Open Smart Card Infrastructure for Europe

v2

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

Part 7: **Telecom operator requirements**

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

INFORMATION SOCIETIES TECHNOLOGY
(IST)
PROGRAM

Contract for:

Smart.IS
Accompanying Measure

D5.1:Telecom requirements as RFC Document

Project acronym: **Smart.IS AM**
Project full title: **Smart.IS AM, Accompanying Measure for accelerating Electronic Business and New Transactional Information Systems**

Contractor no.: CR-5 TELEFÓNICA INVESTIGACIÓN Y DESARROLLO
Related to other Contract no.: -

Date of preparation of deliverable : 29 May 2002

Proposal number: IST-1999-13114

Operative commencement date of contract: January 2002.

List of Authors

D5.1:Telecom requirements as RFC Document

Sara Carro Martínez	Telefónica
Jose A. González	Telefónica
Juan J. Andrés	Telefónica
Francisco López	Telefónica
Jorge Lorenzo	Telefónica

Annex 1 to D5.1: PKI cost and standards related

Sara Carro Martínez	Telefónica
Jose A. González	Telefónica
Juan J. Andrés	Telefónica
Francisco López	Telefónica
Jorge Lorenzo	Telefónica

Annex 2 to D5.1: Business survey (*)

Jérôme Tollet	Axiome
Frédéric Halter	Axiome
Bertrand Thery	Axiome
Alain Grossmann	Axiome
Jacques Michel	Axiome

(*) → Annex 2 is presented on another separate document.

Table of contents

List of Tables

List of Figures

Abbreviations

ANSI	American National Standards Institute
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
CA	Certification Authority
CMP	Certificate Management Protocol
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DIR	Directory
ECC	Elliptic Curve Cryptography
ETSI	European Telecommunication Standardisation Institute
GPRS	General Packed Radio Services
GSM	Global System for Mobiles
HTTP	Hypertext Transfer Protocol
ICC	Integrated Circuit Card
IP	Internet Protocol
IPSEC	IP Security
ISP	Internet Service Provider
KA/RA	Key Archiving and Recovery
KGA	Key Generation Authority
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAP	Mobile Application Part
MIME	Multipurpose Internet Mail Extensions
NAME	Network Access Module for Internet End-user
NAME.ES	Network Access Module for Internet End-user with advanced electronic Signatures functions.
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCI	Peripheral Component Interconnect (local bus)
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure

PKIX	Public Key Infrastructure X – IETF Working Group
PSE	Personal Security Environment
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir & Adleman
S/MIME	Secure Multipurpose Internet Mail Extensions
SIM	Subscriber Identification Module
SMS	Short Message Service
SRA	Suspension Revocation Authority
SSL	Secure Sockets Layer
SWIM	SIM with embedded WIM
Telco	Telecommunications Company
TLS	Transport Layer Security
TSA	Time-stamping Authority
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USIM	UMTS Subscriber Identity Module
USB	Universal Serial Bus
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WIM	WAP Identity Module
WML	Wireless Mark-up Language
WPKI	WAP Public Key Infrastructure
WTLS	Wireless Transport Layer Security

Executive Summary

The objective of the Smart.IS AM project aims at developing and promoting standard specifications for the provision of authentication and advanced electronic signature functions based on interoperable and secure smart card systems to be used for electronic transactions and over the Internet. Smart.IS AM foster the emergence of a smart card system architecture for e-business, new TIS and e-commerce in general.

Smart card solutions combined with PKI infrastructures could provide the reference security architecture for end users, technology providers and service and content providers. Smart.IS AM rely on such PKI smart card systems.

This concept of a common Authentication and Advanced Electronic Signature module to secure Internet access will accelerate the development of e-Commerce, and e-Government applications since it will bring the required level of Trust and Confidence which is currently restraining the widespread use and development of new Internet applications and services.

In this context the D5.1 appears covering the business and technology content of the project. And more concretely studying the business requirements for Telecom Operators**,** taking into account the banking environment, and defining a common business model for the use of NAME and NAME.ES modules.

The main objectives and points covered on this study can be divided into several different areas:

- Generic Security Requirements for e-services for the authentication of end users with the NAME module, and for Electronic Signature with the NAME.ES module.
- Business requirements for Telcoms: Generic security requirements for mobile commerce.
- General Business model and business requirements.
- General review of applications which need to use NAME and/or NAME.ES, such as e-commerce, mobile banking and mobile commerce.
- PKI infrastructure and overall architecture and PKI services.
- Requirements for PKI in mobile services: GSM/WAP and UMTS.
- Business model based on PKI/smart card considering the NAME&NAME.ES modules.
- Service Interoperability issues
- Market analysis

This document has been produced with the valuable collaboration of experts in the areas studied.

This study is divide into two part, a technical part and 2 an annexes, one with the PKI cost from different vendors and the standards related and another one with the business survey.

The present document is an RFC document. The purpose of this document is to have a working document, in order to circulate it for comments and produce the final deliverable collecting and taking into account the feedback received.

1 Introduction

This RFC document is focused in the business and technology content of the SMARTIS project. And more concretely is focused on the business requirements for Telecom Operators**,** taking into account the banking environment, and defining a common business model for the use of NAME and NAME.ES modules.

The structure and areas covered on this document are the following ones:

- **Business requirements for Telcos: Generic security requirements for mobile commerce.**

  This chapter evaluates the requirements and needs of Telecom Operators, Banks and Financial, and Internet Service Providers in m-commerce and m-banking of a common card holder authentication module for any Internet end-user, always taking into account the integration with the NAME and NAME.ES modules. The security and services requirements are also included.

- **General business model**

  A business model, based on industry standards, internet standards and security standards established by other associations or entities (Visa, MasterCard, RSA Laboratories, etc.) and standards developed by international standardisation organisations and integrating the NAME and NAME.ES modules have been created. Its functioning is also explained.

- **Business requirements: services and application scenarios**

  Three applications and scenarios where the secure exchange of information is crucial, and therefore the integration of the NAME/NAME.ES modules are explained on this chapter. We have mainly focused in applications for the GSM/WAP environment. Together with these services and scenarios, the security needs and requirements in the e-business world are presented as well as the different secure services associated needed. The applications explained are: mobile e-commerce and 2 different ways of mobile banking.

- **PKI Infrastructure**

  This section presents in detail a PKI Infrastructure, its components and the integration with the NAME and NAME.ES modules. We have mainly addressed to the components as well as to the authentication process based on the SMARTIS modules, NAME and NAME.ES.

  This chapter also includes a section comparing specific secure aspects of the GSM/WAP environment to the fixed networks.

- **Overall architecture and PKI services**

  This section is focused on the specific PKI architecture provided by different vendors. The following architectures are explained in detail and a comparison table between them are also presented:

- Baltimore solutions
- Certicom suggested architecture
- Entrust solution
- Verisign solutions
- Nokia suggested architecture
- SmartTrust
- Microsoft Certificate Server

- **Business requirements**

  This point explains what the business requirements on the authentication and electronic signature modules for the network operators are, what their constraints are, what the economic elements which would make the use of such modules viable and better than other solutions are.

  We explain in detail the general secure m-commerce requirements that can be solved with the conjunction of a Public Key Infrastructure and NAME and NAME.ES modules; the business requisites that must be matched for network operator and e-commerce service providers and how NAME and NAME.ES modules fulfill with these requisites; the market segments that may be benefited from the usage of NAME and NAME.ES modules and the reasons why every market segment should adapt them as well as the business requirements related to multi-application systems.

- **Functional and interface secure requirements in a GSM/WAP environment.**

  This chapter shows the functional and interoperability requirements needed in order to provide a complete security framework, and therefore the PKI in conjunction with the NAME and NAME.ES modules.

- **Business Model for PKI/smartcard/NAME&NAME.ES**

  Following the context of the project, this section documents a business case approach that can be utilized by organizations considering an investment in Public Key Infrastructure (PKI) on smart cards, in conjunction with the NAME and NAME.ES modules, for its applications. Among other things the cost, benefits and risks are presented.

- **Interoperability issues**

  The interoperability of services as well as the interoperability with programming languages and the interoperability NAME and NAME.ES must provide to integrate themselves in a generic smart card and its own operating system have also been studied.

- **Technical constraints**

  What the technical constraints of implementation are, in particular in regards to the actual standards implemented by the network operators are explained on this section.

- **Requirements for PKI/NAME-NAME.ES in UMTS**

  This chapter is still under construction and are focused in the requirements for PKI to support end-user applications in a UMTS environment integrating the NAME and NAME.ES modules. We are also focused in the survey of UMTS security requirements relevant for PKI and the modules.

This document also includes 2 annexes. The first one presents the PKI cost from different vendors as well as the standards related and the other one the business survey.

2 Requirements and Infrastructures

This epigraph is dedicated to the requirements and infrastructures to be provided in order to offer the secure means, methods and services required for e-commerce basing on the usage of NAME and NAME.ES modules. This approach will be focused on the Network Operators, the Internet Service Providers, and the Customers.

Every role for these characters may be assumed in a variety of manners. In this sense, the Network Operator may provide the Public Key Infrastructure, or maybe it can be provided by an Internet Service Provider willing to offer higher levels of privacy and closure for their users. In a similar way, the Internet Service Provider might be either a private enterprise whether a portal offering other services held by the Network Operator, by instance.

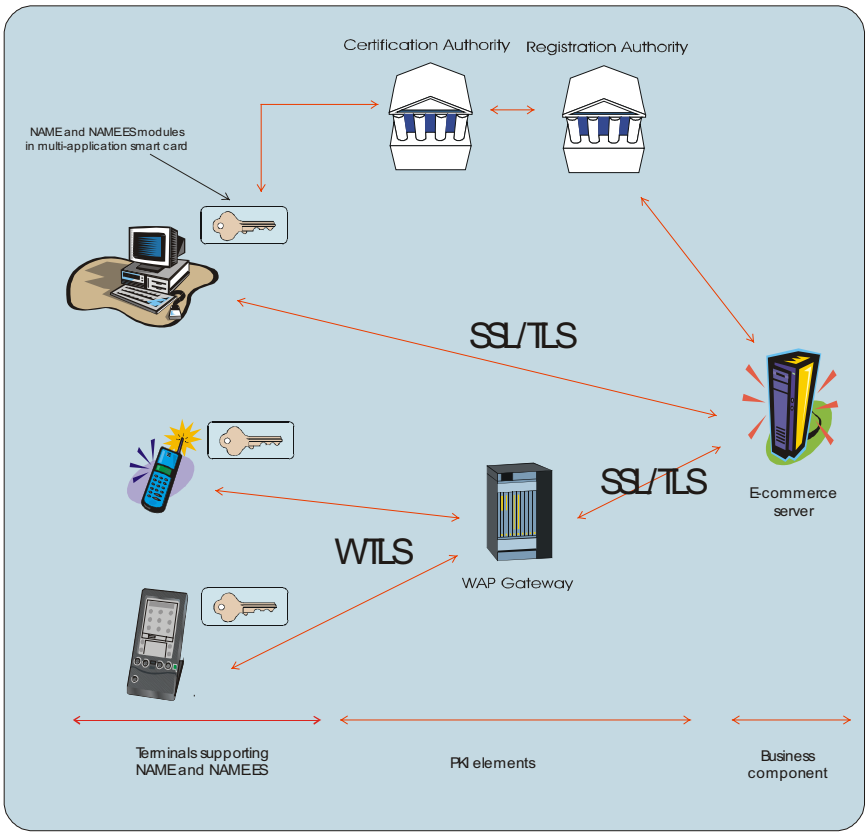


Figure 1: General architecture based on security modules

Figure 1 shows the general architecture for a secure service over Internet. We will focus on the two basic groups of infrastructures:

- The infrastructures to provide access to the service.
- The infrastructures required to provide security to the service.

Many users can 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, PDAs, e-books, etc. These devices may contain

the NAME and NAME.ES modules in a smart card an access it in different ways. Maybe, the computer access it from a standard card reader, the mobile phone in a slot designed for it, and a PDA if is smart card-enabled.

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

There must be a Public Key Infrastructure to provide and manage the digital certificates and revocation list in the system. The end-user applications must access easily and seamlessly to this infrastructure. Basically, it is composed of a Certification Authority, that validates, manages and creates the digital certificates, and a Registration Authority that passes the request to the Certification Authority. Not necessarily should both users and internet service providers obtain the digital certificates from the same Certification Authority, but Figure 1 shows just one possible scenario.

Now, the digital certificates are stored in the NAME module and they can be used to authenticate every party using asymmetric and symmetric cryptography to secure the communications. Together, NAME and NAME.ES modules provide confidentiality in e-commerce transactions and in other possible aspects of communications.

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. This is also considered in this document. For example, imagine a mobile phone accessing Internet uses WAP protocol, which uses the WTLS layer to assure the communication. On the other hand, we would access from a personal computer using TLS or SSL security layers. NAME and NAME.ES modules are to be designed thinking of their support to these protocols.

Therefore, we will ask ourselves questions like: what is the business model NAME and NAME.ES modules are going to be applied? What are the PKI infrastructures required to provide security together with NAME and NAME.ES modules? What do we have to take into account when implementing these modules?

We will also focus on the business requirements needed to support NAME and NAME.ES modules and on the technical constraints that can be found when implementing these modules and its use in the real environment. In this regard, we will get answers for questions like: What market segments are interested in adopting NAME and NAME.ES modules? What are the reasons? What does this solution make it more interesting than others? What technical details must be considered when designing the security modules?

3 Business requirements for Telcoms: Generic security requirements for mobile commerce.

This chapter will evaluate the requirements and needs of Telecom Operators, Banks and Financial, and Internet Service Providers in m-commerce and m-banking of a common card holder authentication module for any Internet end-user.

Mobile Electronic Commerce, also known as m-commerce, can be defined as any kind of transaction with a monetary value implied using a mobile telecommunication network channel.

Telcoms and Service Providers need an application-level infrastructure to control which resources the user is authorised to access and which transactions he can execute. This application-level access management system must also audit a user's actions 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 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 mobilizing the industry to develop a standard format for presenting Web content on mobile devices, and it provides an integration point for securing wireless access to sensitive content and transactions.

WAP gateways manage access to a Web server, provide encryption through the Wireless Transport Layer Security (WTLS) specification and authenticate users to enable a secure connection between the wireless device and the application server. WTLS, which is a version of TLS/SSL that has been optimized for wireless communications, provides data integrity, privacy, authentication and denial-of-service protection.

M-commerce is based in transactions with e-shops by means of WAP. One store offers its site to the Internet, and wireless terminals can access it through WAP. Most of the times, communications between users and commercial sites involve sensitive data transmission, and this communication should be secured.

As in wired communications we use a SSL layer to secure a communication, the WAP Forum has specified a transport layer to secure wireless communications. This is WTLS.

WTLS can secure communications in any m-commerce transaction. NAME should support WTLS operations in m-commerce transactions.

Implementations of WTLS can support different features, defining the following classes:

Class 1	The basic class where neither client (WAP terminal) nor WAP gateway are authenticated.

Class 2	The same as Class 1, but including WAP gateway authentication (this is the implemented equivalent SSL in the Internet).
Class 3	The same as Class 2, but including WAP terminal authentication. It is mandatory exchange of key, server digital certificate, client digital certificate, ciphering and MAC.

Including digital certificates and private keys in WAP terminals, WTLS Class 3 could be implemented in the future.

Telecom operators are interested in offering value-added services to their subscribers. They need to do this to be competitive. If a mobile terminal can be used as a type of payment for goods and services, the mobile operator is not interested in others to manage the transaction. Security measures need to be taken to perform these kind of services, since many of their processes involve critical information.

The advantage for operators is that they have a relationship with the client, which includes invoicing, as pre-paid or post-paid invoice (in a periodic base), and operators are the base to make the mobile terminal a popular type of payment.

There is a constraint for telecom operators. It is difficult to provide their services to other customers out of its own operator.

Banks and financial institutions establish strategic alliances between them and with operators to positioning in the market. Businessmen offer new services, but they need operators.

The percentage of business for the operator is not defined yet. Let's suppose that a customer buys a ticket for a concert for 30 € with his mobile phone, and he is charged with 2,50 €. The operator could receive this charge plus a small percentage of the price of the ticket, while the content provider could receive the 90% or 95%. On the other hand, banks also want to get their own benefit. Besides, the benefit for the service providers will not too high, and they propose that it is enough for the operators to be happy with an increase in the usage of their infrastructures.

From the user's point of view, he himself pays using his telephone. The transaction is made by any of these two ways:

- The mobile operator registers the payment adding an entry in the user's invoice or reducing his pre-paid payment credit. This operation benefits from the relationship between operator and user.
- The operation registers in an independent system, which enables the invoice. Here, the operator is neutral.

Attending to the amount of the invoice, we can see the similarities between the terminal and other common payment objects. Besides, the more relevant actors change:

- **Micropayments.** Pre-payment or charge in the phone bill: the terminal is used an electronic purse. The more relevant actor is the operator.
- **Bigger payments**. There is a similarity with credit or debit cards. The more relevant actor is the bank or the service provider.
- **Services admitting big and small payments**: The wireless terminal is used as an electronic purse or a credit or debit card.

Mechanisms to guarantee confidentiality and integrity of data should be incorporated, to provide enough security for banking and m-commerce applications. It should be possible to cipher data, to verify secret PIN codes, and to sign messages.

3.1 Security

Different wireless m-commerce and m-banking applications have different requirements for security:

Secure payment transactions for mobile commerce and mobile banking:

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

Secure exchange of documents:

- Reliable user authentication
- Data integrity
- Confidentiality
- End-to-end security

A classification of security requirements is going to be provided depending on the type of m-commerce applications: WAP and non-WAP applications.

The former is referred to m-commerce services using WAP protocol, and they are WAP sites offering m-commerce and m-banking applications. WAP offers a security layer called WTLS and security needs can be supported by the NAME module. On the other hand, WMLScript helps user interactivity between user and browser. WMLScript provides a cryptography library that enables NAME module to interact with.

The latter is related to other m-commerce and m-banking services based on different protocols such as Short Message Services, and they have a need of security for the exchange of sensitive data in their communications. These applications are based on its own business model and require integrity, privacy and authentication.

3.1.1 WAP m-commerce requirements

3.1.1.1 WTLS requirements

Since WAP is the relevant protocol in wireless communications to establish an m-commerce and m-banking relationship, the main layer to secure the communication is Wireless Transport Layer Security (WTLS).

Therefore, the security requirements for m-commerce and m-banking over wireless environments met those handling cryptographic operations over digital certificates and private keys in WTLS procedures. In m-commerce, WTLS is fundamental for the secure communication of sensitive data. WTLS authorise on-line transactions in the hands of mobile Internet users. WTLS is TLS adapted to the UDP-type usage by WAP. Basically, it enables encryption and authentication in any WAP communication.

A tamper-resistant device should contain the security objects needed in the WTLS protocol operations.

Security requirements for every process in WTLS are explained next.

NAME module should support functions related to secure a communication through WTLS. Therefore, security requirements for WAP m-commerce and m-banking solutions related to NAME module are (functions to support WTLS through NAME module):

Security requirements for WTLS handshake:

- When a customer uses his/her micro-browser to buy in a WAP site secured with WTLS sends a “Client Hello” message to the WAP server requesting for a WTLS session. The micro-browser should read user’s digital certificate. The NAME module may generate a 12 bytes random number for “Client Hello” message or it will be the micro-browser that generates it.
- The WAP server responds by sending the customer its server certificate.
- Customer’s micro-browser relaying on the NAME module verifies that the server's certificate is valid and has been signed by a CA whose certificate is stored in the NAME module (and who the buyer trusts). NAME module verifies CA signature from server’s digital certificate.
- The micro-browser reads user’s digital certificate from the NAME module if it is required by the server.
- If the certificates are all valid, customer's micro-browser relaying on the NAME module generates a one-time, unique "session" key and encrypts it with the server's public key. His/her micro-browser sends the encrypted session key to the server so that they will both have a copy.

The server decrypts the message using its private key and recovers the session key. At this point the user is conscious of two things:

- Authentication: The WAP site s/he is communicating with is really the one it claims to be (its identity has been verified).
- Uniqueness: Only the user's micro-browser and the WAP server have a copy of the session key.

His/her micro-browser and the WAP server can now use the session key to send encrypted information back and forth, knowing that their communications are confidential and tamper-proof. Security requirements for this functionality are:

- Data encryption/decryption. PKCS#1 must be taken into account to perform RSA encryption on data. For decryption, NAME module should have inputs for ciphered data and the identifier for one private key stored in the module.

3.1.1.2 WMLScript requirements

WAP Forum regards WMLScript for WML as a scripting language that can enable certain cryptographic functions. Security requirements for WMLScript should also be taken into account in any m-commerce and m-banking scenario in order to provide functionalities for an e-commerce environment.

Although WTLS enables client authentication during a WTLS connection, this is not persistent for transactions taking place during the connection. It could be enabled associating a digital signature to data generated as a result of a transaction. Therefore, the micro-browser provides a WMLScript function called Crypto.signText, to sign a text string.

One method call views the text to sign and ask for user's confirmation. If the user accepts the operation, s/he will be asked to enter a non-repudiation key (such as a PIN or password). If the value is correct, data altogether with its signature are sent over the network. Now the server can extract the signature and validate it, and even store it for accounting purposes.

