

Open Smart Card Infrastructure for Europe

V2



Volume 4: Public Electronic Identity, Electronic Signature and PKI

Part 6: Requirements of terminal manufacturers and convergence model for multi-platform access to services

Authors: Smart-IS A.M. and eESC TB12 AES

NOTICE

This eESC Common Specification document supersedes all previous versions. Neither eEurope Smart Cards nor any of its participants accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from use of this document. Latest version of OSCIE and any additions are available via www.eeurope-smartcards.org and www.eurosmart.com. For more information contact info@eeurope-smartcards.org.



Smart-IS A.M.

IST Project n° 1999-13114

Project funded by the European Union under the Information Society 5th Framework Programme 1998-2002

Smart-IS AM, Accompanying Measure for accelerating Electronic Business and New Transactional Information Systems

WG3 Report : Requirements of terminal manufacturers and convergence model for multi-platform access to services

Deliverable : D6.2

Version: V 02.0

Date of version: 14 November 2002

Classification: Internal

Contract period: 1 June 2000 – 31 December 2002

Co-ordinator: Eurosmart

Participants: Axiome, CyberCOMM, Euralia, Magicaxess, Meta Group, Smart-IS Marketing, Telefonica I&D

Authors: Thierry COLLIN : THALES-E-TRANSACTION
Ladan PEGAH : CESYS
Bjorn TUFT : META GROUP

Versions

Version	Authors	Modifications
0.1	Thierry COLLIN – Ladan PEGAH	Creation
0.2	Thierry COLLIN – Ladan PEGAH – Bjorn TUFT	Drafting of the first version
0.3	Thierry COLLIN – Ladan PEGAH – Bjorn TUFT	Additional items
0.4	Norbert LIPSZYC	Corrections
0.5	Thierry COLLIN – Ladan PEGAH – Bjorn TUFT	Additions and Modifications
0.5R1	Thierry COLLIN – Ladan PEGAH – Bjorn TUFT	Additions and Modifications
0.6	Thierry COLLIN – Ladan PEGAH – Philippe LE CLECH	Additions and Modifications
0.6R1	Norbert LIPSZYC	Corrections
0.7	Norbert LIPSZYC -Thierry COLLIN – Ladan PEGAH	Additions and Modifications
0.8	Yves Le Roux – Norbert Lipszyc	Additions and corrections
01R1	Thierry COLLIN – Ladan PEGAH	Additions and integration of received comments
01R2	Thierry COLLIN – Ladan PEGAH	Additions and integration of received comments
01R2.1	Norbert Lipszyc - Bjorn TUFT	Additions and Corrections
01R3	Bjorn TUFT – Thierry COLLIN – Ladan PEGAH	Additions and Modifications
02.0	Thierry COLLIN – Ladan PEGAH- Bjorn TUFT	Additions and Modifications

Table of Contents

0. ABBREVIATIONS.....	5
1. FOREWORD	7
2. REFERENCES	8
3. INTRODUCTION	11
3.1 OBJECTIVES AND SCOPE OF THE REPORT	11
3.2 STANDARD SURVEY	11
3.3 STANDARDS ORGANISATIONS.....	12
3.4 CONTRIBUTION OF OTHER STUDIES	12
4. CURRENT MAJOR CONSIDERATIONS	14
4.1 GENERAL	14
4.2 CONSIDERATIONS AT TECHNICAL LEVEL.....	16
4.2.1 <i>NAME general specifications</i>	16
NAME CERTIFICATE PROFILE	17
4.2.2 <i>NAME.ES general specifications</i>	20
4.2.3 <i>Telecom considerations</i>	22
4.2.4 <i>Public key infrastructure and certificate</i>	24
4.2.5 <i>Card Accepting Device</i>	24
4.3 CONSIDERATIONS AT MARKETING LEVEL.....	25
4.4 CONSIDERATIONS AT SOCIETAL LEVEL.....	26
4.5 CONSIDERATIONS AT LEGAL LEVEL	27
4.5.1 <i>The Directive 1999/93/EC</i>	27
4.5.2 <i>The Advanced Electronic Signature</i>	28
4.5.3 <i>Secure signature-creation devices</i>	29
4.5.4 <i>Secure signature-verification devices</i>	31
5. ANALYSIS OF THE NEEDS AND REQUIREMENTS	32
5.1 ANALYSIS OF COMMON AND SPECIFIC REQUIREMENTS	32
5.1.1 <i>Security</i>	32
5.1.2 <i>Authentication</i>	33
5.1.3 <i>Electronic signature</i>	34
5.1.4 <i>« What you see is what you sign »</i>	36
5.1.5 <i>Card or other « portable support »</i>	36
5.1.6 <i>Requirements at hardware and software levels</i>	36
5.1.7 <i>Device Authentication</i>	37
5.1.8 <i>Interoperability</i>	37
5.1.9 <i>Smart Card Management Framework</i>	38
5.1.10 <i>Smart Card Management System</i>	39
5.1.11 <i>Other requirements</i>	40
5.2 EXAMPLES OF REQUIREMENTS BY BUSINESS APPLICATIONS AND SERVICES	41
5.3 OVERVIEW OF EUROPEAN E-GOVERNMENT APPLICATIONS AND SERVICES.....	43
5.4 ANALYSIS OF GENERIC NEEDS.....	46
5.4.1 <i>Publish</i>	46
5.4.2 <i>Transact</i>	47
5.4.3 <i>Collaborate</i>	50
5.5 ANALYSIS OF THE « ROAMING APPLICATIONS »	51

6. BUSINESS MODEL ANALYSIS.....	52
6.1 APPROACH FOR BUSINESS CASE ANALYSIS	53
6.1.1 <i>Process to develop a business case</i>	53
6.1.2 <i>Building a business model</i>	54
6.2 BUSINESS MODEL PROPOSED.....	55
6.2.1 <i>Value Chain Analysis: A federated trust model for authentication</i>	55
6.2.2 <i>Trust Domains</i>	58
6.2.3 <i>Challenges</i>	59
6.2.4 <i>Evaluation of Identified Risks</i>	60
6.3 TARGETED VALUE CHAIN.....	61
6.4 VALUE PROPOSITION IN THE MARKET SEGMENTS	62
6.5 BRANDING	65
6.6 VALUE TRANSFER MODEL / PRICING MODEL	65
6.7 COMPETITION	65
7. RECOMMENDATIONS	66
8. ANNEXES	68
8.1 CHARACTERISATION OF USER TERMINALS:	68
8.2 AUTHENTICATION SERVICES ISSUES: BIOMETRICS	70
8.3 TECHNOLOGIES	72

0. Abbreviations

API	Application Programming Interface
CSP	Certification service provider
ETSI	European Telecommunication Standardisation Institute
GPRS	General Packed Radio Services
GSM	Global System for Mobiles
GIF	Global Interoperability Framework
IAS	Identification, Authentication, Electronic Signature
ICC	Integrated Circuit Card (also called smart card)
ISP	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
MHP	Multimedia Home Platform
NAME	Network Access Module for Internet End-user
NAME.ES	Network Access Module for Internet End-user with advanced Electronic Signature functions
OASIS	Organization for the Advancement of Structured Information Standards
OLTP	Online transaction processing
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SAML	Secure Assertions Markup Language
SIM	Subscriber Identification Module
SMS	Short Message Services
SSCD	Secure Signature Creation Device
SCAD	Smartcard Accepting Device
UDDI	Universal Description Discovery and Integration



UMTS	Universal Mobile Telecommunication System
URL	Uniform Resource Locator
USIM	UMTS Subscriber Identity Module
WAP	Wireless Application Protocol
WIM	WAP Identity Module
WSDL	Web Services Description Language
WTLS	Wireless Transport Layer Security

1. Foreword

The present document comes within the scope of the Smart. IS –Accompanying Measures project , resulting from an initiative undertaken by the European IT and Smart Card Industries. The main objective of the Smart. IS –Accompanying Measures is to develop cross-industry, cross sector co-operative studies between users, network operators and manufacturers in the basis of **interoperability and security** of smart card E-Commerce and M-Commerce solutions.

To this end, Working Groups are organised and prepare the deliverables within a wide co-operation with other working groups such as ETSI/EESSI and CEN/ISSS ,who bring inputs on electronic signature standards. An effective liaison is also established with the Trailblazer 12 (TB12) concerning the Advanced Electronic Signature issues.

The Working Group 3 aim is to investigate what are the requirements for enabling common card-holder authentication and electronic signature modules to work with any type of Internet terminal to access open networks and services (e.g.: PDA, GSM, Web-phone, PC,...).

The present report is divided into six chapters:

The Chapter 1 – Foreword: this chapter.

The Chapter 2 – Reference

The Chapter 3 – Introduction : presents the objectives and the scope of this report, the standards, organisations and the other studies contributing to the preparation of the present report.

The Chapter 4 – Current major considerations: presents current context, concepts, processes and technologies to be considered in 4 domains : Technical, Marketing, Societal and Legal

The Chapter 5 – Analysis of the needs and requirements: Presents the main common and specific requirements that are considered by terminal manufacturers, provides significant examples of applications and services in the areas of E-Commerce, E-Business and E-Government.

The Chapter 6 – Business model proposed: Presents a first level of business model for terminal manufacturers and proposes to provide a first characterisation of terminals able to connect in the secure way the users with the different types of application.

The Chapter 7 – Recommendations

The Chapter 8 – Annexes

2. References

The standards-related work based on the European Electronic Signature Standardisation Initiative (EESSI) project is carried out by the Electronic Signature Infrastructure (ESI) working group of ETSI SEC, and by the E-sign workgroup of CEN's Information Society Standardisation System (CEN/ISSS).

ETSI SEC is working on the following subjects :

Subjects	Reference of documents	Title and description
The use of X.509 public key certificates as qualified certificates;	TS 101 862	Qualified certificate profile The purpose of this standard is to specify format and contents of Qualified Certificates. The standard is based on the IETF draft "X.509 Public Key Infrastructure Qualified Certificates Profile", specifying amendments to meet the requirements as laid down in the European Directive on electronic signatures (1999/93/EC), in Annex 1.
Security Management and Certificate Policy for CSPs issuing qualified certificates;	TS 101 456 v.1.1.1	Policy requirement for certification authorities issuing qualified certificates The purpose of this standard is to specify policy requirements on the operation and management of certification authorities issuing Qualified Certificates as laid down in the European Directive on electronic signatures (1999/93/EC).
	STF178 Task 5 (TR 102 030 v.0.0.29)	Provision of harmonised Trust Service Provider status information
Electronic signature syntax and encoding formats, and technical aspects of signature policies	STF178 Task 3 (TS 101 903)	XML Advanced Electronic Signatures (XAdES) This draft standard specifies the XML format for Advanced Electronic Signatures satisfying the requirements defined in the European Directive for Electronic Signatures, and with long term validity.
	TS 101 733 v.1.2.2	Electronic Signature Formats
	STF178 Task 3 (TR 102 038)	XML format for signature policies This technical report tries to accommodate the information for Signature Policies defined in ETSI TS 101 733 to XML syntax. It is seen as the starting point of much more extensive work that should be done in a near future on this topic.
	STF178 Task 4 (TS 101 733)	Technical, organisational and legal issues related to signature policies Drafted new Annex to TS 101 733 (Annex G: Signature Policy in an Informal Free Text Form), which describes example content of a signature policy in a free text format as an alternative to using ASN.1.
	STF178 Task 2 Draft G (TS 102 042)	Policy requirements for certifications authorities issuing public key certificates This draft standard specifies policy requirements for Certification Authorities (CAs) supporting the broad range of applications of public key certificates. It is based on TS 101 456, but has much wider applicability and includes CAs supporting electronic signatures, digital signatures, encryption, key exchange and key agreement mechanisms.
Protocol to inter-operate with a Time Stamping Authority.	TS 101 023	Policy requirements for time-stamping authorities This draft standard specifies policy requirements on the operation and management practices of Time-Stamping Authorities such that subscribers and relying parties may have confidence in the operation of its time-stamp services.

	TS 101 861 v.1.1.1	Time Stamping Profile The purpose of this standard is to specify format and protocol for time stamping. The standard is a profile of RFC 3161 “Time Stamp Protocol”.
--	-----------------------	---

The CEN/ISSS is working on the following subjects:

Subjects	Area	Reference of documents	Title and description
Security requirements for trustworthy systems and products	D1	CWA 14167-1	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures; Version 0.17 (approved)
	D2	Draft CWA 14167-2	Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP); V 0.18 (approved)
Security requirements for secure signature creation devices	AA1	CWA 14255	Guidelines for the implementation of Secure Signature-Creation Devices; Version 0.91 (approved)
	AA2	CWA 14365:	General Requirements for Electronic Signatures, Version 0.63,
	F		Explanatory memorandum concerning the two versions of the CWA Drafts on Area F
	F		Memorandum: CC-Evaluation of WS/E-Sign CWA Area F (approved)
	F	CWA 14168	Secure Signature-Creation Devices, version ‘EAL 4’, 2001-03-01* (approved)
	F	CWA 14169	Secure Signature-Creation Devices, version ‘EAL 4+’, 2001-03-01* (approved)
Signature creation environment	G1	CWA 14170	Security Requirements for Signature Creation Systems; Version 3.0, 2000-10-08 (approved)
Signature verification process and environment	G2	CWA 14171	Procedures for Electronic Signature Verification; V 1.0.5, 2001-03-13 (approved)
Conformity assessment of products and services for electronic signatures	V		Inventory of European Economic Area Member State Strategies for implementation of European Directive 1999/93/EC, 2000-08-30 Minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3 (4) of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 2000-11-28
		CWA 14172-1	EESSI Conformity Assessment Guidance: Part 1 – General, 2001-03-15 (approved)
		CWA 14172-2	EESSI Conformity Assessment Guidance: Part 2 – Certification Authority services and processes, 2001-03-15 (approved)
		CWA 14172-3	EESSI Conformity Assessment Guidance: Part 3 – Trustworthy systems managing certificates for electronic signatures (approved)
		CWA 14172-4	EESSI Conformity Assessment Guidance: Part 4 – Signature creation applications and procedures for electronic signature verification (approved)
		CWA 14172-5	EESSI Conformity Assessment Guidance: Part 5 – Secure signature creation devices (approved)
		CWA Group K	Application Interface for Smart Cards used as Secure Signature Creation Device

E-Europe Smart Card is composed of 12 trailblazers :

- TB1 - Public Identity
- TB2 - Identification & Authentication
- TB3 - Protection profiles, security certification
- TB4 - Generalised card reader
- TB5 - e-payment and m-payment
- TB6 - Contactless smart cards
- TB7 - Multi application smart cards
- TB8 - User requirements
- TB9 - Public transport
- TB10 - e-government
- TB11 - Healthcare
- TB12 - Advanced electronic signature

Documents are developed within the **SMART IS – Accompanying Measures** project by different Work Groups:

SMART IS – AM : NAME V1.0 White paper (Draft of February 2002)

SMART IS – AM : NAME-ES

SMART IS – AM : Telecom Requirements as RFC document (draft of April 2002)

Embedded FINREAD Consortium :

Embedded FINREAD - Business requirements (version 2002-06)

Embedded Financial Transactional IC Card Reader

Embedded FINREAD – Functional Architecture and Technical Requirements (version 2002-06)

European Community :

Directive 1999/93/CE decided by the European Council presenting the legal framework for the use of Electronic Signatures (13/12/1999).

