

The security aspects are not addressed separately for each of the four phases (i.e. e-Tendering, e-Ordering, e-Despatching and e-Invoicing) and are thus kept very general.

The confidentiality aspects, particularly important in the tendering phase are concerned with end to end confidentiality, i.e. not simply communication security while the data is in transit. It is however quite important to separate the response in the e-Tendering phase into two parts: one administrative part and another part for the detailed response which should not include information allowing to identify the submitter. The detailed response to the bid shall be confidentiality protected so that only a group of experts should be in a position to open it, when the call is closed. The way this concern is addressed in the CWA leaves room to further examination.

Similarly, it is not clear when and where electronic signatures, whether they are advanced electronic signatures or qualified electronic signatures, may or should be used.

The various roles needed in the context of e-Procurement are not clearly identified in the CWA. Had they been standardized they could be used in an interoperable manner. For example, they could be indicated within the end user certificates.

In eProcurement there is often a need that several parties have to sign the same document and thus the need to verify that a transaction bears the right number of electronic signatures from parties that have a given role. The standards that have been developed under the EESSI do not allow to verify globally that a given document bears the right number of signatures, keeping in mind that each individual electronic signature can be done under a different signature policy. Verifying that a transaction bears the right number of electronic signatures from designated persons is still to be addressed.

7 e-Registered mail

7.1 UPU EPM

7.1.1 UPU Electronic PostMark Overview

The Universal Postal Union (UPU) Electronic PostMark (EPM) standard provides services which ensure that the electronic content of email may be preserved for future validation. It provides verification of electronic signatures, time-stamping and maintains logs as necessary to support "non-repudiation" services. It includes optional services for data encryption. It includes optional facilities for end user signing but is more focused at providing services to enhance the electronic signature to provide "non-repudiation".

It claims to support the following forms of non-repudiation:

- Non-repudiation of Origin.

- Non-repudiation of Submission.

- Non-repudiation of Delivery.

- Non-repudiation of Receipt.
- Non-repudiation of Knowledge (the exact meaning of this term is unclear).

It supports evidence relating to an email for:

- Who sent it?
- When it was sent?
- When it was received?
- Have both parties been notified of transmission?
- Has the content been tampered with?

EPM claims support for both CMS and XMLDSig based electronic signatures. It also claims to use RFC 3161 time-stamping and OCSP and to preserve the data required for the signature type ES-C as defined in TS 101 733/TS 101 903. However, it has not been possible to verify these technical details from the available documentation. It was released as a UPU standard in 2003 (Ref: UPU s43 Electronic PostMark Interface). This specification concentrates on the interface to services enhancing the signature (e.g. verification, time-stamping, audit logging), rather than the requirements of the end-user signature itself.

UPU is working with CEN to have it adopted as a joint standard with the Postal Services Technical Committee, and also with the OASIS Digital Signature Services technical committee to define a profile of the DSS (committee draft) standard for EPM. The UPU specification is currently being enhanced to align with OASIS DSS.

Both Canada and Italy are using an EPM-compliant service (same software solution in use). Several others are piloting or considering pilots (US, Australia, Poland, South Africa). Still others are building to the specification (Brazil, France, Portugal).

Further details are available from the UPU EPM web site at: http://www.globalepost.com/.

7.1.2 Recommendations

EPM provides a use case which can be used to identify requirements for the use of electronic signatures.

7.2 Posta Elettronica Certificata - PEC in Italy

With the Decree by the President of the Republic No 68 of 11 February 2005 a new electronic service called Posta Elettronica Certificata - PEC is being launched in Italy in year 2005, after a three years long experimental phases concluded in November 2004. A Decree with the Technical rules, already available in draft from the URLs http://www.cnipa.gov.it/site/_files/DPCM%20PEC%20%5B12_05_05%5D.pdf

And:

http://www.cnipa.gov.it/site/_files/pec-def.pdf, unfortunately only in Italian, is supposed to be officially issued by 2005 end.

This service purpose is simple and therefore not invasive: to provide e-mail with at least the same services as the registered ordinary mail.

Its basic functions are the following:

1) senders, upon authenticating themselves to their service providers (this implementation is provider's specific), submit their provider the to be sent e-mail and get back an acceptance receipt, signed by the server;

2) if viruses and similar malicious code are present the e-mail is rejected and the sender is notified;

3) the sender's server adds information of the mail: date of acceptance, sender, recipients, subject, and signs the whole of it; the output of this is called "transport envelope";

4) the "transport envelope" is sent to all involved recipients" servers, that, after having checked it again for the presence of virus and having verified the sending server's signature validity, send back a signed acceptance/non acceptance receipt;

5) if the "transport envelope" is sound and valid it is delivered to the recipient's mail box and a signed delivery receipt is sent back to the sender's server to be eventually forwarded to the sender; if delivery to the recipient's mail box is not possible the sender is notified;

6) servers must keep all the e-mail related event logs for at least 30 months, and must time stamp the log file every day. This log file can be exhibited as an evidence of sent/received e-mails;

7) registered e-mails can also be sent to non PEC users, as well as non registered e-mails can be received by PEC users. Obviously only the PEC-side services will be implemented in these cases.

All servers' signatures are advanced signatures, issued through an HSM. These signature profiles are not yet defined, but they will just be basic AdES, since their security for the required 30 months is provided by the above described organizational means.

PEC services convey the e-mail as it is (if no virus or other malicious code is detected), therefore the senders are the sole responsible to sign, timestamp, encrypt the documents they include in the e-mails they send.

The PEC service, in addition to providing a secure transmission means with the same features as the ordinary registered mail, provides also the possibility to actually rely on the servers" logs as an evidence of sent/received e-mails. No restrictions are placed on the exhibition of this evidence, that implicitly must, in any case, abide by the Italian rules of law on data protection.

Because of the PEC service provider reliability, the time associated to a registered e-mail can be used as a time reference.

It interesting to remark that it is mandatory for all Public Administrations from 16 May 2007 to be PEC users and to use it with citizens/companies that require making use of this service.

8 e-Authentication

8.1 Overview of the CEN WS activity and their technical approach

This CEN Workshop had its kick off meeting on 23 April 2003, was officially started on 16 September 2003, and was finalized on 11 February 2005. Its purpose was to lay down a common understanding of the e-Authentication problems, and to propose a viable solution. It was primarily intended to address the e-Government domain.

Among its declared contextual basis the most remarkable are:

- eEurope Smart Card Charter, the outputs of which could be brought into the public domain as CWAs.
- Open Smart Card Infrastructure for Europe (OSCIE).
- Existing pre standardization work in the eESC domain: CWA, Global Interoperability Framework (GIF), TrailBlazers documents.

The following deliverables have been approved and published: abstracts of them are presented in annex B.

1. 'Towards an electronic ID for the European Citizen, a strategic vision'

This document is available also at URL http://europa.eu.int/idabc/servlets/Doc?id=19132.

This document scope is to summarize the "state of the art developments, threats and opportunities in the electronic identification services for the European citizen". Chapter 1 "The vision" also states:

> *"The document is aimed at Central Government policy makers in the domain of electronic ID, the European Commission, the Smart Card industry and in general those organizations interested in implementing electronic ID".*

It is also said:

> *"The document is positioned in the smart card domain but heavily relies on supporting technologies as digital signature and biometrics for strong cardholder verification purposes".*

And its goal is:

> *"To establish cornerstones for an interoperable electronic identity and authentication and electronic signature (IAS) infrastructure for European-wide usage".*

The WS supports hardware tokens, namely smart cards, where a "authentication high" level is required, where not only the electronic data necessary for e-Authentication can be securely stored and used, but also personal data relevant to personal identification can be printed on and are therefore readily available. These hardware tokens can also be used to generate electronic signatures. In this case in order to meet the requirements of Directive 1999/95/EC [1], the specifications produced within the EESSI initiative by ETSI and CEN are to be considered. An explicit reference is made to the Qualified Certificate Policies produced by ETSI as TS 101 456 [3].

Standards taken into account are the ISO standards on smart cards (developed by ISO/IEC/JTC1 SC 17), on biometrics (developed by ISO/IEC/JTC1 SC 37), the deliverables under the aegis of CEN TC 244 like
CWA 14890.

An interesting overview is also presented in chapter 3 on the status of the eID cards in various nations.

Chapter 4 highlights the following Recommendations:

Recommendation 1. e-Authentication, and more specifically smart card based electronic ID, should be considered as a necessary European wide infrastructural element for enabling the information society.

Recommendation 2. A legal system for cross border acceptance of e-Authentication/eID should be installed in the European domain.

Recommendation 3. Participation from European experts in eAuthentication/eID related standardization activities i.e. in the fields of Smart Cards, Biometrics, Digital signature and eAuthentication/eID as such should be encouraged and supported by all necessary means.

Recommendation 4. A European wide e-Authentication pilot project should be conducted.

Recommendation 5. European Coordination on eID development is needed.

5.2.1.1.1 Comments on the document

Aside from some mention of the ETSI Qualified Certificate Policy TS (TS 101 456 [3]), being the focus been mainly on eAuthentication, the Qualified Electronic Signature (QES) subject has not been addressed, as well as the various electronic signature formats.

There is therefore room to address these formats and to highlight the difference between a QES for content commitment purposes and a signature for eAuthentication purposes, and that it is advisable to use them separately.

2. CWA15264-1: 'e-AUTHENTICATION - Part 1: Architecture for a European interoperable eID system within a smart card infrastructure'

This document "defines the interoperability architecture for the implementation of a smart-card based interoperable public eAuthentication/eID infrastructure across Europe to be primarily used in the eGovernment domain."

This applies to contact, contactless and combined cards, with either 2 or more chips on board, or 1 chip with both contact and contactless communication capabilities.

It does not exclude the use of SIM card based eID, especially when used for authentication and digital signature purposes.

Chapter 1 states:

> *"This document models the Interoperability (IOP) problematic from different perspectives in the following order:*
>
> - *Context, concluding requirements;*
> - *Concepts:*
>   - *functional "view";*
>   - *technical architecture for a smart card based eID system using on-line eGovernment applications;*
>   - *dataflows "view" (description independent from technical solutions);*
>   - *interoperability issues;*
> - *Specifications/common requirements for interoperability.*

The CWA considers the Identification, Authentication and electronic Signature function (IAS) as a generic one to be used for accessing online eGovernment services with smart cards".

This document defines a common set of data that should be stored in the card to meet the minimal interoperability architecture requirements. This information is subdivided into public and private or secret elements, as well as into mandatory and non-mandatory elements.

The document envisages all possible interactions of applications where e-Authentication is required, not only within a single domain, but also cross-domain.

Explicit reference is made to the Directive 1999/93/EC [1], and specific requirements on authentication certificate issuance, protection, use, revocation, are made, that are consistent with the ETSI ESI specifications detailed in TS 101 456 [3], that is neither quoted nor referred to.

NOTE: An ETSI member representative's comment on the opportunity to add ISO/IEC 15693 to the standards relevant to contactless cards has been rejected because ICAO specifications have been used as a paradigm for contactless requirements, which lead to envisioning only ISO/IEC 14443.

3. CWA15264-2: 'e-AUTHENTICATION - Part 2: Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services'

This document scope is clearly specified in its chapter 1 Scope:

> *"This document is directed at central government and local government Card Scheme Operators. It provides guidance and recommendations on the practical operation and extension of government schemes that exploit cards incorporating a reliable pan-European interoperable public e-ID for identification, authentication and electronic signature services".*

This document provisions cover mainly organization and legal matters, providing guidelines on liabilities, good practices for eID cards implemented via Multi application cards.

4. CWA15264-3: 'e-AUTHENTICATION - Part 3: User Requirements for a European interoperable eID system within a smart card infrastructure'

This documents makes an analysis of the issues that need to be addressed when considering User Requirements in an eID environment supported by smartcards. Again, the document purpose is clearly stated in some paragraphs of chapter Scope:

> *"The scope of this manual is restricted to the elements of the "interface" between the User and the system, i.e. the smart card, some elements of the terminal, and the communication between the card and terminal."*

This document sets down user requirements for user interactions where the smartcard is used in the authentication process.

The document content is structured on two large chapters:

> Chapter 2: Deals with the generality of User requirements and describes the best practice in *users dealings with smartcards*; it mainly addresses user interfaces specifications and, as far as it is possible, the needs of users with special requirements;
>
> Chapter 3: Deals specifically with the use of smartcards in European interoperable eID systems and addresses user requirements for *authentication within an eID system*; the usability is seen from the perspective of a user's usage of the system.

Referred standards are those relevant to the above described goals, like EN 1332-4 regarding coding the User's preferred interface on a smart card; and CEN/ISSS Workshop Agreement CWA 13987-1, providing guidelines and specifications aiming to supports the use of different types of smart card for accessing multiple applications at different types of system terminal within a Card Community.

8.2 Applicability of existing ESI standards and potential additional requirements on ESI standards

As this CEN WS is now closed, no action can be done to enhance harmonization between their effort with ETSI ESI deliverables and findings.

TS 101 862 [5] and TS 102 280 [8] are listed among the referenced standards.

The following comments have not been accepted (the involved document part is annex A):

1) For the keyUsage the document requests nonRepudiation, while at the same place it is given the following explanation: "This extension defines the purpose (e.g. authentication) of the key contained in the certificate". It is not clear the overall meaning of this: the annex regards "non repudiation", so the nonRepudiation setting is correct, but it conflicts with the specified "authentication" purpose.

2) Signature suite 1.2.840.113549.1.1.5 is referenced, corresponding to sha-1WithRSAEncryption: no reference is made to SHA-256 or other algorithms, despite the weakening of the SHA-1 algorithm was already known. This decision was taken because the Work Shop had decided to comply with the Open Smart Card Infrastructure for Europe (OSCIE) Volume 4, Part 1, where this position appears as being clearly specified.

8.3 Any recommendations

No direct recommendation can be suggested for this already closed CEN Workshop.

It is instead suggested for ETSI ESI to carefully monitor other CEN Workshops. A particular attention should be given to the keyUsage and SHA-1 matters, in order to propose to harmonize the above decisions to what was largely accepted in the EESSI environment, both by the ETSI ESI and by the now closed CEN/ISSS WS El-sign. Where applicable, decisions on signature format profiles should be monitored and supported, as well as on mechanisms to allow identification and authentication of Trust-service providers within or outside a specific environment.

A strict cooperation in such areas would be, in fact, synergic to both ETSI ESI and CEN/ISSS.

9 CEN/TC 224 Machine Readable Cards

9.1 Context

CEN has decided to transfer the maintenance of nine CWAs related to electronic signatures to CEN/TC224. The list is the following:

- **CWA 14167-1:** "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".
- **CWA 14167-2:** "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)".
- **CWA 14167-3:** "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)".
- **CWA 14167-4:** "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP".
- **CWA 14169:** "Secure Signature-creation devices "EAL 4+"".
- **CWA 14170:** "Security requirements for signature creation applications".
- **CWA 14355:** "Guidelines for the implementation of Secure Signature-Creation Devices".
- **CWA 14890-1:** "Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements".
- **CWA 14890-2:** "Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services".

NOTE: All CWAs related to electronic signatures are available on the CEN web site at the following address: http://www.cenorm.org/cenorm/businessdomains/businessdomains/isss/cwa/electronic+signatures.asp

A TC 224 meeting to decide on how to organize the work has taken place in Munich on 14 and 15 April.