To summarize, cryptographic requirements for WMLScript usage in m-commerce environments related to NAME module are:

Digital signature	WMLScript Crypto.signText method signs data. The private key used to sign the data should be protected by some kind of password or PIN. Data to be signed should be sent to the NAME module.
Key unwrapping	deciphering a message including a secret key using public-key cryptography.

3.1.2 Non-WAP m-commerce requirements

On the other hand, many m-banking and m-commerce applications are based in GSM SMS or other non-WAP applications. These applications are based on the processing of such messages which carry sensitive user's information. Basic requirements about security in these systems are also related to signing and encrypting/decrypting of short messages. These facilities can be viewed as application level security functions.

Legacy m-banking and m-commerce applications are based on transmission and reception of SMS messages. These messages are to be signed, validated, encrypted and decrypted in order to secure communications.

Therefore, security requirements for non-WAP m-commerce and m-banking solutions based on the exchange of SMS messages related to NAME module are:

- **Digital certificates storage**. Those cases digital certificates are too large to be stored in the NAME module, one URL pointing at the digital certificate should be stored in the NAME module. Otherwise, X.509 digital certificates would occupy too much room in the NAME module for non-WAP m-commerce applications. Functions to save a digital certificate in the NAME module should be provided in order to authenticate parties in a communication. The module should be able to save digital certificates for future use, and it should have the ability of selecting one digital certificate to use.

- **Private keys storage**. A PIN should protect the key. Several keys may be stored in the tamper-resistant module. The application should be able to select the key to use for a certain usage case.

- **Data encryption/decryption.** For decryption, NAME module should have inputs for ciphered data and the identifier for one private key stored in the module. PKCS#1 must be taken into account to perform RSA encryption on data.

- **Hash signing.** The mobile terminal uses a hash function to generate a digest for the data to sign. This digest is sent to the NAME module in order to be signed. The NAME module returns the signature. Digest information should be input for the NAME module.

- **Signature validation**. NAME module should have as inputs the digital signature, the digest and information about the public key to use from those digital certificates stored in the NAME module.

Other possible applications:

- SSL client authentication with private keys

- TLS client authentication with private keys
- S/MIME

3.2 Services and Applications

3.2.1 Mobile Shopping applications

- **Access to e-shop catalogues** – Shows the catalogue of the e-shop where the customer can find the products the store offers.
- **Check availability online** – Reports the user if the selected item is available.
- **Online ordering** – Ability to select an item offered by an e-shop in order to purchase it.
- **Online payment -** Ability to transfer money between any the buyer's accounts once s/he has decided to purchase a selected product.
- **Loyalty services** – information can be stored apart from the NAME module in the smart card and secure communication for stored points for transactions can be achieved.

3.2.2 Mobile banking applications

- **Account Inquiry –** Provides the ability to request for account balance information on various current, savings, fixed deposits and credit card accounts.
- **Transaction History** – Ability to access the account's last transaction information.
- **Funds Transfers** – Ability to transfer money between any the consumer's accounts like checking, savings or credit card on a realtime basis.
- **Bill Payment** – Ability to make bill payments to pre-designated payee organizations in real-time basis.
- **Rates Inquiries** – Ability to request for the latest bank interest rates, foreign exchange rates, loan and lending rates and other rate information.
- **Electronic Purse**

3.2.3 Mobile Information Servicing

- **Vehicle positioning service** (handset tracking) where applications must be protected with username and password
- **Medical applications**
- **Provided identification of citizens by Government**
- **Driving licences**
- **Social security**

- **Mobile Stock Trading**

3.2.4 Mobile Ticketing applications

- **Ticket reservation for theatres -** online scheduling, online availability check, online reservation and online payment.
- **Ticket reservation for flights -** flight scheduling, flight booking and rebooking, online check-in and online payment.
- **Reservation for car rental -** car reservation, online contract and online payment.
- **Bus/Rail season ticketing**

3.2.5 Mobile Gaming

- **Gambling**

4 General business model

4.1 Introduction

This business model is to be based on:

- Industry standards
- Internet standards and security standards established by other associations or entities (Visa, MasterCard, RSA Laboratories, etc.).
- Standards developed by international standardisation organisations.

In this point, the global functioning for the business model base on smart card is being explained.

4.2 Actors

4.2.1 Buyers and Sellers

Potential buyers are connected to sellers by means of an open public network such as Internet from personal computers, mobile phones, PDAs, etc. an application used by the buyer to perform the purchase runs on these devices.

The seller offers his/her products over the same network the buyer is connected to. It owns a server application running on an adequate machine for the services the seller offers.

Communication between seller and buyer is intended to follow the client/server model. The buyer application acts as a client and the seller application acts as a server.

The buyer owns an bank account or a credit in an entity. Purchases performed by the buyer are charged on his/her account.

It may be possible to bind a bank account with an e-mail account and a card. When the buyer purchase something, s/he is identified against the seller by the credit card. NAME module has here the main role. The seller sends credit card data and transaction data to the e-commerce service provider centre and it authorizes or rejects the purchase.

4.2.2 E-commerce service provider centre

The e-commerce service provider centre is the set of systems providing e-commerce services for both sellers and buyers. Financial entities wanting their clients to purchase on the Internet must be registered on the e-commerce service provider centre. The same way, sellers wanting to use this system to market their products have to be registered also.

The e-commerce service provider centre is in charge of validating purchase transactions, and if needed, charge them on the corresponding financial entity. Validating transactions involves checking that both seller and buyer are registered on the system and transactional data committing are coherent and allowable (the buyer has enough credit, etc.).

The seller does not communicate directly with financial institutions. The e-commerce service provider centre dialogues directly with the financial entities on behalf of the seller. In this respect, the e-commerce service provider centre is the interface between the financial institutions and the e-commerce system. Operations performed between the e-

commerce service provider centre and the financial entities are out of the scope of this model. With a view to the latter, it is seamless that the e-commerce service provider centre is to communicate with the financial entities or containing enough information to be able to validate transaction on its own.

The buyer communicates the seller to perform his/her purchases. The seller communicates, on one hand, with the buyer, and on the other, with the e-commerce service provider centre to perform electronic payment related operations. Eventually, the buyer communicates with the e-commerce service provider centre to check the documents relating purchases and electronic transactions.

4.3 Security

4.3.1 Certificates and private keys

Every actor in the business model, Seller, Buyer and E-commerce Service Provider Centre has two digital certificates and two private keys. A certificate and its associated private key are used to open electronic envelopes coming from the owner and for authentication processes. This certificate and this key are called exchange certificate and exchange key.

The other certificate and its corresponding private key are only used to:

- Electronic and/or dual signature.
- Others being able to verify electronic and/or dual signatures

This private key can only be used if the owner explicitly decides so. This certificate and key are called signing certificate and signing key.

The user's financial account is associated with the owner's certificates. From the point of view of the financial authority, each of these certificates defines uniquely the account dealt.

The seller's certificates identify him uniquely against the buyers and against the E-commerce Service Provider Centres s/he is registered.

4.3.2 Communications

The three actors communicate each other two by two.

The system guarantees confidentiality and integrity of every datum transmitted between two actors by means of SSL protocol or WTLS in case of mobile communications. So then, SSL authentication process employs certificates and private keys for the exchange of every participant in the communication.

SSL is an open protocol where both parties communicating can negotiate what security mechanisms are going to use in their transmissions. The required security level for this model demands determinate mechanisms. In the model, both parties negotiate so SSL operates with fixed parameters. If any of the parties does not support any of mechanisms, the session may be aborted.

On the other hand, the buyer has to send certain information to the E-commerce Service Provider Centre, which the seller must not know, but during the trade-off, the buyer does

not talk directly with the E-commerce Service Provider Centre, but through the seller. SSL cannot protect this information, since in this phase, buyer and E-commerce Service Provider Centre communicates through the seller, i.e. they do not have an open SSL session. To secure this information, the seller sends it encapsulated in an electronic envelope to the E-commerce Service Provider Centre. This envelope reaches the seller in one or various SSL session messages holding with the buyer. This way, confidentiality for transmitted data between buyer and seller is guaranteed.

4.3.3 Digital signatures

When a party sends the other an electronic document and the one receiving it wants to place on record that the recipient knows and accepts the terms of the document, must send it with his digital signature. The digital signature is a non-repudiation proof that who the document's author is and for the integrity of the document. To sign a document electronically or dually, the signer must use his signing private key.

SSL is in charge of transmitting data between parties without anybody understanding them. SSL does not provides digital signing service to applications. Therefore, NAME module may provide such a service.

4.3.4 Smart Cards

The buyer's card is a smart card. His certificates and private keys are stored in his card inside the NAME module. Private keys never leave the smart card. Digital certificates are free reading.

In some phases in the protocol for the business model, buyer's private keys are used to encrypt or decrypt. These ciphering or deciphering processes with every buyer's private key are performed by the NAME module. This makes for two things. On the one hand, the buyer cannot access the e-commerce service without his smart card. On the other hand, NAME module supports the PKI cryptographic algorithms.

To use these cryptographic services, the user must previously enter a correct PIN.

Computers the buyer accesses the e-commerce system from must have a card reader/writer unit plugged. This unit must provide a keyboard to enter the smart card PIN to open the door to the cryptographic services of the NAME module. For a higher level of security, the PIN must go directly the smart card through the unit without passing through the personal computer.

4.4 System infrastructure

4.4.1 Seller

The seller has a web server to market his/her products on the Internet. This server communicates with its clients over SSL protocol to secure their communications.

To establish a secure session, SSL uses the seller exchange digital certificate and private key. This certificate and this private key are not stored in the NAME module, since the server must be in a secure place and it does not change its location, and speed is a constraint for the server. The private key must be stored in a safe place.

The seller may hold a database with the orders, authorisation requests, authorisation responses and purchase invoices corresponding with the sales purchased together with buyers' signing certificates.

4.4.2 Points of sales

Buyers can access the e-commerce system from personal computers wired to the Internet. The connection program to connect to Internet may be any commercial web browser. The browser will download one or more web files from the seller's server. From now on, these pages will be called sale pages. These pages will tell the buyer operations to commit (fill in a form, insert card in the card reader…) to acquire a service or product. The browser itself guarantees the confidentiality and integrity by means of SSL. NAME module will support cryptographic functions used by SSL protocol.

Every computer attached to the system must have one card reader attached.

Buyers insert their smart card with the NAME module and the set browser-sale page will request the security services to the NAME module.

4.4.3 Buyer

The buyer owns a smart card with NAME and NAME.ES module supported where s/he will store his/her certificates and private keys. The NAME.ES module will do every digital or dual signature and open electronic envelopes for the recipient. So that the smart card performs these functionalities, the user must provide it with a correct password. Every piece of information required for the user to enter the system is found in the NAME module. Actually, the NAME module ciphers and deciphers with one of its private keys what the software of the PC wants.

The digital certificate is associated with a financial account to a financial entity registered in the e-commerce system.

The buyer also has an e-mail account. The purchase orders, invoices and associated payment instructions (documents in an electronic format electronically signed) are sent by e-mail to this e-mail account. These documents goes over the network in an electronic envelope to the buyer in such a way only the buyer can open. The buyer may, if desired, keep the purchase invoices just in case s/he has to lodge a complaint or just as a receipt.

4.4.4 E-commerce service provider centre

The e-commerce service provider has two certificates and two private keys, as the seller and for the same reasons, they are not stored in the NAME module. The private key must be stored in a safe place.

A copy for the certificates is installed in every point of sale and other in sellers' systems.

The e-commerce service provider communicates with the seller's server and with the buyer's PC by means of SSL supported by the NAME module. To establish a secure session, SSL uses exchange certificates and private keys of the e-commerce service provider.

The e-commerce service provider keeps a virtual database with the registered buyers' certificates and other data (contracted services, credit…). It also keeps a database with signing and exchange sellers' certificates and another for the buyers. Eventually, it has a database with payment instructions, authorisation requests, payment requests and authorisation responses about the purchases.

5 Business requirements: services and application scenarios

This chapter shows some applications and scenarios where the secure exchange of information is crucial, and therefore the integration of the NAME/NAME.ES modules. We are going to focus mainly in applications for the GSM/WAP environment. This services and scenarios show the security needs and requirements in the e-Business world and the different secure services associated needed.

Applications for the GSM/WAP environment cover several different services ranging from weather forecasts to financial information, from yellow pages to Internet portals. Because of the increasing importance of WAP in the world market this examination will be focused mainly on products offered for this standard. WAP phones are much more than normal phones; they incorporate an Internet browser, an e-mail client, an authentication device, an information client and an e-wallet.

It is useful to classify WAP services according to their content and to the security mechanisms required in order to implement and operate them in a reliable way. Up to four categories can be identified:

1. Information (news, stock quotes, applet downloading, …).
2. Communications (email, wireless remote access, chat, ICQ, …).
3. Transactions (remote banking, e-commerce, stock exchange, ticket booking, …).
4. Entertainment (games, date arrangement, …).

Security is a very strong requirement in the first three groups, therefore the importance of the use of the NAME/NAME.ES modules. For each group a set of mandatory security services and a set of optional security services is indicated:

Table 1: Security services for WAP applications

Category	Mandatory services	Optional services
Information	Authentication of origin Integrity of contents	Authentication of recipient Encryption of contents
Communications	Authentication of sender and recipient Encryption of contents Integrity of contents	Non-repudiation
Transactions	Authentication of sender and recipient Non-repudiation Encryption of contents Integrity of contents	Commitment

The optional services are not strictly required and they may be applied whenever the parties involved desire a stronger protection of data.

A small group of relevant scenarios where the presence of a secure mechanism, and therefore the use of a PKI in conjunction with the NAME/NAME.ES modules plays a considerable role is now presented and described. These scenarios describe the generic business secure requirements needed for these applications. In order to use the NAME module in these applications these secure requirements have to be taken into account.

5.1 Mobile e-commerce

Mobile e-commerce is defined as the use of a terminal and a public mobile network to access information and conduct transactions that result in the transfer of value in exchange for information, services or goods. It can be done with just a mobile phone, a PDA connected to a mobile phone or even a portable PC connected to a mobile phone.

Unlike the traditional communications over Internet, mobile phones incorporate from the beginning very strong authentication features.

Phases

1. Browsing
2. Merchant authentication
3. Customer authentication
4. Order generation and delivery
5. Order confirmation

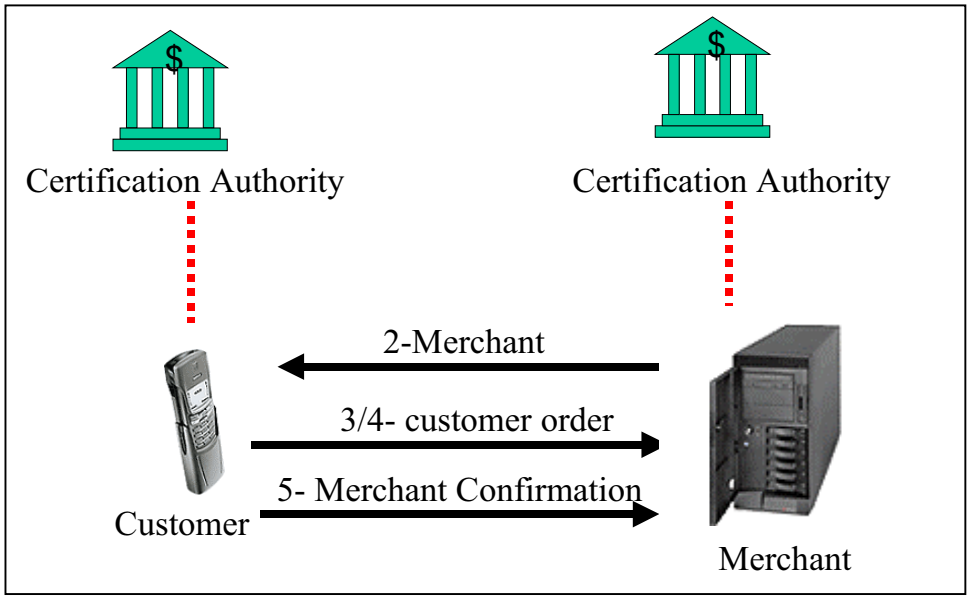


Figure 2 : Interaction between parties in mobile e-commerce

Description

1. In the initial browsing phase there are no security service requirements, web malls and shops are usually open to the public. Some web sites require the user to enter a username/password to have access to the shops; this is done essentially to have the possibility to offer personalised services and customisation of web pages rather than to perform identification and access control.
2. The customer wants to be sure about the identity and reliability of the merchant before sending the order information. A public-key authentication protocol is a reliable solution to provide such assurance. Normal certificates or certificates with special attributes, enabling the merchant to perform e-commerce and receive credit card payment, may be used.
3. Customer authentication protocol may be avoided, since it is implicitly included in the following point.
4. Once the customer has verified merchant identity, the order may be sent. Integrity services must be applied to protect the message against modification, cancellation and replication. Non-repudiation service is also required to prevent the customer to deny the order submission. The digital signature appended to the order satisfies both requirements (if used together with time-stamping or secure audit trail service). Confidentiality of the entire message is an open issue: the information regarding the payment method (credit card number, bank account number, check number, etc.) must be encrypted, unless it is transmitted over a secure communication channel, but the full description of goods/services may be in cleartext (in any normal shop everybody can see what customers are buying…).
5. The merchant first verifies the order received. With positive validation he sends back to the customer a proof of correct delivery of the order and a formal engagement of execution. This message needs protection with integrity and non-repudiation services, the computation of digital signatures represents the ideal solution. The transaction is considered concluded when the customer receives the confirmation signed by the

merchant. Confidentiality is again an open issue that depends on the information included in the message.

Once we have describe the mobile e-commerce scenario with all the secure requirements needed and we have also read the previous chapters, we see the importance and needed of integrating the NAME/NAME.ES module in this scenario as well as the functions and requirements this module has to accomplish.

The following figure depicts the Mobile e-commerce scenario integrating the NAME/NAME.ES module.

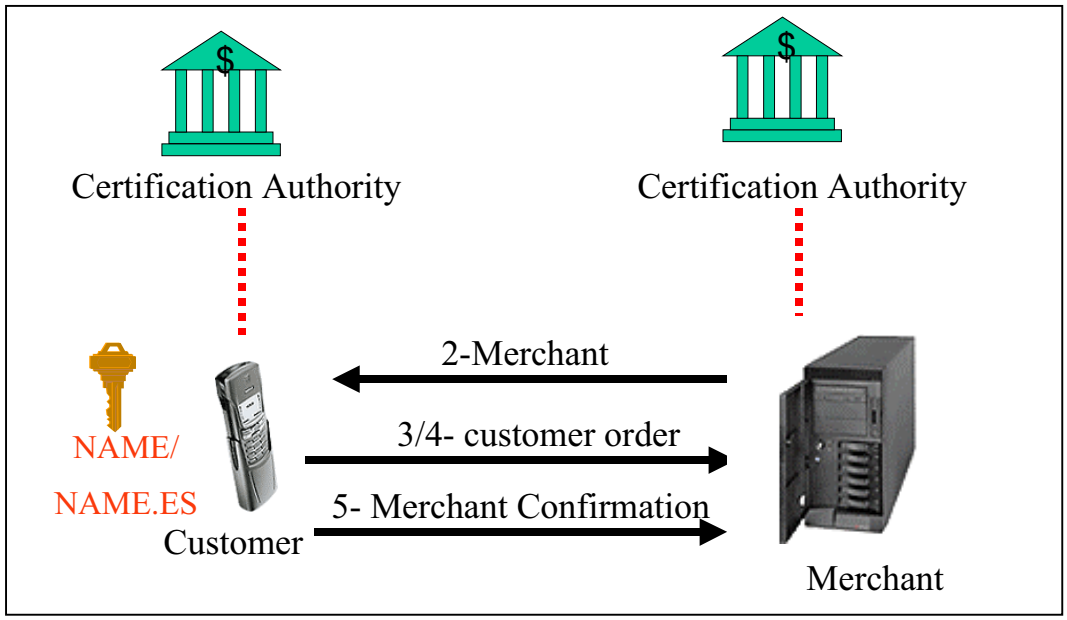


Figure 3: Mobile e-commerce scenario integrating the NAME/NAME.ES module.

5.2 Mobile Remote Banking

Remote banking refers to services offered by bank on the Internet to residential and business customers who are not physically located at any bank branches.

Informational services, bank account statements, financial transactions like money transfer and stocks dealing are the most common and most important services offered by many banks.