Directive 95/46/CE decided by the European Council related to the protection of Personal Information (24/10/1995).

3. Introduction

3.1 Objectives and Scope of the Report

The Working Group 3 (WG3) aim is to investigate what are the requirements for enabling common card-holder authentication and electronic signature modules to work with any type of Internet terminal to access open networks and services (e.g.: PDA, GSM, Web-phone,...). It includes the definition work for mainly the concept specifications and the impacts on the system at different levels : card, card accepting device, server and network, essentially to answer the following questions:

- What does the notion of « roaming applications » cover ? Some examples could be PDAs, GSMs, Internet terminal like network computers.
- Which services can benefit from interoperability between smart card systems ? Some services that have been already identified are : electronic signature, non-repudiation of payments, development tools,...
- What are the target markets for these services ? The study will only cover business sectors for which authentication and identification requirements are of a prime necessity. The study will give a segmentation of the market (by business sector and by geography area) and will determine the specificity of each segment as well as volume forecasts for the two to three years to come.

Working Group 3 addresses the following issues:

- Technical specifications for the implementation of the authentication and electronic signature modules on various types of terminals
- Comparison with other types of solutions and comparative economic impacts.
- Tracking, referencing and collating economic and investment analysis research concerning interoperability technologies.
- Constraints, success factors and alternative solutions to the use of NAME and NAME.ES modules by terminal manufacturers.

3.2 Standard Survey

The following communities are mainly involved:

- Telecom and mobile: mobile terminals will be one of the main devices for accessing internet services, and have defined or adapted different standards to take into account the specificity of mobile transmission.
- Banks and financials: since they are involved in electronic business, and have already deployed electronic payment solutions,
- Internet community: which defines standards for internet,
- Standards Organisations: which define international standards (ISO, ETSI, etc.)

We note also the work conducted by the Mobile Payment Forum.

3.3 Standards Organisations

Following the European Directive on electronic signature, different initiative to define and normalise the way of making advanced and simple electronic signature are in progress. More over other standardisation organisation have defined or are defining different specifications.

The different projects are mainly:

- EESSI The European Electronic Signature Standardisation Initiative. The specification of standard are carried out by the European Standards Organisations CEN and ETSI.
- E-Europe Smart Card: an initiative aims to accelerate and harmonise the development of smart cards across Europe. EESC is composed of Twelve trailblazers, each of them concerning specific subjects like public identity, or advanced electronic signature.
- IETF: The PKIX working group which specify the RFC standards on public key infrastructure with X509 certificate.

3.4 Contribution of Other Studies

Within this report, some initiatives and recommendations considered as relevant to the development of the present report are taken into account :

- The document entitled « Application Interface for Smart Card used as Secure Signature Creation Device » is provided within CEN/ISSS : WS/E-sign Draft CWA-Group K. This document relies on requirements of existing standards for secure signature creation devices (relevant for electronic signatures for the respective EU-directive). This document describes the European standardisation activities and solutions for Smart Cards as a special type of a Secure Signature Creation Device (SSCD). This document explains the reasons for which the Smart Cards are selected as representative for SSCDs.
- The work achieved by « Embedded FINREAD Consortium » allow to identify the business requirements for an Embedded FINREAD IC card reader. It is driven by the intention of the participating international financial schemes, network operators and the manufacturing industry.
Several reasons are inhibiting the manufacturing industries from developing a secure and interoperable access device with a secure reader able to be universally applicable to a wide range of business needs. Indeed, each IC card project needs to develop its own specific components.
The specifications should ensure that an Embedded FINREAD IC card reader or a device hosting the Embedded FINREAD functionality will be capable of becoming the standard platform for security related applications in domains such as payment, government or health.
An Embedded FINREAD device is based on the architecture, infrastructure and the services of a hosting system (e.g. mobile device such as mobile phone, Web Pad, PDA,

PPC, or Mobile Card Terminal, and stationary devices like set-top-boxes, PC and many more.

- The Smart Card Charter : Global Interoperability Framework for Identification, Authentication and Electronic Signature (IAS) with Smart Cards – Part 1 : Contextual and conceptual modelling (version 2.0 of 28 june 2002).
The objective of the « Interoperability Framework for IAS with smart cards » is to provide both smart card communities and e-service communities with the necessary concepts and guidance on the tools required for access to e-services and for security of transactions over the Internet where special « high-end » requirements must be fulfilled concerning identification, authentication (tokens and persons), non-repudiation (by electronic signature), encryption and integration with other applications.
The guidance includes :
 - *preparing information systems for interoperating i.e. providing the rules and standards which should be used within information systems in order to be able to guarantee IAS interoperability fr internet transactions.*
 - *Organising the operation of this IAS interoperability i.e. the ability of an e-service community to verify the identification and the validity of the authentication and electronic signature of a member from a different e-service community.*

4. Current Major Considerations

4.1 General

The use of the authentication and electronic signature services by sensitive applications operating within the most of the business sectors is now growing. Significant contributions of financial institutions in this way are well recognised and constitute a successful experiences for the development of the security services.

As noted in the document entitled Embedded FINREAD – Business Requirement, « Due to the rapid evolution of E-Commerce and M-Commerce and the growing number of access devices which are increasingly used to access theses services, the need to expand the existing specifications to include a more wider definition of services became apparent. Till now, the standard was limited to devices connected to PC. By addressing devices such as mobile phones, set-top boxes or personal digital assistants (PDAs), the initiative has been expanded to include new partners, representing the interests and technology of new industries.

At present there is a lack of standards to access financial services based on IC cards via the wide range of different access devices available in the market ».

Generally, the manufacturing industry are facing some difficulties in the development of a secure and interoperable access device with a secure reader, which could be universally applicable to a wide range of business needs:

- Non standardised software architecture generally in use,
- Multiple hardware architecture of access devices,
- Technical complexity of platforms,
- Different application requirements in terms of security (payment, financial, health, government, exchange of confidential information, etc),
- Different security rules in different schemes (payment, financial, health, government, exchange of confidential information, etc),
- Different administration rules addressing different types of users,
- Societal constraints not yet resolved,
- Legal aspects not well understood by the professionals (lawyers, legal experts)

The need for a secure Smart Card reader by the European industries constitutes an important opportunity. Indeed, it is essential to take into account the current situation concerning the use of security services.

IT infrastructure organisations have been deploying simple, rudimentary authentication services as part of an overall identity infrastructure since the early 1990s. The traditional approach used changeable passwords as the "secret" needed for access. Products and processes have evolved to define and manage passwords, from password synchronisation to Web single sign-on. Currently, more than 80% of authentication services are still simple password systems.

The renewed emphasis on secure infrastructure access and the evolving business demands of inter-enterprise commerce demand more than simple authentication. Enterprises intent on improving secure access to applications and other IT resources are seeking stronger forms of authentication than mere user IDs and passwords. The following trends are evident:

From static to mobile: A key characteristic of well-defined identity is the ability of a user to have the necessary authentication information in mobile form to use anywhere on any point of interaction.

From weak to strong: Passwords alone, in spite of the products and processes available to improve use, are no longer adequate for many business requirements. This year will see stronger authentication options (such as Kerberos and PKI) entering mainstream identity infrastructure.

From moderate to large volumes: Authentication engine scalability has grown from enterprise and first-generation e-business implementations (<1 million users) to large-scale government and e-business initiatives (>30 million users).

From enterprise to inter-enterprise: Enterprises continue to show increasing interest in deploying authentication services spanning multiple enterprises as a result of e-commerce, supply chain, or community-of-interest networking. This involves domains of trust as well as technology elements; such technology will be slow to develop, gaining some usage in 2003, but more pervasive use after 2004.

From unfocused to focused management: Building stronger, more mobile authentication services will drive the need for focused *identity management*, a discipline that includes single-point and delegated administration services, provisioning, workflow, and self-registration.

From person to application: Although most authentication services are devoted to providing identity verification for people access to applications, requirements continue to expand for application authentication (i.e., verifying one application's access to another). This is particularly important for successful Web services deployments, where a chain of application interactions may be required to complete a single end-to-end transaction. Middleware security will become an increasing concern for many enterprises seeking to expand enterprise application integration outside protected network boundaries during 2003-05.

From medium to larger threats: As authentication services expand to become shared enterprise and inter-enterprise infrastructure, current attempts to steal identity will continue to take the form of password-level attacks (e.g., password masquerade, file thefts, keystroke and network sniffing) and increasingly complex defences. As strong authentication services bring encryption, certificates, and tokens to the mainstream in 2002-04, users can anticipate equally sophisticated attempts to steal and crack the secrets protecting a user's identity. Users can also expect increasing legal and governmental scrutiny as identity theft threatens the privacy of such information, resulting in complex legislation.

In this context, it is essential to take into account some major considerations at different levels:

- Technical
- Marketing
- Societal
- Legal

4.2 Considerations at Technical Level

As described in the Smart Card Charter, the “Smart Card System” is seen as one of the “building blocks” of an information system including the following components :

- The **smart card**, used by a smart-card holder,
- The **infrastructure**, including card readers, card interaction devices, remote servers and private or public telecommunication networks,
- The front office **application** divided in :
 - The application which delivers a service to a user with a smart card.
 - The nucleus application for the process and criteria for strong **identification** of the smart-card holder (and the smart card and infrastructure components as well). This is the core of the interoperability framework as presented in this document. The nucleus needs to be integrated in the business application.

In the framework of the present report, specific functional and technical considerations are reminded concerning NAME and NAME.ES modules.

4.2.1 NAME general specifications

NAME (Network Authentication Module for internet End-users) has been developed within an accompanying measure called SMART.IS, sponsored by the European Union. This project aims at promoting standard specifications for interoperable and secure smart card systems, to be used for e-business and transactional information systems over the Internet.

A second phase called NAME ES will address the use of NAME module for electronic signature.

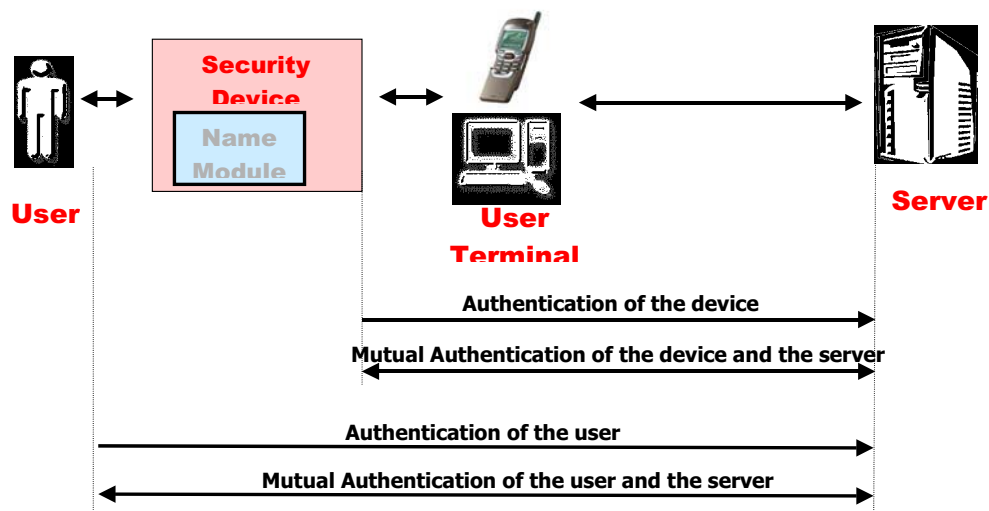
The specifications should include the following elements:

SECURITY : key management, certification procedures...

- **SERVICES** : payment (protocols,...), loyalty, e-trading, data-transfer
- **APPLICATIONS** : B to B, B to C, B to A

NAME could be implemented on **multi-function cards** issued by network operators based on current international specifications (EMV, SET, WAP, UMTS,...), for secure access to **interoperable services** through open infrastructures **and standardised secure readers**.

In order to carry out end-user authentication on the internet or another network, it is necessary to interface the device with the user terminal which is connected to the network as shown in the figure below:



NAME Certificate profile

For NAME the use of an X509 certificate is mandatory.

The profile of an X509 certificate is :

- **Version** : Version of the certificate
Value is 2 to indicate an X509V3 certificate.
- **SerialNumber** : CertificateSerialNumber,
An integer assigned by the CA to each certificate. It **MUST** be unique for each certificate issued by a given CA
- **signature** : AlgorithmIdentifier,
The OID of the algorithm used by the CA to sign the certificate. The commonly accepted OIDs are :
 - md2WithRSAEncryption
 - md5WithRSAEncryption

- sha1WithRSAEncryption
- issuer : NAME,
 - identifies the entity which has signed and issued the certificate. It MUST be a Distinguished NAME following the type X501 NAME.
- validity : Validity,
 - defines the time interval during which the certificate is valid. It contains two UTCtime dates (notBefore and notAfter)
- subject : NAME,
 - identifies the entity associated with the public key of the certificate. It MUST be a Distinguished NAME following the type X501 NAME. The DN must be unique for a given CA.
- SubjectPublicKeyInfo : SubjectPublicKeyInfo,
 - carry the public key and the OID of the algorithm with which the key is used. The commonly accepted OIDs are :
 - md2WithRSAEncryption
 - md5WithRSAEncryption
 - sha1WithRSAEncryption
 -
- issuer UniqueID UniqueIdentifier
 - Shall not be used.
- subjectUniqueID UniqueIdentifier
 - Shall not be used.

Extensions

The following standard extensions defined in RFC 2459 [2] are used according to the above rules.