9.2 Outcome of the TC 224 meeting in Munich on 14 and 15 April 2005

TC 224 has decided to create two working groups:

- **WG 16:** Application Interface for smart cards used as SSCD; and
- **WG 17:** Protection Profiles in the context of SSCD.

Document CEN/TC 224 N 1546 contains the resolutions of the meeting where resolutions 693 and 694 are dedicated to the creation of these two WGs with the following allocation of documents:

WG 16 has been allocated the following two work items:

- **CWA 14890-1/2:** "Application Interface for smart cards used as Secure Signature Creation Devices".

WG 17 has been allocated the following seven work items:

- **CWA 14355:** "Guidelines for the implementation of Secure Signature Creation Devices";
- **CWA 14167-1/4:** "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures";

- **CWA 14169:** "Secure Signature-Creation Devices "EAL 4+"";
- **CWA 14170:** "Security Requirements for Signature Creation Applications".

The WGs convenorship has been undertaken as follows:

- DIN takes the secretariat of WG 16 with Mrs Gisela Meister as chairwoman;
- UNINFO takes the secretariat of WG 17 with Mr Actis Dato as chairman.

National bodies (NBs) are expected to nominate the experts willing to participate to the two working groups.

9.3 TC 224 WG 16

This Work Group, whose title is: "Application Interface for smart cards used as Secure Signature Creation Device" is responsible to transform CWA 14890-1 and CWA 14890-2 into a EN.

WG16 will prepare a working draft for the new European Standard EN Application Interface for smart card used as Secure Signature Creation Device based on the CWA 14890 parts 1 and 2. The same document numbers will be kept, i.e. the document's numbers will be: EN 14 890-1 and EN 14 890-2.

According to the previous division of the CWA 14890-1 and 2 the WG16 will produce two separate working drafts. When the standard becomes an approved EN, it will be submitted for consideration as an ISO standard.

The WG16 Kick Off meeting was held on in Munich (Germany) on 27th June 2005.

The Munich meeting report has been released very late (October 2005). From the report, it appears that another meeting was scheduled and took place on the 13th and 14th September in London by invitation from APACS.

The WG has decided to have an ISO standard after finishing the CEN work. The WG agreed to have two parts of the CEN standard. The main title of both part will be: "Application Interface for IC cards used as Secure Signature Creation Devices". The title of the Part 1 becomes "Basic services", while the title of Part 2 stays as "Additional services".

At the time the report was written (December 2005) the WG was only progressing Part 1. It is planned to finish Part 1 first so that it can be sent to the CEN TC224 Secretariat for circulation and ballot not later than June 2006.

Several topics were added to the proposed work plan. In particular the addition of new algorithms (e.g. SHA-2), different key lengths and elliptic curve algorithms. Several topics from WG 15 are also subject to be included in the present WG 16 work. WG15 members will work out a contribution to WG16.

The ECC (European Citizen Card) Part 2 (data structures and procedures) references CWA 14890. ECC specification adds elliptic curves for smart card/CAD Authentication.

The Munich meeting report has been released very late (October 2005). From the report, it appears that another meeting was scheduled and took place on the 13th and 14th September in London by invitation from APACS.

The last meeting from year 2005 took place on November 16th in Paris (AFNOR premises) by invitation from Axalto.

Denis Pinkas attended as an observer and liaison from ETSI TC ESI. He also attended as a TC 224 WG 17 member. There was no time available for making a liaison on ETSI TC ESI matters during the meeting. Priority was given to written comments and thus there has been nearly no time available for raising new comments during the meeting.

In order to have their comments considered at the next meeting, TC ESI members will need to send in advance written comments to the editor Helmut Scherzer: scherzer@de.ibm.com. It is anticipated to make the next draft document available to the ESI members.

Next meetings:

- 9 February 2005. Madrid.
- 21 and 22 March 2005, starting a 11 a.m. France.

- 26 and 27 April 2005. Germany. Berlin (tbc).
- 7 and 8 June 2005. Munich.

Opinion on the work of WG 16 from TC 224

The overall program from WG 16 is ambitious and goes far beyond Secure Signature Creation Devices (SSCDs). In addition to the non-repudiation service, other security services will be supported, namely authentication, and confidentiality. The scope of the document is now becoming very close to the European Citizen Card (ECC).

Mandatory, optional and conditional functions/features

At this stage, the document does not yet contain a general presentation that explains the general contents of the document, in particular which functions/features are mandatory to support, optional to support (e.g. biometrics authentication) and conditional to support. In order to delimit the perimeter of the document, interested people currently need to read the whole document.

Confusion between electronic signatures and digital signatures

The document contains (in section 5) a mapping between the terminology of the EU Directive and the terminology used in the document. It should be observed that the mapping is incorrect, since the document confuses electronic signatures with digital signatures and also the signature-verification process is reduced to the verification of a digital signature using a public key, while annex IV from the EU Directive states:

"Recommendations for secure signature verification

During the signature-verification process, it should be ensured with reasonable certainty that:

(b) the signature is reliably verified and the result of that verification is correctly displayed;

(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;"

At this stage, a parallel with the vocabulary from the EU Directive does not seem anymore necessary. This section should be deleted.

Use in trusted environments and untrusted environments

The document is making a distinction (in section 5.2) between an SSCD used in a trusted environment and an untrusted environment, however without detailed explanations. In an untrusted environment, a "secure channel" needs to be established to read a display message (which has been previously chosen by the signer). It is unclear whether the secure channel is only required during the reading of the display message or also afterwards. In an untrusted environment, it is believed that the secure channel shall only be required during the reading of the display message.

It is **not** to up the SSCD to protect itself in an untrusted environment; otherwise the SSCD would only be able to work in trusted environments. The document is lacking to say that it is up to the signer to decide whether the environment can be trusted or not (in some cases with the help of the display message) and then it SHALL NOT enter the PIN if he considers that the environment is not trusted.

Use of secure messaging (SM)

Later on in the document (in section 8) it is explained that for every subsequent operation the use of a secure channel is "highly recommended" by means of a Secure Messaging (SM). This means that secure messaging is not mandated for subsequent operations.

This is particularly important to be considered when WG 17 will be revising the Protection Profile (PP) of the SCCD.

Difference between certificates usable for non-repudiation and for authentication

There is no separation (see section 15.9) between certificates usable for authentication and certificates usable for non-repudiation. Both fall into the same category called DS certificates (with DS meaning digital signature). This implicitly means that Part 1 is not simply covering non-repudiation, but also authentication, which is somewhat in contradiction with the scope of Part 1.

Different PINs for non-repudiation and for authentication

A separation between certificates usable for non-repudiation and certificates usable for authentication should be made, since the same PIN SHALL not be used to activate private keys used for authentication and private keys used for electronic signatures (i.e. non-repudiation).

This comes from the fact that the SCCD has no knowledge of the external protocol being used and thus it is important that a challenge that might be, for example, the hash of a contract can never be signed using a private key corresponding to a certificate that is used for non-repudiation purposes. The classification between certificates used for authentication and certificates used for encryption needs to be done when writing a public key certificate, since, for an SSCD, a public key certificate is an opaque string of bytes and information details like "key usage" encoded using ASN.1 can not be understood by an SCCD.

If an SCCD supports authentication in addition to non-repudiation, then the PIN to unlock certificates to be used for non repudiation (i.e. electronic signatures) SHALL be different from the PIN to unlock certificates to be used for authentication. In this way, it becomes possible to use an SCCD in an untrusted environment for authentication purposes, while it is still possible to use the same SCCD in a trusted environment for electronic signature purposes.

Use of biometrics information

Secure Messaging (SM) is currently mentioned in the document as mandatory for biometrics. This is highly questionable, since an end-user SHALL NOT enter either his PIN or his biometrics information, if he is in an untrusted environment and does not see the Display Message. When biometrics information is being used, it is believed that should be protected in the same way the PIN is protected.

It is unclear whether biometrics authentication can be used alone to activate a private key or in addition to the PIN. Since the same PIN SHALL not be used to activate both private keys used for authentication and private leys used for electronic signatures, biometrics authentication alone only cannot be used for both security services. One solution would be to either use it only for electronic signatures (with or without a PIN), or to use it for both with different PINs.

Link between a certificate and a private key

In order to use an SCCD there must be at least one public key certificate (or an unambiguous reference to it) and the associated private key in the SSCD. Key-pair generation may be made by:

- the SSCD, and then public key export and certificate import (or unambiguous certificate reference import) using secure messaging; and
- a Certification Authority, and then private key and certificate import (or unambiguous certificate reference import) using secure messaging (section 10.3).

There are some concerns to be mentioned:

- in the general case, it is unclear how a public key certificate (or an unambiguous public key certificate reference) is linked with a private key;
- when the key-pair is generated by the SCCD, it is unclear how the certificate will be correctly linked with a given private key, since the writing of a certificate can be done asynchronously, i.e. a few hours later.

Update of certificates is currently unspecified

Since functions like "Delete private key" and "Delete certificate" are not mentioned, an SCCD that would comply with this specification would not be able to have its certificates updated. At the minimum the document, should indicate that the "Delete file" command described in Part 9 from ISO 7816 shall be used for that purpose, otherwise application programmers would not know how to update certificates and associated private keys. These commands could also be mentioned as being mandatory or optional.

New SM protocol specific to contactless card ?

A specific SM protocol (see section 8.6) is intended to be used in the case of a ECC (European Citizen Card) contactless card supporting electronic signatures. The goal is to protect the wireless communication between the ICC and the IFD (InterFace Device). The ICC and IFD have public key certificates containing signature algorithms and a Diffie-Hellmann key exchanged is being used to establish the channel. The protocol is supposed to have "non-traceability" (?) properties, which is quite unclear.

Note that, once the protocol is supported, it could also be also used for contact cards. The issue is whether this protocol would be mandatory for contactless card, but would remain optional for contact cards (it may seen as a little bit paranoiac in the case of contact cards).

9.4 TC 224 WG17

This Work Group, whose title is likely to become: "Protection Profiles in the context of electronic signatures", is responsible, as per its Terms of Reference:

> *"for the development and maintenance of a set of cross-industry European Standards defining different Protection Profiles (PP), in accordance with Common Criteria version 3, for Information and Communication Technology (ICT) products in the context of electronic signatures.*
>
> *These ICT products are expected to be used for the generation of electronic signatures according to the Terms of the European Directive on Electronic Signature 1999/93 and, in particular, to be suitable for the production of "Qualified electronic signatures" that fulfil the requirements of Article 5.1 of the Electronic Signature.*
>
> *The CEN/TC 224/WG 17 is also responsible for the technical compatibility of the standards developed under its authority should the legal framework for qualified electronic signatures be modified by the European authorities."*

The ToR also specifies: *"To ensure backward compatibility, the standards to be produced will align with the existing CWAs to a maximum extent" and "the Protection Profiles defined in these standards shall take into account the evolution of the Common Criteria (CC) and, in particular, their new version: CC v3."*

The WG objectives are prioritized as follows:

Priority 1.

1) a PP based on the CWA 14169, to cover SSCD;

2) a PP based on FR DCSSI PP "Signature Creation Applications", and CWA 14170, to cover SCA;

3) a PP focused on Identification and Authentication services, complementary to the SSCD, and aligned with the ongoing work of WG15 and WG16.

Priority 2.

1) a number of PPs based on CWA 14167;

2) a Technical Report based on the CWA 14355.

Priority 1 documents should be finalized by July 2006.

Priority 2 objectives have been set aside for the moment for lack of WG participants.

The WG17 Kick Off meeting was held on in Turin (Italy) on July 8th 2005, with participants from Italy (UNINFO is the Convenor), France, Spain, Germany. One ETSI ESI expert (Denis Pinkas) partially attended it via conference call, while another (Franco Ruggieri) also tried to participate via conference call, but, due to the bad line conditions, he had to give up.

During that meeting Franco Ruggieri was appointed as liaison between the WG17 and the ETSI ESI.

The three Priority 1 objectives will be worked on upon formal approval of respective NWI definitions by the TC 224 Secretariat. As of today, the NWI status is:

1) a PP based on the CWA 14169, to cover SSCD aiming to achieve EN status = approved by the WG members, submitted to the TC 224 for approval;

2) a PP based on FR DCSSI PP "Signature Creation Applications", and CWA 14170, to cover SCA aiming to achieve EN status = submitted to the WG approval;

3) a PP focused on Identification and Authentication services, complementary to the SSCD, and aligned with the ongoing work of WG15 and WG16 aiming to achieve EN status = submitted to the WG approval.

The Kick off meeting minutes reads: "*D. Pinkas will prepare a list of suggested changes to CWA 14169 Secure Signature-creation devices "EAL 4+" and make it available after approval by the mirror French committee. Comments are requested in the subsequent two weeks time period*".

This document has been sent to WG 17 on 26 September 2005.

The document WG 17 N 8 "Terms of reference" has been sent to CEN/TC 224 Secretariat for circulation to TC 224 and formal approval.

The next meeting will be held in Turin after CEN/TC 224 Plenary meeting (Poland - 25-26 January 2006). The currently suggested dates are the following: 15 or 16 February 2006 or 15 or 16 March 2006.

Opinion on the work of WG 17 from TC 224

The overall program from WG 17 is ambitious and the number of participating people is limited. An important effort from the WG will be necessary to accomplish this program given the short time available, since the task is not simply to rubber stamp the existing documents:

1. for the PP on SSCDs, both changes and improvements are expected to the input document, i.e. CWA 14169. On July 20, Giesecke & Devrient has indicated that Wolfgang Killmann has agreed to be available as the editor of the document.

2. for PP on SCA the French input is a good starting point that must be thoroughly evaluated by the participants

3. the name of the working group is supposed to become: "Protection profiles in the context of electronic signatures". However, the PP on "Identification and Authentication" is not related to the work on Electronic Signatures. If it is confirmed that this PP is indeed developed in this working group, it should be noticed that the work is rather important, but quite different. Axalto is willing to provide an editor for this document. No other support has yet been expressed.

CWA 14171

It should be remembered that CEN/BT in its Resolution BT 51/2004 of November 18, 2004 has transferred the maintenance of CWA 14171 "General guidelines for electronic signature verification" to ETSI/ESI, implying that any future versions will be published as ETSI deliverables, at which point the CWA will be withdrawn.

Annex A: CEN/ISSS e-Invoicing Focus Group

What follows is a summarization, made of both abstracts and extracts (the latter ones between quotes and in *italic)*, of this final report. Not all sections have been summarized or quoted: only those that relate to EESSI standards. Where this was done the section title may have been quoted as well, to facilitate the reader in referencing the original document.

The Directive 2001/115/EC [2] lays down the requirements to guarantee the electronic invoices integrity of content and authenticity of origin for the time required by the applicable law. Therefore this Directive does not only address the electronic exchange of the invoices but also their storage.

This Directive also imposes that invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the contents are guaranteed:

- by means of an advanced electronic signature (AES); member States may however ask for the advanced electronic signature to be based on a qualified certificate;

- or by means of electronic data interchange (EDI) as defined in Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects.

Invoices may, however, be sent by other electronic means subject to acceptance by the Member State(s) concerned.

The CEN report "*describes the main issues around the implementation of electronic invoices for VAT purposes in the European Member States; the report identifies standards available and makes recommendations for usage of electronic invoices across Europe. The report is based on the contributions from the members of the e-Invoices Focus Group and on the contributions received during the Open Conference held in Brussels, where some 150 participants reviewed the first draft of this report*".