Phases

1. Bank authentication
2. Customer authentication
3. Message exchange

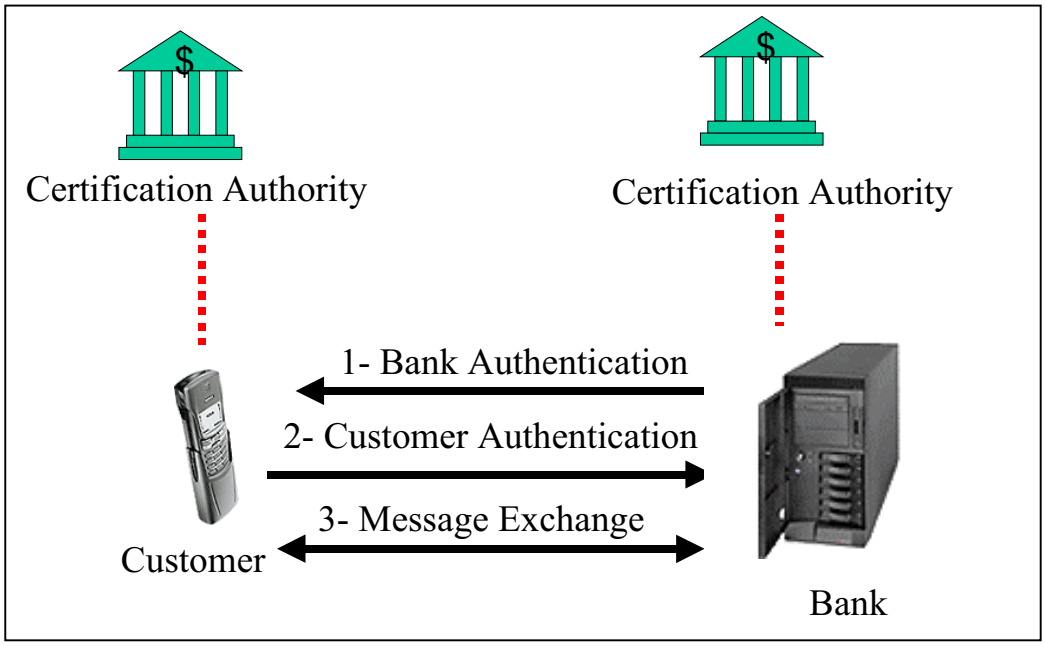


Figure 4 : Interaction between parties in Remote Banking

Description

1. Strong bank authentication is provided by means of a public-key algorithm.
2. Strong customer authentication is provided by means of a public-key algorithm. These two first phases may be carried out together with a challenge-response mechanism that grants mutual authentication.
3. The message flow between client and server requires confidentiality, integrity and non-repudiation. Symmetric encryption, message digests and digital signatures satisfy the requirements; efficient and properly implemented CRL and time-stamping services are essential for the correct realisation of the transaction.

5.3 Download money on cash card

With special equipped mobile phones it is possible to download money on a normal cash card. One of the first examples comes from the Motorola StarTac-D handset with an integrated smart card reader. The user can simply insert his/her cash card in the slot of the specially modified phone, connect to the bank and download the required amount of money. The card can then be removed and used in any shops and places that accept cash cards.

Phases

1. Bank authentication
2. Customer authentication and download request
3. Cash card and bank account verification
4. Cash downloading

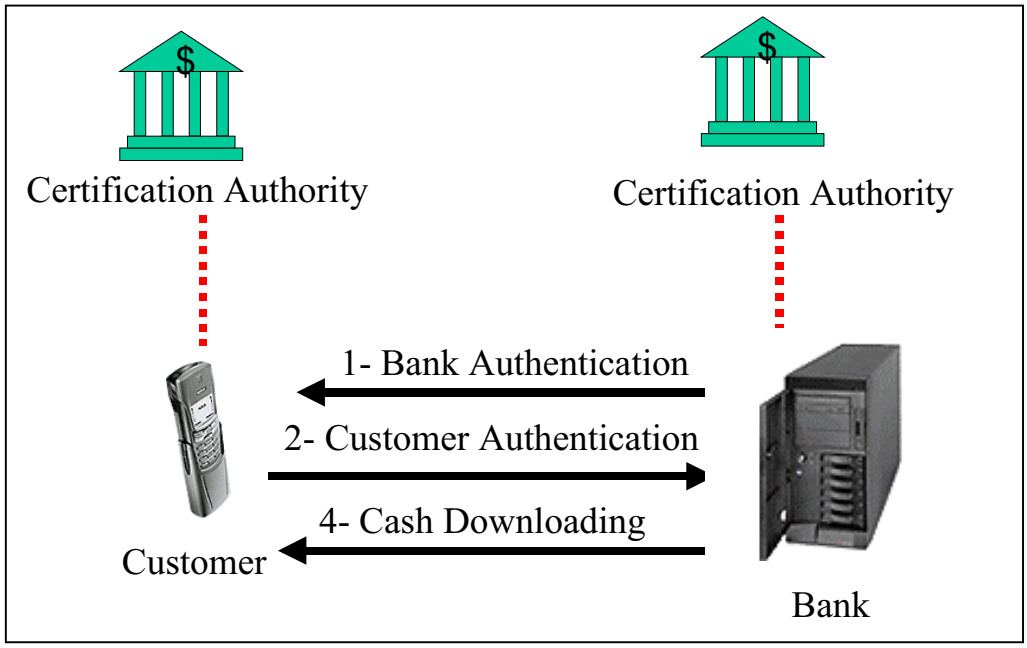


Figure 5 : Interaction between parties in download cash card.

Description

1. Strong bank authentication is provided by means of a public-key algorithm.
2. Strong customer authentication is provided by means of a public-key algorithm. These two first phases may be carried out together with a challenge-response mechanism that grants mutual authentication. What is actually authenticated in this step is the cash card inserted in the extra slot and its cardholder. After sending his/her credentials, the customer creates and sends a message containing all the information to require the money downloading (amount, bank account). This information needs confidentiality, integrity and message origin authentication. Symmetric encryption, message digests and digital signature satisfy the requirements.
3. The bank server verifies that the information requiring the money download is valid. The cash card is checked to be valid and a confirmation that funds are available in the bank account must be obtained.
4. When all checks are satisfied the funds are transferred to the cash card. The phone confirms that the download has been completed and the amount can be debited from the bank account. Messages exchanged in this phase need confidentiality, integrity and message origin authentication. Symmetric encryption, message digests and digital signature satisfy the requirements.

The mobile remote banking and the download money on cash card scenarios require strong secure mechanism for their transactions. Therefore the relevance of the use of the NAME/NAME.ES modules in order to assure the authentication of the device and the authorised user, the integrity of communications and to provide the electronic signature service.

As it was presented in the e-commerce scenario, these two scenarios (mobile remote banking and download money on cash card) describe the secure requirements for these applications and therefore the relevance of integrating the NAME module, according to the General Business Model described in previous chapters.

The following figures (Figure 6 and Figure 7) depict these scenarios (Mobile Remote Banking scenario and Download money on cash card) including the NAME/NAME.ES module.

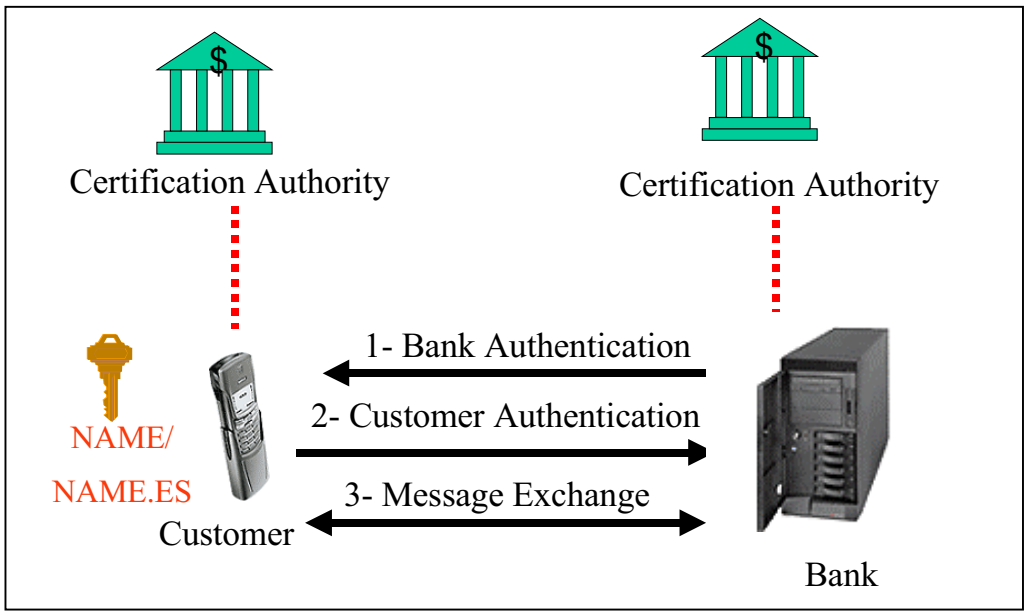


Figure 6: Mobile Remote Banking scenario including NAME/NAME.ES module.

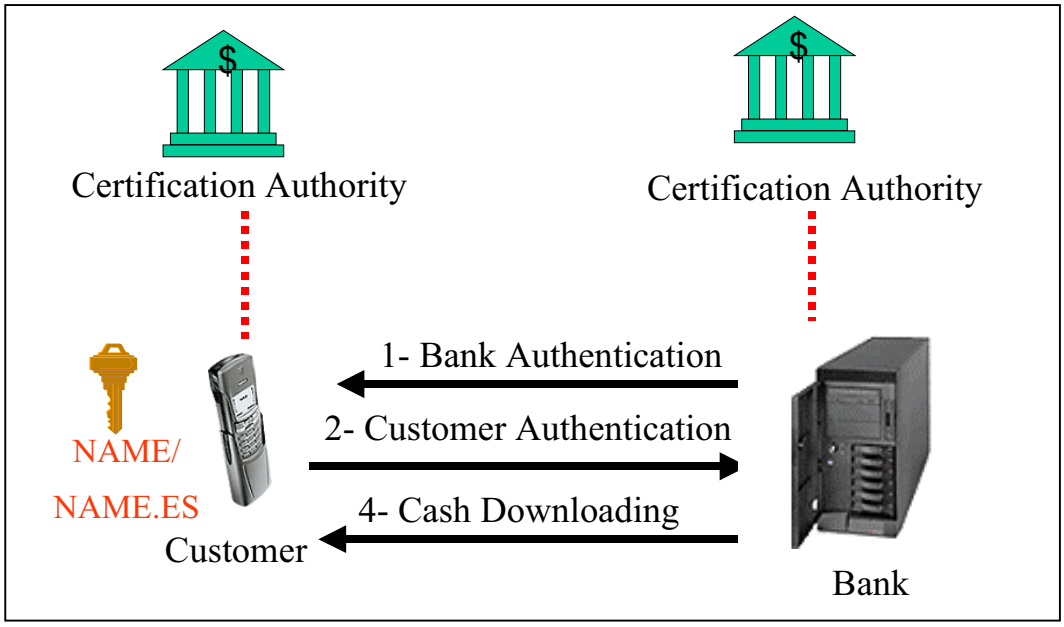


Figure 7: Download money on cash card scenario including NAME/NAME.ES module.

6 PKI Infrastructure

The PKI infrastructure presented follows the guidelines provided by WPKI (Wireless Application Protocol PKI) WAPForum's standard. This standard is an enhancement of the PKIX standard for wireless environment. It is a generic PKI infrastructure for mobile environments advisable for m-commerce scenarios.

The PKI infrastructure will be in charge of managing relationships, keys and certificates to enforce m-commerce business policies.

6.1 PKI components

Figure 8 shows the components included in any PKI infrastructure for a mobile environment and the relationships between them. The next point will explain how these elements relate each other in order to provide the functionalities for PKI.

The components are:

- End-Entity Application
- Registration Authority
- Certification Authority
- PKI Directory

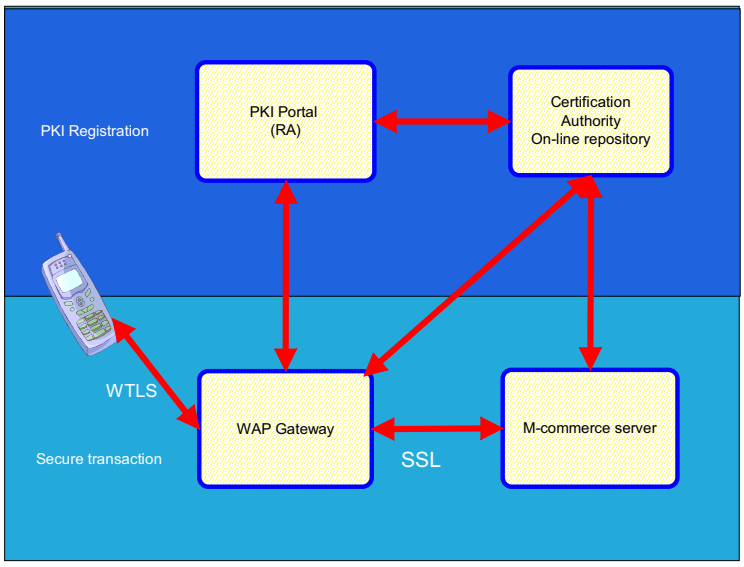


Figure 8 : Functional Architecture of wireless PKI

The architecture is completed with these additional elements:

- WAP terminal with NAME and NAME.ES modules
- Smart Card where NAME and NAME.ES modules are implemented
- M-commerce server with SSL or TLS support and the secure service application running

- WAP gateway with WTLS and SSL/TLS support

6.1.1 Entity Application

It is implemented on the smart card of a WAP terminal directing operations for:

- The generation of public key pairs
- The storage of such public key pairs
- The consecution of digital certificates
- The understanding of the contents included in digital certificates
- The search of revocation information (access to revocation lists…)
- The capability of renewing a certificate
- The capability of requesting a certificate revocation
- The validation of digital certificates
- The generation and verification of digital signatures

It uses the facilities provided by NAME and NAME.ES modules for cryptographic functions. It holds WTLS sessions and uses WMLScript methods to provide security functionalities.

6.1.2 Registration Authority

It is implemented by the PKI Portal in this PKI infrastructure. It is a PKI operator node in the PKI infrastructure. It interworks with the WAP end-entity applications and the Certification Authority. The PKI Portal verifies user requests for a digital certificate and tells the certificate authority to issue it.

It acts as a wireless registration authority point with authentication and signing certificate request support.

It must also have capabilities to access the Directory and the certificate revocation list.

6.1.3 Certification Authority

It issues and manages security credentials and public keys for message encryption. It checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate, and it is delivered to the WAP terminal.

6.1.4 PKI Directory

It may be implemented either on the certification authority’s component or apart from it. It stores digital certificates for users and revocation information to be retrieved by end-entity applications.

6.2 Processes

Processes involved with the PKI infrastructure are briefly explained following. These processes are:

- PKI registration
- Secure transactions

6.2.1 PKI Registration

The process starts when a WAP terminal or a WAP gateway uses the end-entity application to obtain a digital certificate from the PKI infrastructure. First, the end-entity application generates a keys pair (public key and private key). Then, it creates a certificate request and sends it to the PKI Portal assuming RA functions. The RA approves the certificate request and sends it to the CA.

Then, the CA creates the digital certificate for that user and sends it back to the PKI Portal and to the directory, where it is also stored.

The CA notifies the WAP end-entity application that its digital certificate has been created by using an URL pointing to this digital certificate.

Then the WAP end-entity application accesses and gets the digital certificate.

On the other hand, the ISP server (the server providing with m-commerce functions) can obtain these digital certificates and revocation information from the PKI Directory.

6.2.2 Secure Transaction

Now, the WAP terminal is able to maintain a secure session with the m-commerce server. It establishes a WTLS session with its corresponding WAP gateway, and it intermediates with the m-commerce server by means of SSL or TLS if the server is Internet-based or by WTLS if it is WAP-based.

6.3 Authentication in WTLS using PKI infrastructure

There are three types of authentication involved in WTLS. For every type, the PKI could be used in different manners to provide authentication. Following, we explain how the infrastructure previously described can do it.

Table 2: types of authentication involved in WTLS

Feature	Class 1	Class 2	Class 3
Server certificate	Optional	Mandatory	Mandatory
Client certificate	Optional	Optional	Mandatory

Therefore, we could summarise the types of WTLS with their functions as:

- WTLS Class 1

Confidentiality

Integrity

- WTLS Class 2

Confidentiality

Integrity

Gateway authentication

- WTLS Class 3

Confidentiality

Integrity

Gateway authentication

Client authentication

We are going to explain the PKI configurations that should be accomplished with each type of WTLS and their implications with NAME and NAME.ES modules.

6.3.1 WTLS Class 1

In this case, both server certificate and client certificate are optional. Therefore, the WAP terminal and the WAP gateway (client and server in the WTLS session) need not be authenticated.

Anyway, NAME and NAME.ES modules should be used to cipher and sign data in every interaction in the WTLS process.

6.3.2 WTLS Class 2

Now, the server certificate is mandatory, but not the client certificate. Therefore, server authentication is required, and the WAP terminal is able to authenticate the identity of the WAP gateway.

We can find two different models for server authentication:

- Two phase security model
- End to end security model

In both scenarios, the end-entity application is the WAP gateway requiring the services from the PKI.

Following, we explain the use of the PKI for both models.

6.3.2.1 Two phase security model

In this model, the WAP gateway creates the keys pair and generates a certificate request which is sent to the PKI portal.

The PKI portal confirms the identifier and sends the request to the certification authority.

The certification authority generates the digital certificate (Gateway Public Certificate) and sends it to the WAP gateway.

The certification authority aggregates the certificate to the repository for all the clients enrolled in the PKI.

Now, the authentication is two-phased. First, the WAP terminal establishes a WTLS session with the WAP gateway. Secondly, the WAP gateway establishes an SSL or a TLS session with the m-commerce server.

With more details we can describe the steps in the following order as depicted in the Figure 9.

Assumption: the CA Root Certificate is pre-installed in the WAP device.

One-time preparation steps (initialisation):

1. The WAP Gateway generates its own key pair – public key & private key.
2. The WAP Gateway exports the public key together with a certification request to the WPKI Portal.
3. The WPKI Portal (acting as a RA) confirms WAP Gateway's identity, and forwards the request to CA.
4. CA certifies the public key, and sends the digital certificate back to the WAP Gateway.
5. CA populates the On-line Repository with WAP Gateway certificate.
   (The WTLS class 2 certificate is now established and can be taken into use)

Authentication steps (setting up two links):

6. WTLS session established between WAP Device and WAP Gateway:
   - The WAP Device sends a challenge to the WAP Gateway;
   - The WAP Gateway signs the challenge and returns this together with its certificate;
   - The WAP Device verifies the received certificate by using the CA root key;
   - The WAP Device verifies the signed challenge by using the WAP Gateway's public key (retrieved from the certificate).
7. SSL/TLS session established between WAP Gateway and the ISP server (the server providing with the m-commerce functions).

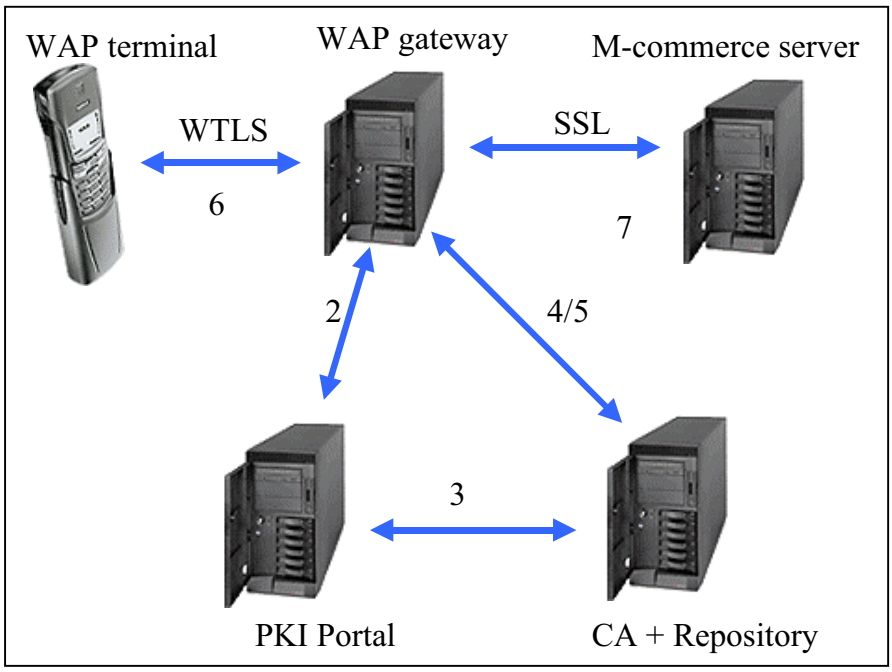


Figure 9 : Two phase security model

6.3.2.2 End to end security model

In this model, there is a WAP server gathering both services of WAP gateway and ISP server in the same machine. The WAP server communicates directly with the WAP terminal without a gateway.

A WAP server is similar to a web server, except that it uses the WAP protocols instead of the HTTP protocol. This allows the WAP server to communicate directly with WAP phones without a Gateway. A WAP Server may be used to achieve end-to-end security. There are currently two proprietary WAP servers on the market from Nokia and Tantau.

The WAP server creates its keys pair and sends the certificate request to the PKI Portal. The PKI Portal confirms the request and the identifier and sends the request to the certification authority.

The certification authority generates the digital certificate and sends the Server Public Certificate to the WAP server.

Now, the WTLS session may be established from the WAP terminal to the WAP server.

With more details we can describe the steps in the following order as depicted in the Figure 10.

One-time preparation steps:

1. The WAP Server generates its own key pair – public key & private key.

2. The WAP Server exports the public key together with a certification request to the WPKI Portal.
3. The WPKI Portal (acting as a RA) confirms WAP Server's identity, and forwards the request to CA.
4. CA certifies the public key, and sends the digital certificate back to the WAP Server.
5. CA populates the On-line Repository with WAP Server certificate.
   (The WTLS class 2 certificate is now established and can be taken into use)

Authentication step:

6. WTLS session established from WAP Device to WAP Server.

- The WAP Device sends a challenge to the WAP Server;
- The WAP Server signs the challenge and returns this together with its certificate;
- The WAP Device verifies the received certificate by using the CA root key;
- The WAP Device verifies the signed challenge by using the WAP Server's public key (retrieved from the certificate).