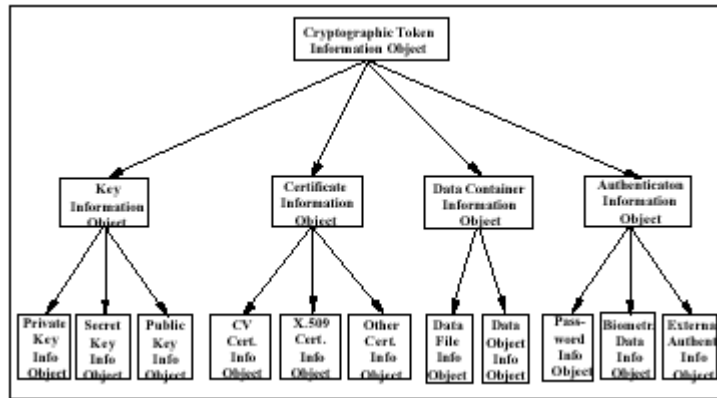
The NAME certificate **MUST** contain one of these two extensions :

- CRLDistribution Point
- Authority Information Access

The NAME certificate **MUST** contain the key usage extensions:

Object definition

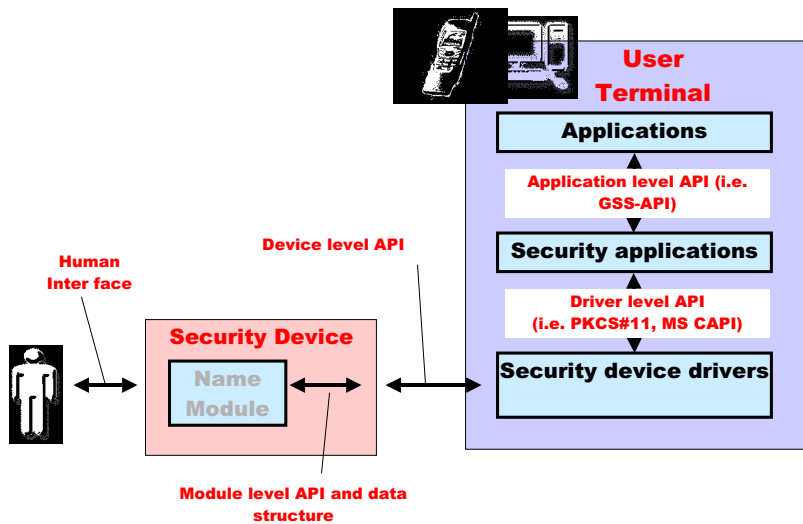
The object used by NAME module are defined in ISO 7816-15 [15]. The_cryptographic token information object hierarchy described in ISO 7816-15 is :



Remark

It has been established that the present NAME document will only cover user authentication and not mutual or server authentication. Nevertheless, the precaution has been taken to allow the possibility to implement mutual authentication and other services like session key generation, etc. as an option of NAME. These precautions will be described as optional recommendation.

As described in the figure different elements need to interact with the NAME module at different levels.



The NAME document gives requirements on these different interfaces:

- Human interface
- Module level API and data structure
- Device driver API
- Applications level API

4.2.2 NAME.ES general specifications

4.2.2.1 Functions to be included inside the smart card:

Hashing : A hash function H takes an input m and returns a fixed-size string, which is called the hash value h (that is, $h = H(m)$). Document Hashing inside the module is optional on the NAME-ES module. If existing, it must be using SHA-1.

Formatting : Security can be brought via formatting functions such as the ones specified in ISO 9796, or via hashing (no message recovery) as specified in PKCS#1.

- Signing
European algorithms and parameters for secure electronic signatures should be used.
- Managing certificate and keys

User verification : The NAME-ES module provides two-factors user authentication :

1. The smart card, unique and tamper resistant
2. Something the user alone knows (PIN code) or something that is unique to him (biometric identification)

Data structure and file system management : the files on the card must be securely managed as specified in ISO 7816-15.

4.2.2.2 Services to be provided by the Smart Card:

Digital signature service :

The digital signature service allows NAME-ES to be considered as a secure signature creation device (SSCD) according to EU directive annex 3.

The digital signature service is mandatory for a NAME-ES module.

Authentication service :

The authentication service is mandatory for a NAME-ES module.

Decipherment service :

The decipherment service is optional for a NAME-ES module.

4.2.2.3 Smart Card Application Interfaces needed**E-Sign application interface :**

The command sequence is defined

WIM application interface :

The signature can be initiated at the WIM application level in different ways.

If several certificates are available that match the criteria indicated in parameters, the choices should be indicated to the user, using e.g., labels of the certificates. If the user approves the operation, the browser **MUST** ask for user verification information for the private key (e.g., the WIM PIN for a non-repudiation key). If the user enters the correct information, signText signs the specified string and returns signedString to the script as String formatted as base-64 [RFC1521] encoding of SignedContent.

Commands used :

The NAME-ES module must support the following security commands as defined in ISO 7816-4 and -8:

Verify	
Code	Value
CLA	'8X'
INS	'20'
P1	'00'
P2	PIN ref.
Lc	YY
Data	FormattedPIN
Le	-

Manage Security Environment	
Code	Value
CLA	'8X'
INS	'22'
P1	Must support SET and RESTORE
P2	See ISO 7816-8
Lc	See ISO 7816-8
Data	See ISO 7816-8
Le	-

Perform Security Operation	
Code	Value
CLA	'8X'
INS	'2A'
P1	Must support '9E9A' (Compute Digital Signature) and '90A0' (Hash)
P2	
Lc	YY
Data	FormattedPIN
Le	-

Some other APIs may be optional:

- Mapping of general requirements to asymmetric techniques
- Command and responses seen at the interface to the ICC
- Cryptographic application information
- Usage of signature schemes according to the European and national algorithm catalog for electronic signatures
- Device authentication
- User verification management (knowledge based, biometrical)
- Storage and retrieval (loading) of certificates (roots) of different kinds and levels
- Application selection
- Card management related aspects

4.2.3 Telecom considerations

It will be possible to many users to access the services provided by a Internet Service Provider from many different types of devices enabling NAME and NAME.ES modules. Some of these devices can be mobile phones, personal computers, Pas, e-books, etc.

The access to the Internet also depends on the device being connected. The personal computer may access through a LAN or a modem, the PDA through a LAN using Bluetooth, and the

mobile phone by a WAP, for example. Depending on the way these devices access the Internet, the Public Key Infrastructure (PKI) may vary, and interfaces between terminals and the network change. It is not the same scheme for a network operator users accessing from a wireless terminal or those from a personal computer.

The access from different terminals can be made from different protocols, which have to be taken into account in order to use the security modules.

Telecom operators and Service Providers need an application-level infrastructure to control which transactions he can execute. This application-level access management system must also control (or audit) a user's action to provide non-repudiation of transactions. This requires a very open and extensible infrastructure that can integrate with complementary security and m-commerce technologies.

It should support multiple authentication methods – including Personal Identification Numbers (PINs), passwords, WTLS (Wireless Transport Layer Security) certificates and Public Key Infrastructure (PKI) – and should provide APIs (Application Programming Interfaces) for integration with legacy applications.

The emergence of the Wireless Application Protocol (WAP) is mobilising the industry to develop a standard format for presenting Web content on mobile devices. WAP gateways manage access to a Web server, provide encryption through the WTLS specification and authenticate users to enable a secure connection between the wireless device end the server. Generally, m-commerce is based in transactions with e-shop means of WAP.

Telecom operators are interested in offering value-added services to their subscribers. If a mobile terminal can be used as a type of payment for goods and services, the mobile operator is not interested to manage the transaction. Indeed, appropriate security measures need to be implemented.

Secure payment transactions for mobile commerce and mobile banking requires :

- Transaction-oriented security
- Security schemes accepted by e-commerce/banking organisations
- Non-repudiation
- End-to-end security

Generally, devices will become more specialised. Multi-modal interfaces e.g. full browser, micro browser, WAP browser, voice command and text-to-speech will become common. These devices are natural choices as card accepting devices. This will have a major impact on connections, like wireless LAN, DSL, cable modem and wide-area wireless networks. The demand for high-speed wireless data services continues to grow and in addition to traditional cellular technologies, carriers and start-ups are exploring the use of alternative wireless technologies, namely those operating in the unlicensed frequencies (e.g., 2.4GHz and 5GHz).

IEEE 802.11b wireless LANs represent an attractive technology for wireless data hot spots for Internet connectivity due to the increasingly widespread adoption of the hardware by enterprises and consumers, as well as the relatively inexpensive deployment costs (e.g., no licensing is required). Wireless LANs (IEEE 802.11b) will not displace existing cellular-based services; instead, localised hot spots will coexist with, and extend, traditional wireless

carrier networks for high-speed wireless data services. The technology is well suited to localised deployments and is scheduled to expand its current bandwidth capabilities beyond 11 Mbps to 54 Mbps, with the arrival of enterprise-class 802.11a hardware.

Bluetooth differs from 802.11b in that it is slower (1 Mbps, similar to the original 802.11). It was designed for low-cost, low-speed transmission and reduction into silicon, eventually becoming an embedded device. Power consumption is low and Bluetooth is well suited for small portable devices with stringent power requirements. IEEE 802.11 a/b and Bluetooth will coexist and achieve critical mass by 2003.

4.2.4 Public key infrastructure and certificate

When using a public key to verify signed data, it's necessary to be able to guarantee the integrity of this key and to link it with the owner of the associated private key.

The certificate is the element that provides the link between the public key and the identity of the owner of the associated private key.

The public key infrastructure is a set of rules, specifications, and procedures that describes the complete system.

The use of PKI is not mandatory, but recommended as PKI is the best candidate as cryptographic algorithm due to its built-in non repudiation future.

The use of a Smart Card as a secure portable device has been deeply studied : it may bring a very high security level.

But, even a secure crypto Smart Card with public key generation brings no security at all if other parts of the system are not.

4.2.5 Card Accepting Device

The importance of independent card access devices in the generation of Advanced Electronic Signature must be underlined. Indeed, it is necessary to precise the role of the card accepting device within the system architecture.

During the next three to five years, companies will re-engineer their computing environments and enable access by numerous pervasive computing devices (e.g., hand held devices, smart phones, auto PCs, Web TV, info appliance, game consoles and kiosks to name a few).

Devices will become more specialised. Multi-modal interfaces e.g. full browser, micro browser, WAP browser, voice command and text-to-speech will become common. These devices are natural choices as card accepting devices

4.3 Considerations at Marketing Level

The awareness in smart cards as a device for strong authentication has been increasing as smart cards represent a possible solution to the architectural problem of secure, mobile identity.

The standard architecture for Smart Cards-based secure transactions will facilitate electronic commerce for business-to-consumers, business-to-business and business-to-administration applications. In particular, this architecture will make use of a module called NAME (Network Access Module for internet End users). This module enables the secure authentication of the smart card owner and will give access to:

- The Smart Card user id;
- Signature of the transaction based on a X 509 V3 certificate;
- ISP references;
- Payment functions;
- Etc.

It is assumed that there will be no global identity solution available in the timeframe of the current work. The study will assume there are multiple trusted authorities that manage identity solutions that can be used as a basis for authentication.

Interest in using smart cards for authentication is on the rise. Prices for smart card read/write units are dropping to less than \$15 and primitive, limited functionality smart card units cost as little as \$1 through promotions and volume purchases. Low-volume unit costs usually range from \$5 to \$20. Systems integration expertise with smart cards is also growing.

With current deployment rates, it is apparent that smart card use as an authentication mechanism is gaining acceptance in several key market sectors. Furthermore, the concept of bundling additional functions onto the smart card - such as physical building access, multiple logon IDs/passwords, and digital signature capabilities - provides enterprises with opportunities for acceptable return on investments.

Identity and permission management infrastructures will evolve to provide directory, authentication, authorisation, delegated administration, and data quality for e-business applications within 12-18 months. External solutions will migrate into the enterprise. Directory interoperability issues will drive integration standards (e.g., LDAPv4, XML-based) and improved meta-directory services.

Smart card deployments are approaching critical mass world-wide for specific government, banking, retail, and mobile needs. Widespread use within enterprises for strong authentication is now possible, though temporarily hampered by proprietary solutions, competing operating systems, and lack of robust card management services.

Various smart card form factors *e.g., USB "token" smart cards, biometric-locked smart cards) are spurring various card reader/writer infrastructure options like keyboard readers, USB-attached readers or combination of biometric/smart card scan readers.

The following table presents the Smart card market Growth Forecast provided by Eurosmart

	1999	2000	2001 (Forecast)	2001	2002 (Forecast)	2005 (Forecast)
Banking	108	120	140	140	170	540
HealthCare	30	30	30	30	16	120
Telecom	200	370	500	390	415	1 250
Transport	3	3	12	8	12	40
Pay TV	29	20	30	25	35	80
	(Including IT)					
IT (internet ID)		5	15	5	15	150
Loyalty / retail			15	11	12	60
Government ID						150
Other	28	3	25	4	5	70
Total	398	551	767	599	689	2 460

- Banking: important evolution due to EMV cards roll-out
- Wireless: an average 40% increase per year, due to new services in mobile networks
- IT: major roll-out in Internet ID applications (mainly B2B and C2A)
- Transport: world-wide replacement of paper/magstripe by chip in new generation ticketing systems
- 2001- Global yearly CAGR for smart card industry: 20% (in volumes)
2005 - Global μ processor cards volumes have overtaken memory cards markets

4.4 Considerations at Societal Level

Authentication is the process or ability to identify a person, resource, or system that is requesting access to another person, resource or system. Without authentication there can be no security, as even the strongest security measures are rendered irrelevant as one person can easily assume the identity of any other. The issue of identification is complex and has political and social ramifications. It is also a fundamental issue and a core element of civil society in general and of security in particular.

Any technological change such as widespread authentication has to take into account the relative maturity of potential users. Authentication may imply complex steps that not all users may accept. There is also the challenge of different user interfaces in different cultures, a fact that travellers are frequently exposed to.

This diversity in technological prowess may be mitigated by standardising the user interface, including the sequence of steps required to carry out an authentication or a signature to the point that it can be carried out in a foreign culture. Most people are capable of using a phone in a foreign country, largely due to its simplified user interface and standardised procedure.

It is essential that any authentication and signature process be not only simple but also standardised relative to the event that requires these acts. This requires a high level of collaboration between the parties having an interest in the success of a widely used authentication scheme within a defined social situation. It also requires training and education of users, a cost that should be included in any business case.

These considerations will be different according to the scope. A local use, like paying for the parking will have different constraints than a e-commerce solution with a world-wide impact.

The main societal considerations relating to the use of Smart Cards by different categories of consumers are the following :

- Knowledge and usage of PCs, mobile phones, etc.
- Flexibility of solutions : customisation, day-to-day utilisation, functional evolution ability
- Pricing of solutions
- Awareness of security processes : authentication and electronic signature.

4.5 Considerations at Legal Level

The European Directive 1999/93/CE decided by the European Council allows to describe the legal framework for the use of Electronic Signatures (13/12/1999).

The satisfactory application of this directive within the European community requires the harmonisation of legal context in the different European.

Legal requirements addressed to the NAME.ES module consist in two major points :

- Be able to authenticate the signer
- Be able to prove the consent of the signer.

Finally, the terminal must be able to include technical features in order to meet these requirements.