The report main conclusions are:

- business and tax administration are urging to have a standardized approach to e-Invoices;

- interoperability issues on EDI and on electronic signatures hamper European harmonization in electronic commerce, especially cross border, and this is worsened by too diverse legislations on these domains and on VAT in Member States.

Therefore the report proposes an "*Electronic Invoices Forum Europe, which should:*

- *link and network the various national electronic invoices fora;*

- *look specifically into developing the appropriate required standards;*

- *continue to improve existing standards and bring them up-to-date".*

A.2.2 CEN/ISSS e-Invoicing focus group scope

"*The scope of the CEN/ISSS e-Invoicing Focus Group (e-IFG) was:*

- *to provide an overview of the standardization aspects of electronics invoicing;*

- *to assess existing standards and their implementation;*

- *to provide proposals for additional activities should these be considered necessary".*

A.2.3.5 Summary of recommendations

The proposed recommendations are substantially addressed in the Business Plan and in the Work program of the consequently and subsequently launched CEN Workshop on e-Invoicing, where they were assigned to separate Task Teams to develop.

A.3 Overview of the current situation

After a brief reminder that the Directive 2001/115/EC [2], being an evolution/amendment of the Directive 77/388/EEC, addresses paper invoices as well, the report recalls the two basic requirements laid down in the Directive on integrity and authenticity, that are to be guaranteed:

- *"by means of an Advanced Electronic Signature (AES)…. Member States may however ask for the advanced electronic signature to be based on a qualified certificate,*

NOTE 1: The ETSI Liaison Officer proposed to amend this acronym in AdES to avoid confusion with the AES symmetric algorithm and consistently with the ETSI TS 101 903 title, where XAdES is mentioned.

- *or by means of Electronic Data Interchange (EDI) as defined in Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects…".*

It is also mentioned the third possibility, regarding integrity and authenticity:

"Invoices may, however, be sent by other electronic means subject to acceptance by the Member State(s) concerned."

NOTE 2: This may add a requirement on software developers to produce country specific applications; if the topics above are not addressed by standards makers this might lead to interoperability problems.

Other remarkable items of the Directive are summarized, the most prominent of which are listed below, on the basis of their impact on integrity and authenticity, and on interoperability:

"Member States shall not require invoices to be signed".

NOTE 3: Debates are alive on the interpretation to be given to this provision in countries that make it mandatory to apply a qualified signature to the e-invoices, as per the possibility allowed by the Directive. Some doubt that, by applying a qualified signature to an eInvoice, these countries may require something equivalent to an autograph signature and with the same meaning, thus violating the above requirement by the Directive 2001/115/EC [2].

"Taxable persons shall ensure that copies of invoices issued by himself, by his customer or, in his name and on his behalf, by a third party, and all the invoices which he has received are stored."

This requirement on e-invoices storage opened the way to a specific Task Team of the currently operative CEN WS.

Another topic is addressed by the CEN WS, as a consequence of the e-Invoices storage:

"*The authenticity of the origin and integrity of the content of the invoices, as well as their readability, must be guaranteed throughout the storage period. The information they contain may not be altered; it must remain legible throughout the aforementioned period. If the invoices are stored in a message format, i.e. EDI syntax, then the required directory and code sets required for converting them to the clear format must also be stored for the required period*".

EDI is covered extensively in several parts of the Focus Group Report.

The Commission Recommendation 1994/820/EC is mentioned where it says that EDI: "*was developed on the request of European trade and industry EDI user groups to provide the required legality, acceptability and security in the use of EDI in European Member States. The Recommendation includes the "Model European Interchange Agreement", which was developed in line with the work carried out by the International Chamber of Commerce and several major industry sectors, e.g. automotive, electronics, retail and distribution. Trading partners prior to commencing the exchange of EDI messages are advised to agree and sign interchange agreements based on the European model*."

This led to opening a Task Team of the CEN WS with the specific purpose to propose amendments to 1994/820/EC regarding EDI and to clarify the legal status of EDI.

About formats both of EDI and XML, the following Recommendation is proposed:

"*Within the UN/CEFACT Forum, several industry and trade sectors, such as EAN International, Eurofer, are developing messages including the invoice message. The invoice core components information contained in the ebXML transactions and other XML transactions used within Member States should comply with Directive 2001/115/EC*".

The following interesting remarks are done about the EDI security: they underscore **the responsibility of the involved parties** in setting up a suitable secure set of measures: there are no measures per se secure as is the case with advanced electronic signatures.

a) **Authenticity of origin:** The trading parties must define themselves the rules on how to mutually identify. The systems used for EDI must register these identification data to check the information exchanged. "*It is **up to the trading parties** to make sure that the identifiers used are unique within the respective systems, and that any use of identifiers not registered in advance are reported on an error list*".

b) When UN/EDIFACT (ISO 9735) is used

   i) **Integrity:** Communications between parties are implemented through interchanges. *"An interchange is a structure to secure the transfer of one of more messages (e.g. invoices) at one and the same occasion. Each interchange is designated a unique interchange control reference by the sender. The precise provisions for the designation of references **are to be agreed by the parties**".*

   ii) **Message:** An EDIFACT message is made of segments that must follow the order indicated in a messages directory, *"where a segment is a predefined and identified set of functionally related data element values. Each message is designated a unique message reference number **by the sender**. The precise provisions for the use of the reference **are to be agreed by the parties**, but commonly the messages are numbered sequentially within the interchange".*

   iii) **Syntax:** *"The EDIFACT syntax rules and the predefined structure of the message and its segments (according to the specification in the message directory) reduce the risk of segments or messages being inadvertently modified, as this is likely to generate syntactical errors".*

c) **Protection against deliberate alterations:** Scenarios exist where the invoice is "protected" by the context of a previous document exchange **between the parties**. In other contexts this may not be assured. In such cases other, external to the EDIFACT, protection measures may be necessary, like protocols to secure the communication channel (e.g. SSL or S-HTTP). Where the invoice does not require to be structurally modified, i.e. no format conversion is necessary, electronic signatures is an intrinsically secure means.

These comments on EDI are highlighted to specify where the electronic signatures provide a per se intrinsic security, and, therefore, where their usage provides advantages versus EDI.

A.3.1.5 Electronic signatures

A summarization of the electronic signature legal characteristics relevant to e-Invoices is presented in this section, among which the possibility to protect the invoice by means of AdES and the possibility for Member States to require qualified signatures.

It is also interesting to remark that the report, based on what is stated in art. 12 of Directive 1999/93/EC [1], reminds that "*The European Commission has to review the operation of the Directive [1] and report to the European Parliament and to the European Council by 19 July 2003 at the latest*".

A few comments on the EESSI effort are worth reporting:

"The EESSI standardization deliverables have widely been acknowledged for being generic, flexible and applicable in a multitude of transactions. EESSI deliverables, however, can be further extended to reflect the specific needs of industry and governments."

This, coupled with the remark that EESSI focussed mainly on qualified signatures and advanced signatures in the light of the non-repudiation requirement, although other signature types have been addressed, leads to the conclusion on the EESSI effort that additional work on electronic invoices is necessary where authentication is addressed.

A list of the documents published at that time by ETSI and CEN is presented, along with a brief description of their scopes.

Another interesting point is: "*is it necessary, that an electronic invoice has to be "signed" electronically by a physical person? Authenticity and integrity are the sole and clear requirements of the Invoicing Directive for electronic invoices. Following this intention it has to be indicated that this requirements can be fulfilled by any electronic invoice may it be signed by a legal or a physical person. Both scenarios are possible. For the purposes of the Directive, the word "stamp" is probably more appropriate than "signature", which wrongly leads the thought in the direction of the handwritten equivalent of a signature*".

However, among the section "Final recommendations" this can be read: "*Although many technologies exist that may be called "advanced electronic signatures", at least digital signatures based in X.509v3 certificates should be accepted by all Member States. EESSI standards should be adopted as common technical interpretation, instead of creating new standards, to foster interoperability*."

A.3.1.6 Other means accepted by Member States

A reference is made to Finland and to UK, where there are no strict requirements on e-Invoices.

A paragraph says:

> *"the authenticity of origin and integrity of the data" is NOT categorically guaranteed EITHER by an advanced electronic signature OR by EDI (within the meaning of the Directive), but where there are alternative controls employed that DO offer an equivalent level of assurance - for example, the use of (virtual) private networks, where access to authorized users is controlled by unique IDs/ passwords, or the application of internal controls such as matching invoices against purchase orders/goods received and payments, that may otherwise substantiate the invoice transactions."*

It is not, anyhow, explained how these other alternative controls may ensure authenticity an integrity over time: this issue is addressed further on as an open item.

A.3.2.1 Invoicing and the fiscal system

"*This section outlines how the collection of VAT information and tax authorities control relate to the invoices, as used in an average business process.*"

Cornerstones of this section is adoption of ERP systems that include management of the general ledger, e-Invoices issuance is a function of.

The following cases are vetted:

1) paper invoices: these is a risk of errors when the debtor inputs these invoices in its own processing system;

2) electronic invoices: it is pointed out that "*as not all kinds of electronic messaging have the same security requirements and the implementations of the invoicing Directive may put specific requirements with regard to the electronic invoices exchanged*":

   a) it is recognized that *"electronic signatures can secure the external transmission between the parties"*, but it is highlighted that "if third party conversions are needed specific problems arise as discussed elsewhere in this report;

   b) on the other hand: *"EDI with an agreed procedure for security is more likely to originate from the parties" commercial needs and should reflect good business practice as deemed appropriate by them. Such provisions might cover also (some of) the internal process steps but it is not likely that one general, homogenous business practice will ever evolve"*.

This paves the way to a debate between electronic signatures and EDI supporters.

The rest of this clause then addresses the status of the implementation of Directive 2001/115/EC [2] in the Members States, that is not summarized here, since it is not relevant to technical standards, let alone the EESSI deliverables.

A section follows that addresses the possible ways to exchange invoices:

1. on paper, to be subsequently converted from analogic to digital support by scanning and, where applicable, applying OCR;

2. electronic invoices not preceded by an electronic documents exchange: in these cases an e-Invoice is just an event that has no previous electronic support: it "*cannot build on the business process for automatic control/verification. Instead manual measures and data contained in the message to provide security are used to determine its correctness. Electronic signature can be one such instrument"*;

3. electronic invoices submitted via web forms: "*if additionally designated as the point of access for orders to the supplier, the amount of invoicing data to be entered by the supplier can be significantly reduced. The buyer, on the other hand, has full influence on the format of invoices so that the documents can be processed automatically after receipt*"; "*the web site can be operated by the buyer or by a third party*"; depending on who, between seller and buyer, has the greater clout, he can be the one that drives the e-Invoices format;

4. e-Invoicing under trading partner framework agreement: in this case the e-Invoice is the final act of a previous document exchange, that provide a context under which aegis all the trade conditions and agreements subsist;

5. e-Invoicing through a third party/marketplace/hub: beyond the obvious advantages for parties to relieve themselves from the burden of establishing and maintaining a suitable information processing system, this has the additional advantage that such "hub" is a kind of proxy that can securely convert the invoice format from the seller's format to the buyer's.

The subject of "format" is then addressed, taking into account different possibilities, ranging from zero to more than one service provider.

A.4.3 Directive 2001/115/EC on Electronic storage of Invoices

This subject, that brought to the birth of a specific Task Team by the CEN Workshop, is addressed by specifying that the storage can be implemented by the taxable person or by a third party, that can also be in a different state, in which case a prior notification to the tax authorities is required: this affects the way documents can be accessed.

The duration of the storage varies depending on the legislation, and this may have consequences on the signature format, where used, of on the adoption of specific processes to ensure the stored invoices validity over time.

This has impact on the legal aspects, like the applicable legislation, as well as on technical ones, like the need to keep alive at least for the necessary period also the directory relevant to the EDI syntax format, or the need to ensure that the technical means necessary to visualize the stored invoices are also kept for the required time.

It is also recommended to establish a number of common arrangements governing the use of electronic invoicing, that should not be "*subject to the outright imposition of nationally-orientated, specific and over-prescriptive control requirements, by competent authorities, but should also take into due consideration the security/control environment(s) that business itself commonly applies to safeguard its own commercial interests.*" In other words: co-regulation.

An entire section is dedicated to the self-billing, that is openly permitted by the Directive 2001/115/EC [2]. This clause is not summarized here.

The report then briefs on the practices in force in Finland, Belgium, Greece, Norway, Austria.

In a subsequent section on Best Practice in Fiscal control and on invoice-handling systems, two practices are explained that are implemented by large traders:

- Automation of trading processes, that, where frequent procurement of standardized articles/services is involved, builds on framework agreements that allow for integrated computer support for information exchange and control.

- Coherent internal handling of invoices: acknowledging that 100 % electronic invoicing is far away, traders have to accept invoices in various forms and formats; in these cases the solution is to unify the internal handling of invoices, supporting capturing, processing and archiving of invoices in a controlled and coherent process flow.

NOTE: From the above items, requirements may stem for the ETSI ESI STF on signature profiles, to specify profiles that may help implementing them.

A.6 Recommendations

Finally the following recommendations are stated:

A.6.1 EDI and e-Business standards

a) *To bring Commission Recommendation 1994/820/EC October 1994 up to date with requirements of Directive 2001/115/EC and present day e-Commerce practices.*

b) *The invoice content details identified in the Directive should be submitted for the creation of the relevant UN/CEFACT ebXML Core Components.*

c) *To permit the use of internationally recognised organization identifiers and product identifiers in electronic invoices as alternatives to the name and address of an organization or the description of a product or service.*

d) *To develop codes, standardised at community level, to replace standard clauses (text) being inserted in messages, that usually require human intervention for processing.*

e) *The term "EDI" in the Directive 2001/115/EC should have the widest possible meaning of formatted exchanges, not dependent on a specific "Technology" (EDIFACT, X-12, XML, etc..), nor limited to specific international, national or sectorial standards.*

A.6.2 Electronic signature

f) *Care should be taken not to inadvertently restrict the use of advanced electronic signatures ("AES") to natural persons to achieve authenticity and integrity of the electronic invoices as it may render current practice with automatic generation of invoices impracticable/illegal.*

g) *In cases where communications are channelled through an intermediary service provider (e.g. in the context of a marketplace or a hub), and AES are used, there may be a need for re-signing (or re-"stamping") the invoice between parties. This should be taken into account so that, if AES are to be considered, the law allows the use of re-signed AES.*

h) *It must be indicated, that additional work needs to be carried out to further detail the standardization objectives of authentication for the purpose of using them in electronic invoicing. This recommendation assumes that the current review of the electronic signature Directive will not result in any major changes. The detailed proposals for standardization should therefore take full account of the findings of the review.*

A.6.3 Specific and fiscal procedures

i) *In view of multinational companies having central computer operation, possibly outside the EU, e-IFG recommends that provisions be introduced to allow electronic storage of invoices in non Member State provided the required conditions for inspection and data protection are met.*

k) *Explore the possibility for remote access to "audit of traders" computerized tax records and/or downloading transaction files from traders onto tax administration systems will disturb traders far less and allow administrators to work freely.*

k) *In furtherance of the objective of the EU Directive on Invoicing "to establish a number of common arrangements governing the use of electronic invoicing", it is recommended that the competent authorities in all EU Member States should consider further opportunities for implementing the Directive in a compatible way, in particular, for cross-border electronic invoicing."*

The above recommendations have been assigned to corresponding Task Teams of the CEN WS on e-Invoicing to develop. These recommendations have been verbatim quoted since WS Teams working on them may define requirements for specific signature profiles.