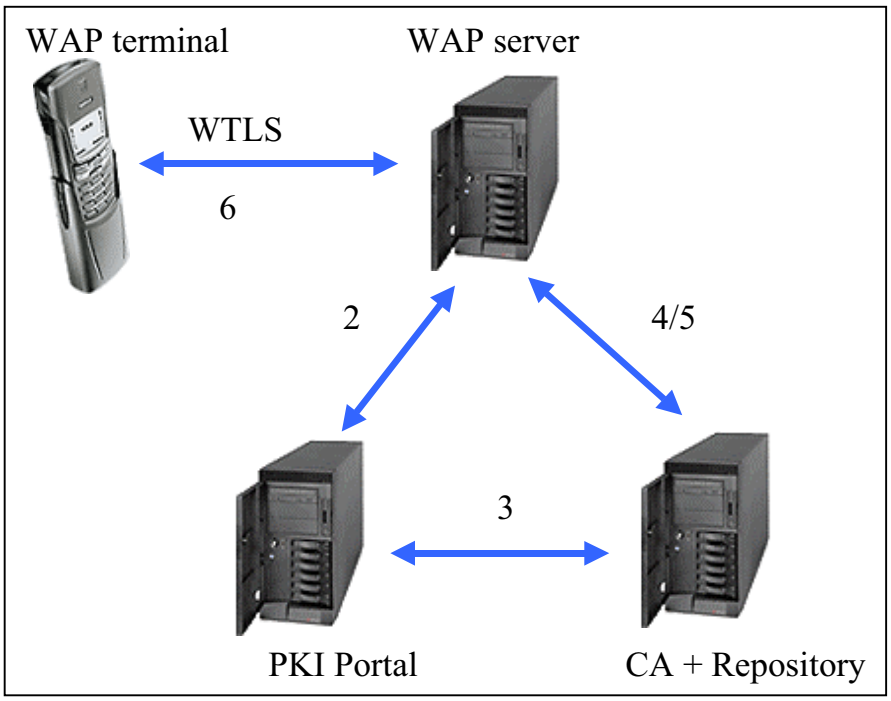


Figure 10 : End to end model

6.3.3 WTLS Class 3

This type of WTL requires both client and server authentication, because both client and server certificates are required. The WAP terminal authenticates the identity of the WAP gateway and the WAP gateway authenticates the identity of the WAP terminal, as well.

The NAME and the NAME.ES modules may be used for private signing, key storage and signature computation.

In this case, the client signs a challenge string from the WTLS server to authenticate itself. This is the method used in WMLScript to sing a message using the SignText method.

Following, we explain the authentication steps for WTLS Class 3.

The WAP terminal requests for a certificate from the PKI, and sends the request to the PKI portal. The PKI portal validates the identifier and forwards the request to the certification authority. The certification authority generates the digital certificate (User Certificate) and sends the certificate URL to the WAP device, where it is stored in the NAME module. Alternatively, the certification authority may send the complete certificate to the terminal. Eventually, the certification authority stores the digital certificate in the directory.

For authentication, the end-entity application running on the WAP terminal signs a string challenge and sends the string challenge, the signature and the Certificate URL (or the entire certificate) to the m-commerce server. The signature is done by the NAME.ES module.

The m-commerce server uses the Certificate URL to get the user certificate from the directory (if it does not possess it yet), and verifies the signed challenge string from the WAP terminal.

6.3.4 Specific secure aspects of GSM/WAP environment compared to fixed networks

This chapter describes specific secure aspects of mobile environment in comparison to fixed network. We have mainly focused in the Transport Layer Security compared to its mobile version, WTLS, and the certificate verification process, where the integration with the NAME/NAME.ES module is crucial to obtain the secure services required.

WAP architecture has been designed in order to be employed for the provision of data services to the users of portable devices such as mobile phones and PDAs. These services are assumed to be provided through a variety of wireless access networks with GSM being the most potential one, at least as far as imminent implementations are concerned. Therefore the data services provided over a WAP/GSM environment would reflect the characteristics of both GSM and WAP architectures. These characteristics of the convergence of wireless data and the Internet are subject to comparison to fixed networks, which have so far dominated in the field of data service provision.

6.3.4.1 WTLS versus TLS

Basically WTLS is only a miniature form of TLS. In functionality there is no much difference.

In WAP, the implementation of the requirements for secure mobile commerce, is made in the safety's layer WTLS (Wireless Transport Layer Security). WTLS provides the key security elements of confidentiality, integrity and authentication. WTLS is a security protocol based upon the industry-standard Transport Layer Security (TLS) protocol, formerly known as Secure Sockets Layer (SSL).

WTLS differs from TLS in some aspects: it supports datagram transports (e.g. UDP) and uses optimized handshake and data structures. There is provision for on-line key refresh that allows for long-living connections. WTLS offers data privacy through the use of a symmetric algorithm (RC5, 3DES, DES, IDEA), integrity using a MAC algorithm (HMAC with SHA-1 or MD5) and key exchange (using RSA, Diffie-Hellman, or ECC). In addition both points may engage in authentication procedures. There are three types (or WTLS classes) of authentication. Possible levels include:

- **Class 1**: Implies Anonymous Authentication, each party cannot be assured of the identity of the other party.
- **Class 2:** Implies Server Authentication, the client is strongly assured of the server's identity (and thus trusts them to send them confidential data such as credit card numbers).
- **Class 3:** Implies Client Authentication where the server is assured of the client's identity (and thus may allow them access to restricted resources for example). Normally a server that demands client authentication (for it is the server's interest to do so) will usually offer Server Authentication ensuring that both parties are authenticated to each other. Currently very few products support Client Authentication. In order to have authentication, the server and/or the client must possess a public key certificate. Normally these would be X.509 certificates, however the WTLS specification allows the server to use a WTLS certificate or an ANSI X9.68 certificate (currently in draft). The WTLS certificate is an optimised version of the X.509 certificate. The optimisations are to reduce the size and processing required for X.509. In the current

WAP model, WAP Gateways / Servers use WTLS Certificates to identify themselves and mobile device users use X.509 Certificates to identify themselves.

WTLS is intended for use with the WAP transport protocols and has been optimised for use over narrow-band communication channels by providing an optimised handshake (initiation of a secure session) through dynamic key refreshing. Dynamic key refreshing allows encryption keys to be updated on a regular and configurable basis during a secure session.

The conjunction of the PKI and the NAME/NAME.ES module, the security elements of verified authentication, authorisation and non-repudiation are provided (a powerful set of standards and policies, which manages keys and certificates, establishes a trustworthy network environment, and enables the use of encryption and digital signature services for several applications).

6.3.4.2 Certificate verification process

In a traditional PKI, for example X.509, the client performs all certificate processing. The client must obtain the certificate, obtain the certificate revocation information, parse the certificate, verify the signature on the certificate, check that the certificate contains the correct policy and naming information, and repeat the process for each certificate in the certificate path ending at a trusted root. While this is a reasonable model for a relatively unconstrained client, in a significantly constrained environment such as GSM/WAP, performing these operations may be a challenge.

Different solutions have been introduced in order to reduce or solve this problem. The first one is Online Certificate Status Protocol that allows a client to obtain revocation information from a central server about the certificate being considered. While parsing the OCSP response is simpler than parsing a CRL and the amount of information that must be retrieved is less, all the basic steps in validating a certificate remain. Other separate protocols have been proposed: the Simple Certificate Validation Protocol and OCSP extensions, such as Delegated Path Discovery and Delegated Path Validation. These protocols off-load the certificate validation operation to central servers. They are designed for general PKI use, so they are somewhat heavyweight with many options that do not apply to the wireless environment and, for the most part, they assume the client has access to and can parse the certificate to retrieve the desired contents.

Only two protocols address specifically the problem of resource-constrained handset devices:

1. WAP Security Group proposes a solution in which WTLS servers may implement the short-lived certificate model, as the means of satisfying revocation requirements. With this approach, a server or gateway is authenticated once in a long-term credentials period, typically one year. However, instead of issuing a one-year-validity certificate, the certification authority issues a new short-lived certificate for the public key, with a lifetime of, say, 48 hours, every day throughout that year. The server or gateway picks up its short-lived certificate daily and uses that certificate for client sessions established that day. If the certification authority wishes to revoke the server or gateway (e.g., due to compromise of its private key), it simply ceases issuing further short-lived certificates. Clients (in this case, WTLS servers) will no longer be presented with a currently valid certificate, hence will cease to consider the server authenticated.

2. The Wireless Application Public Key Access and Status Protocol (WAPKASP) is a simple, lightweight protocol in which the client simply provides an identifier for a certificate and the server responds with either the public key and name from the certificate (if the certificate is valid within a given PKI) or an error message (if the certificate is not valid). The client does not have to perform any of the tasks required for full certificate validation, including obtaining and parsing the certificate; it just has to make one simple request to a server.

7 Overall architecture and PKI services

On this section we are going to focus on the specific PKI architecture provided by different vendors. We explain in detail the architecture proposed by:

- Baltimore solutions
    - Baltimore UniCERT
    - Baltimore Telepathy
    - WPKI Baltimore Architecture
- Certicom suggested architecture
- Entrust solution
- Verisign solutions
- Nokia suggested architecture
- SmartTrust
- Microsoft Certificate Server

We also present in this chapter a generic PKI architecture for mobile devices.

We have focused in this section on the technical solutions, explaining in detail each solution. In the annex 2, Business survey, some more information, completing this part and with a commercial point of view can be seen.

7.1 Overall architecture, including communication and PKI infrastructures

The evolution of PKI services in wireless environments is rapidly advancing. The integration of the Internet and the mobile world needs technologies that can assure basic security functionality across technological boundaries.

The introduction of PKI in the current WAP architecture provides:

- Authentication of Web/WAP server, WAP gateway and WAP client;
- Access control and secure service access;
- Creation of a secure channel between the application server and the client that offers confidentiality, integrity and non-repudiation.

7.2 Baltimore suggested architecture: Baltimore solutions

7.2.1 Baltimore UniCERT

We will take a brief glance to Baltimore UniCERT solution for PKI.

UniCert is the Baltimore's solution for a Public Key Infrastructure. UniCERT is a software suite composed of the following components:

- Certification Authority (CA) signs and publishes certificates and CRLs. The CA operates according to its own policy, configured by the CAO.
- Certification Authority Operator (CAO) is the security officer of the PKI. It controls all the administration functions and grants privileges to other UniCERT modules.
- Registration Authority (RA) acts as a router between the users and the CA.
- Registration Authority Operator (RAO) approved certificate requests to be certified by the CA. Each RAO has rights to issue certificates according to policies that are configured by the CAO.
- Token Manager manages the different security and cryptographic functions of smartcards and HSMs (tokens).
- Gateway receives remote requests and returns certificates and informational messages. The gateway may interwork by email or a web interface (HTTP).

The first four components are mandatory to set up a minimum configuration of UniCERT.

All these components can be added, removed, modified or upgraded depending on the PKI operator. We could run different components in the same machine or in different ones to balance the workload.

There must be Oracle databases installed to store data such as:

- Activity logs
- Certificates issued
- Certificates revoked
- Declined certificate requests
- Etc.

There is an optional LDAP component. UniCERT requires a LDAPv3 compliant server.

CA configuration

The CA runs as a NT service. It is in charge of managing:

- The period of validity of the CA's keys. They can be generated for RSA or DSA with a maximum length of 2048 bits.
- The way of handling CRLs
- The definition of the LDAP and the OCSP server
- Etc.

UniCERT supports the following sources to generate keypairs:

- Software
- RACAL 722
- PKCS#11 Tokens
- PKCS#11 Smartcards

PKI Scheme

The CA is in charge of the PKI scheme configuration. UniCERT software suite provides with a graphical tool to create the layout. This is achieved by adding, removing components in the graphical tool. The components are CAs, RAs, CAOs, RAOs, DataBases, Gateways…

Security policies

The CAO establishes the rules and characteristics that apply to a category of certificates:

- Certificate validity period
- Signed key length
- Hash algorithm…

UniCERT supports two different groups of security policies:

- Face to Face Certificate Request: the requestor attends physically the RAO and requests for a certificate.
- Request sent remotely: this is the case when a form is exposed over the Internet to request for a certificate via web, or when a SSL server requests for a certificate.

The RA and the RAOs can be distributed anywhere in a network. Each can have different security policies and administer certificates in different ways.

Administration and operation of a UniCERT CA is made with the CAO. The CAO creates new policies, drops others, modifies the PKI schema and adds new RAs and RAOs. The CAO permits viewing all the certificates issued by the CA and optionally revoke any of them.

7.2.2 Baltimore Telepathy

Baltimore Telepathy is the Baltimore's wireless e-security architecture based on Wireless PKI (WPKI), handsets and smartcard (S/WIM) technologies quickly constructing a WPKI for Mobile Operators, Financial Institutions and Enterprise customers. It allows enrolment of up to 100 users. Telepathy solution includes:

- Software development kits to enable secure sessions between applications;
- Gateway solutions providing unbroken security from a mobile phone to a WAP server;
- Set of digital certificates solutions for authenticating digital identities;
- Digital signature toolkits to enable the processing of wireless digital signatures.

There are several Baltimore solutions for WPKI, categorised depending on possible organisations:

- Telepathy for network operators
- Telepathy for content providers
- Telepathy for technology vendors

The 'Baltimore Telepathy' architecture is designed to extend the existing PKI based security systems for wired systems to accommodate the new mobile users. It easily integrates with new and legacy applications and systems that are PKI aware, including

secure web, e-mail, e-commerce, e-business, payment and Virtual Private Network systems.

Telepathy is fully compatible with the UniCERT PKI architecture. Standard UniCERT modules and systems can be deployed to complement Telepathy based Wireless security systems.

The Telepathy Operator Solution provides the wireless PKI portal. It is a central system from which to manage trust services for customers and partners. This PKI portal acts as a gateway to Certificate Authorities, providing a manageable and scalable platform to process requests for user registration, certificate retrieval, signature verification, and certificate validation and user revocation.

The components of the Baltimore Telepathy solution are:

Baltimore Telepathy PKI Registration System (TRS) allows wireless users to seamlessly enter into a WPKI, providing their digital identities and the technology to bind them to their Digital Certificates. It enables users to authenticate themselves and participate in mobile commerce. TRS delivers two systems to suit any model of registration:

- Point-of-Sale/Channel System: A simple non-obtrusive solution for users and operators. Integrates with the subscription model during purchase of devices at retail outlets. Mobile users automatically register into a PKI when subscribing for operator services.
- On-line 'Over-The-Air' (OTA) System Advanced solution allowing users to register into multiple PKIs via a Web based interface accessed on the wireless Internet. Open and extensible framework based on providing a wireless PKI portal as defined in WAP Forum's WPKI specification.

Baltimore Telepathy PKI Validation System (TVS)

A unique digital certificate retrieval and validation system with minimal bandwidth and storage requirements, providing a seamless introduction of certificate IDs to mobile devices. It retrieves X.509 certificates using certificate IDs rather than the complete Digital Certificates, thereby allowing access to multiple certificates without requiring local storage.

KeyTools Telepathy m-Sign

A developer toolkit allowing to build systems to process wireless digital signatures. Digital signatures are used for authentication, confidentiality, integrity and non-repudiation. It implements the WAP digital signature specification, allowing content providers to receive signatures from mobile devices and verify their validity using a PKI.

This architecture solution also includes:

WAP Security toolkit:

It is a software development kit that allows an application developer to create secure encrypted session communications. It contains an implementation of WTLS. It allows secure encrypted sessions between client and WAP server of WTLS class 1 and class 2.

WST (WAP security toolkit) enables developers to build confidentiality, integrity and authentication into a system. Authorisation and non-repudiation can be achieved by integrating it with a PKI system. The WST has built-in functionality to do this.

The WST include fully configurable support for:

- Session caching;
- Security re-negotiation;
- Temporary key usage;
- Dynamic re-configuration during a session;
- Integration into datagram layers defined in the WAP specification i.e. UDP/IP and WDP.

WST supports a number of standards regarding the secure storage of private keys and digital certificates. It includes PKCS#1, #7, #8, #12, allowing private keys and certificates to be integrated into security applications. Smart cards and hardware tokens can also be integrated using WST (typically using a PKCS#11 interface).

WST support a wide range of public key cryptographic algorithms, which can be configured within its cipher suits:

RSA	DES, Triple DES
Diffie-Hellman	SHA-1
RC5	MD-5

WTLS Gateway:

It provides WTLS authentication, confidentiality and integrity as a stand-alone application independent of the gateway/server. It acts as a WAP Server, listening on the two reserved ports for secure WAP connections from clients. Port 9202 is reserved for connectionless WTLS, i.e. WTLS which uses WDP (Wireless Datagram Protocol) as the transport layer; port 9203 is reserved for connection oriented WTLS, i.e. WTLS which uses UDP as the transport layer.

There are plans for:

- Client authentication;
- Client Certificate look-up;
- Client certificate validation (CRLs, OCSP);
- Hardware security module support (e.g. smart cards);
- Telepathy Validation System Integration.

PKI registration system:

It is a server application for handling the registration of wireless users into PKI. It allows a fast and easy entry for wireless users into PKIs. It provides the technology to bind mobile devices users to their digital certificates stored in PKIs and the infrastructure for digital certificates, identities and signatures. It enables users to authenticate themselves and

participate in mobile commerce. This system can be used for both WAP and GSM/SIM phones.

PKI validation system:

It is a digital certificate retrieval and validation system, with minimal bandwidth and storage requirements. This system retrieves and validates using certificate identifiers rather than the complete digital certificate, requiring minimal storage on mobile device and low bandwidth.

Digital Signature Toolkit:

It is developer toolkit that allows content providers to build systems to process wireless digital signatures generated on the mobile device. WAP 1.2 specifies digital signatures in WMLScript. This toolkit implements that specification and allows content providers to receive signatures sent from a mobile device and verify their validity using a PKI.

WAP certificate Authority:

It is based on the existing wide range of UniCERT modules for wired users, it is an extension to produce WTLS Certificates.

WAP certificates:

WTLS server certificates for server authentication is available from Baltimore Technologies as part of the Telepathy range. There are plans for clients certificates.

7.2.3 WPKI Baltimore Architecture

We are going to depict one of the possible Baltimore architectures that can be implemented to provide a secure m-commerce environment based on PKI. We will try to match the PKI infrastructure explained in the epigraph 5 with the corresponding Baltimore configuration.

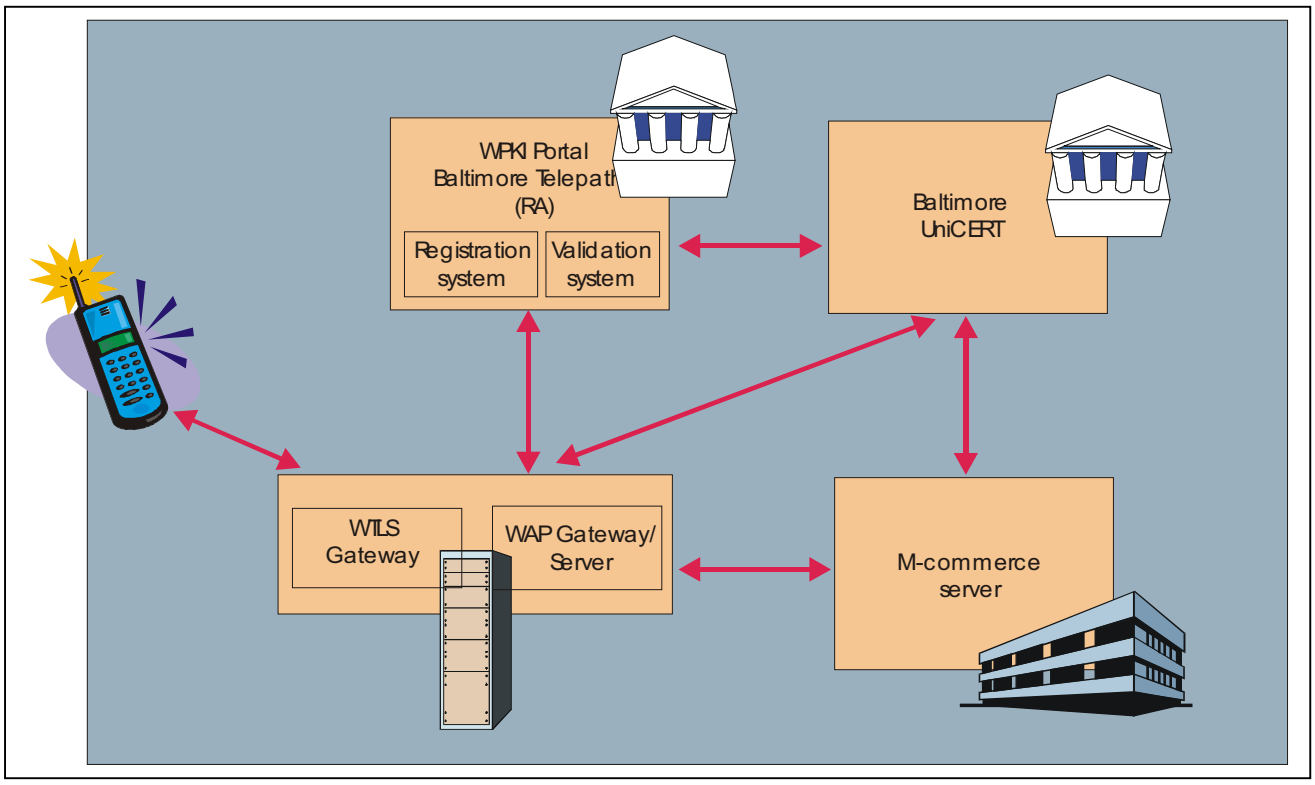


Figure 11: Baltimore WPKI Architecture

Following this architecture, the mobile terminal seamlessly enters into the network operator through a WAP gateway, and into the WPKI through the WPKI Portal composed by the Baltimore Technology software suite. This product acts as a gateway with the Certification Authority, which can be implemented by Baltimore UniCERT solution.