4.5.1 The Directive 1999/93/EC

The *Directive 1999/93/EC on a Community Framework for Electronic Signatures (ESD)* was issued after the adoption of some national laws, regulating electronic signatures, which did not share very much in common. For example the German Digital Signature Act 1997 provided for a mandatory accreditation scheme coupled with high security standards for certification service providers. In contrast, the prevailing notion in England has been that of business self-regulation.

The Directive, therefore, aims to prevent divergent rules with respect to legal recognition of electronic signatures and the accreditation of *certification-service-providers* in the Member States, which may create a significant barrier to the use of electronic communications and electronic commerce. Furthermore, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies (ESD, recital (4)). Moreover, the ESD contains also a liability provision. Considering that all member states have to comply with the Directive, it is reasonable to expect that the entire EU will have a twofold digital signature system . There will be, on the one hand, an *advanced electronic signature* that will have the same value as a hand written signature and be admissible as evidence in legal proceedings (ESD, Art.5 (1)). On the other hand there will be a 'regular' *electronic signature* which may, at least, not be denied legal effectiveness and admissibility as evidence on the grounds that it is in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an

accredited certification-service-provider, or not created by a secure signature-creation device (ESD, Art.5 (2)). An advanced electronic signature is based on a *qualified certificate* and is created by a *secure signature creation device* (ESD, Art.2 (10)). In addition, in Art.3 (2), the EC Directive provides for the introduction of a voluntary accreditation scheme for certification-service-providers, here just mentioned for the sake of completeness.

Accreditation is based on an enhanced level of certification-service provision. If implemented in national law, certificates issued by these certification-service providers are most likely be used in the public sector, where additional requirements for the recognition of electronic signatures are permissible under Art.3 (7) ESD.

4.5.2 The Advanced Electronic Signature

An “advanced electronic signature” is an electronic signature meeting the following four requirements:

- uniquely linked to the signatory;
- capable of identifying the signatory;
- created using means that the signatory can maintain under his sole control; and
- linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Everybody will notice that these requirements are formulated in a very general and technology-neutral manner. In practice the market offers today only one solution that meets these four requirements: electronic signatures based on the digital signature technique or, in other words, making use of public key cryptography. In the framework of EESSI, a format for advanced electronic signatures has been described in the ETSI Technical Specification (TS 101 733). It is based on the existing standard format that dominates the e-mail and document security market (i.e. Internet specification RFC 2630). It also specifies how time-stamping or trusted archiving services may be used to ensure that the electronic signature remains valid for long periods so that it can later be presented as evidence in case of a dispute. The document defines how the Internet specification RFC 2630 cryptographic message syntax should be used for advanced electronic signatures and defines additional fields and procedures, which are compatible with this syntax, to support long term validity. The evidence provided through use of the ETSI format can prevent the signatory later attempting to deny (repudiating) having signed a document, and can be verified even after the validity of the supporting certificate expires.

A “signatory” is defined as “a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents”. The European Parliament suggested here to specify that a signatory could only be a “natural” person but this amendment was not integrated in the final text. The probable reason for this is that in some Member States, such as the United Kingdom, a document is not only considered to be “signed” if it contains a hand-written signature by a natural person but also when it bears a company’s seal, a stamp or simply a name, as long as the authentication is sufficiently clear. Following current technical standards, however, only a natural person can be the holder of a “qualified” digital certificate.

Contrary to the original draft the signatory is no longer “the person who creates an electronic signature”: it is the person who holds the signature-creation device. Such a device is defined in Art. 2.5 as: “configured software or hardware used to implement the signature-creation data”. A common example of a signature - creation device is a *smart card*, but there are many other possible devices such as a *smart pen* , a mobile phone, a PDA or a computer hard disk.

The signatory is the person who holds this device and who acts in order to generate a signature. The signature can be either on behalf of the signatory himself or on behalf of a natural or legal person or entity he represents.

Signature-creation data are “unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature”. The term “signature-creation data” consequently refers to the private key, whereas “signature-verification data” – defined as “data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature” – is used as a technology-neutral synonym for the public key. The software or hardware used to verify the public key is called “signature-verification device”.

Signature-creation devices and signature-verification devices are both part of the more general category of “electronic signature products”. These are defined in Art. 2.12 as “hardware or software, or relevant components thereof, which are intended to be used by a certification service provider for the provision of electronic signature services or are intended to be used for the creation or verification of electronic signatures”.

4.5.3 Secure signature-creation devices

According to Annex III to the Directive, secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

- the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
- the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
- the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

Annex III further requires that secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

These requirements for secure signature-creation devices ensure the functionality of advanced electronic signatures. They do not cover the entire system environment in which such devices operate. There are no formal requirements in the Directive regarding the signature creation process and environment. However, a CEN Workshop Agreement (CWA 14170) supports the objectives of the Directive by specifying “voluntary” security requirements for the signature creation systems that create advanced electronic signatures with the help of secure signature-creation devices and qualified certificates by means of

- a model of a “signature-creation environment” and a functional model of “signature-creation systems”,
- overall requirements that apply across all of the functions identified in the functional model, and
- security requirements for each of the functions identified in the signature-creation system, excluding the secure signature-creation device.

Two CEN Workshop Agreements (CWAs 14168 and 14169) define more specifically the security requirements for secure signature-creation devices. The security requirements are

formulated in a Protection Profile following the rules and formats specified in the international standard ISO 15408.

Article 3.4 of the Directive provides that appropriate public or private bodies designated by Member States shall determine the conformity of secure signature-creation-devices with the requirements laid down in Annex III. In a Decision of 6 November 2000 the Commission, pursuant to the procedure laid down in Article 9, established criteria for Member States to determine whether a body should be designated. 61 Article 2 of this Decision states that, “where a designated body is part of an organisation involved in activities other than conformance assessment of secure signature-creation-devices with the requirements laid down in Annex III to Directive 1999/93/EC it must be identifiable within that organisation” and that “different activities must be clearly distinguished”.

Following Art. 3 “the body and its staff must not engage in any activities that may conflict with their independence of judgement and integrity in relation to their task. In particular, the body must be independent of the parties involved. Therefore, the body, its executive officer and the staff responsible for carrying out the conformance assessment tasks must not be a designer, manufacturer, supplier or installer of secure signature-creation-devices, or a certification service provider issuing certificates to the public, nor the authorised representative of any of such parties. In addition, they must be financially independent and not become directly involved in the design, construction, marketing or maintenance of secure signature-creation-devices, nor represent the parties engaged in these activities. This does not preclude the possibility of exchange of technical information between the manufacturer and the designated body.

Article 4 of the Decision provides that the accreditation body and its personnel must be able to determine the conformity of secure signature-creation-devices with the requirements laid down in Annex III to Directive 1999/93/EC with a high degree of professional integrity, reliability and sufficient technical competence.

Following Article 5, the body has to be “transparent in its conformity assessment practices and shall record all relevant information concerning these practices. All interested parties must have access to the services of the body. The procedures under which the body operates must be administered in a non-discriminatory manner. Article 6 states that the body must have at its disposal the necessary staff and facilities to enable it to perform properly and swiftly the technical and administrative work associated with the task for which it has been designated. In Article 7, the Decision specifies that the personnel responsible for conformity assessment must have:

- sound technical and vocational training, particularly in the field of electronic signature technologies and the related IT security aspects, and
- satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate experience to carry out such assessments.

Article 8 of the Decision of 6 November 2000 states that the impartiality of staff shall be guaranteed. Their remuneration shall not depend on the number of conformity assessments carried out, or on the results of such conformity assessments. Following Article 9 the body must have adequate arrangements to cover liabilities arising from its activities, for example, by obtaining appropriate insurance. Article 10 provides that the body must have adequate arrangements to ensure the confidentiality of the information obtained in carrying out its tasks under Directive 1999/93/EC or any provision of national law giving effect thereto, except vis-à-vis the competent authorities of the designating Member State. Finally, following Article 11, where a designated body arranges for the carrying out of a part of the conformity assessments by another party, it must ensure and be able to demonstrate that this party is

competent to perform the service in question. The designated body must take full responsibility for the work carried out under those arrangements. The final decision remains with the designated body.

A determination of conformity with the requirements laid down in Annex III made by the bodies designated by a Member State has to be recognised by all other Member States. As far as the conformity of secure signature-creation devices is concerned, an accreditation in one Member State is, in other words, sufficient for the distribution of the device in all the other Member States.

4.5.4 Secure signature-verification devices

According to Article 3.6, Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer. Annex IV recommends that, during the signature-verification process, it should be ensured with reasonable certainty that:

- the data used for verifying the signature correspond to the data displayed to the verifier;
- the signature is reliably verified and the result of that verification is correctly displayed;
- the verifier can, as necessary, reliably establish the contents of the signed data;
- the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
- the result of verification and the signatory's identity are correctly displayed;
- the use of a pseudonym is clearly indicated; and
- any security-relevant changes can be detected.

In order to fulfil this goal, a CEN Workshop Agreement (CWA 14171) contains a specification for the signature verification procedure, including both the products used for verification, and their management.

The standard identifies the security requirements for the various elements of a signature verification system. Beyond the verification process itself, the standard identifies the various interfaces, i.e. Application Programme Interfaces (APIs) or Man-Machine Interfaces (MMIs) that are needed, in particular, to select the signer's document and the electronic signature to be verified, to present the signer's document with the right format, to get the signer information and the output status after signature verification, to get additional data for long term verification and to fetch information from various CSPs.

The CWA identifies the data that need to be captured and archived so that they can later be used for arbitration, should a dispute occur between the signer and verifier. The document uses the concept of a signature policy as the basis for verification of an electronic signature.

5. Analysis of the Needs and Requirements

This chapter is organised as follows :

- Analysis of common and specific requirements comprising :
 - Security
 - Authentication
 - Electronic signature
 - “What you see is what you sign”
 - Card or other portable support
 - Hardware and software
 - Device authentication
 - Interoperability
 - Smart Card Management Framework
 - Smart Card Management System
 - Other requirements
- Examples of requirements by business applications and services
- Overview of European E-Government applications
- Analysis of generic needs
- Analysis of the “Roaming Applications”

5.1 Analysis of Common and Specific Requirements

5.1.1 Security

The security requirements identified by the Embedded FINREAD initiative are as follows :

- Meet the requirements from major payment schemes
- Trustworthy and secure
- Physical protection of the device
- Protection of information
- Handling of confidential information
- Interaction with the user
- Transparent access
- Exclusive access to IC card reader resources
- Support of cryptographic functions
- Downloadable and certified software modules
- Authentication of an Embedded FINREAD device

5.1.2 Authentication

Authentication systems are composed at least one of the following elements :

- 1) What you have (Smart card or key, a private key stored on a smart card)
- 2) What you know (Password or PIN)
- 3) Who you are (biometrics, like fingerprint, iris scan or voice recognition)
- 4) How you do something (The way in which you sign your name)

Smart cards can now support items number 1 and 2. Biometric developments will eventually provide item number 3 by using a smart-card-stored biometric to unlock the smart card to gain authentication and application access, though reader infrastructure availability will be a limiting factor. Some biometrics may be built into mobile phones, like recognition of the voice patterns, of the iris or fingerprints or dynamic of physical signatures, turning the mobile phone into an authentication device. The fourth item will probably not be used by Smart Cards in the near future although the technology exists.

Identity (ID) infrastructures are based on directory, authentication, single sign-on, and management utilities are prerequisites for adaptive e-business.

IT infrastructure organisations have been deploying simple, rudimentary authentication services as part of an overall identity infrastructure since the early 1990s. The traditional approach used changeable passwords as the "secret" needed for access. Products and processes have evolved to define and manage passwords, from password synchronisation to Web single sign-on. Currently, more than 80% of authentication services are still simple password systems.

The renewed emphasis on secure infrastructure access and the evolving business demands of inter-enterprise commerce require more than simple authentication. Enterprises intent on improving secure access to applications and other IT resources are seeking stronger forms of authentication than mere user IDs and passwords.

Authentication of Identity is the most atomic, granular component of service offering i.e., verifying unique users. Without a definition of identity and authentication, complexity increases, identity management costs rise, security risks grow and deployment timelines for new public services and applications lengthen. For an authentication architecture to be effective, a definition of identity is required that meets at least **six major criteria**.

Criterion 1: Identity Must Be Unique. Enterprises historically have numerous credential stores for user authentication and authorization, supporting multiple applications. Each implementation has resulted in a different definition of identity, each specific to the services and application the stores serve.

Criterion 2: Identity Must Be Mobile. The proliferation of devices to access applications requires identity to be mobile i.e., identity must be associated with the user, not the device. For authentication, this association is now possible by distributing credentials through the mechanisms of smart cards, enabling the user to take the client portion of identity with him or her. Credential information for permissions (and authentication verification) is still stored centrally. As peer-to-peer networking evolves, identity mobility will evolve to support a more decentralized approach to authentication and authorization by leveraging the loose coupling of infrastructure services and the platforms supporting stateless session initiation.

Criterion 3: Identity Must Be Easy to Use. The history of applications (different platforms, different development environments, different methods of authentication and authorization, etc.) tends to paint identity definitions as complex. However, all applications have a basic set of requirements for authenticating user access and for permitting varying levels of access. Infrastructure developers must construct identity definitions to reflect minimum common requirements for all services and applications, and use a standard authentication infrastructure to deliver services to all applications.

Criterion 4: Identity Must Be Complete. Infrastructure developers must ensure identity definitions are comprehensive enough to accommodate future application requirements. Finding the balance is critical to success and requires careful analysis of the credential audit and requirements information as well as participation from application architects to move identity and permissions into commodity services standard across deployments.

Criterion 5: Identity Must Be Secure. No identity definition is complete without accommodating the move from weak to strong authentication and the protection of distributed identity. Public key infrastructure remains a driving force in the move to stronger authentication; other technologies (e.g., biometrics, smart-card combinations) continue to mature.

Criterion 6: Identity Must Be Managed. Once defined, identity definitions undergo continual updates as users, applications, and methods of access change and grow. Delegated administration has always been a key element of identity / authentication solutions, but with the existence of multiple credential stores with enterprises, single-point administration (SPA) has also become an important requirement.

5.1.3 Electronic signature

5.1.3.1 Concept and definition

Indeed the word “signature” is used to define :

- **A mechanism:** encryption using an asymmetric algorithm and a private key,
- **A function:** using the signature mechanism on data to prove the origin (the owner of the private key) of the data,
- **A service:** using the signature function on data that have a meaning for the owner of the private key. This is the traditional interpretation, which refers to the hand-written.

The main difference between the electronic signature function and an electronic signature service is the acknowledgement by the signer of the understanding of the data that are signed. Indeed for authentication purposes, unpredictable data, which are meaningless for the signer, are signed to prove the possession of the private key (as described in the next paragraph). The principle of the challenge is that the signer (end-user to be authenticated) is unable to forge one. Therefore, the challenge must be unique. The combination of a unique serial number plus a random number is the most common technical solution used to comply with the uniqueness of the challenge.