Finally, annexes are added, that:

1) compare the replies to a questionnaire on the invoices subject as filled in by most EC Member States;

2) copy the 2001/115/EC [2] Directive;

3) copy the CEN e-Invoice Focus Group Terms of Reference.

Annex B: CEN/ISSS Workshop on Electronic Authentication

The CEN/ISSS Workshop on Electronic Authentication was kicked off on 23 April 2003, was officially started on 16 September 2003, and was finalized on 11 February 2005.

What follows is a summarization, made of both abstracts and extracts (the latter ones between quotes and in *italic)*, of the main topics, covered in the documents issued by this CEN WS, that appear relevant to the ETSI ESI.

Section titles in this annex are built in the following manner: the title part that is in *italic* is the same as in the original document. The titles of the document sections are copied for the sole purpose to facilitate links to the documents content, therefore there are discontinuities in the clauses numbering.

The documents issued by this CEN/ISS Workshop are:

1) a document named "Towards an electronic ID for the European Citizen, a strategic vision", that summarizes the state of the art developments, threats and opportunities in the domain of electronic identification services for the European citizen; this document is not summarized here, since it only makes some passing reference to TS 101 456 [3], without much detail, so it was not deemed relevant to the ETSI ESI activity;

2) CWA 15264, in three parts detailed further on, that considers the ***I***dentification, ***A***uthentication and electronic ***S***ignature function (***IAS***) as a generic function to be used for accessing online eGovernment services with smart cards. This CWA also intends to support migration from a situation where each eID-card system has its own infrastructure and trust services into a situation where card body, microprocessor, smart card infrastructure as well as trust services *may be shared between/can interoperate among* different eService providers.

The CWA is based on:

1) eEPOCH project, already implementing the Global Interoperability Framework (GIF),

2) CWA 14890,

3) TB 7,

4) TB 8,

5) CEN/TC 224,

6) PORVOO e-ID Group findings,

7) FP 6 projects,

8) CWA URI, eSIGN,

9) EUROSMART,

10) FORUM on Global interoperability of IAS,

11) NICSS V1.0 activities,

12) GSC-IS V2. (NIST) activities,

13) TB 10 requirements (e-government application environment).

B.1 Part 1: Architecture for a European interoperable eID system within a smart card infrastructure

Clause titles in this annex are generally built in the following manner: where the title is in *italic* the clause number is the same as in the original document.

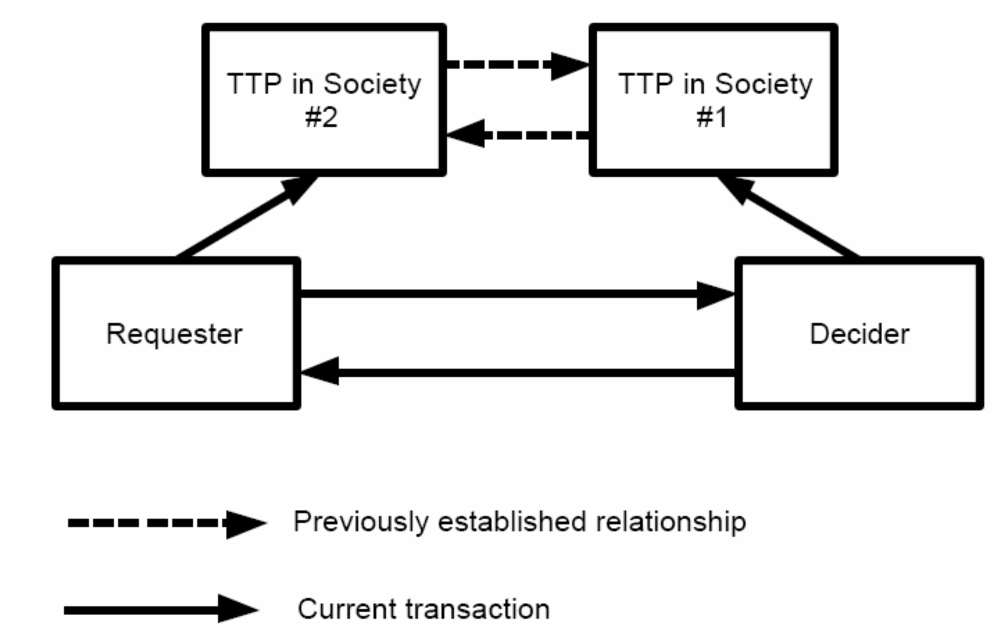
B.1.*1 Scope and objectives*

"*This part of the CWA defines the interoperability architecture for the implementation of a smart-card based interoperable public eAuthentication/eID infrastructure across Europe to be primarily used in the eGovernment domain.*"

The workshop considers "*contact cards, contactless cards and combined cards with either 2 or more chips on board or 1 chip with both contact and contactless communication capabilities.*"

B.1.*2 Contextual Model for IAS interoperability*

All possible interactions of applications are envisaged where e-Authentication is required, not only within a single domain, but also cross-domain. The following figure, taken from the document, shows the schema to achieve trust and interoperability in a four-entity Trust model, involving two domains.



This 4-entity Trust model deals with interactions between 2 different security domains that have developed trust in isolation. This model is based on two trusted third parties who are described as operating under different schemes having their own security domain, with their own rules for creating and managing trust, and that have previously established some relationships e.g. at technical, administrative and legal levels.

The scope of the interoperable IAS nucleus covers:

- The creation, provision and maintenance of Identification, Authentication and digital/electronic Signature services using secure smart cards.
- The registration of real persons and organizations to use and provide services (including issuing them with the necessary tokens, tools and digital data in a secure manner).

The CWA underscores that, for interoperability to be possible between two schemes:

- The security policies and processes of the two schemes have to be compared to allow establish the limits of trust.
- The different entities participating to the schemes must be identified and their respective role in the Trust model must be defined.
- The roles support delivery of common IAS services and establish the trust between them. These performed processes are classified as primary (i.e. operational), secondary (i.e. supportive) and tertiary (i.e. business), depending from the relationship they have with the core IAS functions.

- The system architecture for interoperable (IOP) IAS services must be built, which includes the different components and the interfaces enabling to carry out transactions across scheme boundaries in a manner which allows authentication and signature functions to be trusted according to the requirements.

The following assumptions have been made in the definition of the IAS IOP framework:

- *"Digital identity, attributes and signatures will be issued to natural persons by trusted organizations, and will be held in certificates which also contain public security keys".*
- *"An electronic trusted (secure) token will be used to store certificates and support IAS functions".*
- Legal recognition is based on the use of the trusted token.
- *"The most usual physical form of the trusted token is a credit-card sized smart card, regardless of its electrical interface: contact and/or contactless".*
- *"On-line transaction methods must be securely implemented (including being capable of secure operation across insecure networks such as the Internet)".*
- *"For Europe, the Electronic Signature Directive 1999/93/EC [1] (E-sign) applies, as well as the European Union Directive 1995/46/EC for personal data privacy".*

B.1.*3 Conceptual model for IAS interoperability*

The CWA restricts its scope to:

- *"high level (strong) security functions, using asymmetric cryptography and a Public Key Infrastructure (PKI) (although the possibility of other methods is acknowledged)"*, and
- *"eID smart cards issued under the control by a central administration, which combines or is the ultimate responsible for several roles"* among those detailed further on.

"*In this context, included on the smart card as a minimum are:*

- *Authentication information for the card.*
- *Identification information (name, etc.) for the card holder.*
- *Security objects, such as a PIN and/or biometric authentication information for the card holder, security keys; and possibly a software to perform IAS services using the card."*

B.1.*3.1 Roles*

The model developed in the CWA is oriented towards eGovernment context schemes, where the primary purpose is to provide the citizen with e-government related services, that can be "*government centric (meeting requirements of local and central administrations)*", or "*citizen centric (assisting them to access citizen services and information services). Third party services (such as professional services) are also expected to benefit from deployment of smart card schemes based on the model, and the model is also open for additional stakeholders to join.*"

If one organization (entity) assumes more than one stakeholder role, this may have important consequences on the security policy recommended for adoption by central administrations for e-government schemes.

The basic roles within a Smart Card Management Framework are exercised by the following stakeholders:

- *"The **card holder (CH)** is a real person (in the legal sense, i.e. an individual human being, not a company or other legal structure) who has been issued a smart card by a card issuer" to be used for IAS purposes to access services provided by service providers.*
- *"The **card provider (CP)** is to securely supply smart cards certified as per the profile stipulated in the card issuer security policy".*
- *"The **registration authority (RA)** registers card holders: i.e. obtains sufficient proof of their identity by traditional means".*

- *"The* ***card issuers (CI)*** *are to … issue smart cards to card holders according to scheme policies and rules, and manage the issued cards throughout their lives". "Independently from its issuance policy, the card issuer in the present model has also the overall responsibility for all that is relevant to the card issuance and maintenance infrastructure".*

- *"The* ***certificate service provider (CSP)*** *or the certificate authority (CA) role is to":*

  - Issue IAS certificates and other certificates, necessary to the smart card information system or to the business service, revoke them and publish their status information according to a policy, under the responsibility of the stakeholder who ordered them.

  - Provide an on-line certificates validation service, that may be delegated to a Validation Authority (VA).

- *"The role of the* ***card application issuer (AI)"*** *is to securely issue applications, originally stored on-card or subsequently down-loaded upon authorization, and to manage the entire applications life cycle security.*

- *"The role of the* ***eService provider (SP)"*** *… "is to provide business services to the card holder using the smart card as an IAS token and/or in conjunction with one or more other specific on-card applications", including all the necessary contractual arrangements.*

- *"The role of the* ***card scheme operator (CSO)*** *is to administer, monitor and support the relationships between the card issuer, the access provider(s) and service provider(s) in order to ensure the integrity of the smart card community".*

- *"The* ***access provider (AP)*** *is the entity in charge of managing the hardware, software and communication networks infrastructure to be used by the card holder for accessing the offered services and managing card content".*

- *"The* ***content provider (CP)*** *is in charge of keeping the content of the service provider up-to-date". The CP "does not play any role in IAS interoperability".*

B.1.*3.2 Processes*

The CWA distinguishes between:

- *"Primary IAS processes: enable interactions between the IAS services and the services requiring them.*

- *Secondary (supportive) IAS processes: are the pre-requisites which create the Trust required to operate the primary processes.*

- *Tertiary IAS processes: are part of the eService delivery to the card holder. They justify the need for primary and secondary processes. Tertiary processes are not detailed in the CWA".*

B.1.*3.2.1 Primary IAS processes*

1. Card activation process: a smart card communicates with a terminal.

   - *"A physical connection (contact/ contactless) between the card and the reader is established".*

   - *"The reader and/or the terminal accept or reject the connected card.*

   - *The terminal initiates a secure communication channel with the card".*

   - *"The communication may require a one-side or a two-side authentication between the card and the terminal and the establishment of an encrypted communication between them. When PKI is used in this process, some certificate validation is required".*

2. "*By the connection to an eService process the terminal initiates a communication to the eService*".

   - *"The communication may require a one-side or a mutual authentication between the terminal and the eService and the establishment of an encrypted communication between them. When PKI is used in this process, some certificate validation is required".*

3. *"During the interaction process with an eService the user initiates a session with the IAS services, according to the security policy rules and the applicable business rules".*

- The identification data required for accessing the eService and, where required, a private key under the sole control of the user, are (optionally) PIN/Biometric protected inside the smart cards.

- Authentication and signature process differ in encrypting a random with the private key, rather than encrypting the digest of the signed object.

- When a BioPIN is in use, the biometric template authentication "*includes the "live and wellness" of the source from which the it has been derived*".

4. By the closing process of the eService connection of the above processes are terminated.

5. "*By the card deactivation process*" … "*the user or the eService securely terminate the communication between the smart-card and the terminal*".

The above processes and communications are to be securely terminated by the user or the eService.

B.1.*3.2.2 Secondary (supportive) IAS processes*

The following secondary (supportive) IAS processes establish the Trust required for operating the primary processes.

- Create a Smart Card Community (SCC) that includes also development of security policies and PKI certification of the relevant stakeholders.

- Issue and maintain/manage cards throughout the entire cards life cycles.

- Implement an eService (including ex post registering of users wanting access rights to a eService or acquiring an onboard application added on the card -an applet), that consists in testing/accepting all components.

- Managing community and infrastructure, including all commercial, service and security related aspects.

B.1.*4 The IAS functional model*

This model is made of, and addresses modelling of, the following functions:

- *"The IAS nucleus (including the Platform function).*

- *The Crypto (or PKI) function.*

- *The Application.*

- *The Connectivity function.*

- *The Human Interface (as this function is subject to Part 3, no further details will be provided in Part 1).*

All these functions are connected with an interface".

B.1.*5 IAS system architecture*

The services require their users to be authenticated, based on the electronic identity (eID) data and the IAS platform on their smart card, before they are authorized to access the services. PKI-based certificate services are needed in the authentication process.

B.1.*5.1 The Smart Card layer*

"*The Smart Card used to carry the cardholder's eID application contains the private key(s) and corresponding certified public key(s) of the Cardholder, or link(s) to it/them. The card may be a multi-application card containing other applications too. Those are, however, relevant from the eAuthentication point of view only in the case they also use the IAS services of the card*".

B.1.*5.2 The Infrastructure layer*

The Infrastructure layer consists in the following sub-layers:

- "*A User Access Point, or the local part of the Infrastructure*", made of a terminal device that may have a biometric sensor, and local application(s).

- "*An eService Access Point, or the remote part of the infrastructure*", including a network site suitably secured, and possibly, an interface where the IAS functions required by the eService are implemented: this remove these aspects from the eServices.

- "*PKI services (Validation Authority) for supporting the eAuthentication and eSignature procedures*".

- "*A Network sub-layer is also part of the infrastructure*" to communicate with the eService Access Point and PKI services, and with PKI services.

B.1.*5.3 The eService layer*

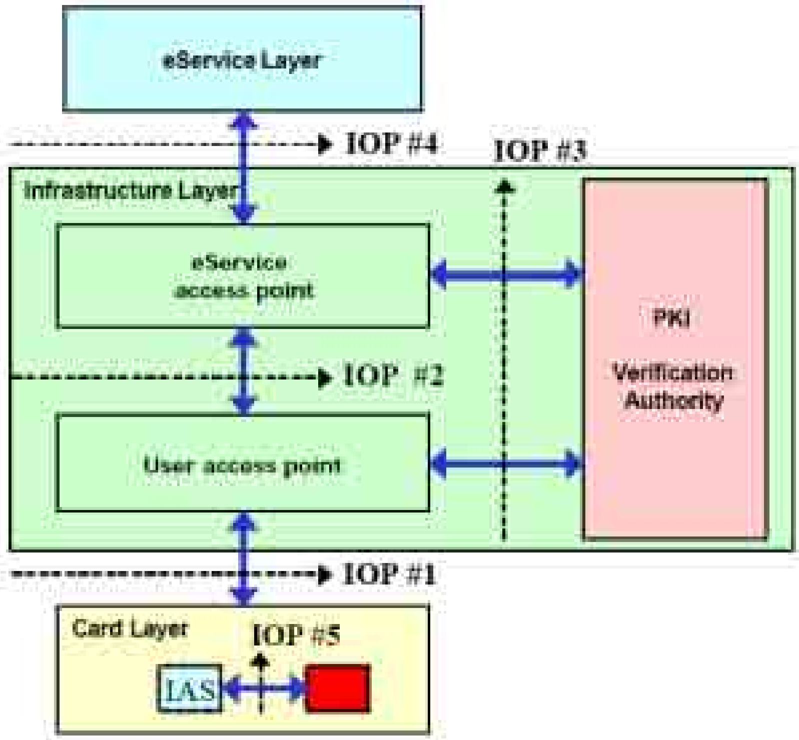
"An eService is any business service that can be accessed electronically through an ICT system.