While the mobile terminal comes across the WPKI through Telepathy, the enterprise providing e-business may access through the conventional Baltimore UniCERT RA.

7.3 Certicom suggested architecture

Certicom current proposal for a global PKI architecture is based on "MobileTrust™". This is a managed certificate service that delivers a comprehensive set of tools and services to provide a complete security solution for the mobile computing environment. It provides standards-based digital certificate services that support client/server authentication and privacy for mobile device users. The system offered can act as a global Certification Authority for wireless applications, and in addition, enable enterprises to form secure communities of trust. One distinctive feature is the design of tools, products and services that provides an integrated ECC-based (Elliptic Curve Cryptography) public-key infrastructure. ECC employment maximises the performance of mobile devices and servers by accelerating the processing of cryptographic calculations, reducing bandwidth usage and decreasing battery requirements.

This PKI is completed with a package of tools and products to offer a comprehensive solution; the whole set comprises products for authentication, VPN, development and hardware components.

Authentication is based on:

- MobileTrust™: the above-mentioned infrastructure for issuance and management of digital certificates.
- Trustpoint®: the following set of software components, products and tools for PKI development and deployment.
  - Trustpoint® Registration Authority: a complete, scalable, and highly configurable solution for implementing PKI registration authority subsystems (RA/PKI Portal).
  - Trustpoint® Certificate Authority: a standards-based certificate issuance and management platform for creating, issuing, publishing, and revoking public-key certificates to both servers and mobile clients. The CA is hosted in a highly secure and reliable facility to ensure guaranteed service.
  - Trustpoint® PKI Toolkits: a set of object-oriented components for public-key certificate creation, consumption, and life cycle management. Tools are available in two different technologies: Trustpoint/Java provides comprehensive Java classes and implement online certificate management protocols including CMP, Trustpoint/C provides rich C and C++ interfaces.
  - Trustpoint® Administrative Console: an application used to configure system policies and perform other administrative tasks.

VPN is based on:

- Handheld VPN Client: a product specifically designed for handheld devices that targets interoperability with popular VPN gateways and supports the IPSec security standard. It allows organisations to easily and securely incorporate popular mobile and wireless devices into sensitive corporate VPNs.

Development is based on:

- Security Builder®: a complete suite of algorithms for developers to easily integrate encryption, digital signatures, and key exchange mechanisms into applications running in servers, desktops and new class of handheld and wireless information appliances. The toolkits are available in Java and C technology.
- SSL Plus: a toolkit that provides for plug-and-play integration, enabling developers to add SSL functionality rapidly and with confidence to their networked applications and embedded systems. SSL Plus supports a broad range of encryption algorithms in SSL protocol versions 2.0 and 3.0 and TLS version 1.0.
- WTLS Plus™: a toolkit providing for plug-and-play integration of WTLS functionality to WAP servers and client devices. It combines ECC, SSL and embedded platform expertise to offer highly efficient client and server software, totally compliant with the official WTLS specification.
- Smart Card Developers' Toolkit: a toolkit that allows an application to make use of Certicom's smart cards via a standard interface such as Security Builder API or PKCS#11.

Hardware components are based on:

- Smart Cards in two different versions: SC-400 series smart cards are designed to provide end user identification and authentication services based on ECC. SC-500 series smart cards are personal enterprise authentication tokens.
- Certilock™: a PCI based security module that provides permanent storage for secret and private keys in a tamper resistant/tamper evident housing. Cryptographic operations using the secret and private keys are performed by the processor on the Certilock without revealing the values of the keys to the host system. The Certilock Security Module is ideally suited for high security applications, including Internet secure servers, secure messaging platforms, certification authorities and secure payment gateways.

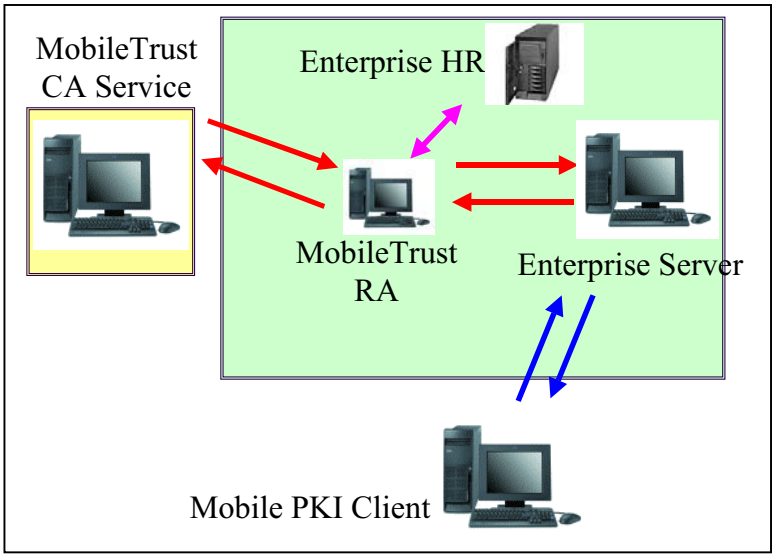


Figure 12: Certicom MobileTrust architecture

7.4 Entrust solution

7.4.1 Entrust Authority

Entrust Authority generates and manages keys and public key certificates, and provides management of Internet security across applications including through wireless devices. This product is made up of customizable software modules that can be configured to match the organization's security policies without interfering with how end users work.

The following components are mandatory to set up a minimum configuration of Entrust Authority:

- Security Manager: it is the Certification Authority to generate and issue X.509 public key certificates.
- Third-party Directory: Certificates are stored in and managed by the LDAP-compliant directories.
- Security Manager Administration: enables information security operator to add and delete users, revoke certificates, specify password rules, generate reports, and perform key recovery operations.
- Entrust Entelligence Desktop Manager: it is a client-side software that provides full key and certificate life cycle management to Web browsers and servers through software enhancements.

The optional module that can be included is:

- Enrollment server for WAP: it provides certificates for Wireless Application Protocol (WAP)-enabled mobile devices such as cell phones and personal digital assistants

(PDAs). It allows Security Manager to issue certificates enabling Wireless Transport Layer Security (WTLS) in wireless environments.

7.4.2 Entrust architecture

One of the various deployments Entrust provides is shown in Figure 13. Entrust Authority provides a full Public Key Infrastructure for any type of terminal. The WAP terminal retrieves its digital certificates from the Enrollment Server for WAP. On the other hand, the m-commerce server (ISP) gets the digital certificates directly from the core of Entrust Authority. Entrust authority enables the use of digital signature, digital receipt, encryption and permissions management services across various applications.

Entrust also provides additional components that give other security facilities like these:

- M-validator: it is a security application that enables the validation of digital certificates used during mobile transactions.
- M-register: it is a security application that provides end users with a way to acquire digital certificates to be used for mobile transactions.

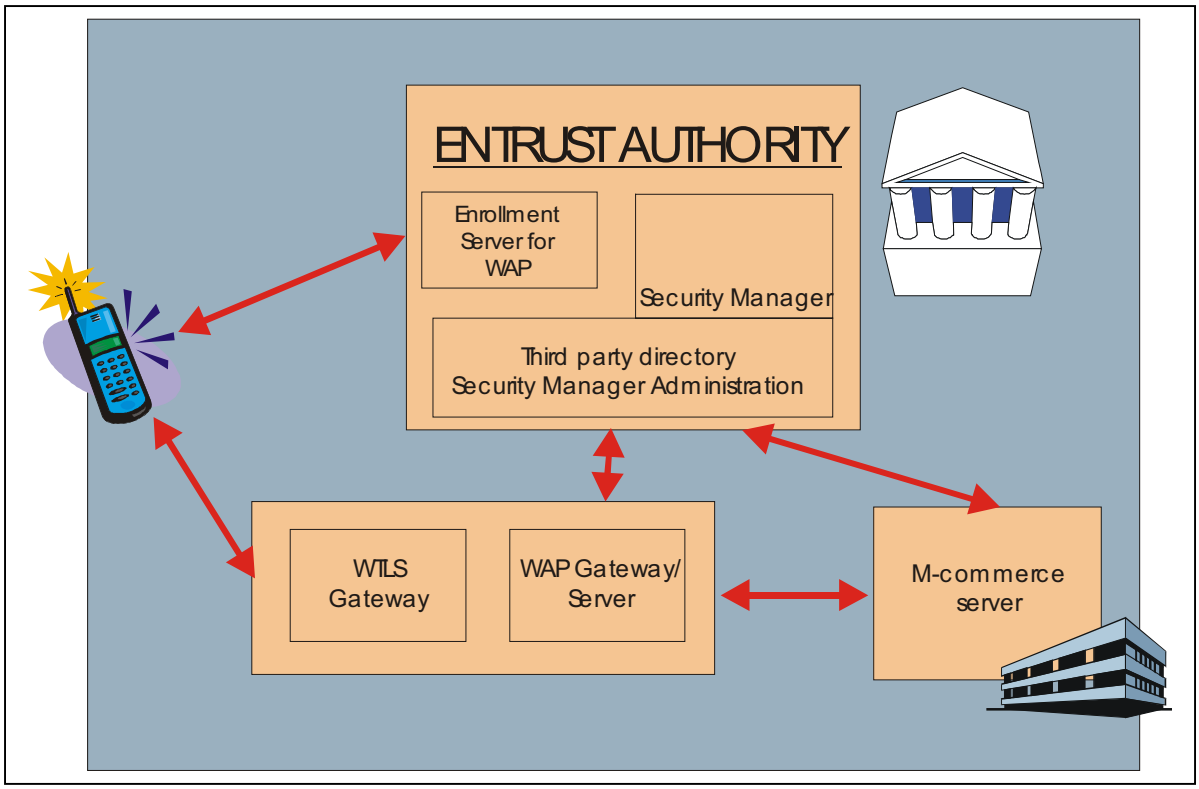


Figure 13 : Entrust Proposed Architecture

7.5 Verisign solutions

7.5.1 Verisign wireless managed PKI service

VeriSign Wireless Managed Public Key Infrastructure (PKI) service is a fully integrated wireless PKI platform designed to secure wireless intranet, extranet, and Internet applications by combining maximum flexibility, performance, and scalability with high availability and security. The service allows an enterprise or wireless operator to quickly and cost-effectively establish a robust wireless PKI system, comprising a Registration Authority (RA) and Certification Authority (CA) system, with complete control over security policy, PKI hierarchy, authentication, and certificate lifecycle management.

- Customized Certification Authority Management: VeriSign provides advanced Web-based configuration wizards, administration and support tools, report generators, and application integration modules, to give an enterprise or wireless operator full control over its CA and to provide the critical link to VeriSign processing centres. VeriSign capabilities provide full support for end-user registration and certificate renewal, with screens customized to a company's specific look and feel for each application.
- Lifecycle Management Control: Management of the certificate lifecycle process is performed through the VeriSign Control Centre, giving the enterprise or wireless

operator full control over the registration and authentication process. Functions such as revocation, audit, and day-to-day management can also be distributed to an unlimited number of administrators, providing complete separation of administrative roles. VeriSign provides extensive audit trails and reporting capabilities along with auditable security practices—all features that support non-repudiation of certificate-based transactions.

Components in the Verisign Solution:

- Wireless PKI Portal: The wireless PKI portal enables certificate enrollment for users and devices, and can optionally populate these issued certificates into an LDAP-compliant database.The wireless PKI portal also automates the registration authoring functions, allowing transparent authentication of users or devices directly from pre-existing administrative systems or databases.
- Verisign certificate processing centre: VeriSIgn issues the certificate on behalf of the enterprise or operator.
- LDAP server where the issued certificates are stored. This element is not mandatory.

7.5.2 Versign Architecture

Following the patterns of the previous architectures here discussed, we will try to trace a parallelism with the architectural schema shown in chapter 5.

In this figure we can see that the WAP terminal accesses the network operator's or enterprise's enrollment page and requests for the digital certificate. Then, the WAP gateway redirects the information to and from the WAP terminal and application server via secure WTLS and SSL/TLS sessions.

The Verisign PKI Portal approves the request for the digital certificate and forwards it to Verisign Certificate Issuance Service. This is made by a TLS session.

The Verisign Certificate Issuance Service is placed in the Verisign Certificate Processing Center, and it is there where Verisign issues the certificate on behalf of the network operator or m-commerce enterprise.

The request is sent back to the PKI Portal, and it stores the digital certificate to an LDAP directory.

Eventually, the PKI Portal delivers the digital certificate or an URL pointing to the certificate to the user's device via the WAP gateway.

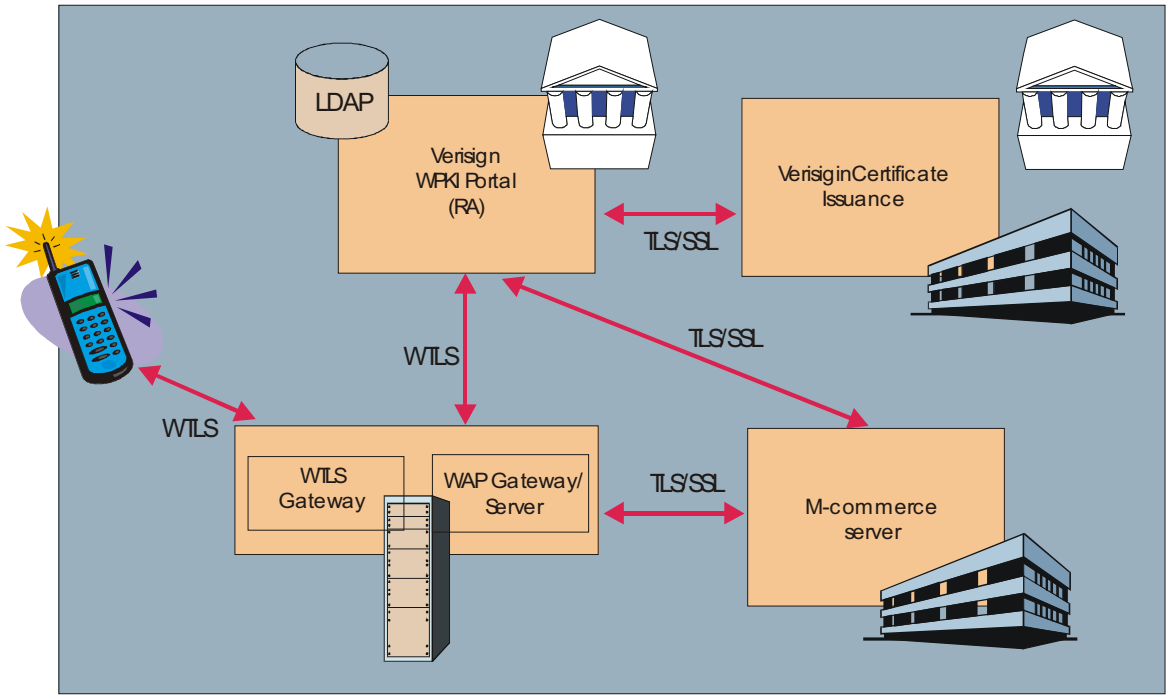


Figure 14: Verisign proposed architecture

7.6 Nokia suggested architecture

Processes

The architecture should provide a framework for processes needed for

1) deployment of the mobile e-commerce system including end user terminals and
2) supporting the every day use of that system.

These processes include for example:

- Root certificate delivery to end user terminals;
- Certificate enrolment (End entity, WAP Gateway, ISP);
- Certificate lifecycle management (End entity, WAP Gateway, ISP);
- Support for operative service use by providing validation service.

WPKI support

The architecture should be based on open standards and compatible with WAP/WIM capable terminals. The architecture should consist of different subsystems, which can be used all together or independently to provide full WPKI support to mobile e-commerce service providers. This support includes the following features:

- Strong authentication of both business sides (WTLS Class 3);
- Certificate validity check and user information to application level;
- Digital signature creation and check;
- User certificate creation support with integration to PKI portals.

Overall system architecture

The suggested overall system architecture comprises the following elements:

WAP Gateway with WTLS class 3 and SSL support.

IP Network with SSL support or, alternatively VPN support.

ISP running secure Service Application(s).

PKI comprising at least CA, RA, Directory and CRL functionality.

Validation Server for online validation of signatures and certificates. Validation Server is capable of accessing the Directory and the CRL of the Telco/CA as well as those of third parties.

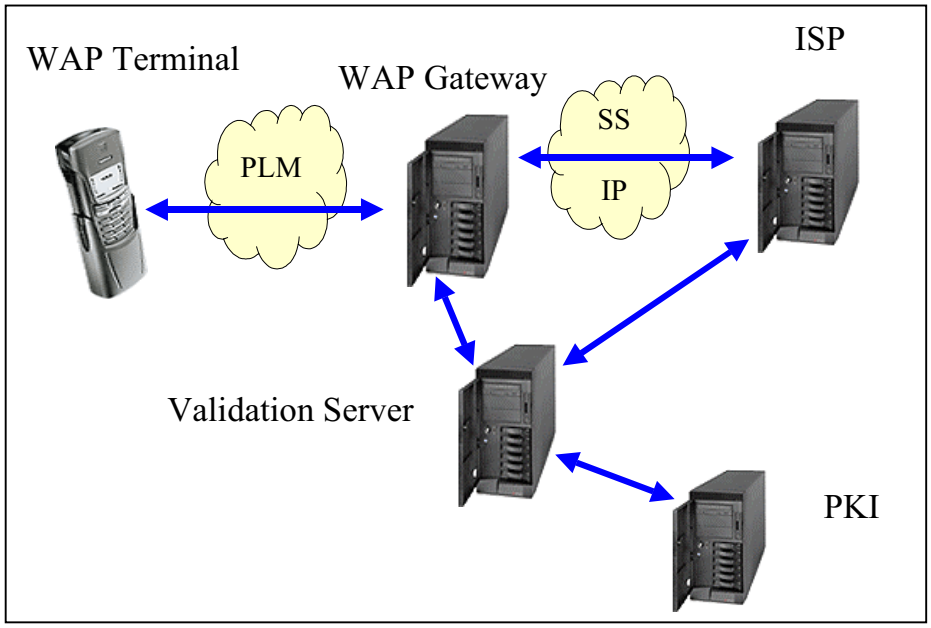


Figure 16: Nokia system architecture

Key and Certificate distribution

Distribution of certificates and keys is not shown in the figure. The ISP and the WAP Gateway receive their certificates from the PKI online.

Terminals can carry root certificates, key pairs and EE certificates (or URLs to certificates). Those can be distributed for example during personalization process of the SWIM or using the WAP PKI specified PKI Portal environment.

Authentication

With WTLS class 3 capable terminals the authentication is handled by the WAP Gateway with the help of the Validation Server according to the WTLS class 3 specification.

Signature creation and validation

The WML Script Crypto Library specification provides means for end user signature creation and validation.

7.6.1 Available Nokia product features for WPKI deployment

WAP Functionality

- WAP 1.1.compliant
- Nokia WAP Protocol Stack with WTLS implementation
- Class 1 and Class 2 WTLS implementation

Security Algorithms

- Asymmetric cryptography: RSA and RSA anon
- Bulk encryption: RC5
- MAC algorithm: SHA-1

Bulk Encryption Algorithms

- 56-bit key length for symmetric algorithms (Security Pack 56-bits)
- Up to 128-bit key length for symmetric algorithms (Security Pack 128-bits)

Asymmetric Encryption Algorithms

- Up to 768-bit key lengths for asymmetric algorithms (Security Pack 56-bits)
- Up to 1024-bit key length for asymmetric algorithms (Security Pack 128-bits)

Secure Socket Layer (SSL) Encryption

- HTTP connection from Nokia WAP Gateway using SSL encryption

WTLS certificate management

- Creating self-signed server certificates and certificate signing requests
- Installing certificates signed by trusted Certificate Authority organizations

Planned new product features include for example:

- Client authentication (WTLS class 3)
- Validation of signatures and certificates
- On-line access to Directories and CRLs

7.7 SmartTrust

SmartTrust PKI is mainly focused in the use of smartcards. The main difference between PKI services offered by SmartTrust and the others is that SmartTrust pre-personalizes smart cards using PKCS#15 or SEIS profiles. Other vendors support the use of smartcards and tokens using the pre-personalization made by the smart card manufacturer. This approach requires the smart card manufacturer to provide the libraries which implement the PKCS#11 API. SmartTrust implements its own PKCS#11 and CSP modules for a great variety of smartcards. The RA front ends have been integrated with card printers, so with the Smart Trust Software it is possible to make a complete personalization of the smartcards. Software certificates are also supported and can be used as virtual smartcards.