However for a signature service (which corresponds to the term signature in the paper world), the signer has to understand what he signs. Moreover multiple types of signature services can be identified (non exhaustive list):

- Signature for integrity and proof of origin purposes: the aim is only to prove that the data have not been modified and that they come from the signer,
- Signature for non repudiation of reception or proof of reading: the aim is to prove that the data have been received or have been read by the signer.
- Signature for commitment purposes: the aim is to prove that the signer accepts the meaning of the data and that it commits the signer.

A signature service involves items other than signature functions, such as the way data are displayed to the user, the What You See Is What You Sign concept, the needs for time-stamping, the signature verification process, etc.

5.1.3.2 Electronic signature application

Referring to the document entitled « Application Interface for Smart Card used as Secure Signature Creation Device », electronic signature applications require standardisation at three levels :

- User level : the quality of electronic signatures shall be acknowledged by the user
- Format level : the format for electronic signatures and their certificates shall be interoperable
- Device level : the device interface (physical, logical and application interface) shall be interoperable at least for the same device type.

The signature may be created at a different location by the user :

- Under provider control, in a public location (e.g. airport, hotel), with the use of a public signature terminal
- Under user control in an environment, mobile or location dependent, with the use of a home PC, office PC or mobile phone.

Within this process ESIGN application is selected. A signature application is identified by its Application Identifier (AID). The ISO 7816-4 defines the mechanisms of logical channel for the usage of signature application

A signature card may contain more than one authentication or signature key , the selection of appropriate key for each case is realised by the usage of the command `MANAGE SECURITY ENVIRONMENT`. This command could be applied to the following operations :

- Selection of user verification method (PIN, Password or biometric)
- Signature creation
- Verification of certificates.

5.1.4 « What you see is what you sign »

In this area, the requirements are the following:

- Ensuring a secure Man-Machine Interface:
 - Secure display
 - Secure keyboard (PIN protection)
 - Secure Smart Card Interface
- Implementing secure processor that manage interface
- Implementing secure time stamping
- Ensuring secure link to host
 - To check validity of certificate securely
 - To record all transaction data securely

5.1.5 Card or other « portable support »

The Smart card may be :

- with contacts
- Contactless
- In a Bluetooth Card Acceptance Device (CAD)

Other portable supports are given as examples :

- The revised of the ISO/IEC 7816-2 will allow to use the contacts N° 4 and 8 of a Smart Card as contacts of USB standard interface, in order to connect a PC via a passive connector, without the use of a Smart Card reader.
- The biometrics are considered as a market evolution, but this technology id not mentioned in the European Directive.

5.1.6 Requirements at hardware and software levels

The following requirements are considered :

- At hardware level :
 - Secure portable signature device (Smart Card or SIM)
 - Secure Man-Machine-Interface device (Terminal)
 - Secure revocation list management and secure storage
- At software level :
 - Specification of global platform/Small terminal interoperability platform (Stip)
 - Including terminal management requirement

It appears relevant to remind the works achieved by the Global Platform Forum, described in the report developed by the TB7 concerning « Multi-application Systems » .

Global Platform is an international, cross-industry forum, founded in September 1999 to focus on the development, management and promotion of specifications for multiple application smart cards, smart card applications, and enabling devices. With support from its global member organisations, which totalled 50 in March 2001, Global Platform promotes a standard framework facilitating the implementation of smart card programs in any industry

around the world. Global Platform allows flexibility in the choice of technologies and vendors through an emphasis on open standards for cards, terminals and support infrastructure.

The Open Platform card and terminal specifications developed by Visa are the first open standards adopted by Global Platform and will provide a solid foundation from which the organisation will define the future of multiple application smart cards.

5.1.7 Device Authentication

An Embedded FINREAD device is based on the architecture, infrastructure and the services of a hosting system (e.g. mobile device such as mobile phone, Web Pad, PDA, PPC, or Mobile Card Terminal, and stationary devices like set-top-boxes, PC and many more).

The Embedded FINREAD IC card reader offers the means to :

- Process an IC card
- Interface with the user
- Provide security functions to applications using it
- Provide network capabilities and/or local communication facilities.

Referring to the document entitled « Application Interface for Smart Card used as Secure Signature Creation Device », device authentication requires mandatory steps in order to provide a secure authentication. A device authentication is mutual and combines two mechanisms :

1. a device verifies the existence of a certified secret key on the other part
2. the devices negotiate or exchange information in order to establish common session keys for subsequent operation.

5.1.8 Interoperability

NAME could be implemented on **multi-function cards** issued by network operators based on international standards (EMV, WAP, UMTS,...), for secure access to **interoperable services** through open infrastructures **and standardised secure readers**.

As described in the Smart Card Charter, a common set of issued smart cards, sharing the same infrastructure and using a common identification system in shared applications will be indicated as a “**smart card community**”.

In the smart card community, the stakeholders of an e-Government or *business application*, including the frequent users, are the “**e-community**”. A smart card community consists of at least one ‘e-community’. Often more than one e-community is involved.

The goal and definition of interoperability between smart card communities is:

- To allow freedom to choose different or alternative cards, devices, OS and servers
- For more than one application or service in one domain and
- To enable the possibility to use the trusted identification (i.e. authentication)
- For an application residing on or accessible with a card issued in one domain for transactions on a device of another domain.

eEurope Smart Card Charter interoperability will typically allow citizen to use his/her card to access:

- e-Government, e-Business or other service of his own country (smart card community)
 - Via the (domestic) home infrastructure and
 - Via a foreign (host) infrastructure (for an illustration on how this interoperability works in principle,)
- e-Government, e-Business or other services of a foreign smart card community, accessed from:
 - A (foreign) host ‘environment’ (for an illustration on how this interoperability works in principle,)
 - The (domestic) home infrastructure.

A basic principle that will be applied is that interoperability has to be achieved using the least complex solutions as possible, whilst still complying with existing standards and market driven solutions.

Interoperability requirement for NAME and NAME.ES modules is evident. These modules could be implemented on **multi-function cards** issued by network operators based on international standards (EMV, WAP, UMTS,...), for secure access to **interoperable services** through open infrastructures **and standardised secure readers**.

5.1.9 Smart Card Management Framework

A Smart Card Management Framework (SCMF) is defined at conceptual level as a system constituted of a set of roles and corresponding entities which enable and make use of smart cards within a smart card information system.

The basic processes within a Smart Card Management Framework are executed by the following actors :

- *The card holder :e.g. user, consumer*
- *The card issuer : issues the smart card to card holders. While the card issuer holds the legal responsibility, most of its operational tasks are likely to be delegated or sub-contracted to specific entities such as a card manufacturer or the certificate provider.*
- *The certificate provider also known as CSP provides mainly IAS certificates and attributes related to the card holder*
- *The service provider ensure business services to the card holder using the smart card as an IAS token (e.g. an e-commerce company) and/or as a support for a specific on-card application (e.g. the health services)*
- *The SCC Administrator administers, monitors and supports 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.*
- *Access provider is in charge of managing the infrastructure (i.e. the card readers and necessary drivers, communication network and servers) to be used by the card holder accessing the offered services*
- *Content provider is in charge of keeping the content of the service provider up-to-date, in accordance with the content service requirements and agreements concerned.*

(Reference : GIF Part 1 V2.0 of June 2002).

The roles and responsibilities of each actor must be defined.

5.1.10 Smart Card Management System

The Smart card is not considered as an information system as such but one of the functional components of an information system. The smart card information system is made up of three architectural layers defined as follows :

1. The smart card layer
2. The infrastructure layer
3. The front-office application layer

5.1.10.1 The smart card layer

The smart card is an electronic trusted token with capabilities to securely store and operate IAS functions.

The smart card is an application server and acts as a server in a client-server relationship.

Within this context, the concepts of « off-card » and « on-card » are introduced :

- The « Off-card » application is defined as the software which resides in the infrastructure (terminal, front-and back-office servers).
- The « On Card » application is defined as the software which needs to be present on the card.

The level of security required varies for different applications or services, the security capabilities of the card are essential for interoperability between smart card communities. The IAS nucleus must be protected against unauthorised changes, and should be easily readable. The card must also support different read and write criteria, under the responsibility of the on-card applications issuer :

- No access restriction,
- After PIN/Biometric-verification (e.g. ensuring only the card holder can offer the access)
- Off-line protected by the terminal (e.g. after a card holder has duly identified himself to the terminal as having access to the data or the application)
- On-line protected by the host (e.g. for very critical data that may only be accessed by the issuer or the application provider) ;

5.1.10.2 The Infrastructure Layer

The infrastructure layer of a smart card information system includes all technical components required to enable and support communication between all other layers of the architecture.

5.1.10.3 The Front Office Application layer

The front office application layer of a smart card information system includes all off card components required to deliver a service to the card holder.

Services are provided to the card holder via two separate and different roles :

- The service provider who has identified the business needs, defines the business policy ,provides and manages the necessary means for accessing desired content

- The content provider who keeps the content of the service up-to-date or who interacts with the user.

Note that the business application component uses :

- The IAS functions
- The key infrastructure application
- The standards or protocols for using the human interface
- The standards to be used for the platforms
- The network standards.

The e-Government / e-Commerce applications and information systems could for instance include the following services :

- Secure e-mail services
- Access to generic and specific Government information
- Transaction like submitting forms, applying for permits, funds transfer and settlements.

(Source : GIF Part 1 V2.0 of June 2002).

5.1.11 Other requirements

The other major requirements are as follows :

- Ease of use (of services)
- Cost effective services
- Ability to trace and audit operations
- Security profile based on the critical level of operations
- Reliability of service
- End-to-End security
- Non- Repudiation of operations
- Willingness-to-Sign
- Speed of service (authentication in real time)

5.2 Examples of Requirements by Business Applications and Services

The following table sets up a non-exhaustive list of business applications and services by sector and proposes the relating security requirements.

Business Applications and Services	REQUIREMENTS		
	Authentication	Signature	Comments
Healthcare			
• Medical costs reimbursements	A		
• Medical records communication	A	S	For the sender and the receiver
• Tele-medicine	A	S	Including application to application
• Orders for medical acts	A	S	For sender and receiver
Pharmacy			
• Distribution of confidential documents	A	S	
• Sensitive transactions	A	S	Authentication or Signature
Administration / E-Government (A to C applications)			
• Tax declarations	A	S	
• e-voting	A	(S)	
• Providing Critical Information	A	S	
Transport			
• Ticketing	A	S	
B to B applications			
• Secure e-mail	A		
• Secure e-forms	A	S	A or A+S
• Secure ERP applications (back office)	A		
• E-Procurement	A		
E-banking			
• Clearing	A		
• On-line banking	A	S	
• Billing	A		
• Cash management	A		
• Fund transfer	A	S	
• Letters of credit	A	S	
• Critical documentation	A		
B to C applications			
• Home banking	A	S	



Business Applications and Services	REQUIREMENTS		
	Authentication	Signature	Comments
• Secure payment	A	S	A or A+S
• Billing	A		
• Secure e-mail (customer oriented)	A		
• Subscriptions to services for individual customers	A	S	
• Purchasing	A	(S)	

(A): Authentication service is required

(S): Signature service is required

5.3 Overview of European E-Government Applications and Services

An analysis of E-Government applications within Europe and Israel is provided in the document entitled « ESCP-EAP Report-SISGEM - Masters in European Business » (june 2002).

The objective of this report is to provide extensive study on the e-Government development in the European countries and Israel, according to the level reached in the implementation of e_government projects - Online Government.

This development called the e-democracy has led to the involvement of the population and has created the potential for the facilitation of the relationship between Citizens and the Administration (C to A) and the Business sectors and Administrations (B to A).

The following table presents the main e-Government projects realised or initialised within European countries and Israel (countries are « classified » according to the level of the implementation of e-Governments projects and programmes):

Country	Main e-Government projects	Use of Smart Card	Status (Operational, Pilot, Study)	Definition of Services
GERMANY	MediaKomm Arbeitsamt Online ATLAS ELSTER VAT			E-Voting Employment Office Customs Administration Secure data module Validity queries
IRELAND	e-Courts BASIS OASIS			Online Courts Services Business Access to State Information & Services Online Access to Services Information & Support
UNITED KINGDOM	E-Tendering & SmartCities UKONLINE DFEE Job Bank			Local services Job search by Web sites and Kiosk Sheffield Public DataWeb Job search by Websites and Kiosk
FRANCE	Health Professional Card Inter Administration services E-call tenders Tax teleprocessing Paris Trade Register Sesame-Vitale Tax teleprocessing Services organised by the Ministry of Education Titre Fondateur	Y Y Y	O O O O	A to A services = = B to A services = A to C services = = = =

Country	Main e-Government projects	Use of Smart Card	Status (Operational, Pilot, Study)	Definition of Services
FINLAND	Satakunta Electronic Identity card Public Services Portal Population Register Centre			B to C services C to A services = =
BELGIUM	Cybervote InterVAT Job search services Social Security contributions Public procurement			E-voting A to B services A to C services = =
SPAIN	Euro-Cities Submission of Data to Statistical Offices Income taxes Social Security contributions Public Libraries			A to A services = A to C services = B to C services
LUXEMBOURG	Legilux On Line Forms GEIDE On-line tax payment			Official jurisdiction documents (on-line) On-line administration forms Gestion Electronique d'Information et de Documents A to B services
SWEDEN	All Governmental Departments Online Online Customs			« An Information Society for All » All the traditional custom services and new services
PORTUGAL	Online Tax Office National Registry Online			A to B & A to C services =
ISRAEL	Government Information Gateway Pay Government Smart cards Merkava			B to A = Persona ID cards, driving licences, transport cards A to C services
NETHERLAND	The Municipal Tax of Office of The Hague Smart cards for global PKI services Government-Citizen Communication Digital Tax Department Programme			A to B services = A to C services =
AUSTRIA	Secure Electronic Signature & Info Boxes Social Security Card			B to A services A to C services
DENMARK	New Company Registration E-training Democracy on the Net On Line File Documentation Income Tax Online			A to B services At to A & At to B services A to C services = =

Country	Main e-Government projects	Use of Smart Card	Status (Operational, Pilot, Study)	Definition of Services
GREECE	Application for Building Permission Income Taxes Job Search Services Car Registration VAT			A to B services = A to C services = =
ITALY	Interchange Service Multi-service organisation Card and Electronic Identity Card Electronic Identity Card On Line Fiscal Services Income Tax On Line Payment Order via PKI ICI On Line Interactive Export Market			A to A services = A to C services = = = = = B to B services

5.4 Analysis of Generic Needs

NAME lists the following generic needs:

- Access to information
 - ➔ Public
 - ➔ Individual
 - ➔ Confidential

- Transactions
 - ➔ Low value
 - ➔ High value

This distinction is close to the model used by META Group:

- Publish (Access to information)
- Transact
- Collaborate

5.4.1 Publish

To the need for accessing information there is a corresponding publishing of information with its related authentication and authorisation requirements. The publish pattern is for read-only access to information/data. Although the publish patterns may support interactivity (submitting queries for processing), they do not support write activity (changing the state of stored data). This is the fundamental difference between the publish patterns and the transact patterns. At its most “generous” level, when the information is generally available to the public at large, there is little need for authentication. However, there is a strong need for *discrimination* where each users or customer is treated differently where a strong authentication scheme becomes critical. Many business models and customer relationship models dependent upon the capacity to discriminate between users in order to provide different levels or types of information to different individuals or classes of users. Corporations want to restrict access to information to confidential information.