In this context, eServices that have the need to limit access to them for authenticated users only, or that need digital signature functionality, are relevant.

One or several eServices may share an eService Access Point that takes care of security and access control for the service applications integrating the IAS front-end functionality. The eService Access Point is interpreted here as an Infrastructure component".

B.1.*5.4 The layer interfaces*

"*Each of the layers and sublayers are interconnected through interfaces. There are 5 interfaces and they are called interoperability interfaces (IOP) because they will be the basis for technically implementing IAS interoperability.*"



B.1.*5.4.1 Interoperability interfaces #1 (IOP#1)*

"*IOP#1 is the interface between the Smart Card and the access Infrastructure. It is the interface through which the terminal and the local application(s) implementing the User Access Point as well as the biometric sensor (if any) communicate with the Card and its applications, e.g. the IAS platform.*

Compliance with the ISO 7816 standard is assumed for the interface."

B.1.*5.4.2 Interoperability interface #2 (IOP#2)*

"*IOP#2 is the interface between the User Access Point and the eService Access Point, i.e. between the local terminal application(s) and the remote access point to eService(s).*

Most typical cases are TLS/SSL connections through the Internet, or WTLS connections through the GSM network."

B.1.*5.4.3 Interoperability interface #3 (IOP#3*)

"*IOP#3 is the interface between an Infrastructure component and a PKI service used to verify the validity of certificates presented as a credential for a user or a system component.*

It is assumed that some standard certificate-check mechanisms are used between a service requester and a PKI service provider. These mechanisms are either based on CRLs retrieval/check or on standard on-line protocols like OCSP."

B.1.*5.4.4 Interoperability interface #4 (IOP#4)*

"*IOP#4 is the interface between an eService Access Point and an eService.*

If we consider the eService Access Point as an IAS front-end, this interface propagates, if needed by the eService application:

- *The identity of the user authenticated by the IAS front-end layer,*

- *When digital signature is used, it propagates the data, once the signature has been verified by the IAS front end layer.*

When the eService access point acts as an HTTP reversed proxy, the protocols implemented are HTTP/HTTPS.

The detailed definition on this interface is out of scope of the CWA.".

B.1.*5.4.5 Interoperability interface #5 (IOP#5)*

"*IOP#5 is the interface between the IAS platform and another on-card application wanting to use the IAS/eID functionality.*

This interface is represented by the libraries exposed by the IAS platform so that other on-card applications can call the IAS generic functions.

Even though it is an internal interface of the Card, it cannot be used without external interaction of the on-card application with some external application associated with it."

B.1.*6 The functional model in the IAS system architecture*

The above layers are broken down in this clause in five functions each, not always present in each layer:

- The platform function, e.g. the smart card operating system.

- The IAS platform function, e.g. the set of libraries implemented on the card.

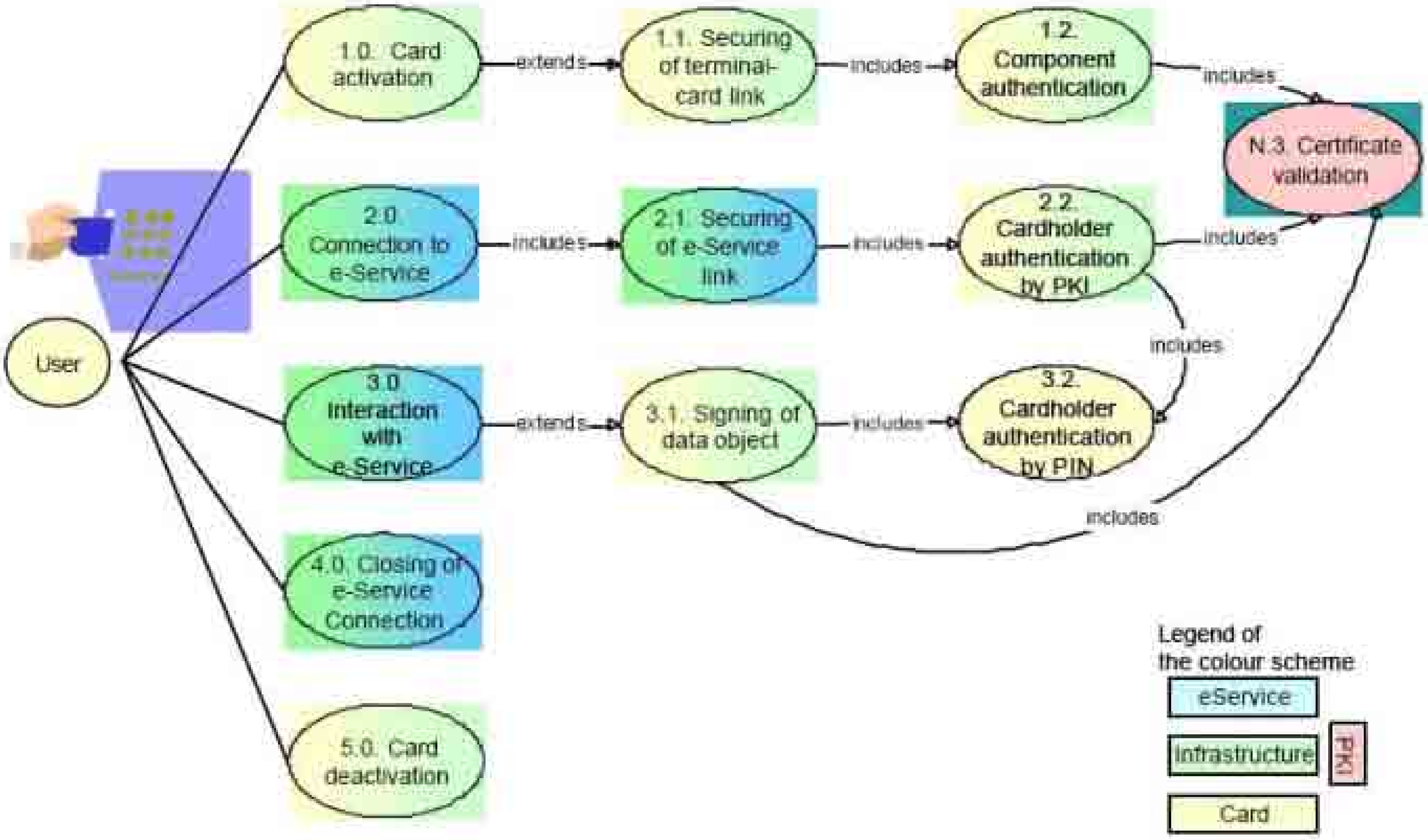
- The crypto function, e.g. the cryptographic libraries and algorithms implemented.

- The connectivity function, e.g. the set of libraries implementing the protocol stack enabling the communication.

- The application function, e.g. the set of on-card applications.

B.1.*7 High level description of the primary processes - formal* description

The figure below models all primary processes, that are broken down in detail in this CWA section. The processes details cover the following topics: Beginning state, End state, Description, Exceptions.


User
1.0. Card activation
extends
1.1. Securing of terminal-card link
includes
1.2. Component authentication
includes
N.3. Certificate validation
2.0 Connection to e-Service
includes
2.1. Securing of e-Service link
includes
2.2. Cardholder authentication by PKI
includes
includes
3.0 Interaction with e-Service
extends
3.1. Signing of data object
includes
3.2. Cardholder authentication by PIN
includes
4.0. Closing of e-Service Connection
5.0. Card deactivation
Legend of the colour scheme
eService
Infrastructure
Card
PKI

B.1.*8 IAS interoperability*

B.1.*8.1 IAS interoperability scenario*s

This clause deals with "*how to create interoperability for using an on-us card is a not-on-us environment, should this be for using a not-on-us access point or for accessing not-on-us services*".

NOTE: "On-us"/"not-on-us" mean access by a user to a service belonging to the same or to a different Smart Card Community (SCC).

"*All different eAuthentication interoperability scenarios are listed below, except the trivial all-on-us case, which does not call for interoperability functions. These scenarios can be classified in three interoperability levels, where level 1 presents the most simple, and level 3 the most complex case*".

The following table defines a functional model applicable to all the IOP scenarios defined henceforth.

	Card	**Infrastructure**		**Eservice layer**	**PKI**
		User access point	**EService access point**		
L1: eService IOP	On-us	On-us	Not-on-us	Not-on-us	On-us
L2: Card IOP - 1	On-us	Not-on-us	On-us	On-us	On-us
L2: Card IOP -2	On-us	Not-on-us	Not-on-us	Not-on-us	On-us
L2: Card IOP -3	On-us	Not-on-us#1	Not-on-us#2	Not-on-us#2	On-us
L3: On-Card IOP -1	On-us	On-us	Not-on-us +	Not-on-us	On-us
L3: On-Card IOP -2	On-us	Not-on-us	Not-on-us + Applet	Not-on-us	On-us
L3: On-Card IOP -3	On-us	Not-on-us#1	Not-on-us#2 + Applet	Not-on-us#2	On-us

B.1.*8.2 IAS Interoperability architecture*

At the various IOP levels, interoperability is achieved through the combination, relevant to the specific case, of various functions among which:

1. capability for the user card/eID application to communicate with the User Access Point,
2. secure communication links between the User Access Point and the eService Access Point,
3. trust agreements between Service provider and eID issuer,
4. trust agreement between Service provider and the User Access Point Manager,
5. agreement on the eID related certificate format.

IOP Level 0 (L0): Closed eID scheme

"*This is the trivial case of total "on-us" environment, where the eID can be used only for the services of its issuer (provided the issuer is also a Service Provider). The purpose of eAuthentication specifications is to offer a way out of this kind of closed schemes*".

IOP Level 1 (L1): eService interoperability

"*This is the case where a "not-on-us" eService welcomes users with "on-us" eIDs connected to "on-us" User Access Points. The Service Provider trusts not only the certificates of its own users' eIDs but also a number of foreign users' eIDs*".

"*An example would be a Finnish citizen at home in Finland accessing an EU server to make an application for an EU job using a token with his/her Finnish national eID on it to authenticate him/herself and to sign the application*".

IOP Level 2: Card interoperability

"*This is the case where a smart card containing the eID can be used in foreign, "not-on-us" environments to access eServices. From the user's point of view, the eServices may be either "on-us" or "not-on-us" services, depending on what the access environment allows. The following three cases are possible at this interoperability level*".

"Case 1: "On-us" service is accessed through a "not-on-us" User Access Point"

"*An example would be a Finnish Member of the European Parliament (MEP) at her office in Brussels accessing Finnish government eServices using his/her Finnish citizen card to authenticate him-/herself*".

"***Case 2: A "Not-on-us" service is accessed through a "not-on-us" User Access Point***"

"*An example would be a Finnish MEP at his/her office in Brussels accessing EU services using his/her Finnish citizen card to authenticate him-/herself*".

"***Case 3: A "not-on-us" service is accessed through an intermediary "not -on-us" User Access Point***"

An example would be "*a Finnish MEP at his/her office in Brussels accessing Spanish eServices using his/her Finnish citizen card to authenticate him-/herself.*

On this level of interoperability, the technology used in the smart card (e.g. Java Card, Multos, native card) is transparent to the rest of the environment.

From user point of view, the only limitation of this level of interoperability is that he/she can load on his/her card only "on-us" applications, i.e. applications that are compatible with his/her type of card (of course if allowed by the issuer of her card)".

IOP Level 3: Card application interoperability

"*This is the case where a smart card containing the eID can be used to load "not-on-us" applications, i.e. card applications that have not been specifically designed to work on that card but are able to use the services of the on-card IAS application (eID). The following three cases of the scenario are possible*".

"Case 1: A "not -on-us" applet is interacting with a "not-on-us" service through an "on-us" User Access Point"

"*An example would be a Belgian citizen temporarily working in Finland downloading a Finnish library application on his/her Belgian citizen card, and using it during a vacation back in Belgium".*

"***Case 2: A "not-on-us" applet is interacting with a "not-on-us" service through a "not-on-us" User Access Point***"

"*An example would be a Belgian citizen temporarily working in Finland downloading a Finnish library application on his/her Belgian citizen card, and using the Finnish library service from his/her Finnish workplace*".

"***Case 3: A "not-on-us#2" applet is interacting with a "not-on-us#2" service through an intermediate "not-on-us#1" User Access Point***"

An example *would be a Belgian citizen working in Finland downloading a Finnish library application on his/her Belgian citizen card, and using the Finnish library service from a Spanish Internet kiosk during his/her vacation.*

B.1.*8.3 IAS interoperability processes*

B.1.*8.3.1 Interoperability of the primary processes*

"*The interoperability of the primary processes will be achieved by implementing the above architecture, model and technical requirements*".

The eService Provider needs to define the minimal level of assurance to be achieved in authenticating with a supplied eService.

This, as well as the authentication mechanism, "*is to be dealt with on a case-by-case basis, depending from the required minimum level of assurance. It has to be noted that the provided level of assurance will also be depending from the interoperability reached at the level of the secondary (supportive) processes*".

B.1.*8.3.2 Interoperability of the secondary processes*

"*When negotiating interoperability between SCCs, both SCCs should not only be technically interoperable, but should also create mutual Trust, e.g. confidence in the reliability of the registration process of the card holder.*

For establishing and maintaining trusted interoperability, it is required to:

- *"Create interoperability specifications";*
- *"Establish interoperability agreements";*
- *"Install and maintain rules and policies".*

B.1.*9 Securing interoperability*

B.1.*9.2 Securing the Card-Terminal interface (IOP#1)*

This is recommended in untrusted environments.

The following two mechanisms, as defined in CWA 14890, are implemented:

- card and the terminal mutual authentication implemented with three different schemes:
  - Key transport protocol (based on PKI mutual authentication);
  - Device authentication with privacy protection (using Diffie-Hellman key negotiation);
  - Symmetric authentication scheme, requiring a symmetric key infrastructure available;
- Secure messaging, based on symmetric session keys, between the card and the terminal to ensure integrity and confidentiality of the data exchanged (like the PIN or the biometric template).

This is only possible (and practical) with secure terminal devices.

Where this interface cannot be secured, mitigation measures will be required to be included in interoperability agreement between two SCCs.

B.1.*9.3 Securing the User Access Point - eService Access Point link (IOP#2)*

A secure communication link is required between the user access point and the eService Access Point, based, e.g. on TLS/SSL, WTLS, SSH, VPN, etc.

Mutual authentication of the communication parties is required.

B.1.*9.4 Securing the access to PKI services (IOP#3)*

"*The link to the PKI service verifying the validity and revocation status of a certificate does not need to be secured.*

The PKI service, however, has to authenticate itself to the requestor".