One of the weak points of SmartTrust PKI is that it does not support key backup/recovery.

SmartTrust provides a module which pre-personalizes smart cards creating PKCS#15 or SEIS profiles and then the key pairs are generated in the smartcard so it is not possible to extract them. This is the behavior required with digital signature and non repudiation keys, but it is a problem when encipherment services must be provided. If the smartcard is stolen or gets damaged it is not possible to recover the encrypted information. To support key backup, the encipherment key pair should be marked as extractable (some smart cards do not allow to do that) or the key pair should be generated in software, backed up and then stored in the smartcard.

7.8 Microsoft Certificate Server

Microsoft Certificate Server is an integral part of Windows 2000 Server technology. It is provided as an add-on component of Win2000 Server and Advanced Server products. MSCS enables an enterprise to exploit PKI and X.509 based applications and services, and fulfils its security demands for authentication, authorization, confidentiality and data integrity.
Microsoft first introduced Certificate Server in NT 4.0 platform including it as an extra component in the NT4.0 Options Pack. In Windows 2000 Server platform Microsoft refers to the new Certificate Server 2.0 as Windows 2000 Certificate Services, providing it as an optional component.

There are two ways that the product can be valued. First as a standalone set of services, and second as an integrated component of Windows 2000 Server platform.
As a standalone product it can provide services such as key generation, certificate request generation and certificate issuing to the PKI system. Certificates can be delivered via a variety of mediums such as smartcards, floppy disks and the Web. Multiple mediums can be supported by using the suitable Cryptographic Service Provider (CSP). Currently there are CPSs for various smartcards and cryptographic tokens that can be used in combination with MS Certificate Server.
As part of Windows 2000 Server, Certificate Services are enhanced with Active Directory and other add-on components integrated in the platform.

7.9 Services Comparison

This chapter provides an overview of how the various PKI offerings provide the required services for a PKI. Each offering has a column, telling which services are in the offering, and which are not. Notes following this table identify any specific issues that may be relevant. We have only focused in the following offering:

- Entrust
- VeriSign
- SmartTrust
- Microsoft Cert.Server
- Baltimore UniCERT

Required Service	Entrust	VeriSign	SmartTrust	Microsoft Cert.Serv	Baltimore UniCERT
key pair generation	X	X	X	X	X
Certificate request generation		(4)	X	X	X
Certificate request validation	(1)	(4)	X	X	X
Naming	(1)	X	X		
Certificate issuing	X	X	X	X	X
PIN + PSE Distribution (on-line, smart cards, floppy disk, USB tokens, etc.)	(2)	X	X	X	X
Directory Service	X	X	(7)	X (9)	X
Certificate Verification Services	X	X	X	X	X
Key Archiving	X	(5)		(8)	X
Key Backup	X	(5)		(8)	X
Key recovery	X	(5)		(8)	X
Non-Repudiation			(6)		
Certificate (un)suspension	X	X	X		X
Certificate revocation validation	(1)	X	X		X
Certificate revocation / CRL updating	X	X	X	X	X
Time-stamping	X (3)	X			X

NOTES:

1) **Entrust**: The service is present as an in-built function of the product, it is integrated in a more global functionality of the product, but cannot be invoked as such.
2) **Entrust**: Token support: although Entrust PKI supports the use of tokens from release 4, the performance is reportedly poor.
3) **Entrust**: Timestamping is supported with the product Entrust/Timestamp.
4) **VeriSign**: Certificate request generation/validation is done by the RA. VeriSign has such RA's in many countries. Companies may become an RA by associating themselves with VeriSign and complying with the conditions VeriSign has set in their policies.
5) **VeriSign**: Key archiving, backup, and recovery are part of the optional Key manager module for use with On-Site. VeriSign itself does not store private keys.
6) **SmartTrust** PKI does not provide a non repudiation service, but when issuing smartcards, one of the keys generated is marked as a non repudiation key. Keys are pre-generated in the KGS module inside the smartcard when possible, so no backup, recovery or archiving services are provided.
7) **SmartTrust** does not provide a Directory Service but can use any LDAP v2 compliant server.
8) **Microsoft Certificate Server**: The above table lists the basic services that Microsoft Certificate Server provides after the installation, with little or none further tuning. More services such as Key Archiving and Key Recovery can be embedded using MS CryptoAPI. This of course implies programming skills from the deploying party.
9) **Microsoft Certificate Server**: Directory Services are provided through Microsoft's Active Directory. General LDAP integration is also viable with little effort.

8 Business requirements

In this point we are going to discuss what the business requirements on the authentication and electronic signature modules for the network operators are, what their constraints are, what the economic elements which would make the use of such modules viable and better than other solutions are.

8.1 General secure m-commerce requirements

General requirements for secure m-commerce that can be solved with the conjunction of a Public Key Infrastructure and NAME and NAME.ES modules are:

- Confidentiality of transactions between mobiles and e-commerce/e-business sites
- Authentication of wireless e-commerce and e-business sites to consumers and businesses
- The secure delivery of credit card information between mobiles and e-commerce sites
- The secure delivery of transactions between the wireless e-business sites and the backend systems
- Secure remote access to Internet connections over wireless networks using wireless PC modems.

8.2 Business requisites

There are a number of elements that make the usage of these modules leverage certain market segments.

Following we explain the business requirements that must be matched for network operator and e-commerce service providers, and we will see how NAME and NAME.ES modules fulfill with these requisites.

Economic elements and hence the business requisites required for network operators and e-commerce service providers that make the use of authentication and electronic signature NAME and NAME.ES modules profitable and better than other implementations are:

- **Personal security.** NAME and NAME.ES modules provide personal security since they are thought to reside in certain environments such as smart cards, portable by a certain user. Non-repudiation is assured, since NAME.ES enables digital signing, fundamental part for non-refusing. Digital signatures cannot be forged and access control cannot be violated. Digital signatures cannot be compromised, since they are signed with the private key contained in the modules.
- **Portability.** Its usage in mobile devices, these modules are running on portable terminals enabling millions of people to access to the Internet and commerce chances.
- **Mobility.** These modules have the ability to securely store and transport public/private keys anywhere. They provide secure Internet commerce sessions from Internet kiosks in universities, malls, airports, amusement parks, and even cafes and coffee shops. It may be an element for globalisation and European integration.

- **Immediacy.** They support access to real-time services over the Internet with the added value of security. The NAME and NAME.ES modules are portable in a smart card and therefore can be placed in any mobile device permitting accessing services anytime.
- **Ubiquity.** Permitting their usage in mobile devices, the desired services may be reached remotely from almost any place on the world. The NAME and NAME.ES modules are portable in a smart card and therefore can be placed in any mobile device permitting accessing services from almost anywhere.
- **Cheap solution.** NAME and NAME.ES modules are thought to run on a plastic chip. This is a non-expensive component.
- **Interoperability with hardwired applications.** There is support of newer applications for smart cards to secure transmissions with SSL (e.g. Netscape has been developing new APIs to smart cards in Communicator suite and so has Microsoft) in personal computers and mobile devices. In the future, many more applications are supporting interoperability with smart cards.
- **Easy support of secure protocols to commerce through the network.** The personal digital certificate is a means for exchanging public keys and providing two parties to a transaction with positive identification verified by a mutual, trusted third party. From these certificates, each will know the other's public key in order to communicate securely. The merchant's web server to provide entry to access-controlled web pages may also use the client's digital certificate. Web server authentication can be simplified through the usage of digital certificates instead of basic password protection.
- The secure use of paid services leverages **small-value purchases**, enabling relatively secure means of small payments through smart cards. Using these modules to secure payment, users need not to carry change.
- **Securing e-cash.** NAME and NAME.ES modules give support for secure transmission of monetary exchange on smart cards. Clients' advantage is that smart cards are suitable to use on travel to foreign destination where tourists do not typically have a local bank account to draw from. It can be used by children and the destitute who typically do not maintain bank accounts. Advantage for countries where a well-developed back-end financial infrastructure for processing credit card transactions does not exist. It may be part of e-cash methods such as CAFE, DigiCash, CyberCoin, Modex, Visa Cash…

To summarize, the two main advantages to be considered to adopt these modules as a means to get better business chances are:

- They facilitate the commerce over the Internet providing secure methods to exchange sensitive data.
- Portability, ubiquity and immediacy provided by the means they are carried, i.e., a tiny smart card.

8.3 Market segments

According to the previously defined economic elements we can find the market segments that may be benefited from the usage of NAME and NAME.ES modules and the reasons why every market segment should adapt them:

- **Internet Service Providers**: especially for mobile commerce service providers.

- They secure end-user services and provide reliability to users. The number of services is expected to grow rapidly.
- Support the security of end-user applications. Service providers therefore will benefit from the ability to market their secure services to millions of Mobile Internet-enabled device users.

- **Network operators**:
  - Provides network security in their networks and when interworking with other network operators by means of a proper PKI supporting NAME and NAME.ES modules. The number of network operators is expected to grow rapidly. Network operators need to interwork with partners and other network operators in a secure way.
  - Operators will be able to get new markets and obtain benefits from technologies like WAP and GPRS.
  - They may provide an e-commerce portal to provide security and payment services to merchants.
  - Network operators need to protect their information systems and databases.
  - Network operators need to provide a seamless global security for their customers, using a PKI supporting NAME and NAME.ES modules.

- **Financials**: the benefits they can get come from:
  - They will be benefit from the increase of the number of transactions made due to e-commerce processes. This is because of the higher reliability of the users on the secure transactions.
  - The mobile devices will be a channel for m-banking and m-commerce and a lot of tailored services.

- **Consumers**:
  - They benefit from the trusting relationship with technology, and from the acquisition of new secure services providing them with new facilities of m-commerce, m-banking, etc.
  - They also benefit from the usage of secure e-cashed to trust in and transactions based on stored-value payment systems.

8.4 Business requirements related to Multiapplication systems

It is a business requirement that NAME and NAME.ES modules must live together in the same smart card because of different reasons. One reason is simply to save card slots in the hardware where the modules are integrated. It would be impossible to have over two slots in a wireless terminal, by instance, one for NAME module, other slot for a business application and other slot for the SIM, etc.

Other important reason for a general multiapplication application system is that it could be a synergy between applications that can be useful to save resources or even more, to make the whole application work.

In order to permit any business on wireless terminals, it is required that these terminals or card readers work with smart cards supporting a multiapplication operating system, i.e., that several applications can live together in the same smart card.

The multiapplicative card holds personal information about the user, and the customer is afraid that this information could be seen when s/he is using the card for other purposes. The multi-application operating system must guarantee that applications must not know sensitive information if they are not allowed to. The operating system must follows a security model.

The price of a multiapplication system should be cheap if we want it to be successful. This has been a problem for the issuers, since they have traditionally been very expensive. There should be a common infrastructure that reduces the costs and makes the usage of the smart card increase.

The sharing of the card for many applications involves that costs of these multiapplication smart cards reduces, because also the cost is shared among organization placing their different applications in the same smart card. From our point of view, an enterprise programming a light m-commerce applet over a smart card could place its application in the same card where NAME and NAME.ES modules are placed. It could make use of our modules to secure communication and transactions, then sharing the price of the smart card with the issuer of the multiapplication smart card.

The usage of multiapplicative cards allows a certain business model to save costs, since other applications may be reusable if they are interoperable. Modules can be developed to be interoperable with applications in a way that these modules perform generic functions. This way, they could be used as DLLs for applications.

To achieve this, one issue should be solved. The applications or modules in a multiapplicative card should be interoperable. They should work together seamlessly they had been developed from different vendors.

Another point is the allowance of the issuer to download certain applet to the multiapplication card. The application provider should have any kind of authorisation from the issuer to get his application downloaded. The multiapplication operating system should only allow applications signed by the issuer to be downloaded, so that the application provider could also share the costs of the multiapplicative card, because s/he is using some space in that smart card.

There are some business requirements concerned with the actual short-term in business deployment. Those are growth and security. It is a business requirement that the number of business cases based on smart cards increases, since online revenues come from the amount of business models from the one hand, and from the number of users of those business models based on cards, on the other hand. Apart from it, security is a prime concern in business requirements. As online revenues increase, the fraud will be more frequent, and means to avoid fraud should be taken into account in relation with multiapplication smart cards.

There are many applications that can live together with our security modules and profit from the advantages of our security modules. A business requirement for the success of the NAME and NAME.ES modules is that there were many applications that could use them. This could be leverage if many applets could be downloaded in the same card and these applications could interoperate each other and with the security modules. In order to reach this situation, new business models should be created to generate new business opportunities and benefit from the fact of interoperable modules in a multiapplicative card. Additional modules providing other functionalities different from security should be created to generate certain synergy with the existing modules in order to get a better benefit from this interactivity.

9 Functional and interface secure requirements in a GSM/WAP environment.

9.1 Functional requirements

As we have explained, a complete security framework, and therefore the PKI in conjunction with the NAME and NAME.ES modules, to provide a secure mobile commerce must meet the following requirements:

- Authentication of origin and recipient: knowing whom you are communicating with, provided that with Digital Signatures.
- Confidentiality: knowing that communications are private and confidential. Provided by Encryption and/or Digital Envelopes
- Integrity of contents: knowing the information being communicated is correct and has not been modified. Provided by Digital Signatures
- Non-Repudiation: knowing that agreements can be legally enforced. Provided that by Digital Signatures, Certificates and Time-stamping.

In a GSM/WAP environment, security functionality can be supported by PKI services, supporting NAME/NAME.ES module in:

- The protocol WTLS (Wireless Transport Layer Security), used for the creation of an encrypted channel between the WAP mobile phone and WAP Gateway, through provision of keys and certificates;
- Application level security, accessible using the Wireless Mark-up Language Script Crypto Library, through provision of keys and certificates.

WAP Certificates

A certificate for WAP needs to be reduced, but without loss of the functionality that make the certificate meaningful and useful. The certificate must identify the holder of the public key and also provide a secure binding between the key and its holder.

The WAP Certificate should work interchangeably with other X.509 certificates in certificate-processing Internet applications in order to leverage the existing infrastructure.

Certificates issued in conformance with recommendations and requirements will be reasonably compact, and mobile devices are required to handle certificates of size up to at least 700 bytes.

Requirements of a WAP User Certificate

- Certificate Serial Number: CAs claiming conformance with this specification should avoid using serial numbers longer than 8 bytes.
- Signature Algorithm: the only algorithms defined for signing the certificate are **sha1withRSAEncryption** (signature calculated according to [PKCS#1[1]]) and **ecdsa-with-sha1** (signature calculated according to [X9.62[2]]).

[1] [PKCS#1] RSA Laboratories, "PKCS#1 RSA Encryption Standard", version 1.5, November 1993.

- Subject Public Key: the only admissible public keys are **rsaEncryption** and **id-ecPublicKey.** RSA keys should be 1024 bits or longer. ECC public keys should be 160 bits or longer. Certificate-processing applications are not required to handle keys longer than 2048 (RSA) or 163 (ECC).

Other security requirements for a GSM/WAP environment are common to a wired environment. It means that the services provided by a PKI, supporting NAME/NAME.ES module, for a wired environment should be provided for a wireless environment.

Here's the list of the services provided by a PKI:

Certification Services:

This set of roles relates to the issuing and management of digital certificates:

Table 3: Certification Services

Activity	Description	By who (*)
Key Pair Generation	Generation of a public/private key pair.	KGA
Certificate Request Generation	Generation of a certificate request.	KGA
Certificate Request Validation	Validation of a certificate request by means of: verification of public/private keys matching, additional authentication of the subscribing entity, verification of entity's right to obtain a certificate.	RA
Naming Authentication	Name a subscribing entity and/or validate the proposed naming of the subscribing entity by checking a dependable source of information.	RA
Certificate Issuing	Issuance of the certificate.	CA

[2] ANSI, "The Elliptic Curve Digital Signature Algorithm", ANSI X9.62 working draft, September 1998.

Activity	Description	By who (*)
PIN + Software PSE Distribution	Distribution of a single PIN + PSE pair. Properly code cryptographic credential of an entity into a Personal Security Environment, to protect it with a Personal Identification Number and to securely deliver them to the intended entity	KGA
PIN + PSE on Tokens (smart cards, floppy disk, USB tokens, etc)	Distribution of a single PIN + PSE pair. Personalise a secure hardware token with the cryptographic credential of an entity, to protect it with a Personal Identification Number and to securely deliver them to the intended entity.	KGA
Directory Service (certificate validation services)	Storage and publication of the certificates, the IDs, and the certificate revocation list. Provide status on the validity of certificates.	DIR
Certificate Suspension/ Unsuspension Validation	Validation of the suspension request related to a specific entity certificate.	SRA
Certificate Revocation Validation	Validation of the revocation request related to a specific entity certificate.	SRA
Certificate Suspension/ Unsuspension	Perform the suspension/unsuspension related to a specific entity certificate.	CA
Certificate Revocation and CRL Updating	Perform the revocation related to a specific entity certificate and update the CRL.	CA

Complementary Services:

This set of roles relates to the provision of trust services used in the processing of business transactions.

Table 4 : Complementary Services

Activity	Description	By who (*)

Time-stamping	Provision of a tamperproof notation that indicates the correct date and time, a unique reference and the identity of the initiator (person or device) of an action.	TSA
Help Desk	Information point capable of accepting and handling help requests about services provided by the trust centre.	HD
Camouflaging	Concealing the communications and frequency of data flows between parties.	CS
Key Archiving	Safe storage of cryptographic keys.	KA/RA
Key Recovery	Safe recovery of decryption keys.	KA/RA
Notarisation (e.g. non-repudiation)	Provision of protection against the threat of denial by one of the parties involved in a communication. Notarisation may provide some of the following kinds of services: Proof of origin Proof of posting Proof of delivery Proof of simultaneous signing of contracts	NA

(*) The entities likely to provide these offerings are:

KGA	Key Generation Authority
RA	Registration Authority
SRA	Certificate Suspension/Revocation Authority
CA	Certificate Authority
DIR	Directory Management Authority
TSA	Time-Stamping Authority
HD	Help Desk
CS	Camouflaging Service
KA/RA	Key Archiving and Recovery
NA	Notarisation Authority

9.2 Interoperability requirements

The following table presents a list of interoperability issues dealing with the particular aspects of the GSM/WAP environment. The intent is to identify the specific algorithms, data formats and services that are not part of a PKI designed for a traditional wired network.

Table 5 : WAP interoperability requirements

Requirement	Description	Minimum/ Desirable
WAP certificate and CRL profiles	Special profiles for client and CA certificates may be used to accommodate a X.509v3 certificate to the WAP unique requirements.	Compatibility with the specific profiles
Alternative certificates	WTLS and X9.68 certificates should work seamlessly with any WAP gateway/server.	Compatibility with different certificate formats.
Certificate URL	Client certificates can be stored in a special network repository; the client sends only a certificate pointer to the server.	Compatibility with URL pointer instead of complete certificate.
Short-lived certificate	WTLS server certificate with validity limited to typically one day.	Issuance of new server certificates daily.
PKI portal	Integration with the portal, that is the interface between the CA and WAP clients/servers/gateways. The portal is an entity performing RA and/or CA functions.	Provision of an entity that offers a set of basic PKI services to all WAP actors.
Digital signature format	The signature is represented in a WTLS special version of PKCS#7 (compressed header)	Conversions from and to the WTLS encoding format.

10 Business Model for PKI/Smartcard/NAME&NAME.ES

10.1 Introduction

Following the context of the project, this section documents a business case approach that can be utilized by organizations considering an investment in Public Key Infrastructure (PKI) on smart cards, in conjunction with the NAME and NAME.ES modules, for its applications. The methodology presented on this section will help organizations in building business models that examine using smart cards and integrating the NAME/NAME.ES modules in concert with a PKI in order to provide a secure method to be used for authentication, access control, and electronic commerce (e-commerce).

By following the business case methodology presented in this document, decision makers will be able to determine for themselves whether the investment costs for PKI/smart cards are justified and whether investment benefits outweigh the risks. Decision makers are also given guidance on evaluating the economic impact of alternatives, comparing alternatives, and ultimately monitoring the investment.

E-commerce represents a radical change to the way business has been conducted. To support this radical change, the organizations are being required to increase overall network security including providing information assurance. Electronic authentication issues are leading many organizations to consider PKI/smart cards as a probable solution to the security challenges presented by e-commerce. While it is possible to use PKI without smart cards or vice versa, this section focuses on the joint use of PKI and smart cards, in order to integrate the NAME/NAME.ES modules.

This document provides an approach for determining the costs, benefits, and risks of PKI/smart cards. A brief discussion of alternative technologies is also provided.

10.2 Business Case Methodology

Business case analyses often give some comments to the following points:

- Environmental factors influencing the investment decision.
- Technical, business, and regulatory factors related to the technology being investigated (i.e., PKI/smart cards/NAME&NAME.ES).
- Feasible alternatives can meet the business and process needs of the organization.
- Relevant costs associated with each alternative.
- Realistic life of the technology (e.g., PKI/smart car/NAME&NAME.ES) and can costs and benefits accurately be predicted over this time period.
- Cost risks associated with the estimates.
- Relevant benefits associated with each and have all those associated benefits been quantified/assessed?

The following points explains the mains steps needed to be followed to compose a business model, based on the cost, benefits and risks.