Remote access via Web browsers will dominate in less than two years and increasingly wireless devices will be used to access sensitive data. Current authentication practices (user name/password) are not sufficient and more sophisticated mechanisms to manage user identity/authentication such as smart card based authentication will be needed.

- Public
- User classes
- Individual

5.4.2 Transact

The transact patterns are business cases requiring read/write access to data records. However, there are different transact patterns. They range from batch-processing applications or online transaction processing (OLTP) applications without logical abstraction between presentation, application, and data logic to 3/n-tier transact applications with a thin, presentation-logic-only client (or Web or other presentation server for n-tier) communicating with a client-neutral, server-based application logic, which in turn communicates with a back-end database server.

5.4.2.1 Financial Transactions

Financial services organisations and telecommunications companies are increasingly partnering to provide traditional banking services over mobile devices or broadband. These alliances will become much more strategic. The market will tend to split by transaction types, with telecommunications companies providing low-value cash or prepaid account transactions, and banks providing higher-value account, debit, and credit transactions.

Voice-call revenues continue to decrease, and telecommunications companies are relying on data services to generate new revenue opportunities. To do this effectively, a range of low-value transactions capability must be included with other content-based subscription services.

By 2006, micro-payment initiated via mobile devices will replace stored-value smart cards for many applications. These micro-transaction applications include parking, vending, ticketing, etc. Telecommunications companies will ultimately facilitate many of these micro-transactions by extending credit or providing prepaid options through existing phone billing systems. Stored-value cards will remain popular for transport and some telecommunications services, but a move toward account-based commerce will become more prevalent.

Consumers concerns over loss, misuse, or abuse of cards, are further supported by the desire of governments and financial institutions not to remove considerable cash reserves from the financial system in stored-value cards. European Commission directive 2000/46 will also enable non-banking institutions to take on account-style transactions without the need for a traditional banking license (expected to pass 2002).

Due to their inability to handle high-volume, low-value transactions and a lack of robust, scalable infrastructure to access end-user devices, banks and other financial services providers will let telecommunications companies assume this role. Banks will increasingly pursue transactions of higher risk or "managed accounts" (i.e., larger personal transactions -- wealth management or corporate purchasing), offering higher value-added services.

Similarly, two-part transactions where messages are separated at the point of contract of sale and rejoined through negotiation by independent "trust brokers" will form a major part of commerce services beyond 2008. This is necessary to minimise fraud and enhance the consumer's perception of trust in the medium.

5.4.2.2 Examples of banking and telecommunications companies relationship

Banking and telecommunications companies relationship are given as examples:

- Dutch bank Postbank formed an agreement with Dutch telecom company Telfort to provide a mobile banking and payment service to 500,000 users, currently using both SMS and WAP.
- Both Orange and Vodafone have registered banking descriptive domain names in preparation for the European Commission directive on electronic payments. This effectively opens up the banking market for non-traditional financial services providers by removing the need for banking licenses.
- Western Union Financial Services (subsidiary of First Data Corp.) signed a multiyear contract enabling customers of Verizon Wireless's prepaid wireless telephone services to reload cash values on their accounts through Western Union's SwiftPay service.
- Movilpago, a 50/50 joint venture between Telefonica Moviles of Spain and Banco Bilbao Vizcaya Argentaria, Spain's largest bank, planned to roll out a wireless payment solution with banks that will provide the necessary credit and payment functions, and telecommunications companies will provide the wireless access infrastructure.
- MobilCom launched a joint banking venture with German state bank Landesbank Baden-Wuerttemberg.
- KPN Telecom of the Netherlands and ABN Amro Bank announced they would collaborate on a wireless online venture called Money Planet, but the venture has now been withdrawn.
- Omnitel, an Italian mobile operator, launched a new financial services department and was co-operating with several Italian banks to deliver online banking applications, including Banca Intesa.
- Orange Communications and NatWest have already run trials of a wireless financial service in the UK. Competitors BT-Cellnet and Lloyd's have also engaged in developing mobile commerce applications.
- Germany's Mannesmann-Vodafone group planned to give customers a bank account with the same number as their mobile phone number.
- Deutsche Telekom has a joint financial service venture with Commerzbank to become, among other things, a "huge billing and transaction company serving a wide range of industries."
- Sweden's Telia and Swedbank are collaborating on a payment system for secure banking and e-commerce over mobile phones.
- Sprint PCS lists Harris Bank as its financial services portal on all of its new Web-enabled cellular phones. In return, the bank provides free financial information, as well as access to news, stock quotes, and weather to the cell phone users (previously provided by TD Waterhouse Group).
- NTT DoCoMo purchased equity in Japan Net Bank and provides access to Citibank services to consumers free of charge.

- The Carcenac report committed to the French government on 19/04/2001 (extract of chapter 1 / Middle term proposals): « The users of public services should be given access to an electronic signature with the Vitale 2 card. In order to do that, this card should be manufactured in conformance with the ISO-EMV (Europay-Mastercard-Visa) standard by using existing bases that can be found in the industry. This will put an end to the proprietary format that was chosen in the mid 90s and thus will enable applications interoperability, that is to say the use of the Vitale 2 card as a generic electronic signature medium. »
- Use of a smart card in Portugal for an e-citizen project: in order to facilitate the life of Portuguese taxpayers and reduce the management of paper, the Portuguese tax administration has decided to give Portuguese citizens access to a smart card that will enable them to pay their taxes in a simple way. In order to do that, the Portuguese inter-banking consortium SIBS (Sociedade Interbancaria De Serviços) has signed with BULL a first contract of 100.000 smart cards that will be distributed at first to Lisboa and Porto inhabitants. With this card, they will be able to pay their taxes with any bank automat as soon as they receive their tax notice next year. In Portugal, contrary to France, bank automats located on the corner of the streets have been true interactive terminals for years. One can use them to buy theatre places or train tickets for example.
- Contactless Smart Cards for urban transports in Valenciennes: About 6 000 users of urban transport have been equipped with a contactless smart card (that is to say a Smart Card that can be read without being introduced into a machine) by the company of urban transports in Valenciennes. Bull PTS developed this Smart Card. This innovation enables a multi-service usage. Soon, the entire population will be equipped (50 000 people).
- E-poll: European voting machine project : this project will develop an Internet based voting system that can be adapted throughout all of Europe. Led by Siemens Informatique, E-Poll counts amongst its associates the Aquitaine Region, the Italian police Department, the consulting company Sopra and Municipium, France Télécom R&D (the operator's research centre), Ancitel (computing subsidiary of the association of Italian city mayors), as well as the Polish organisation that is responsible for developing Internet in the Polish local communities. This project insists on the measures needed for authentication, notably by designing a Smart Card reader reinforced by a digital fingerprints reader. A limited number of next-generation voting offices will be tested as soon as 2002 by 8000 users with terminals that will be installed in hospitals and hospices of Arcachon and Méridnac.

5.4.2.3 Pay-TV / Pay-per-View

Today there is a mix of analogue and digital boxes. The current set top boxes are based upon proprietary standards. The digital set top boxes are expected to move to the upcoming Multimedia Home Platform (MHP) over the next two years. The MHP boxes will use smart card authentication. The business model is pay-TV.

MHP defines a generic interface, de-coupling different provider's applications from the specific hardware and software details of dissimilar MHP terminal implementations. It will enable digital content providers to address all types of terminals ranging from low-end to high-end set top boxes, integrated digital TV sets and multimedia PCs.

Moving to MHP will enable enhanced broadcasting with local interactivity, interactive services using a return channel and high-speed Internet access. The technology will enable a modified market model with competing companies in different market segments:

- Receiver and terminal manufacturers
- Infrastructure companies providing network and transport
- Services companies providing conditional access
- Broadcasters and web sites providing programmes and services
- Application & content producers and distributors

The telecommunication companies are looking for new services to increase annual revenues per subscriber. New services like games and gambling will provide new services but also new challenges. Transactions will involve partners and companies with which the telcos has worked little with so far. The billing engine will have to handle more complex transactions. The Pay Per View will require the additional functionality of the modern set top boxes and the tracking by the billing engine.

5.4.3 Collaborate

The business case for the collaborate patterns is person-to-person communication, usually centred on shared documents or groups of documents. Although both this and the transact patterns enable read/write access to information, the transact patterns are designed to handle shared read/write access to records, whereas collaborate patterns are designed around shared read/write access to documents. We can distinguish between real-time collaborate, store and forward collaborate and structured collaborate patterns. Structured collaborate (a.k.a. "workflow" or "document management") implements automated co-ordination of changes (version control, check-in/check-out, data validation) that the store-and-forward collaborate pattern lacks. Trust relationships required for collaborative patterns will be contingent upon strong authentication capabilities.

There is a trend is toward increased use of collaboration tools, which are often run on top of a core messaging infrastructure e.g., instant messaging, data conferencing, team ware, custom-built applications. Also defined business processes between partners, employees, customers, and suppliers will lead to a new generation of collaborative solutions to optimise their interrelationships. Application architectures will integrate operational, analytical, and collaborative customer relationship; enterprise marketing automation applications and call centres will converge into unified customer interaction frameworks. Business intelligence will merge into operational business processes through the introduction of new and expanded analytical application solutions that converge operational, analytical, and collaborative capabilities. These solutions will help optimise and measure business processes and will be mapped into individual jobs and functions. Portals are becoming the primary mechanism for delivering these solutions.

5.5 Analysis of the « Roaming Applications »

Recent developments in mobile computing and Web-based roaming applications have proven that we are now living in a “multi-channel world”. Leveraging one channel's resources (e.g., code, graphics, intellectual property, content, employees, infrastructure services) to enhance other channels will offer more flexibility and consistency at the point of interaction. Roaming applications need to address a n-channel architecture and address the needs of multi-channel and multiple point-of-interaction systems. Channels should not be assumed to be static.

Organisations should view the demands of roaming applications as part of a pattern of expanding channels, and respond with an adaptive, n-channel architectural process that encourages reuse and consistency among channels. The need in customer interaction management to handle multiple points of interaction consistently is an example of a roaming application architectural process.

The movement from n-tier to n-channel architectures is driven by the need to increase manageability and scalability across customer channels and across devices. The business issues around channel integration are:

- Consistency
- Responsiveness (ability to react to the need for new channels or changes to existing channels)
- Efficiency/leverage
- Simplicity
- Management

IT challenges around channel integration are:

- Reuse of data and content
- How to architect for unified management (deployment, tracking, error flagging)
- Exploiting intra-channel synergies (between channels in a channel set; i.e., are visual themes in a TV promotion followed through in the in-store displays)
- Exploiting inter-channel synergies (between channel sets; how customer feedback is consolidated across customer service, sales, and marketing channel sets)

Emerging principles of n-tier architecture include:

- Separating business logic into generic and channel-specific
- Determining a hierarchy of channels that can share components
- Designing the presentation layer last
- Designing for the ability to adapt to new channels

Within this report, a first characterisation of the main class of user terminals “able” to access “easily” to different categories of application will be provided. Please see some examples in the paragraph 8.1.

6. Business Model Analysis

The Embedded FINREAD Consortium proposes the following **classification for Smart Card accepting devices** covered by this standard:

- **Private devices** as a definition for devices used in the private environment such as IC card readers connected to a PC, set-top boxes, etc.
- **Personal devices** as a definition for devices that are mobile, but used under the control of an individual, such as mobile phones, PDAs, etc. Compared with devices used in the private environment, the user of a mobile device is already aware of the risk of loss and theft of his device.

We add to this classification **Public devices** including public phones, cyber-café, public internet devices (in the public administration offices, airports, etc).

Note that, for the B to A and C to A transactions it is necessary :

- To characterise relative certificates in accordance with the security required by the applications
- To ensure an appropriate key management.

Indeed, as detailed within the GIF Part 1 document, **an open framework** is required : full standardisation of complete trusted e-services and products in a market with many types of suppliers and different national histories is not feasible and is not required. Any standardisation must allow sufficient flexibility so as not to impede developments in smart cards technology and infrastructure.

A minimal architectural nucleus for e-Ids within a general common conceptual framework can provide the required answer for pan-European and wider needs of the following stakeholders for the foreseeable future:

- Smart card users
- Significant issuers of Smart cards and Smart card services
- Card management suppliers
- Providers of public and private key infrastructure schemes
- Application and service suppliers that are or will be connected in session using the common interoperable e-ID Smart card token
- Suppliers of Smart cards, system components and infrastructures.

The present chapter is organised as follows :

- Approach for business case analysis
- Business model proposed
- Targeted value chain
- Value proposition in the market segment
- Branding
- Value transfer model - Pricing model
- Competition

6.1 Approach for Business Case Analysis

The Approach For business case for a Common Authentication and Electronic Signature using Smart Cards is described hereafter.

Four types of markets will co-exist: Intra-Enterprise, Business to Consumers, Business to Business and Business to Administration (Government).

In enterprises during 2002, the use of smart cards as strong authentication mechanisms will gain momentum during pilots and limited enterprise deployments, expanding gradually during 2003/04 as card reader infrastructure becomes widely available for PCs and other points of interaction. Robust card management services will lag deployments, providing crude functionality during 2002/03 before improving significantly in 2004. Numerous smart card and biometric combinations will be attempted during development, with fingerprint and iris scanning biometrics dominating after 2004.

While public key infrastructure services will enjoy a revival due to smart card use on the Internet (2002-04), B2B spaces and symmetric key cryptographic services (e.g., Kerberos) delivered via smart cards will account for more than 80% of enterprise smart card use, primarily as a result of network operating system (NOS)-based symmetric key authentication availability.