B.1.*9.5 Securing the eService Access Point - eService link (IOP#4)*

"*No specific security measures have to be applied to this interface*".

B.1.*9.6 Securing the on-card applications - IAS function interface (IOP#5)*

"*There must be a "firewall" on the card preventing unauthorized access to the IAS/services by on-card applications/applet.*

In the context of Java cards, the objects belonging to an applet are not made available to another applet unless a specific sharing mechanism is involved between the two applets".

B.1.*10 Common requirements for IAS interoperability*

B.1.*10.1 Requirements on primary processes*

For each of the following functional requirements the document proposes Technical/Organizational system solutions (not specified in the present document).

Smart Card eID- system elements	Functional requirements
Overall System Requirements	The system shall support different security profile The system shall be future proof The IAS function shall be executed in a secure and controllable way.
Smart Card	The execution of the eID and eAuthentication function shall be convenient and fast The smart card shall be secure The system shall be trustworthy for the card holder.
Card holder ID requirements	The system shall support a secure and reliable card holder identification function.
Card holder Authentication requirements	The system shall support a secure and reliable card holder authentication function.
Electronic Signature requirements	The system shall support a secure and reliable card holder electronic signature function for the purpose of legal validity of the positive consent of the card holder and to guarantee non-repudiation in relation to a signed information object.
User Access Point requirements	The system shall be trustworthy for the card holder. It shall be reliable and shall protect card holder data present on the card The system shall ensure a secure and trusted communication channel between the card and the user access point The system shall be easy to use by the card holder and behave consistently across interoperable SCCs.
Supporting PKI requirements	A certificate validation mechanism needs to be supported for the benefit of the Service Providers.
eService Access Point requirements	The eService layer has to remain independent from any particular IAS implementation.

NOTE: ICAO specifications have been used as a paradigm for contactless requirements, which lead to envisioning only ISO/IEC 14443 among the contactless reference standards, thus leaving ISO/IEC 15693 out.

B.1.*10.2 Requirements on secondary processes*

B.1.*10.2.1 Organization issuing eID-cards*

The Card Issuer role "*creates and exploits the Smart Card Community, setting the objectives and the limits of the SCC, defining the architecture specifications, the terms of references for its relationships with each type of stakeholders (i.e. the Card Holders, eService Providers, Access providers, …), the cost sharing policy, the ownership of the cards and the data, the limits of their usage, the card appliance policy, the user interface policy …*".

"*Ultimately, … the Card Issuer is responsible for the trustability of the SCC towards all the stakeholders.*

An eID-card consists of a smart card provided by the Card Issuer (CI), and containing private keys and certificates issued by a Certificate Authority (CA) on the basis of the card holder data collected or verified by a Registration Authority (RA). Although these roles may be taken care of by different organizations, the Workshop assumes that, in the particular case of an eID-card, it will always be a central administration (i.e. central Government) that would take the ultimate responsibility for these different roles.

The liabilities of and between different parties should therefore be defined according to the national legislation of the Member State of the Card Issuer."

B.1.*10.2.2 Card holder's registration procedures*

The Registration Authority (RA) is responsible for face-to-face verification, in accordance with national law, of the candidate card holder identity and, where applicable, attributes before starting the issuing of the card and qualified certificates.

"*Evidence of the identity shall be checked directly against a physical person and if available against a national population register. The same requirement applies to biometric enrolment*".

B.1.*10.2.3 PIN code policy*

A global PIN code will be provided to access data (e.g. authentication), including accessing personal data in the SCC and downloading applications to the card, and a different one for electronic signature.

The card holder will be able to change all PIN codes, under his/her sole responsibility.

B.1.*10.2.4 Remarks on biometrics*

Within the IAS scheme, the functionality of the BioCode is on the same level as the normal PIN.

"*Several security measures have to be implemented in order to maintain the integrity of the BioCode:*

- *Protection of the reference template.*
- *Protection of the "life" biometric template (and its creation).*
- *Protection of the biometric matching process.*
- *Interoperability is achieved by adoption of biometrics related standards", still under development."*

B.1.*10.2.5 Other applications on an eID-card*

Upon card holder's request, 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 Card Issuer.

Additional application or information can be installed on the card at issuance time or, if legally allowed by the Card Issuer, after issuance of the card.

Post issuance, where done over an insecure network, should be implemented with appropriate security and trustability measures agreed by the Card Issuer and should be protected by a PIN (and/or biometrics) code. It is recommended to use different, separate PIN codes for different applications.

B.1.*10.2.6 Responsibility for protecting the eID-card*

The security requirement relevant to eID and card protection are specified in this CWA section, with the caveat regarding the bioCode that if compromised, it has to be disabled.

"*The security policy of the card issuer should therefore allow a fall back (i.e. PIN or another biometric) but one should realize that the different types of biometric technologies have all different security profiles which make them not inter-exchangeable at forehand both from the card issuer or the service provider viewpoint*".

B.1.*10.2.7 Renewal of an eID-card*

"*It is strongly recommended that the validity period of the card and its certificates are the same*".

"*Renewal of the certificates is accomplished in accordance with national legislation. The certificates in the card will never have their keys changed. If a key is to be revoked, a new card has to be issued*".

NOTE: This clause reflects the common position of the Open Smart Card Infrastructure for Europe (OSCIE) Volume 4, Part 1, on which this CWA should rely on.

"*The eID-card shall be renewed through a proper and secure procedure.*

If there are other applications on an eID-card, the card holder is responsible for the transfer of these other applications onto the renewed card".

B.1.*10.2.8 Prevention of the use of an eID-card and its certificates*

"*Primarily the card holder himself will decide why 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*".

NOTE 1: This is to be interpreted as "the card holder has the primary responsibility in deciding …". In fact, other authorities may prevent use of the eID card, for instance a judge where legally possible.

"*The use of an eID-card and its certificates has to be prevented upon notification by the card holder to the card issuer.*

NOTE 2: "Or by any competent authority".

The certificates on the eID-card have to be entered in the revocation list or other certificate validity check system so that the use of certificates relating to electronic communication and granted by the issuer is prevented.

In any case the service provider should not be able to derive the reference template from the card, in order to perform other kind of operations with the biometric information.

In any circumstance, the card holder is to be able to choose not to use the BioCode and prefer a standard PIN. It is up to the service provider whether or not to deliver the requested service".

B.1.*10.2.9 Cancellation of an eID-card*

"*Cancellation of an eID-card shall result in revocation of all known certificates.*

The card itself is not necessarily cancelled".

B.1.*10.2.10 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 [1] on a Community framework for electronic signatures). The applied procedure is to be defined in the certificate policy and presented in its certification practice statement.*

The Card Issuer has to ensure that the eID-card has been prepared and personalized according to agreed specifications.

The CA is liable for damage caused to any legal entity or natural person who reasonably relies on the certificate. Liabilities concerning the optional visual identity document on the eIDcard shall be set according to the national legislations".

B.1 Annex A Mandatory field in certificates

In the document annex A the mandatory fields and contents are specified; verbatim: "*The below minimum data content for the signature certificate (non repudiation) will ensure interoperability between SCCs.*"

ETSI ESI member representative comments:

Upon remarks by the ETSI member representative, TS 101 862 [5] and TS 102 280 [8] have been added to the referenced standards.

The following comments have not instead been accepted:

1) For the keyUsage it is requested nonRepudiation, while in the Description cell it is given the following explanation: "This extension defines the purpose (e.g. *authentication*) of the key contained in the certificate". It is not clear the overall meaning of this: the annex regards "non repudiation", so the nonRepudiation setting is OK, but the requisite "authentication" where the meaning of the setting is defined, conflicts with the table relevance.

2) Signature suite 1.2.840.113549.1.1.5 is referenced, corresponding to sha-1WithRSAEncryption: no reference is made to SHA-256 or other algorithms, despite the known weakening of the SHA-1 algorithm, since this suite reflects the common position of the Open Smart Card Infrastructure for Europe (OSCIE) Volume 4, Part 1.

B.2 Part 2: Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services

"*This document is intended for use by central government and local government smart card scheme operators. It provides guidance and recommendations on the practical operation and extension of schemes that exploit cards incorporating a reliable pan-European interoperable public e-ID for identification, authentication and electronic signature services*".

"*This Part of the CWA defines a common set of data that should be stored in the card to meet the minimal interoperability architecture requirements*". These requirements have the purpose to implement a smart-card based interoperable public eAuthentication/eID infrastructure across Europe to be primarily used in the eGovernment domain.

This information is subdivided into public and private or secret elements, as well as into mandatory and non-mandatory elements.

Service Providers are invited to use the government e-ID card IAS services for their own business. "*These providers may accept, refuse or negotiate details. In the event of a positive decision by both parties the card issuer may accept loading on-card data and applications in order to enable service providers offering their services*".

B.2.*5 Multi-application Card Schemes*

B.2.*5.2 Government issued IAS driven Multi-application Card Scheme Models*

"*The government agency multi-application cards are issued with the core IAS functionality and may also contain via pre-issuance or agreed post-issuance additional application related functionalities. They may but do not need to be directly associated with the e-ID capabilities*".

"*The supported applications are available under mutually agreed business terms and conditions between the Card Issuer and the Service Providers. The on-card applications may be:*

- *already pre-personalized in the card and then activated on card holder request;*
- *downloadable in the card on card holder request after card delivery. In this case, the Card Issuer provides the required Infrastructure (Card Management System) to allow the post issuance application downloading process".*

B.2.*5.4.3 Concentration of Roles*

"*Regardless of the specific additional applications loaded onto the card, the following important roles, which may be concentrated into one player, can be identified in the architecture as a Value Chain component for eGovernment issued multi-application cards with core IAS functionality:*

- *the smart card issuer, which provisions and distributes the card;*
- *the card scheme operator;*
- *the service providers, who in agreement with the Card Issuer, load their applications into the card;*
- *the final customers (or card holders);*
- *the e-service community administrators, who control or validate applications in compliance with a specific security policy on behalf of the Card Issuer".*

B.2.*6 Risk Analysis and Policy Management*

B.2.*6.1.2 Based on comprehensive Risk Analysis*

"*Participants, the System Operators, and other involved parties - including final users - should understand clearly the legal/security/financial risks in the system and where they are borne*".

Legal Risk

"*This Risk is one involving an unexpected interpretation of the law or legal uncertainty which leaves a card scheme and especially a multi-application system and its members with unforeseen financial exposures and possible losses*".

Loss or Theft of the e-ID card

"*Irrespective of the use of the smart card, a primary risk that users face is physical loss or theft of the token. This risk is countered following the reporting by the card-holder of a missing token*".

Identity Theft

"*A more dangerous risk is theft of keys and discovery of the associated PIN or password used to unlock the keys, without damaging or removing the smart card. Regardless of the protections that are built into the system, if the card is not physically protected, laws and security measures will not be effective. This protection is evolving into a combination of user responsibility for physical possession/compliance with associated policies for use and card protection of the keys during generation and/or use*".

Card Management Issues

"*In an issuer-centric model, the issuer is the only owner of the card and manages all administrative tasks, such as card update and maintenance*".

The "*multi-application updates covered by this CWA are absolutely restricted to the card-issuer-centric model*".

Service Provider Empowerment

"*This model is not in the primary scope of this CWA*".

B.2.*6.1.3 Management of Liability/Security Issues for e-ID/IAS*

In addition to legally relevant matters, stated in a synthetic and large list of requirements, the specific areas to be addressed include:

- *"Analytical procedures which include on-going monitoring and analysis of the risks participants pose to the system.*
- *Operational procedures which include the implementation of risk management decisions through limits on exposure, by collateralising obligations, through the design and management of transactions queues or through other mechanisms.*
- *Redundant design for some key elements of the system in order to improve overall reliability, and collateral arrangements with other MA system schemes to take over in case of incident".*

Also covered are the following topics:

- Secure and prompt financial settlement (where relevant).
- Effective contingency arrangements.
- Fair and open access for Service Providers.
- Effective, accountable and transparent scheme management.

B.2.*6.3 Smart Card Scheme and Third Party Scheme Relationships*

"*In the longer term as a card scheme develops, it will interface with other government card schemes and may also interface with third party schemes (e.g. banking and e-payment schemes). The card scheme operator should have responsibility for managing those relationships*".

B.2.*6.5 Solutions*

NOTE: Adapted from Government Smart Card Handbook/U.S. General Services Administration. February 2004.

The scope of Identity Management Policies is addressed too, and it does not only indicate the scope of policies to be considered, based on **NSCP WP03-1,** but also their range.

The following Policy Major Group are broken down in 84 items:

1) Membership of the scheme.

2) Rule setting processes.

3) Central services.

4) Charges.

5) Applications and services.

6) Security.

7) Branding, Advertising and Marketing/Promotion.

8) Scheme operation.

9) Technical standards.

10) Infrastructure.

11) Third party management.

12) Card holder support.

13) Liabilities.

B.2.*7 Service implementation and legal/administration guidelines*

"*This section outlines the legal and contractual issues required for creation of trust Environment via Cross-Industry*".

"*It also aims to:*

- *describe guidelines for good practice and service connection,*
- *provide a consistent frame based on existing laws, extended when required,*
- *promote trust for the three main participants required for the multi-application system operation, Card Issuers, Service providers and Card Holders".*

B.2.*7.1.3 Card Technology Evolution and Legal Framework*

B.2.*7.1.4 Contractual Relationships between MAS Players*

"*Member States have to assure the juridical efficacy of the contracts which have been concluded on-line that may specifically exclude some categories*".

B.2.*7.1.5 Application downloading with combined e-ID*

"*No application can be downloaded onto the card without express authorization from the card issuer*". In this model, the Application Provider mounting/deleting "*license with the signature of card issuer is a possible requirement from a point of view of assuring safety*". "*If the card requires terminal or server authentication then a mutual authentication procedure will be performed*". "*Depending on the levels of confidence established, the card issuer can grant an AP-mounting license in advance to a service provider*".

B.2.*7.1.6 General Legal Framework*

"The question of the need for a legal framework for a European e-ID is currently open. Although significant experience in the practical application of regulations has been achieved since the publication of the European Directive for Electronic Signature in 1999 in enabling the deployment of PKI systems, it has been agreed in recent reviews that at present insufficient evidence exists for changes to the Directive. In any event, at minimum common issues arise that are outlined in more detail henceforth".

B.2.*7.1.7 Regulations concerning procedures etc. when issuing e-ID*

"*The link between the person/e-ID holder and the information in the e-ID must be secure, so that a 3rd party can accept the e-ID as a valid ID*".

B.2.*7.1.8 The content of the e-ID (data quality) and the verification of the e-ID*

In a number of countries there exists already a unique national ID number. The questions are if it can/should be used to ensure the link between the holder and the e-ID, and in the countries where it does not exist, what should be used as unique personal identifier and how to solve this problem at international level.

Data protection, liability, revocation are also addressed in the CWA and, regarding revocation, it is recommended an effective revocation system, for example an enhanced security system that includes a single EU contact point (i.e. an easily remembered unique phone number, valid and identical within any member state) to revoke an e-ID.

B.2.*7.1.9 Interoperability between Card Schemes*

"*The entities (in particular Card Scheme Operators and Card Issuers) have to agree mutual responsibilities, functional issues and business/financial issues*".

"*"Interoperability" relates to the IAS services, and is arranged between one card scheme (on-us) and another (not on-us). This can be arranged on 4 levels: card, infrastructure, e-service, and PKI/certificate level*".