- **Analyze the Current Environment and Assess Affected Areas**

The first step is to conduct an analysis of the current environment and an study of affected areas. It is critical to understand the current business processes and technologies in place and to determine the shortfalls or deficiencies associated with the current environment. Environmental study can include reviewing technology inventories, architectures, business processes, etc. Almost every investment, either in facilities, personnel, technology, or knowledge affects numerous parts of the organization. Organizational implications (costs and benefits) must be assessed. Understanding how a potential organizational change impacts the current environment is critical to evaluating the return on investment and the expected short and long-term values of the project.

Data needed for this and all other steps of the business case analysis can be collected through a number of mechanisms including:

- Financial analysis of program data
- Documentation review
- Survey responses from the stakeholders
- Market research
- Interviews.

- **Establish a Baseline and Set Targets for Improvement**

To obtain the relevant costs and associated benefits of implementing PKI/smart card within an organization, a baseline for comparison must be established. This can be done by comparing the findings concerning the current environment with stated objectives for an organization. The outcome of the comparison enables shortfalls of the current environment to be determined and opportunities for change to be identified. By doing this, an organization demonstrates why it needs PKI/smart cards rather than other technologies. The discussion should point to business drivers, security drivers, and technology drivers that led to the conclusion to pursue this solution.

- **Identify Viable Alternatives**

In this step, all options to achieve an organization's stated information assurance goals should be captured. At this stage, many alternatives can be considered. Cost and feasibility should not preclude an alternative from consideration.

- **Determine the Costs**

The costs of continuing the current process and each of the viable alternatives need to be calculated for a determined period of time (e.g., 10 year life cycle). To do this, a cost element structure needs to be created as a framework for equitable comparisons. This structure should be designed specifically for PKI/smart card initiatives.

- **Determine the Benefits**

Benefits and cost savings/avoidance need to be identified for continuing current operations and for each of the viable alternatives. The business case assumes varying levels of benefits for each alternative in addition to varying costs.

- **Determine the Risk**

The purpose of a risk analysis is to focus the decision maker’s attention on the financial, technical, and schedule risks associated with the alternative under study and to counter-

balance positive financial indicators with real-world factors that could keep the alternative from reaching its estimated potential. Identify the risks associated with the PKI/smart card investment so that they can be managed and controlled.

- **Evaluate the Economic Impact of the Investment**

When all of the cost components have been identified, the current situation should be compared with the viable alternatives. Examples of economic impact indicators include cost savings, cost avoidance, return on investment, payback period and cost benefit ratios.
It is important to remember that the specific financial measures used to evaluate the investment are simple calculations based on complicated assumptions. For example, in estimating the costs, are desktop system upgrades that were needed for other purposes included? Or the implementation of a new directory service that has value for applications other than PKI? It is often very difficult to isolate the costs of PKI in itself. Given this, every effort should be made to ensure that estimates fully state the assumptions on which they are based.

- **Compare and Recommend an Alternative**

After the economic impact of each alternative has been established, the alternatives can be compared with one another as well as with the current situation, and an investment recommendation can be presented.

In the following sections we are going to explain with more detail the points of: analysis of the environment, explore the different possibilities, determine the cost, benefits and risks. We will conclude with the best option. In other words, we will demonstrate that the implementation of a PKI/smartcards/NAME&NAME.ES is the best option.

10.3 Environmental Study and Alternatives

10.3.1 Environmental Study

An environmental study should be performed by mapping representative current processes to the operating environment. These maps will be used to demonstrate how PKI/smart cards/NAME&NAME.ES are needed for a company against other technologies. The discussion should point to business drivers, security drivers, and technology drivers that led to the decision to pursue PKI/smart cards/NAME&NAME.ES. For example, a case for change may be based on:

- Need to improve security posture within the company
- Requirement to comply with legislative, executive, and organization guidance
- Ability to accomplish mission

10.3.1.1 Improve Security Posture

Organizations must improve their security posture by ensuring the integrity and confidentiality of their data, validating all users who wish to access data, and by providing a means for digital signatures that cannot be repudiated at a later date. For example, digital signature provides an audit trail which allows one to determine which user performed a specific action, and under whose authority that action was performed. The security

improvements realized through the use of digital signature provide organizations and their stakeholders greater confidence in the integrity of their systems and the accuracy of their data. Further, organizations will be confident that their data is being used as intended. Without these improvements in security posture, organizations will not be able to become a true competitor in the new e-commerce economy.

Digital certificates provide a means for authenticating transacting parties over the Internet, and thus conducting business with confidence over the Internet. Public key technology enables digital signature functionality that provides authentication of electronic data for a wide variety of applications. The use of digital signature without public key technology may compromise authentication and lack non-repudiation capability. Further, a single infrastructure provided by PKI supports both digital signatures and confidentiality (preferably using two different key pairs and certificates). As a result, many organizations are inclined to use public key technology as a solution.

10.3.2 Information Assurance Alternatives

Although this document focuses on PKI/smart cards and therefore NAME/NAME.ES, it is possible to achieve aspects of authentication, data integrity, confidentiality, and non-repudiation using other technologies. Other security protection alternatives include bar code cards, magnetic stripe cards, PIN/password, non-PKI-enabled smart cards, and biometrics. Although all of these alternatives provide some means of information assurance, only PKI provides a high degree of assurance in all areas. When technologies are layered by using the technologies in combination (e.g., PKI, PIN/password, and biometrics), a greater degree of assurance can result. Figure 17: shows the relative costs, benefits, and potential applications of each (potential) alternative. The technologies introduced in Figure 17: to help organizations build a broad range of information assurance alternatives into their business case.

	Mediums/Technologies	Token	Reader	Infrastructure	Non-repudiation	Authentication	Data integrity	Confidentiality	Scalability	Portability	Interoperability	Efficiency	Data storage capacity	Logical access- network access	Physical access- building access	e-commerce -stored value
Static	Bar Code Card	€	€€	€	L	L	L	L	L	H	H	M	L	N	Y	N
Static	Magnetic Stripe	€	€€€	€€	L	L	L	L	L	H	H	M	L	N	Y	Y
Updateable	PIN/password			€	L	M	M	L	L	H	L	L		Y	Y	N
Updateable	Smart card	€€	€€	€€	M	M	M	M	H	H	H	H	H	Y	Y	Y
cryptographic	PKI			€€€	H	H	H	H	M	L	M/H	H		Y	Y	Y
cryptographic	PKI/smart card	€€	€€	€€€	H	H	H	H	H	H	M/H	H	H	Y	Y	Y
cryptographic	PKI/smart card With biometrics	€€	€€€	€€€	H	H+	H+	H+	H	H	H	H+	H	Y	Y	Y

H	High
M	Medium
L	Low

Y	Yes
N	No

Figure 17: Viable Alternatives for Information Assurance Solutions

In Figure 17:, three mediums of technology are compared: static (cannot be changed), updateable (can be changed), and cryptographic (can be both changed and programmed). The technologies are listed in order from least secure (bar code cards) to most secure (PKI/smart cards with biometrics). For each technology, the relative cost of a token,

reader, and infrastructure is scored. The color schematic uses green for most desirable (lowest costs), yellow for desirable (modest costs), and red for least desirable (highest costs). This matrix shows how cryptographic technologies deliver the most security and operational benefits to organizations, albeit at a higher cost.

In addition to cost, Figure 17: scores the benefits of each technology. First, four security benefits are evaluated according to each technology: non-repudiation, authentication, data integrity, and confidentiality. These benefits map primarily to PKI. The second section of benefits concerns operational and business benefits realized more through the use of smart cards. These benefits include scalability, portability, interoperability, efficiency, and data storage capacity. Technologies yielding the least benefits were scored red; those with some benefit were scored yellow; and those with the most benefit were scored green.

The columns entitled “Applications” at the top right of Figure 17: show the potential uses of the technology for logical access to networks, physical access to buildings, and electronic commerce. 'N' denotes limited, if any, application and 'Y' denotes extensive application.

We explain briefly each of the technologies compared:

10.3.2.1 Bar Code Card

A bar code card is a standard credit-card-sized device with a printed code used for recognition by a bar code scanner. The scanner reads bar codes and converts them into either the ASCII or EBCDIC digital character code. Bar code cards are used for applications that require personal or product information. Although bar code tokens are inexpensive and highly portable, they do not offer security benefits (e.g., authentication, and data integrity).

10.3.2.2 Magnetic Stripe Card

A magnetic stripe card is a standard credit-card-sized device that adheres to standards approved by the International Standards Organization (ISO) to encode digital data on a magnetic strip that is embedded on the card. Data is written on and read from the stripe by a number of types of readers at the time of transaction. Currently, magnetic stripe cards are used for applications such as banking, retail, telephone systems, access control, airline ticketing, and transit fare collection. The life span of a card will vary depending on its intended use. For example, a card may be intended for one-time use (e.g., a subway pass) or for thousands of transactions; however, the typical magnetic stripe card must be replaced in less than two years.

10.3.2.3 PIN or Password

PIN and password technologies are commonly used for numerous Internet and intranet applications due to the fact that these technologies are relatively inexpensive and easy to implement. However, PIN and password technologies are considered to offer only a weak form of authentication. Most users select passwords that are common words and thus susceptible to dictionary attacks. If the PIN or password is either meaningless or really long, it will be harder for the user to remember. As a result, users will write it down or

store it on their computer making it easier for imposters to obtain. Users also tend to use the same PIN or password for different applications. Therefore, if an imposter obtains a user's PIN or password, the imposter can gain unauthorized access to multiple applications. Good PIN and password policy can mitigate some of these problems, but enforcement is still difficult at the user level. Passwords phrases are becoming more commonly used as they are easier to remember but more difficult to decipher. Additionally, policies can mandate frequent updates to PINs or passwords.

10.3.2.4 PKI

PKI has already been explain in full detail in previous section of the document, here some general details are provided, but for more information we reference to the corresponding section.

PKI is the use of public key cryptography, which employs an algorithmic function to create two mathematically related or complementary “keys”, and the PKI technology can be used to deliver functionality such as authentication, data integrity, confidentiality, and non-repudiation. Public key technology uses a public key and a private key to mathematically scramble data. The private key cannot be determined from the public key. One key is used to encrypt the data, while the other key is used to decrypt it. The key itself is actually a series of numbers/bit strings. One key is public and made available to a trading partner, and the other is kept private and is maintained only by the user.

As an infrastructure, PKI comprises Certificate Authorities (CA), Registration Authorities (RA), PKI-enabled applications, policies and procedures, certificate management services, and directories that provide security features such as message integrity, key recovery, data privacy, signature verification, and user authentication. Each public key is made public in the form of a digital certificate where a trusted party, a CA, cryptographically binds the public key to one’s identity by digitally signing the certificate, thus ensuring any attempts to alter the data will be detected.

A CA manages the following:

- Certificate life cycle (which involves issuing the keys)
- Key revocation when a private key may have been lost, stolen, or made public
- Notice as to which key pairs have been revoked.

Registration authorities register subscribers into a particular CA’s domain. Directories are established that contain the public encryption keys and certificates that are used in verifying digital certificates, credentials, and encryption.

PKI supports digital signature functionality that provides integrity of electronic data for a wide variety of applications. A “digital signature” is derived from the data in combination with the private key and is normally appended to the data that is digitally signed. To verify the signature, the signer’s public key is applied to the digital signature. The signing operation is a two-step process: First, the signer hashes the data to a fixed size value. The signer then subjects this value to a private-key operation. Verification is also a two-step process: The verifier hashes the data to the fixed size value. The verifier then examines the value, the transmitted signature, and the signer’s public key. If the signature matches the

hash value and key, the signature is "verified." Digital signatures provide both proof of authenticity and verification of data integrity.

10.3.2.5 Smart Cards

Smart cards are credit-card-sized devices that carry an embedded microprocessor and memory that can store and process information. When inserted into a card reader, the smart card transfers data to and from applications. It is more secure than a magnetic stripe card and can be programmed to cease functioning if an incorrect password is entered more times than the preset limit. Smart cards have a wide range of applications including electronic purse, logical and physical access control, health care, telecommunications, and transportation.

Smart cards can be integrated in both physical and logical access control systems. A physical access control system is an automated system that controls an individual's ability to access a physical location, such as a building, parking lot, office, or other designated physical space. A logical access control system is an automated system that controls an individual's ability to access one or more computer system resources, such as a workstation, network, application, or database.

Smart cards may use three levels of logical access control:

- The association of a set of privileges with a user's password, and the ability to control access to files on the card based on those privileges (also called file access security)
- The ability to detect and respond to a sequence of invalid access attempts with a self-locking mechanism
- The "logical channel"—a logical link between the host system and a file on the smart card.

The use of smart cards for logical access augments the traditional PIN/password logon process.

PKI/smart cards offer an enhanced level of security that includes authentication, confidentiality, data integrity, and non-repudiation. Files may be readable but not writable or vice versa and only accessible within the card. Files may be protected by one or several passwords (PIN) or biometrics.

Also, PKI/smart cards offer an enhanced level of security because public/private keys can be generated, stored, and used to make digital signatures or encrypt data all on the card. This provides a much higher level of security than non-PKI enabled smart cards that store keys on a floppy disk or hard drive and are, therefore, more susceptible to tampering, removal, or duplication. Additionally, the portability of the public/private key pair and digital certificates enables users to take advantage of the benefits of PKI at any location where they are an authorized user.

10.3.3 Appropriate organization to implement PKI-enabled Smart Cards

A profile of characteristics that would indicate if a particular organization is a good candidate for PKI/smart card is presented below. If an organization possesses these characteristics, in part or in whole, it should investigate how this technology could benefit the company as well as consider the applications that could be enabled by the smart cards.

Organizations that deal with sensitive data and therefore have a great need for a high level of security are prime candidates for cryptographic smart cards.

- **Data Integrity.** If an organization's performance relies on the accuracy of its data, PKI/smart cards/NAME&NAME.ES should be considered because they enhance the data integrity. Data integrity relates to the reliability of data and ensures that data has not been tampered with. An organisation depending on reliable data would benefit from using PKI/smart cards.
- **Confidentiality.** An organisation that maintains confidential data (including financial and medical data) is a good candidate for implementing PKI/smart cards/NAME&NAME.ES and where maintaining confidential data is crucial to delivering high-quality customer service to its millions of beneficiaries.
- **Authentication.** Most organisations have a significant need for authentication or the verification of the identity of a user who is logging onto a computer system.
- **Internet-Based Transactions.** The amount of business transacted over the Internet also is a factor for organisations considering the use of PKI/smart cards. The use of electronic signatures is surging. It is given to the electronic signatures the same legal weight as hand-written signatures and recognizes e-commerce as a legally binding transaction. As electronic signatures are used to submit forms over the Internet, the need for a higher level of security is greatly increased.
- **Need for Interfacing with other companies.** An organisation that has a high level of interaction with other companies should explore the use of PKI/smart cards.
- **Mobile Workforce.** An organisation with a significant part of its workforce at multiple locations would benefit substantially from the use of PKI/smart cards. Possible functionality that would benefit this user group includes logical access and physical access. Additional benefits are gained by the PKI-enabled encryption of data on laptops, making them inaccessible to unauthorized personnel.

Following this requisites we conclude that this system is very adequate to the Telcoms companies.

10.3.4 Other Considerations

When an organization has decided to implement PKI/smart cards/NAME&NAME.ES, it must seek answers to the following questions:

- What functionality should be included?
- How will the keys be managed?
- How will the infrastructure be structured and maintained?
- How will the cards be maintained?

10.4 Cost Analysis for PKI/Smart Cards/NAME&NAME:ES

A business case is incomplete without a well-documented section on costs. Most investment decisions rely on the cost analysis as a significant factor in the final decision.

This section presents the cost for each possible alternative and the conclusions based on these data.

10.4.1 Cost Structure

This section identifies the cost elements associated with PKI and smart cards. Each company must determine its actual requirements to forecast the specific cost of PKI/smart cards for the company. General cost information is provided here.

Standard Cost Element Structure:

Planning, application enabling, and operational capability are the three most significant costs categories associated with PKI/smart cards.

We will only focus on the application enabling costs that cover program management, hardware, software, support, and include:

- Program management
- Toolkits
- Application upgrades
- Installation/modifying applications
- Smart cards
- Card readers
- Card issuance workstations
- Test and evaluation
- Support and helpdesk
- Upgrade/product improvement/refresh.

10.4.2 Costs of PKI

Because there are both subtle and large differences among organizations, a uniform formula for determining cost of implementing PKI in every organization cannot be recommended. Certain organizations will have the capacity to include the cost of PKI in their IT budgets, while others may not. Some will have the capacity to implement and maintain the PKI with their existing IT personnel, while others will have to outsource such expertise. This will alter the cost of PKI for an organization as well. Some organizations may have the secure facilities that house a CA, while others will have to construct such a facility.

All of the foregoing considerations will alter costs; however, certain common factors have to be considered in computing the cost. For example, the number of Registration Authorities (RA), CAs, and directories that will be required will have to be determined.

The software upgrades and purchases that will have to be made as a result of this implementation also factor into the overall cost.

Another common factor is to decide whether existing IT resources can be leveraged for the PKI implementation and maintenance or whether these will have to be purchased or

contracted for. The resource requirements associated with the planning, deployment operation, and on-going maintenance of the infrastructure must be defined. Policies and procedures necessary to support external users or external organizations must also be defined. The results of these and other analyses can help organizations for new PKI infrastructure costs as part of the normal IT upgrade budget.

If the PKI is meant to be interoperable, it is essential that a standards-based product and vendor be selected. Without the use of standards, interoperability problems may arise later and would be costly to correct. Liability protection is essential in many cases, especially when interoperability is required with external users or other PKI domains.

10.4.3 Incremental Costs for Increased Levels of Security

This section presents a notional example of an organization that is trying to decide what level of security it needs, what are the costs, and what level of benefits can be achieved at each level of security. We present four options, in order to compare them with the solution we propose: PKI/smartcards/NAME&NAME.ES. This example is based on certain assumptions. They are as follows:

- The organization has 10 000 employees.
- Physical access requires 1 000 readers and all employees will use cards for logical access. Therefore, 11 000 readers will have to be purchased under options 1, 2, and 3, which provide physical and logical access. The cost of a physical access reader is 200 € under all four options.
- Cost of infrastructure in this example includes the cost of standing up PKI, the cost of issuing stations, cost of purchasing kiosks, etc.
- If an organisation requires a commercial off-the-shelf (COTS) middleware package, an additional licensing fee of approximately 75 € per seat will be incurred.
- Overhead and program management costs are assumed to be the same for all organizations.
- The cost of readers, tokens, and infrastructure is based on vendor cost data collection.

10.4.3.1 Option 1—Organization Opts for Magnetic Stripe Cards

This section shows the costs of purchasing a magnetic stripe card solution only. Because magnetic stripe cards can be used only for physical access, just 1 000 readers need to be purchased.

Table 6: Total Cost of Magnetic Stripe Cards

	Unit cost	Quantity	Total Cost
Cost of tokens	0.25 €	10 000	2 500 €
Cost of network readers	200 €		
Cost of building access readers	200 €	1 000	200 000 €
Cost of infrastructure	50 000 €		50 000 €

Total cost of Option 1			**252 000 €**

Table 7: Advantages and disadvantages for Magnetic Stripe Cards

Advantages	Disadvantages
▪ Inexpensive	▪ The network access is impossible with this option. ▪ Magnetic stripe cards offer no security features such as non-repudiation, authentication, data integrity, and confidentiality. ▪ Also, the magnetic stripe cards are not upgradeable and are not a highly scalable medium.

We conclude, that although this is a cheap option, it is not a good one, so we continue with our study.

10.4.3.2 Option 2—Organization Purchases Smart Cards without PKI

Table 8: Advantages and disadvantages for Smart Cards without PKI.

Advantages	Disadvantages
▪ From a functional standpoint, smart cards are better than magnetic stripe cards in many ways. ▪ Smart cards can store up to 100 times more information in them than a magnetic stripe card. ▪ Smart cards lend themselves to a wide range of operations, including financial, healthcare, and transportation. ▪ Both physical and logical access are possible with smart cards.	▪ The major drawback relative to this option is that these cards do not have the added level of security that PKI provides. ▪ PKI benefits such as non-repudiation, authentication, data integrity, and confidentiality are very limited with this option.

Table 9 shows the costs an organization would incur in implementing smart cards without PKI.

Table 9: Total Cost of Smart Cards without PKI

	Unit cost	Quantity	Total Cost
Cost of tokens	8 €	10 000	80 000 €
Cost of network readers	50 €	10 000	500 000€
Cost of building access readers	200 €	1 000	200 000 €

Cost of infrastructure	125 000 €		125 000 €
Total cost of Option 2			**905 000 €**

We conclude, that although this not an expensive option, do not offer very important features related to non-repudiation, authentication, data integrity and confidentiality, so we continue with our study.

10.4.3.3 Option 3—Organization Procures PKI/Smart Cards/NAME&NAME.ES

Table 10: Advantages and disadvantages for PKI/Smart Cards/NAME&NAME.ES modules.

Advantages	Disadvantages
▪ With this option, this organization will accrue all the benefits of using smart cards (physical and logical access, portability, upgradeable, and scalability) with the added layer of protection that PKI provides. ▪ PKI provides strong data integrity and confidentiality compared with smart cards without PKI. ▪ This feature is important because data integrity is critical if sensitive data is stored on smart cards. ▪ Of the technologies considered in this report, PKI provides the highest degree of data integrity. ▪ Information on the card will remain secure so long as no one has access to the private key. ▪ Al the advantages of the NAME&NAME.ES modules are also included.	▪ No main disadvantage is considered.