6.1.1 Process to develop a business case

The process to develop a business case for authentication and electronic signature solutions rests on a proven approach. It starts with an extended value chain analysis consisting of the following steps:

1. **Value Chain Model:** Scope and scale of the value-adding activities forming the extended value chain that addresses the future needs (perceived value) of target customers. The value chain model includes:
 - 1.1. Business and technology trends.
 - 1.2. Analysis of existing value chains.
 - 1.3. Value chain scenarios depicting opportunities for planning, designing, building and maintaining new value chains.
2. **Target Value Chain:** Decision about targeted value chain scenario(s). Another expression for targeted value chain is *market segment*. The analysis focuses on the company's position in the value chain linking suppliers and customers and includes:
 - 2.1. Value contribution of suppliers / partners and distributors and their evolution.
 - 2.2. Supply chain and supplier relationship management
 - 2.3. Planned value delivery capabilities of the company.
 - 2.4. Stake-holder's interest and expectations.
 - 2.5. Value segmentations mapping customer requirements against planned capabilities.

- 2.6. Risks associated with target value chain
3. **Value Proposition:** Value provided by the company, including product, price, distribution, support and product life-cycle management. The value proposition is usually expressed through a brand.
4. **Brand Management:** The brand represents decisions about how the enterprise will communicate its value proposition, how to project, defend, and evolve its relationships with key stakeholders, including customers, suppliers, employees, and strategic partners.
5. **Value Transfer Model:** Billing and invoicing happen according to different dimensions, like time (subscription) or per transaction / service.
6. **Competitive Positioning:** Describes which other companies are addressing the same market with an equivalent value proposition and the market entry barriers. The decisions about competitive positioning must include core competencies analysis. Most enterprises should avoid fixing all that is broken and concentrate of a few capabilities that will help it fend off competitors. Concentrate on strengths rather than correcting every weakness and anticipate competitors' move to build capacity in advance of events is more important than sheer excellence.

The **business model** of a given company is composed of the targeted value chain, value proposition and brand management and the value transfer model.

6.1.2 Building a business model

The **business model** of a given company is composed of the targeted value chain, value proposition and brand management and the value transfer model.

The following value chain and market segments evolutions are evident:

From static to mobile

From weak to strong

From moderate to large volumes

From intra-enterprise to inter-enterprise

From person to application

From medium to larger threats

As organisations pursue high-value business-to-business (B2B) interactions via the Internet, security requirements are increasingly stringent. Beyond basic authentication and privacy requirements, businesses must also ensure transaction integrity and support non-repudiation services.

Although we agree these additional security concerns need to be addressed, organisations must be cautious to ensure the PKI implemented can be used by all applications that require it for example secure e-mail, middleware messaging, not just B2B applications.

6.2 Business Model Proposed

In the most basic senses, a business model is the method of doing business by which a company can sustain itself – that is generate revenue. The business model spells out how a company makes money by specifying where it is positioned in the value chain.

6.2.1 Value Chain Analysis: A federated trust model for authentication

6.2.1.1 Convergence of private and public¹ services is driving the federated model of authentication.

The rapid development of multi-enterprise or cross-government integration for business-to-business, business-to-consumer, business to government transactions and collaboration and a move to a Web services model for applications will drive increasing utilisation within enterprises of Internet authentication solutions. This evolution appears evident as organisations prepare to redefine the concept of the network boundary.

The term “**Web services**” is often used to refer to the collection of technologies that together comprise a means of remotely invoking a function using standard, Internet-based protocols. A more comprehensive definition is that it is a self-describing service that can autonomously perform a complex business function, available through standards-based, Internet-based, interaction technologies. The technologies are: SOAP – Simple Object Access Protocol, UDDI – Universal Description, Discovery and Integration and WSDL – Web Services Description Language.

Web Services Security specification describes how to add encryption and digital signatures to Web services and it also defines a general mechanism for passing around arbitrary security tokens, though it doesn't define how those tokens work. Secure Assertions Mark-up Language – SAML, defines a standard, XML-based approach for passing security tokens defining authentication and authorisation rights. Web Services Security defines how you insert information into a SOAP envelope; SAML defines what the security information is. SAML uses Web Services Security as the appropriate method for "binding" SAML assertions into SOAP messages. Web Services Security is the messaging language and SAML the security language.

Companies will increasingly outsource some of their authenticating services, public and extranet exchanges will morph into trust consortia with their owned trust domains. Concurrently, public services will have to interoperate with the authentication services of the large enterprises. **This will result in a federated authentication model.**

The centralised model, at times envisaged by the telecom companies, has already been tested and has failed. The notion that one authentication service can provide this service on behalf of other companies was part of Microsoft.Net Passport, which is a simple, proprietary identification, authentication and authorisation service in .Net strategy. Passport was based on the notion of Microsoft hosting the world's authentication services.

¹ The word “Public” is used in the sense of being available to the public in large. There is no distinction here of whether the services are offered by organisations that are owned by the governments or not.

This approach will not work. Companies mostly have not succeeded in having one single electronic identity for their employees, let alone their partners and customers. In addition, there is a certain level of mistrust in the industry and in the consumer market about sharing personally identifiable information with any entity. There is not much of an agreement on what level of authentication is required. **Internet services will work through a federated trust network with multiple identity brokers.**

Authentication services need to be hosted by companies internally behind firewalls or to be delivered by trusted consortia that then federate. The federated model also reinforces the brand experience and relationship that companies already have with their customers.

Companies will want to control their own identity and authentication management system. Microsoft has also announced a future federation model, possibly Kerberos-based, that will enable and interact with other types of identity brokers.

There are intense efforts by consortiums of enterprise users, vendors, and standards bodies to publish frameworks and guidelines for new authentication approaches. Stronger authentication (e.g., tokens, smart cards, biometrics) is receiving renewed and broad-based attention by security vendors.

The vendors experiment with combinations of products, systems, and services, all in an attempt **to achieve acceptable price points for enterprise needs.** Standards efforts gathered steam in earnest in 2002. Microsoft's .Net Passport, the Sun-inspired Liberty Alliance, and AOL's Magic Carpet all represent efforts to create a standard identity infrastructure for consumer-based authentication, enabling applications access across multiple enterprises.

Some examples of these efforts are given as follows :

- The Liberty Alliance work is theoretically complementary, rather than competitive, to Microsoft's Passport, the technology being developed is a set of APIs that will be used by authentication systems to exchange information. Passport could be one of those authentication systems.
- The Liberty Alliance, the Secure Assertions Mark-up Language and Web Services Security) are currently battling for vendor adoption. Production-capable solutions for most enterprises will not be appearing before 2005
- OASIS (Organisation for the Advancement of Structured Information Standards) is in charge the Web Services Security and SAML specifications. Web Services Security aims to specify how to secure Web services, including encryption and access control in a platform-independent manner. Most simply, Web Services Security defines a set of Simple Object Access Protocol (SOAP) headers that can be used to implement security measures for Web services, and as such, Web Services Security is an extension to the SOAP envelope header. SOAP is in one way the new lingua franca of the Web and soon SOAP stacks will be as prevalent and standard as TCP/IP stacks are today.
- In October 2002 OASIS formed a Digital Signature Services Technical Committee to develop open XML protocols for digital signature and cryptographic time-stamping services operating in a Web services context.

Another trend is the convergence of mobile and wireless data networks that will affect the market for products and services requiring authentication. Cellular carriers will provide

wireless LAN access services next years, with seamless roaming by 2003/04. A majority of larger corporations will deploy applications to “occasionally connected” users.

Some standards organisation involved in the development of web services and related protocols are :

	www.oasis-open.org
	www.ebxml.com
	www.w3.org
	www.omg.org
	www.rosettanet.org
	www.ietf.org

6.2.1.2 Developments Inside the Enterprise

Enterprises continue to develop and deploy a common infrastructure layer to handle authentication service needs for new applications. These efforts centre on either network operating system (NOS) environments (e.g., Novell NetWare, Microsoft Windows 2000, Windows XP) or an applications-focused Lightweight Directory Access Protocol (LDAP)-capable directory coupled with some form of Web-centric single-sign-on engine. The trend to use browser-based clients in application architectures is enabling enterprise architects to choose between NOS-based or standalone directories and **allow a more flexible authentication model** untied to a particular network operating system.

In contrast, Microsoft Windows 2000 and .Net authentication services remain tied exclusively to use with Microsoft Active Directory (i.e., Windows 2000 authentication services will not work directly with another LDAP directory).

The infrastructure costs for stronger authentication methods (e.g., smart cards, biometrics) remain problematic for average enterprises in spite of intense, renewed interest; nevertheless, they are increasingly found in limited niche instances in high-profile, high-revenue environments where strong authentication methods are critical to business.

6.2.1.3 Developments Between Enterprises

The bulk of recent standards activities have centred on e-business needs for broader and standard authentication services.

The following efforts are deployed :

- The Liberty Alliance, a consortium of both vendors and major customers such as American Express and MasterCard, has completed initial specifications for delivering a federated (i.e., distributed and independent) identity model for authentication services, primarily for business-to-business and consumer e-commerce. This effort is a direct counter to Microsoft's existing Passport services.
- The Liberty Alliance has adopted SAML as an authentication exchange mechanism; other mechanisms may also be supported. Ratification by the standards bodies of Version 1 is due in November 2002, even though several vendors have pre-ratified compliance products available before that time. SAML vendor adoption and implementations will continue to lag as vendors bicker over interpretations however.

SAML is a more tactical specification, used to enable disparate Web single-sign-on products residing in the same or different enterprises to exchange authentication and some authorisation information

6.2.2 Trust Domains

A trust domain is an organisational concept allowing to define a security level used as a reference by application and service providers reflected in access devices. It sets expectations and trust levels that can easily be implemented and communicated by adhering and participating partners.

Different security and trust levels will enable different costs structures and business models to coexist. Different levels of security, organised in a federated model for authentication enables organisations to retain fine-grained and secure control over user identities, profiles, and other business data while participating in a trusted network that delivers a unified experience to users. The trust network is built on a common set of technical and operational guidelines and is open to any organisation supporting those standards.

Typically, a hierarchy of three levels is suitable, with each higher level assuming the security level below as a starting security level.

In the framework of a trust domain definition, the example of Citizen Electronic Card is relevant.

6.2.3 Challenges

Authentication standards developments are a necessary condition to prepare for Web services. But applications to be deployed in 2002/early 2003 and requiring authentication services will continue to rely on :

- optimising existing environments
- the establishment of a common identity infrastructure
- a strong password management,
- token-based stronger authentication for selected groups
- proprietary extensions to existing Web single-sign-on products.

Planning and implementing an infrastructure layer to deliver identity authentication services is the first step to preparing for the evolution of applications to widely accessible multi-enterprise services. **IT organisations should develop an identity service that accommodates federated sources of identity** through standardisation of infrastructure and a trust model for security that adequately reflects capability and risk.

The main constraint of this scheme is penetration. Solution providers will request authentication when such a service is widely available and an authentication solution will be widely available when widely requested, providing access to additional services, not available without an authentication solutions.

It is supposed that the technical constraint is largely a non-issue. Profiles or packages of technology specifications and standards are available. The business case for useful applications has been repeatedly demonstrated. The main issue is that the sum of the parts is bigger than the costs of a widespread implementation but that no player controls a single business case that would justify a widespread implementation by itself.

It is classical case of requiring either a large industry coalition or a governmental incentive to create the initial critical mass.

6.2.4 Evaluation of Identified Risks

There are multiple types of risk and many of them are related. There is the risk:

- For terminal manufacturers not achieving a return of investment, either because of volume and penetration or because of lower revenues per terminal.
- Of insufficient interoperability between authentication solutions.
- Of privacy issues with related consumer backlash.
- Of change in governmental regulations.
- Of change in technology evolutions.
- Of acceptance by solutions providers.

All of them are low individually; taken together they are high and form a threshold. However, the benefits are high as well. The main issue may be that nobody will make money on authentication as such; the value of authentication is one of an enabling technology.

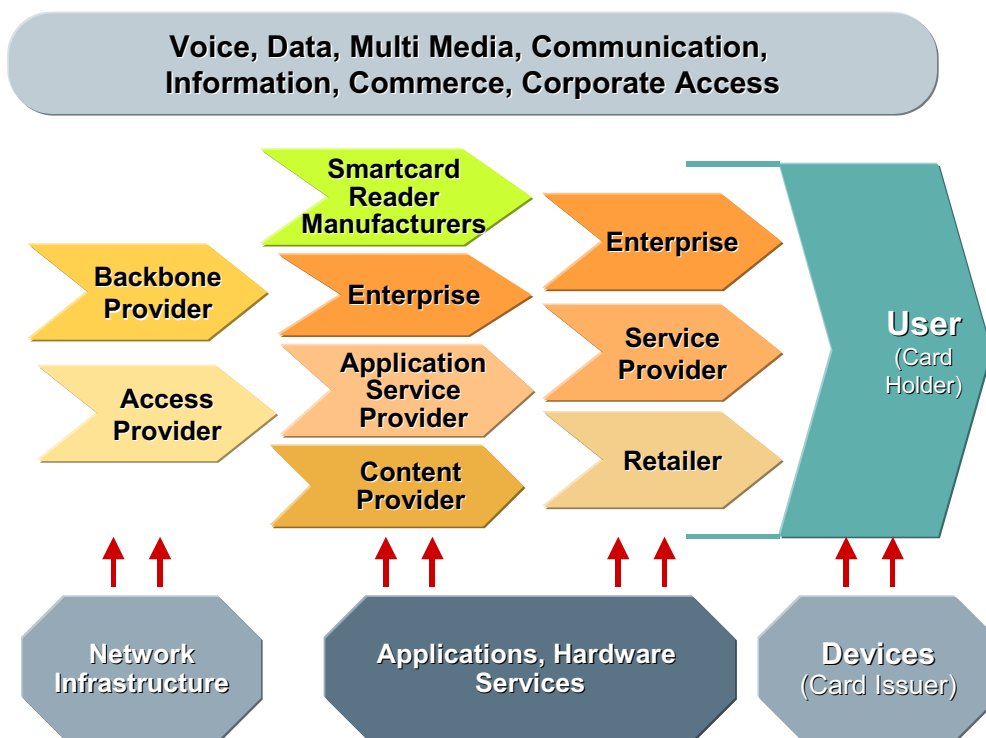
It is important to invest in enabling technologies, having the position to reap the rewards of investment that is not be justified on its own. **It may be that a governmental initiative may be required to kick-start the virtuous circle** (the virtuous cycle of infrastructure, application and content providers).

6.3 Targeted Value Chain

All business plans have to start with an understanding of the value chain.

In the preceding we have described the fundamentals and the evolution of the value chain in which Smart-cards are used. We have described how the enterprise and public services will increasingly merge with enterprise identity and authentication management services.

The result in terms of value chain can be briefly depicted below. Each value proposition will involve one or more of the players in this value chain and will depend upon the smooth operation of the whole value chain.



We have also have the various standards and standards bodies that defined both interfaces in terms of format and protocols as well as the semantics involved in the exchanges and transactions. These standards have been defined for some of the elements but many elements are missing when the full value chain is taken into account.