B.2.*7.3 Privacy Code of Conduct*

General conditions derived from the European Directive 95/46/EC are to be specified in the General Privacy Code of conduct for interoperable smart card systems. More in detail, these principles are to be met: openness, lawfulness and permission to collect personal data, data storage quality and security, and definition of limitations on use.

"*By use of convenient card reader terminals the card user can view their own data (including data for identification, authentication and for a digital signature) in a relatively simple way and when enabled also view the data in the related registers of personal data*".

The Codes of Conduct should provide a set of agreements within a smart card community that prevent uncontrolled and undesired use of personal data by card issuers and service providers.

A GENERAL MODEL FOR A PRIVACY CODE OF CONDUCT is proposed in the CWA.

This Model is divided in the following paragraphs:

PARAGRAPH I: GENERAL PROVISIONS

PARAGRAPH II: GENERAL CARD INTEGRITY ASPECTS

PARAGRAPH III: GENERAL PRIVACY PRINCIPLES

PARAGRAPH IV: RIGHTS OF CARD HOLDERS

PARAGRAPH V: FINAL PROVISIONS

B.2.*8 Business Case Analysis*

B.2.*8.1 Generic Considerations*

The business case assumes varying levels of benefits for each alternative in addition to varying costs:

- Quantifiable benefits.
- Qualitative benefits.

"*In Government to Citizen relations, many benefits realized through an investment will be qualitative and will not lead directly to Euro savings*".

B.2.*8.2 Risk Evaluation methodologies*

"*A risk based qualitative evaluation methodology is highly recommended to identify clearly the risk, liability of the card issuer and which legal and contractual dependencies*".

An example is provided, regarding the security that the PKI card offers to the system.

B.2.*9 Peer Support Mechanisms*

B.2.*9.1 Good practices in eGovernment IAS projects*

"*A continuous and effective exchange of good practices in eGovernment at European level is an ideal way to learn from and transfer good practice experience. Attention is drawn to the Framework to Reinforce the Exchange of good practices in eGovernment, an initiative established by the EC Information Society Directorate eGovernment Unit. Public authorities in the member states, the European institutions and businesses can actively support.*

NOTE: See http://europa.eu.int/scadplus/leg/en/s21012.htm.

B.2.*9.1.1 e-Inclusion and the Digital Divide*

"*The Digital Divide is the gap in opportunities experienced by those with limited accessibility to technology, especially the Internet. This includes accessibility limitations in:*

- *Social issues (age, preference/need to talk to a person etc.).*
- *Cultural issues (language barriers, etc.).*
- *Ability challenges (vision, physical disabilities, etc.).*
- *Economic issues (access to technology devices and means of payment).*
- *Learning issues (overcoming barriers, changing habits etc.).*

Sharing of information across Europe on how government card issuers and card scheme partners explicitly and specifically address the Digital Divide in each of these aspects within their e-ID/IAS projects and applications is encouraged".

B.2.*9.1.2 Pan-European IAS Legal Framework*

It "*is still too early to talk about establishing specific legislation for pan-European eAuthentication*". Information can be provided on experiences, differences already emerging and indications of what may be required.

B.2.*9.2 Participation in the Porvoo e -ID Group*

"*The Porvoo e-ID Group is an informal international network whose goal is to promote and realize the potential of trans-national interoperable Electronic Public Identities using PKI (Public Key Infrastructure) and smart cards*".

"*The Porvoo e-ID Group was established and held its first a meeting in Porvoo, Finland in April 2002. At that meeting 35 participants - government policy makers and technical experts - representing 14 countries (Austria, Belgium, Estonia, Finland, Germany, Greece, Ireland, Israel, Latvia, Lithuania, Norway, Sweden, The Netherlands and United Kingdom) took part. Since then it has met regularly and its activities are ongoing*".

B.3 Part 3: User Requirements for a European interoperable eID system within a smart card infrastructure

"*This document sets down criteria for acceptable User interactions with an ICT system using a smartcard as an access token to ICT based services, where the smartcard also plays a significant role in the authentication process*".

"*This document attempts to balance the technical and design constraints on designers with the requirements of Users, expressed in terms of best practice guidelines, both generally and specifically when authenticating in a European Interoperable eID system*".

"*The scope of this document is to provide ICT product designers, developers, and builders, as well as system integrators and purchasers with an analysis of the issues that need to be addressed when considering User Requirements in an eID environment supported by smartcards.*

The scope of this manual is restricted to the elements of the "interface" between the User and the system, i.e. the smart card, some elements of the terminal, and the communication between the card and terminal".

Structure of this Document

This document is divided into two main sections:

- Chapter 2: Deals with the generality of User requirements and describes best practices in Users" dealings with smartcards.
- Chapter 3: Deals specifically with the use of smartcards in European interoperable eID systems.

- Chapter 2 mainly addresses user interfaces specifications and", *as far as is possible, the needs of Users with special requirements are considered and taken into account*".

In this document the usability is seen from a system user's perspective, thus the following issues have been addressed:

- *"Comfort: Is the User comfortable interacting with the system*
  - *Consistency: For the same goal or outcome, does the same process apply*
  - *Fun: Can we say at least that the process is not boring or aggressive*
  - *Fluidity: Does the system lead the User through the process in a straight-forward manner*
  - *End User Control: Does the system allow the User to drive the system in the way they want (for example, menu driven or via short cuts)*
- *Intuitive operation: Is the use of the system obvious*
  - *Learnability: is the process easy to learn and enticing to do so*
  - *Ease of use: Is the system easy to use for all categories of User*
- *Clarity: What is not intuitive should be made clear to the User*
  - *Simplicity: The ultimate goal of complex system, but where an open User community is concerned, this must be the case from the outset*
- *Enablement: Does the system enable the User to interface properly with the system to carry out the required activities*
  - *Inclusivity: This must be true for as wide a User community as practicable*
  - *Acceptance or rejection: Does the system allow the User to accept or reject a flow of information (for example, to restrict the flow of personal information for this transaction at this terminal in order to keep the interaction anonymous)".*

B.3*.2 General User Requirements for Smartcard Based ICT Systems*

B.3*.2.1 Approach and general principles*

The approach has been to look for a trade off between a "user centric" vision and a "Service centric" vision.

Social acceptability of the mechanism had a part in this trade off, since the system as a whole must be:

- Intuitive to operate.
- Non-intrusive.
- Balanced in its requirement, i.e. the mechanisms, and particularly the security measures must be proportional to the purpose.

Moreover:

- Consistency must be ensured. This means that every single function and if possible every component of a single function should always be controlled in the same way in different applications and devices.
- Information overload should be removed, by trying to go with the "intuitive design" route.
- Applications must be similar to what already exists: this will be regarded as a favourable situation by a User.
- Conformance to natural sequence should be achieved.
- Users must not be mislead.

B.3.*2.3 Common Elements in Supporting User Requirements*

Particular attention was paid to the way the dialog with the User is handled, using consistent terminology, standard symbols, consistent pictograms, icons and symbols, etc.

Similar attention was devoted to error handling and reporting. Examples of messages are provided, as well as examples of different ways to report the user with errors: indicators, symbols and/or legends, audible signals, text messages, error numbers or codes. Minimum requirements on error reporting are also specified.

Requirements on re-entry after error conditions are also explored. In some cases the error condition forces the abandonment of the session or transaction and the need to start again. "*In other cases, the transaction process is still in progress but the flow has been temporarily halted while a recoverable error situation is reported to the User. In these circumstances when an error condition is encountered and that error is correctable by the User, the system should allow the User to resume the transaction from the point at which the error occurred*".

"*The User should not be required to repeat any part of an interaction process if this can be avoided. Repetitive interaction of this kind usually engenders very negative response from Users".*

"*An exception to the above, even where technically the transaction could be continued, would be where retention of data within the system presents an unacceptable security risk*".

Advises are also given regarding the process duration: should it last longer than few (3) seconds, a feed back on the process status should be given to the User. Similarly, where appropriate, different signal types can be used: visual and/or audible alarms should be used.

Remarks are done on the advisability that sensitive operations are conducted in a secure way in a public environment.

The following standards, legislation and guidelines are to be taken into account when designing card access points for public use:

- EN 1332-4.
- CEN/ISSS WA 13987:2003 eURI.
- European Directive on disability discrimination.
- The Disability Discrimination legislation of the host country.
- Design for All guidelines.

"With reference to this issue, precise instructions should be given to Users on any precautionary procedures relating to the handling of contactless cards, both in use and when not in use".

B.3.*2.5.3 Retrieving a Card*

Another item addressed by the document specifies that a terminal should allow the User to retrieve his or her card at any time except during system activity (for example, during code validation or value transfer).

"*However, it is accepted that, in many countries, a card issued by a bank remains the property of the bank and that a terminal operated by a bank may retain that card and refuse to return it to the cardholder. For multi-application cards, where banking applications may co-reside with non-banking applications, it may be important that individual applications can be suspended or cancelled without the necessity of withholding or cancelling the card*".

"*A terminal should also allow the User to retrieve his or her card in the event of a chip, terminal or power supply failure during system activity*".

Similarly, Users should be warned if they forget retrieving the card, as well as they should be informed not to premature remove the card.

Even more important, "*when the card is removed, the terminal should not retain or store any information that might be subsequently accessed by a third party except where this information is essential for secure processing of a transaction, or where information is extracted and retained for risk management purposes*".

"*A terminal should not extract and retain any information for commercial purposes without the knowledge of the cardholder*".

"*When a transaction is complete, and before the User is invited to remove the card, the User should be informed of any changes made to the card, if the terminal is able to do so*".

B.3.*2.6 Doing Things To a smartcard*

The following operations on a smart card are also addressed:

- Issuing a smart card - these requirements widely differ depending on the card type: low or high security card.
- Modifying some of it, including Loading applications, removing something, transferring elements between applications - in these cases the user should be able to securely access the card, to see which applications are available, to abort the updating process in ay moment, etc.
- Managing security including the operation of Identification, Authentication and Electronic Signature.

B.3.*3.1 User Requirements for Authentication within an eID system*

"*The User will want a simple process of identification that does not involve providing more information than is needed for the services they wish to access, and they must be able to choose the level of identification they provide, but must be made aware that this may determine what services they can access*".

B.3.*3.2 Identification and Authentication*

"*Three elements contribute to a person's identity:*

a) Things which you "are" i.e. your Biometric identity. These are attributes that are unique to an individual (e.g. fingerprints).

b) Things that are given to you i.e. your attributed identity. These include full name, date and place of birth.

c) Things that happen to you during your life, i.e. your biographical identity. This includes educational qualifications, electoral register entries, and history of interaction with organizations such as banks".

Any of these elements can be used to ascertain the user's identity, depending on the application and taking into account the proportionality, i.e. the mechanisms, and particularly the security measures must be proportional to the purpose.

B.3.*3.2.1 Re-issuing Cards*

"*When a card is lost or stolen, the User requires a fast method of replacing the card. However the issuer needs to ensure that the applicant is the legitimate User. The problem is more complex with multi-application cards where the User has downloaded application modules to the card. In some cases there may be possibilities for crediting the User with the value of some or all the items on the lost card. If able to do so, the card scheme operator should keep a record of the applications on a card, even if the User has downloaded extra applications from a variety of sources. If the card is stolen, the User should be issued with a new card number so that the lost or stolen card may be permanently hot listed and blocked within the system*".

B.3.*3.2.2 Additional Information*

"*At the request of the User, extra information could be stored on the card. This information could be the preferred User interface, qualification for a discount (e.g. a registered disabled person may qualify for reduced fares on public transport), or some information which speeds up the process of accessing a particular service (e.g. connecting and logging onto a text relay service)*".

"*There is a European standard (EN 1332-4) for coding the User's preferred interface on a smart card; such preferences could be large characters on a screen, speech output, or more time for operating a terminal. A CEN/ISSS Workshop Agreement, CWA 13987-1: 2003, eURI provides guidelines and specifications for designing an open scheme that supports the use of different types of smart card for accessing multiple applications at different types of system terminal within a Card Community. It embodies EN 1332-4 in a profile and preference dataset to enable a single specification to cover all known User requirements for additional data*".

B.3.*3.2.3 Cardholder approval of stored data*

"*The cardholder needs to be provided with the ability to know what personal information is stored on the card. This will include data held within an authentication dataset. Direct access to this data may involve the use of specific terminals authorized to carry out this function. The cardholder should be given clear information about the use to which the data is to be put and who will have access to it, or to specific sub-sets of it. Information should only be stored on the card with the consent of the User. The level of consent will include full use, anonymous use and no use.*

The User should be able to withdraw their consent at any time, have data amended or removed, or have new or updated data added".

B.3.*3.3 Authentication Methodology*

"*Authentication of the Cardholder or User will normally take the form of supplying a PIN or biometric*".

B.3.*3.4 Signature Services*

"*Some transactions are of sufficient importance that their authenticity and origin must be verified such that they cannot be repudiated by the recipient party. In this case the transaction will be sealed with a certificate of authenticity containing, among other things, the User's Electronic Signature. The capability to carry out this process is provided by the smartcard as part of the Identification, Authentication and Electronic Signature (IAS) capability within the eID service*".

Authorization, Informed Consent, Consumer Protection Legislation, are briefly addressed too.

B.3.*3.7 Human Interaction in an eID Context*

Each of the process flows considered in a European interoperable eID scheme from a User point of view are detailed. In some cases the processes may be combined, for example, registration and biometric enrolment.

The processes examined are: registration, biometric enrolment, card issue/delivery/withdrawal, authentication, Electronic Signing, Card/Validity renewal, Lost or Stolen Card Declaration.

NOTE: Where necessary the card can be sent in a locked state and the user will unlock it with a secret code.

A baseline for a card based authentication is detailed too.

B.4 Towards an electronic ID for the European Citizen, a strategic vision

This document describes the "*state of the art developments, threats and opportunities in the domain of electronic identification services for the European citizen*". "*The document is positioned in the smart card domain but heavily relies on supporting technologies as digital signature and biometrics for strong cardholder verification purposes*".

"*The document is aimed at Central Government policy makers in the domain of electronic ID, the European Commission, the Smart Card industry and in general those organizations interested in implementing electronic ID*".

B.4.*1 Chapter 1 The vision*

After a quick overview of the meaning of "Identification", "Authentication", "Electronic signature", and of the need for an eID, the following main drivers for a national eID and moreover for a pan European interoperable eID are summarized:

- "*need for a national support of e-services*";
- "*need for a common and global combating of ID Fraud*";
- "*need for national and as well as pan European anti-terrorism measures*";
- "*need for building a more inclusive European society*";
- "*stimulation of the emergence of new intra European Union services*".

On the other hand the following inhibitors to a Common eAuthentication/eID approach are addressed:

- "*State of the art of technology*"

  The combination of smart cards, digital signature and biometric technologies are relatively new. Moreover, "*smart card standardization is in place and implemented, biometric standardization is almost there but still under construction till early 2005 and smart card supported digital signature standardization has just been accomplished but is not fully implemented by industry*".

- "*Costs and benefits*"

  "*Smart card prices have come down over the years,* while *biometrics checking and the costs of retrieving certificates are relatively high,* but *it's also the organizational costs of (face to face) card issuance and enrolment of the cardholder. On top of that there is not an apparent business case for the Government or the private sector to carry the total of costs*".