6.4 Value Proposition in the Market Segments

The value proposition is the product or service that each player in the value chain proposes and that may or may not be accepted according to the perceived value of the user or consumer.

Traditional ways of authenticating user identity to access IT systems and services are undergoing fundamental reassessment in light of current developments in applications design and use. This necessity becomes clear as enterprises and application providers:

- Enter the mainstream use of Web-centric applications for multi-enterprise use;
- Develop and deploy initial Web services;
- Struggle with integrating multiple “islands of authentication” within many enterprises;
- Provide adequate authentication capability for wireless networks; and
- Apply better security approaches for overall access.

The emergence of new enterprise and inter-enterprise applications based upon the emerging Web services, including directory integration will be one significant value contribution of smart card – based authentication services together with the better known telecom and banking related consumer services.

The combination of the value chain and value proposition can be further analysed according to other segmentation criteria. **The important contribution of the smart card – based authentication is the improved knowledge and control over the targeted segment.**

Since each user is identified, very accurate information about the actions and behaviour can be collected, within the limits of the legislation. Up to now, this opportunity has been available mainly to credit cards consortia.

The following market segments have been identified:

1. Enterprise Identity and Authentication Management
 - 1.1 Information and Data Access
 - 1.2 Application Access
 - 1.3 Facility management
2. B to B applications
 - 2.1 Secure e-mail
 - 2.2 Secure e-forms
 - 2.3 Secure ERP applications (back office)
 - 2.4 E-Procurement

3. E-Banking
 - 3.1. Clearing
 - 3.2. On-line banking
 - 3.3. Billing
 - 3.4. Cash management
 - 3.5. Fund transfer
 - 3.6. Letters of credit
 - 3.7. Critical documentation
4. B to C applications
 - 4.1. Home banking
 - 4.2. Secure payment
 - 4.3. Purchasing (gambling and “life-style services” being the most promising)
 - 4.4. Billing
 - 4.5. Secure e-mail
 - 4.6. Subscriptions to services for individual customers
5. Healthcare
 - 5.1. Medical costs reimbursements
 - 5.2. Medical records communication
 - 5.3. Tele-medicine
 - 5.4. Orders for medical acts
6. Pharmacy
 - 6.1. Distribution of confidential documents
 - 6.2. Sensitive transactions
7. Administration, E-Government (A to C)
 - 7.1. Tax declarations
 - 7.2. E-voting
 - 7.3. Providing Critical Information

-
8. Administration, E-Government (A to B)
 - 8.1. Tax declarations
 - 8.2. Tax payment
 - 8.3. Providing Critical Information
 - 8.4. New company registration

For the Smart-card readers manufacturers, the temptation of the big bang should be resisted. The “big bank business model” assumes there is one “killer application” that is sufficient to recuperate the infrastructure costs.

This scheme creates the virtuous cycle of infrastructure, application and content providers investing in the standards and its implementation. With no killer application, the introduction should happen through a series of projects and initiatives, sequentially with some overlap.

It appears commonly admitted that there is a government-driven initiative capable to create the “big bang” market. The emergence of E-Government applications and services in European countries represents a real opportunity to be taken into account by Smart-card readers manufacturers.

6.5 Branding

The potential for improved branding related to authentication is immense. This is also linked to the emergence of the federated model for authentication. Companies are willing to invest in product and service bundles under various brands when they have better control concerning the target value chain or segment. Companies typically pay consumer today to obtain this knowledge. With authentication they can extract (privacy laws permitting) the information from the network and this may justify the technology costs in many cases.

6.6 Value Transfer Model / Pricing Model

The pricing dimensions, the granularity and the cost of dynamically altering the pricing and billing model is a significant contributor to the bottom line of the enterprise or service provider.

Whether the product and services can be billed on a per transaction basis, monthly or usage basis, value related or a combination of those will determine the final value of the value proposition that the companies will receive. **The possibility to change chose pricing parameters quickly and at low costs is a major business driver.**

The smart cards based authentication can contribute at several steps of the value chain to improve the pricing model. First and foremost, the employee or consumer can be managed as individuals and their actions and decisions can be tracked (again legislation permitting). The cost of a transaction can be reduced. Last but not least, the increased security will enable better performing infrastructure solutions. The increased complexity at then authentication level will enable reduced complexity at the application level.

6.7 Competition

The competitive analysis is linked to the value proposition and brand of each player in the value chain and it is probable that authentication will not alter the competitive environment.

7. Recommendations

The recommend step is to develop a business model and a related business case for each value proposition. It would seem there is no single “killer” application and in consequence, the business model needs to be precise and possibly to be tested to fine-tune the product and service value proposition before a widespread implementation. The return of investment will have to be calculated on a per-project basis. Synergies do exist but are hard to prove.

Government-driven initiatives are able to create the “big bang” market on the basis of authentication and electronic signature services. **The emergence of E-Government applications and services** in European countries represents a real opportunity allowing the development of Smart-card industries.

In the absence of an industry consortia or a governmental initiative the establishment of an authentication and/or signature solution should be handled as an infrastructure investment. For that reason, companies that can bundle initiatives around a single implementation have a higher probability of an acceptable return. Typical infrastructure industries like telecom will therefore be the most likely candidates and beneficiaries of such initiatives.²

Business initiatives should be focused around segments where it is feasible to set up projects that controls and can implement the whole value chain.

For **Authentication**, it seems that this will be the case for the following market segments, in order of priority.

1. Enterprise Identity and Authentication Management
 - Information and Data Access
 - Application Access
 - Facility management
2. B to B applications
 - Secure e-mail
 - Secure e-forms
 - Secure ERP applications (back office)
 - E-Procurement
3. B to C applications
 - Secure payment
 - Purchasing (gambling and “life-style services” being the most promising)
 - Billing
 - Secure e-mail

² The framework for “Framework for IAS with Smart Cards” – IAS stands for Identification, Authentication and electronic Signature, addresses the need to provide high-end e-communities with the necessary specifications in order to provide high-end e-communities the necessary specifications in order to prepare their information systems for interoperating with another high-end e-community, both in terms of rules and standards and operations [Ref GIF4-3.doc]

4. E-Banking
 - Clearing
 - On-line banking
 - Billing
 - Cash management
 - Critical documentation
5. Healthcare
 - Medical costs reimbursements

For **Electronic Signature**, it seems that this will be the case for the following market segments, in order of priority.

1. Administration, E-Government (A to C)
 - Tax declarations
 - Providing Critical Information
2. Administration, E-Government (A to B)
 - Tax declarations
 - Tax payment
 - Providing Critical Information
 - New company registration
3. E-Banking
 - On-line banking
 - Fund transfer
 - Letters of credit
4. B to C applications (Value packages should be created for maximum traction and volume, the infrastructure costs being more important than readers / card costs)
 - Home banking (Linked to purchasing, if not the additional value is less clear)
 - Secure payment
 - Purchasing (gambling and “life-style services” being the most promising)
 - Billing
 - Secure e-mail
 - Subscriptions to services for individual customers
5. Healthcare (Value packages should be created for maximum traction and volume, the infrastructure costs being more important than readers / card costs)
 - Medical costs reimbursements
 - Medical records communication
 - Tele-medicine
 - Orders for medical acts

For **Interoperability**, It seems important to analyse this requirement at different levels of the connections in the following scheme : CHIP → SMARTCARD READER → SERVER.

8. Annexes

8.1 Characterisation of user terminals:

The following table will characterise the type of terminals able to connect in the secure way the users with the different types of application.

:

SERVICES	Requirements A: Authentication S: Signature	Type of Terminal - Mobile Phone - PDAs - PC - Set-top-box - Other	Main hardware and software requirements
Healthcare			
• Medical costs reimbursements	A		
• Medical records communication	A S		
• Tele-medicine	A S		
• Orders for medical acts	A S		
Pharmacy			
• Distribution of confidential documents	A S		
• Sensitive transactions	A S		
Administration E-Government (A to C)			
• Tax declarations	A S		
• e-voting	A		
• Providing Critical Information	A S		
B to B applications			
• Secure e-mail	A		
• Secure e-forms	A or A+S		
• Secure ERP applications (back office)	A		
E-Banking			
• Clearing	A		
• On-line banking	A S		
• Billing	A		
• Cash management	A		
• Fund transfer	A S		
• Letters of credit	A S		

BUSINESS APPLICATIONS & SERVICES	Requirements A: Authentication S: Signature	Type of Terminal - Mobile Phone - PDAs - PC - Set-top-box - Other	Main hardware and software requirements
• Critical documentation	A		
B to C applications			
• Home banking	A S		
• Secure payment	A or A+S		
• Billing	A		
• Secure e-mail	A		
• Subscriptions to services for individual customers	A S		
• Purchasing	A		

The following chart will present the requirements of terminals in terms of deployment and user administration.

SERVICES	Requirements A: Authentication S: Signature	Type of Terminal - Mobile Phone - PDAs - PC - Set-top-box - Other	Requirements relating User Administration
• Medical costs reimbursements	A		
• Medical records communication	A S		
• Tele-medicine	A S		
• Orders for medical acts	A S		
Pharmacy			
• Distribution of confidential documents	A S	PC	
• Sensitive transactions	A S		
Administration E-Government (A to C)			
• Tax declarations	A S		
• e-voting	A		
• Providing Critical Information	A S		
B to B applications			
• Secure e-mail	A	PC, Mobile Phone	

BUSINESS APPLICATIONS & SERVICES	Requirements	Type of Terminal	Requirements relating User Administration
	A: Authentication S: Signature	- Mobile Phone - PDAs - PC - Set-top-box - Other	
• Secure e-forms	A or A+S		
• Secure ERP applications (back office)	A	PC	
E-banking			
• Clearing	A		
• On-line banking	A S		
• Billing	A		
• Cash management	A		
• Fund transfer	A S		
• Letters of credit	A S		
• Critical documentation	A		
B to C applications			
• Home banking	A S		
• Secure payment	A or A+S		
• Billing	A		
• Secure e-mail	A	PC, Mobile Phone	
• Subscriptions to services for individual customers	A S		
• Purchasing	A		

8.2 Authentication Services Issues: Biometrics

Enterprises intent on providing stronger security for access to critical services are evaluating biometric technologies (i.e., the use of an individual's unique physical or behavioral characteristics to recognize or authenticate identity). Although biometrics have been used for more than 10 years in such areas as premises access and criminology, using biometrics to provide strong authentication for application access has been limited, due to inadequate technology and high costs. Although technology and costs have improved and products have now appeared, biometric solutions still suffer from technology and market immaturity and require prerequisite technologies to be ultimately successful in its envisioned role. Biometrics must be able to work with distributed services to establish access applications access.

During 2001-03, biometric-based technologies will be piloted and implemented in increasing numbers (spending on such devices will triple, from \$300M in 2001 to \$900M in 2003) to address specific, targeted areas of business and government, finding niche acceptance in

single-application or appliance-protection roles. Widespread adoption of biometrics for strong enterprise authentication will not occur before native Public Key Infrastructure (PKI) application support matures in 2003/04, particularly for e-business needs. Breakthroughs in technology and affordable prices by 2006 (less than one-third current pricing) will enable some biometric technologies (i.e., fingerprint, iris scans) to become standard in multiple industries, and other forms will remain permanent niche market solutions.

Biometric technologies exploit the physical form of fingerprint scans, hand scans, facial and eye (retina, iris) scans; as well as signature and voice recognition to provide a toolkit of different solutions for authenticating a user.

Therefore, they seem ideal for use in the authentication process of identity infrastructure along with user ID and password. However cost, capability, and completeness remain the primary obstacles to widespread use of biometrics in this area.

Biometric technology has key metrics to measure capability. False acceptance rates (FARs) measure of how often an invalid identity is verified, and false rejection rates (FRRs) measure how often a valid identity is rejected. FAR and FRR can be tuned depending on user need and are inversely proportional. For high customer satisfaction environments, rejects are minimized with a low FRR. For high security environments, a low FAR is required.

Tuning is a major issue for biometrics users and can cause significant problems, as can environmental factors such as temperature, water, dust, background noise, fatigue, illness, intoxication (for voice authentication), and lighting conditions (for camera-based systems). Integration capability with such environments as enterprise directories, Web single sign-on services, applications, and other security services remain difficult. Biometric identifiers are unique identifiers, but they are not keys. They cannot be destroyed if stolen or compromised. Although they are useful in situations where the link between reader and verifier is trusted, biometric identifiers cannot be viewed as replacements for other forms of authentication (e.g. PIN codes, passwords), but as supplements.

Biometric technology works and, for limited requirements, may be considered cost-effective. However, user expectations are still too high regarding accuracy; many are easily spoofed. Biometrics will truly become a mainstream technology for authentication once PKI services for transaction enabling (specifically in the areas of certificate issuance and management) become common. With smart card technology (already common in Europe and growing in the US), certificates can be stored on portable smart cards. With biometric information also stored on the card (instead of a central directory or on a local machine hard drive), one potential implementation will have users interacting with biometric sensors that challenge the stored card information and authenticate upon a match. In fact, placing the template (sensed and reduced biometric ID data) into the smart card eliminates many of the administrative tools requirements.

Industry can take pragmatic steps for eventual adoption of biometrics for authentication:

- Reviewing current biometric technology implementations to develop realistic requirements and expectations.
- Piloting biometrics technologies in a limited, controlled environment.
- Following developments in standards for biometric profiles.

- Ensuring participation from security, identity infrastructure, and application developers during testing and evaluation.
- Avoiding comprehensive biometric services deployments for multiple application environments - staying focused and tactical to enable technology and market maturity to occur. Production deployment should be driven by very specific, clear business requirements for strong, multi-part authentication.

8.3 Technologies

Liberty Alliance and Passport are No Magic Carpets

Microsoft's .Net Passport, the Sun-inspired Liberty Alliance, and AOL's Magic Carpet all represent efforts to create a standard identity infrastructure for consumer-based authentication, enabling applications access across multiple enterprises.

Microsoft's Passport is a proprietary-based simple authentication and identification service that may move to a federated, Kerberos-based strong authentication model in late 2003. The Liberty Alliance is seeking to establish a much broader view of identity and attempt to define standards for both identity and single sign-on. Announced in September, the group has about 35 member companies, including France Telecom, Nokia, Schlumberger, Vodafone, America Online, American Airlines, American Express, Bank of America, General Motors, Nokia, RealNetworks and Sun Microsystems.

The Liberty Alliance work is theoretically complementary, rather than competitive, to Microsoft's Passport, the technology being developed is a set of APIs that will be used by authentication systems to exchange information. Passport could be one of those authentication systems.

The MasterCard International has joined the Liberty Alliance Project, and Microsoft said it's considering signing up.

The World Wide Web Consortium has approved an XML-based language for digital signatures. XML Signature offers basic data integrity and authentication tools that will be used to build more secure Web services.