- "*Not invented here*"

  In Government eID programs domestic specifications are still dominating. Also some people feel that an eID project is complex enough on a national scale and should not be overloaded with (cross border) interoperability issues.

- "*No strong central leadership*"

  "*So far there has been no strong central leadership in the domain of eID cards,* and *the EC has considered eID so far as a political minefield where national interest and privacy issues are dominant and has therefore not stepped in*".

  Yet there are strong examples that under a common European policy positive results may be achieved*:*" *the European Health Insurance card as well as the Tachograph card prove that such a EC action might very well work out*".

B.4 *Chapter 2 How can the vision be realized?*

The eEurope Smart Card Charter, whose results are embodied in the OSCIE (Open Smart Card Infrastructure for Europe) documentation, demonstrates the superiority of hardware tokens like smart cards from the security standpoint.

B.4*.2.2 Minimum requirements for issuing eID*

Scope & General eID Concepts

An interoperable electronic ID and eAuthentication in the eGovernment domain, based on microprocessor chip (contact and contactless) as a trustworthy and convenient token for eAuthentication as well as secure signature creation device for the electronic signature, must be supported by the concept that all smart cards issued and managed by a Government institute (or under its jurisdiction) should lead to the result that all cards from different Smart Card Communities where the IAS capabilities are recognized by a given service provider are accepted.

Basic eID System Functionalities

- *"Electronic identification & authentication of the cardholder to public and private services.*
- *Electronic signatures for legal proof of non repudiation".*

Optional functions

- *"Support of confidentiality services, enabling encryption of data transmitted over a network.*
- *Official Travel document".*

Overall eID System Requirements

- *"The system shall support different security profiles;*
- *The system shall be trustworthy for the cardholder; the system as such shall be reliable and it shall protect the cardholders data present in the card;*

- *The execution of the eID and eAuthentication function shall be convenient and fast, it shall be executed in a secure and controllable way;*
- *The system shall be future proof".*

Cardholder ID requirements

- *"The system shall support a secure and reliable cardholder identification function;*
- *A set of Personal data of the cardholder shall be held in an electronic form. This file is optionally protected by PIN and/or Biometrics;*
- *A set of Card related data shall be held in an electronic form".*

Cardholder Authentication requirements

- *"The system shall support a secure and reliable cardholder authentication function*
- *For this purpose the card will hold support:*
    - *one or more PIN's;*
    - *one or more Biometrics (bio-pin for 1:1 verification);*
    - *a signature key for authentication".*

Electronic Signature requirements

In addition to the need to support a legal validity of a signed information object, and the need for the PKI to be in compliance with the qualified electronic signature as per article 5.1 of Directive 1999/93/EC [1], the document explicitly mentions the need for compliance with the ETSI Qualified Certificate Policy document as well as the Workshop eSign CWA 14890 on a smart card based application profile.

The Commission Decision of 14 July 2003, on the publication of reference numbers of generally recognized standards for electronic signature products in accordance with the Directive, is also referenced to. This Decision makes explicit reference to CWAs 14167-1, -2, 14169.

B.4*.2.2.1 Organization issuing e-ID-cards*

"*In the particular case of an e-ID-card, it will always be a central administration (i.e. central Government) that would take the ultimate responsibility*".

B.4*.2.2.2 The Authentication level*

The document, similarly to what is defined in the UK eGovernment literature and in the US eGovernment literature (see note), proposes 4 levels of authentication:

- *"identification (just reading some cardholder data out of an open file in the card);*
- *authentication medium (same + PIN or Biometrics);*
- *authentication high (same + now a secret key is used to sign the personal card holder data), the smart card has to comply with CEN ISSS WS eSign SSCD requirements;*
- *non-repudiation (another secret key is used to approve of the content of a certain information object, the relevant certificate is "qualified")".*

NOTE: NIST Special Publication 800-63, Draft Recommendation for Electronic Authentication.

Although it is "*up to an individual eID card issuer of service operator to define his own security requirements and environment*", "*for mutual recognition of card holder eID's in the intra Europe and Global domain it's to be expected that operators will put up a relatively high level of security requirements*".

The following factors are specified:

- *"a token (smart card) as proof of possession by the individual;*
- *a password (PIN-code) as proof of knowledge by the cardholder in compliance with ISO/IEC 9654-1;*
- *a biometric verification process that matches a life bio-template from the cardholder to a stored template in the card by an on board card operation as proof of the authenticity of the cardholder in compliance with ISO/IEC 7816-11 and ISO/IEC FCD 19794-2 (fingerprint minutiae);*
- *a proof of possession of a key through a cryptographic protocol (PKI), the key pair(s) having been generated on board the card. Reference to the cryptographic object on the card (keys, certificates, root-certificates) shall be conducted by means of a description application according to ISO/IEC 7816-1;*
- *a strong cryptographic authentication of the card as well as relevant parts of the infrastructure and encryption of all sensitive data transfers between the system components shall comply with ISO/IEC 9798 (device-authentication/Secure messaging);*
- *on board the card generation of the digital signature (signing of the last round of hashing on board the card) for maximum security in the non repudiation process".*

B.4*.2.2.3 e-ID cards and qualified certificates*

The Issuer of certificate(s) supporting the "qualified electronic signature" (non-repudiation) created within/by each e-ID-card "*must comply with the ETSI Qualified Certificate Policy "QCP public + SSCD" (Secure Signature-Creation Device, specified in ETSI document TS 101 456 [*3*]) which is a certificate policy for qualified certificates issued to the public, requiring use of a SSCD*".

B.4*.2.4 The legal issue*

The Porvoo viewpoints were reconfirmed "*starting with the need of avoiding over-regulation in the legal drafting. This is particularly important for e-ID, which is a relatively new field and where new technical solutions appear regularly. A balance should therefore be ensured between technological neutrality and the need to ensure legal predictability*".

B.4*.2.4.1 Regulations concerning procedures etc. when issuing e-ID*

The link between the person/e-ID holder and the information in the e-ID must be secure, so that a 3rd party can accept the e-ID as a valid ID. For a pan-European e-ID, a homogenisation of basic procedural rules is required at least concerning the requirements for the issuing of e-ID: which documents must be presented by the holder to get an e-ID, is personal appearance required, when/at which stage of the procedure, which other evidence for proving the identity is needed, etc.

B.4*.2.4.2 The content of the e-ID (data quality) and the verification of the e-ID*

It is to be defined how to secure the link between the ID holder and the e-ID information, which information is to be in the e-ID certificate, and how to present the data, as well as the way a third party can verify the information given in the e-ID. This is to be solved taking also into account the nations where no unique personal identifier exists.

Also the extent the personal data are to be presented to a third party is to be harmonized.

B.4*.2.4.3 Data protection 2.4.4 Liability 2.4.5 Revocation*

These legal questions are also posed, as items to be solved.

B.4*.2.4.6 Interoperability*

In the context of the eEPoch project such an interoperability agreement has been defined.

B.4*.2.5 Standardization*

B.4*.2.5.1 Smart cards*

The following standardization bodies and standards are mentioned.

ISO/IEC JTC Subcommittee SC 17 that has addressed both the contact and the contactless smartcard domain.

The most relevant series are 7816 for the contact domain (now a 13 part standard covering physical characteristics, electronic signals and transmission protocols, command sets, data elements, etc.).

In the contactless domain relevant standards are ISO/IEC 10536 (close coupled cards, working distance about 2 mm, slot or surface) ISO/IEC 14443 (proximity cards, working distance about 10 cm, wilful act) and ISO/IEC 15693 (vicinity cards, working distance about 50 cm, hands free).

"*The ePassport recommendations mandate the ISO/IEC 14443 standard in type A as well as in type B mode. Interoperability testing of e-Passports in 2004 has however shown that some ambiguities in the standard might need to be addressed*".

"*A new SC 17 work item is in progress to produce a standard for application interfaces providing generic smart card services, the generic smart card services to include global interoperable eID/IAS functionality. The work item is being developed by SC17 WG4 Task Force 9, Application Programming Interface - Integrated Circuit Cards (TF 9 - API-ICC). The group is making fast progress and a draft three part standard is expected in early 2005. This standard ISO/IEC 24727 is envisioned to consist of 3parts: architectural model, high level API for services and a card edge API*".

"*One of the standardization elements still missing is a standard for post card-issuance application downloading and deleting. A proposal for a new work to cover this issue has been accepted by SC 17. This will lead to new dedicated part ISO/IEC 7816-13*".

"*There is no ISO/IEC standard for smart card operating systems. The CWA supports different options like native cards (complying with ISO/IEC 7816) as well as a Javacard environment*".

"*CEN TC 224 on identification cards has a number of working groups in different application areas like banking, public transport, health and also a recently (Q4 2003) installed Working Group 15 on a European Citizen Card. This group has started to work on a Technical standard for both the electronic as well as the physical aspects of the card. There are two Subgroups active one for the logical and electronic aspects and one for the physical and visual aspects*".

The CWA eAuthentication has been an important input document for CEN 224 WG 15.

B.4.*2.5.2 Biometrics*

"*Standardization in the biometrics area is less advanced than in the Smart Cards or PKI domain but due to the imminent need for anti- terrorism measures is gathering speed and trying to fill in the gaps*".

"*Extensive work is under construction in ISO/IEC SC 37 and produces draft standards at a high pace. The most relevant standards for the CWA eAuthentication are:*

- *ISO/IEC 19784-1 BioAPI, BioAPI specification.*
- *ISO/IEC 19785-1 Common Biometric Exchange formats (CBEFF) Part 1: Data Element Specification.*
- *ISO/IEC 19794-2 Biometric Data Interchange Format Part 2: Finger Minutiae Data".*

"*Most of these standards are still under development and in the stage of a FDC (final committee draft). Voting is on for a number of drafts. So at the end of 2004 /early 2005 we may expect a rather complete package of international biometric standards*".

"*SC 37 defines generic Biometric standards. Dedicated to the smart card domain is ISO/IEC S 17. SC 17 has developed:*

- *ISO/IEC 7816 part 11 which addresses personal verification through biometric methods in ID's".*

ICAO (International Civil Aviation Organization) made four relevant choices:

- *"the preferred chip technology for Machine Readable Travel Documents) is contactless (13,56 MHz);*
- *the preferred biometric technology for world-wide interoperability in the border control domain is facial recognition;*
- *the chip should hold the full picture of the biometric characteristic, not the "calculated" template (ICAO recommends 32Kbytes of memory for storing biometric images);*

- *the personal demographic data in the IC of the card is in principle freely accessible but a Member state may decide to make this PIN protected".*

"*Both the US and the European Union have decided to comply with these ICAO recommendations for the border control domain*".

"*A technical specification for the European ePassport is under preparation by the EC and is expected before the end of 2004*".

The Workshop has come up with the following requirements/recommendations:

- *"Biometrics will be used for 1:1 verification.*
- *An Object Identifier will be included to distinguish between different biometrics.*
- *The recommended biometric technology for interoperable access to e-services is fingerprint minutiae.*
- *It is mandatory to have the biometric template on board the card.*
- *The biometric template needs to be protected (read only) and its access may be optionally protected by a PIN.*
- *It is recommended to have the matching of the life bio-template and the stored template done on the card.*
- *Biometric 1: n matching is out of scope of the CWA eAuthentication".*

B.4.*2.5.3 Digital signature*

The most relevant work produced in the electronic signature for the Workshop purpose is CWA 14890 which aims to enabling "*interoperability, so that smart cards from different manufacturers can interact with different kind of signature creation applications. The CWA specifies the application interface to the smart card during the usage phase, where the smartcard is used as an SSCD, to enable interoperability and usage of those cards on a national or European level*".

"*In line with the CWA preferences CWA 14890 is applicable to smart cards supporting file system oriented applications (the ISO/IEC 7816 native cards) as well as for smart cards supporting object oriented applications (e.g. Java applets)*".

"*CWA 14890 has taken the following requirements into account:*

1) *Requirement 1: The format for electronic signatures and their certificates shall be interoperable.*
2) *Requirement 2: The device interface (physical, logical and application interface) shall be interoperable at least for the same device type. A signer should be able to use his signing device in different applications and environments, without having to install specific software drivers depending on the manufacturer of the device".*

"*The Workshop eAuthentication has accepted CWA 14890 part 1 and 2 as the basis for the IAS signature function from a security and interoperability perspective.*

This leads to the following:

- *CWA eAuthentication relies on CWA 14890 for mutual device authentication (smart card and infrastructure checking vice versa each others validity and genuineness).*
- *CWA eAuthentication relies on CWA 14890 for the digital signature for a nonrepudiation function in e-transactions.*
- *In addition the key pair for the digital signature needs to be either PIN protected, biometric protected or both.*
- *CWA eAuthentication has detailed its so called PKI adapter including the functionality of cross border certificate validity check. The CWA eAut envisioned preferred solution for this functionality is a bridge Validation Authority. However this preference will be brought in-line with accepted practice as soon as a final European wide solution for this need emerges".*

B.4*.2.5.4 Standardization of eAuthentication*

There are a number of initiatives in this field:

- Electronic Authentication Partnership (www.eapartnership.org).
- OATH (www.openauthentication.org).
- Wireless LAN Smart Card Consortium.
- Corestreet (www.corestreet.com) in the US.
- Other solutions are under study in France and in The Netherlands.

As an overall conclusion in the standardization domain "*the Workshop concludes that for the three domains (Smart Cards, Biometrics and Digital Signature) all the basic elements are sufficiently in place. However the combination of Smart Card, Biometric and Digital Signature Standards for the purpose of eAuthentication is still to be provided. The CWA eAuthentication is filling this gap and elaborating on the synergy of the three components*".

B.4 *Chapter 3 Deployment of eID in Europe and beyond*

This Chapter first gives an overview of the situation of eID cards in a wide number of nations.

Its report is based on reports by Inside ID, German TAB, Smart Card Charter Trailblazer 1, IDA eGovernment News - Identification and Authentication website EUROPA - IDA Interchange of Data between Administrations, as well as by B&L.

The general findings are:

The Anglo-American regions are not very ID card minded. On the other hand electronic ID cards are booming in the Far East (Japan, China, Hong Kong, Malaysia etc.) as well as in the Middle East.

"*An interesting issue is that China, Japan, Korea, Hong Kong and Singapore have agreed to do a concerted action to develop a common used and interoperable smart card (Silk Road Card). One of the results of this cooperation so far is the establishment of an Asian Smart Card Forum with its first conference in June 2004 in Korea*".

"*There is a relatively large quantity of projects in South America as well as in Africa. In Europe there is only a handful of countries engaged in the roll out phase, the majority of countries are still in the phase of getting political consent and conducting studies and pilot projects*".

"*The choices in the domain of the Public Key infrastructure are various. Only very few European countries are on their way of introducing biometrics for end-user verification in combination with the national ID card. This despite the fact that worldwide more than 70 countries are applying biometrics for card holder verification purposes. However this situation in Europe might change in the near future in the slip stream of introducing biometrics in the Passport book which is very definitely on its way. In general the worldwide focus of the projects is on the domestic market and cross border interoperability is not high on the agenda yet*".

The rest of the chapter deals with:

- The eID market development
- Deployment of eID in Europe
- The eID pan European demonstrator eEpoch
- eID projects in the rest of the world.

The present document does not go into details because this appears as being out of the ETSI ESI scope.

History

Document history		
V1.1.1	March 2006	Publication