Table 11 shows the costs an organization would incur if it chose PKI/smart cards/NAME&NAME.ES to address business and security needs.

Table 11: Total Cost of PKI/Smart Cards/NAME&NAME.ES

	Unit cost	Quantity	Total Cost
Cost of tokens	15 €	10 000	150 000 €
Cost of network readers	75 €	10 000	750 000€
Cost of building access readers	200 €	1 000	200 000 €
Cost of infrastructure	200 000 €		200 000 €

Cost of issuing certificates	125 000 €		125 000 €
Total cost of Option 3			**1 425 000 €**

We conclude that this is a very good option, it has a very good security features with reasonable costs. Its features makes it a very good option for the Telcos companies.

10.4.3.4 Option 4—Organization purchases PKI/Smart Cards with Biometrics

Biometrics is the automated procedure for recognizing a person based on a physiological or behavioral characteristic. Examples of biometrics identifiers include fingerprints, speech, face, retina, iris, handwritten signature, and hand geometry. Biometrics can be used to either identify an individual as part of a known group or verify an individual against a single biometrics.

Biometrics technology provides a much stronger level of security than PKI without biometrics because it introduces another secure form of authentication. This higher level of security is the advantage this option would provide; otherwise, PKI/smart cards offer like benefits.

Table 12 shows the cost an organization would incur if it implemented a PKI/smart card and biometrics solution.

Table 12: Total Cost of PKI/Smart Cards with Biometrics

	Unit cost	**Quantity**	**Total Cost**
Cost of tokens	15 €	10 000	150 000 €
Cost of network readers	125 €	10 000	1 250 000€
Cost of building access readers	200 €	1 000	200 000 €
Cost of infrastructure	300 000 €		300 000 €
Cost of issuing certificates	125 000 €		125 000 €
Total cost of Option 4			**2 025 000 €**

We conclude that this is a very good option for its security features, but the costs are too high. So we recommend the third option, the security features are almost similar and the price is lower.

10.4.4 Conclusions

Magnetic stripe cards are the least expensive option; however, they provide no network security. Because a computer is valuable for the data it stores, logical (network) access is important. Clearly, the option with PKI-enabled smart cards and NAME&NAME.ES is more expensive than either option 1 or 2. However, representatives of many organizations

have clearly stated that a high degree of data integrity is required for the information that they plan to carry on their smart cards. In those cases, PKI/smart cards/NAME&NAME.ES is the best option. The additional protection afforded by biometrics may be required for some companies within certain departments that require a higher degree of authentication. For other organizations, however, the cost of biometric technology would outweigh the benefits.

10.5 Benefit Analysis for PKI/Smart Cards/NAME&NAME.ES

Benefits and cost savings/avoidance need to be identified for continuing current operations (the current situation alternative) and for each of the viable alternatives. The business case assumes varying levels of benefits for each alternative in addition to varying costs. To the fullest extent possible, an organization must identify and quantify benefits that will be derived from alternative investments made in implementing PKI/smart cards/NAME&NAME.ES. Benefits can be expressed as both quantifiable and non-quantifiable (also referred to as qualitative).

- Quantifiable benefits are those that can be assigned a numeric value, such as money, physical count of tangible items, or percentage change. Money valued benefits comprise cost reductions, cost avoidance, and productivity improvements.
- Non-quantifiable benefits include enhanced information security, consistency and compatibility throughout the enterprise, improved quality, enhancement of best practices, adherence to statutory and regulatory requirements, and enhanced modernization.

Quantifiable benefits are calculated by subtracting the cost of an alternative from the cost of baseline operations. The difference is the “savings” that is often referred to as return on investment. Three ways to maximize an alternative's return on investment include are minimizing costs, maximizing returns, and accelerating returns. A relatively small improvement in any of the three may have a major impact on the overall rate of return. A sensitivity analysis can be performed to identify the major cost drivers and assumptions and their affect on the alternative's estimated benefits.

We have to keep in mind that many benefits realized through an investment will be qualitative and will not lead directly to money savings. Improvements in customer service, regulatory compliance, security, and accountability are certainly recognized as benefits, but they rarely can be included in the money-valued benefits stream or return on investment measures.

PKI/smart cards/NAME&NAME.ES may be difficult to reliably and validly quantify in money units, so intangible benefits are vital to understanding the total implementation outcome. These qualitative benefits can be numerically scored by assigning a value to fully meeting, partially meeting, or not meeting stated business or functional drivers. The purpose of this section is to identify the potential benefits of implementing PKI as compared with the potential benefits of implementing only smart cards both with and without PKI. The NAME and NAME.ES modules are also considered with the smart card option.

10.5.1 Benefits of Implementing PKI

PKI permits an enterprise to take advantage of the speed and immediacy of the Internet while protecting business-critical information from interception, tampering, and unauthorized access through secure transactions. Proper management and use of public keys enable PKI to provide information assurance and an enhanced operating environment through authentication, data integrity, non-repudiation, and confidentiality. PKI also offers significant benefits in its interoperability and scalability.

10.5.1.1 PKI Provides Security Benefits Through Secure Transactions

PKI allows users to communicate securely by offering them controlled access to the intranet for all corporate information, such as human resource data, secure e-mail, and various applications. Unlike other information assurance solutions, PKI does not secure the network or communication link but rather secures the actual transaction through encryption. PKI facilitates the exchange of confidential data with business partners by enabling the creation of secure extranets and virtual private networks (VPN) that give select partners easy access to business-critical information stored on internal networks. Additionally, PKI allows the user to take advantage of secure e-commerce capabilities and helps organizations and companies instill confidence in their customers that they can safely purchase goods and services over the Internet.

Authentication.

Authentication is the process of reliably determining the identity of a communicating party, or in other words, verifying that a user actually is the one it/he/she claims to be. In the physical real world, a common method of confirming identification is to check a passport, driver's license, ID-card, or similar item. From an e-commerce perspective, it must be possible to verify the identity of the user remotely.

Authentication enables the recipient to determine who actually sent the message and whether that person is authorized to commit his or her organization to the transaction. Additionally, it grants network access to authorized personnel only. Authentication will facilitate a single sign-on capability to access multiple services. Electronic signatures will provide for authentication of online documents for purposes ranging from routing downloads to e-commerce transactions.

Data Integrity.

Data integrity is protecting against and preventing unauthorized modification of data. Implementing PKI technology will provide for enhanced data integrity. As a result, customers can be certain that data received is accurate and complete, and has not been altered or modified in any manner.

Nonrepudiation.

Nonrepudiation is the act of verifying the origin and/or issuance of a transaction or action. It ensures that the sender of data is provided with proof of delivery and the recipient is

provided with proof of the sender's identity, so neither can later deny having processed the data. It ensures that transactions over the Internet can meet minimum legal standards for electronic commerce and certifies the participants in the transaction (Digital signatures provide both non-repudiation and data integrity.).

Confidentiality.

PKI can be used to encrypt confidential data. Confidentiality ensures that information (e.g., customer data and intellectual property) is not disclosed to unauthorized persons, processes, or devices. Communicating parties can have confidence that data is not viewed, intercepted, or modified by anyone other than the party the message was intended for. Confidentiality is especially important when considering medical data and financial information.

10.5.1.2 Interoperability

Interoperability can be achieved between two organizations when PKI policies are defined. The security of the PKI technology relies on the protection of the subscribers' private keys. Therefore, recommended PKI solutions will be capable of distributing both certificates and public/private key pairs in a variety of media. Recommended PKI solutions will utilize a single certificate, one that is trusted by all entities, and may be used for multiple organizations or multiple applications thus alleviating the problem of distributing secret keys. This process also simplifies the users registration by decentralizing the registration function. Users who may be strangers to each other can use the CAs to establish a "chain of trust" and interact securely with each other. Building PKI on standards will further promote interoperability.

Bridge Certification Authorities.

Bridge CAs permit different PKIs to be linked. The bridge CA is a nonhierarchical hub between several participating CAs. All CAs that choose to interoperate with a bridge CA will have the ability to interoperate with each other. The proper use of a bridge CA can demonstrate interoperability on several levels: between CAs, between directories, and between e-mail users. Perhaps the most useful benefit of a bridge CA is that it offers policy interoperability in addition to technical interoperability. Further, organizations can circumscribe risks by excluding certain subtrees that they do not want to interoperate with.

10.5.1.3 Scalability

The use of PKI technology facilitates "many to many" relationships. PKI enables the use of the same technology for a wide range of applications. PKI creates a trustworthy environment for e-commerce transactions and secure communications over the Internet for both individuals and organizations. The standards-based directory structure can grow as the user base grows.

10.5.2 Benefits of Utilizing Smart Cards

PKI certificates can be stored on smart card tokens. Smart cards have become widely accepted due to the high level of security the card provides compared with PKI certificates stored on a hard drive. Additionally, smart card applications are developed based on standards and using advanced and proven technology. Like PKI, smart card technology also offers significant benefits in its interoperability and scalability, but unlike PKI, also offers portability.

10.5.2.1 Portability

The small size of the smart card allows for people to carry large amounts of pertinent information on an updateable medium with relative ease. Portability is an important benefit that the small size of the cards facilitates.

10.5.2.2 Interoperability

Systems can be designed so that a single smart card has the ability to access multiple services, networks, and the Internet. Smart cards have a wide range of applications including, but not limited to, electronic purse, logical and physical access control, healthcare, telecommunications, and transportation. Using a single card to access all of these applications greatly simplifies the logon process for users and administrators alike. Additionally, using the smart card for multiple applications enables cost efficiency to be realized and implementation costs to be shared across the applicable departments.

10.5.2.3 Scalability

Applications can be scaled using smart cards. Smart cards are scalable with regard to the number of users, number of applications, and the number of certificates. This feature permits organizations to expand their smart card usage as necessary without incurring significant additional expenses. Additionally, because some data is shared by applications (e.g., name, social security number, employee ID, address, phone number), these data elements are written once, but read many times. This overlap of data enables organizations to make efficient use of chip space.

Users.

As the user base grows, more cards and card readers are purchased on an as-needed basis without substantial additional investment expenses. This is due to the fact that the infrastructure is already in place to support the smart card technology and applications. Additional costs will be incurred incrementally and directly related to the number of additional users.

Applications.

Additionally, smart cards are scalable with regard to the number of applications that can be executed. If there is sufficient chip space available on the smart card, additional

applications/functionality may be added. For example, a smart card that is initially being used for stored value and logical access may be expanded to include physical access functionality, chip space permitting.

Biometrics.

The scalability of smart cards also permits organizations to move from a two-factor authentication solution to a three-factor authentication solution through the use of biometrics. Smart cards can be used with biometrics to provide a verification capability that matches live biometrics scans against a single template that is stored on the chip. Various forms of biometrics can be used for authentication including:

- Facial recognition
- Voice pattern recognition
- Iris scan
- Hand geometry
- Fingerprint recognition

Fingerprint recognition is the most commonly used and cost-effective biometrics solution.

Traditionally, smart cards have been used as part of a two-factor authentication system. The first factor is the actual "card," which serves as a token you possess. Secondly, the PIN/password serves as something you know that can unlock secure information stored on the card. A biometrics solution can be used in conjunction with a two-factor smart card and PIN/password solution to provide a three-factor authentication solution.

10.5.2.4 Efficiency

Smart cards can be used to complete digital forms (through the population of required data elements stored on the chip) in a more streamlined fashion than their paper-based counterparts, as shown in Table 13. A smart card stores pertinent, data such as name, address, social security number, and date of birth, all of which can be used when accessing multiple applications. Using a single card to record and store this data reduces paperwork, eliminates redundant data entry, and improves data accuracy as transcribing and data entry errors are eliminated. Also, ease of use is achieved by using a single smart card for multiple applications. Finally, smart cards enable a higher level of throughput to be achieved because they can process information succinctly and quickly but can also operate in an off-line environment.

Table 13: Greater Efficiency via Electronic Forms vice Paper Forms

Paper Forms	Electronic Forms
Increased potential for spelling, transcribing, or readability errors	Core data correctly transmitted from Smart Card
Increased processing time to complete the form	Reduced processing time to complete the form

Increased time to handle, file, and copy the form	Form processed and filed immediately

10.5.2.5 Data Storage Capacity

The data storage capacity of smart cards is far superior to that of magnetic stripe cards and bar code cards. Most smart cards have a 32 Kbyte chip on which data can be stored compared with a magnetic stripe's storage capacity of about 1000 bits. This capacity permits smart cards to store more than 100 times as much data as magnetic stripe cards. As a result of their large storage capacity, smart cards working in conjunction with a terminal can execute complex tasks.

10.5.3 Benefits of Implementing PKI-enabled Smart Cards/NAME&NAME.ES

Although it can be argued that a smart card is not needed to implement PKI, there are some compelling advantages to this security approach. First, it should be noted that all of the benefits attributed to implementing PKI or smart cards also apply to PKI/smart cards/NAME&NAME.ES. These benefits include:

- Non-repudiation
- Authentication
- Data integrity
- Confidentiality
- Scalability
- Portability
- Interoperability
- Efficiency
- Data storage capacity.

For the purposes of this study, however, the focus is on incremental benefits achieved by implementing PKI/smart cards in conjunction with the NAME and NAME.ES modules.

10.5.3.1 Enhanced Level of Security

The enhanced level of security that can be achieved by implementing PKI/smart cards/NAME&NAME.ES can be attributed to several factors. One is that the private keys and digital certificates are stored on the smart card. Another is that it provides authentication and encryption capabilities.

Private Key Stored on Smart Card.

The use of PKI on a smart card can offer an enhanced level of security because private keys can be generated and stored on the card. The much higher level of security is

achieved because the non-PKI-enabled smart cards store keys on a floppy disk or hard drive. PKI-enabled smart cards contain an operating system that prevents the keys from being exposed outside the card. Therefore, they cannot be read, removed, or tampered with by anyone.

Authentication Using Digital Certificates.

PKI/smart cards incorporate cryptographic authentication capabilities that ensure the highest degree of security. PKI/smart cards store digital certificates on the card itself rather than on the certificates on a floppy disk or hard drive, as is the case with other PKI implementations. If stored on a disk or hard drive, a certificate can be copied; but that is more difficult to do if the certificate is stored on a smart card unless the smart card is exploited. A smart card carrying a PKI certificate makes authentication and non-repudiation possible by utilizing built-in functionality to accomplish digital signatures. The user carries the card and has a PIN to enable access to use the signature, which is related to a written signature.

Encryption.

Encryption capability is a key concern when dealing with sensitive data. Encryption is the transformation of data into a form unreadable by anyone without the proper decryption key. Encryption ensures privacy by keeping the information hidden from anyone for whom it is not intended, even from those who can see the encrypted data.

Public key encryption involves a public key and a private key to mathematically scramble data. While the private key must be kept secure, the public key may be widely distributed. One key is used to encrypt the data, while the other key is used to decrypt it. Encryption enhances the security of data in the following ways:

- Restricts access to your computer to only those users with registered certificates on the workstation
- Verifies the identity of the communicating party through digital signatures
- Ensures that data is stored securely on your computer
- Ensures that files are accessible only by intended parties.

10.5.3.2 Portability

The portability of private keys and digital certificates is a significant benefit derived from using PKI/smart cards. Because the private keys and digital certificates are stored in the smart card, the user can access the benefits of PKI at any location where he or she is an authorized user.

10.5.3.3 Scalability

PKI/smart cards are beneficial when they provide a scalable solution. Scalability is advantageous because a public and a private part of keys are involved, and this makes deployment and maintenance of a PKI/smart card easier.

10.6 Risk Analysis for PKI/Smart Cards/NAME&NAME.ES

The purpose of the risk analysis is to focus the decision maker's attention on the financial, technical, and schedule risks associated with PKI/smart cards. When documenting a business model, it is necessary to counter-balance positive financial indicators with real-world factors that could potentially undermine the investment and keep it from reaching its estimated potential. The purpose of this section is to help in understanding the risks associated with PKI/smartcard/NAME&NAME.ES technologies. Risks are inherent to any investment but can be managed to achieve a favorable return on investment.

10.6.1 Risks of Smart Cards

A smart card is a relatively secure device compared to bar code and magnetic stripe cards. It is a safe place to store valuable information, such as private keys, account numbers, passwords, or valuable personal information such as medical records. It is also a secure platform for performing processes that you do not want exposed to the world, for example, performing an encryption using a public key, or a signature using a private key. Nonetheless, smart cards themselves have inherent drawbacks and risks. These include the high cost of readers, algorithm replacement, lack of standards, loss or theft, and the fact that smart cards are susceptible to many kinds of attacks.

10.6.1.1 Cost of Readers

One challenge is planning for the cost of card readers. Readers are an essential part of smart card infrastructure as they provide interface between the token and the network. Smart cards can be the basis of trust for secure interaction in PKI for many organizations and their customers. For this to be achieved, a cost effective and acceptable level of risk must be achieved for all who depend on the associated certificates and keys. Achieving an efficiency of scale between volume of shared PKI-enabled services that use certificates and keys stored on a common token is the desired trade-off. An important element to consider is the high cost of readers.

If the smart cards are being used for physical access, contactless smart card readers cost between 200€ and 300€, whereas contact smart card readers cost between 200€ and 400€. Acquiring and deploying readers can be challenging, especially where there is substantial legacy equipment lacking that capability.

Many computer manufacturers do not outfit computers with card readers; as a result, the additional cost will have to be absorbed by the implementing organization. Targeting incremental deployment of readers associated with the largest evolution of PKI-enabled services has become the key to phased smart card success.

10.6.1.2 Algorithm Replacement

Algorithm replacement is inevitable and as such these replacements and the associated costs will have to be considered at the outset. Algorithm replacement costs and operational impacts to applications and associated smart cards that generate keys should be accommodated through a modular design of algorithm related functions. Every algorithm

will inevitably require replacement due to the increasing computer processing capacity (although algorithm useful life can be extended through the use of larger keys. For example, an RSA modulus of 1024 bits is considered secure today; but if it can be attacked within the next 10 years, one solution is to convert to longer key lengths, such as a modulus of 2048 bits). The careful planning for replacement before the anticipated time when an algorithm cannot protect data satisfactorily should be planned into smart card maintenance schemes.

10.6.1.3 Lack of Standards

Lack of accepted standards within the smart card industry is another drawback. Although smart card readers are standardizing on the ISO 7816 based interface standards, that does not guarantee interoperability with all smart card vendors. Numerous standards exist, and many of them target certain verticals or a certain layer of communications. This leaves out many players. This problem is being mitigated as PKI-enabled Web browsers and other mainstream applications gain the capacity to accept the smart cards and a consensus on basic PKI-based service requests to the smart card. The development of smart card standards, however, is trailing the demands for greater processing and storage capacity on smart cards. In the next section we will present some of these standards.

10.6.1.4 Loss or Theft

Irrespective of the use of the smart card, a primary risk that users face is physical loss or theft of the token. This risk is countered with the inevitable acknowledgement of a missing token and associated revocation procedures to prevent further misrepresentations of the individual's certificate-based trust among associated PKI-enabled applications. A more dangerous risk is theft of keys and discovery of the associated PIN or password used to unlock the keys, without damaging or removing the smart card. This risk poses a far greater threat to the associated trusting PKI-enabled applications and breaches are usually discovered and mitigated only after serious harm occurs, or the certificate is revoked or expires. Regardless of the protections that are built into the system, if the card is not physically protected, laws and security measures will not be effective. This protection is evolving into a combination of user responsibility for physical possession/compliance with associated policies for use and card protection of the keys during generation and/or use.

10.6.1.5 Attacks on Smart Cards

Smart cards are susceptible to attack by bad actors. An attack is defined simply as an attempt to steal or compromise data on the smart card. There are two classes of attackers—those who are parties to the system, and those who are interlopers. Attacks by participants could be a cardholder trying to cheat a terminal owner, a card issuer trying to cheat a cardholder, or similar behavior. Attacks by outsiders could be mounted via card theft, card misuse, or replacement of terminal software or hardware. Attacks by outsiders are often similar to attacks on protocols involving general-purpose computers; however, they may take advantage of various properties of the system created by the separation of roles. Four kinds of attacks can be made on smart cards: logical, physical, trojan horse, and social engineering.

Logical Attacks.

One type of attack is logical attack. A logical attack does no physical harm to smart card, rather, some sensitive information on the card is obtained by examining the bytes being transmitted to or from the card. If successful, this attack creates one of the greatest threats (i.e., potential undetected use increases until substantial damage occurs and is noticed). This attack is difficult to achieve because it involves capturing both the private key and associated PIN to perform private key operations. If the byte level I/O operations are monitored, and processing of PKI functions is not performed on the card, both the keys and PIN are exposed.

Physical Attacks.

Physical attacks are carried out, usually using special equipment, by varying temperature, voltage, or clock frequency, etc., to gain access to sensitive information on the card, or by monitoring card parameters (such as power consumption or the timing of certain card processor operations). Most smart card operating systems write sensitive data to the EEPROM area in a proprietary, encrypted manner so that it is difficult to obtain cleartext keys by directly hacking into the EEPROM. Other physical attacks that have proven to be successful involve an intense physical fluctuation at the precise time and location where the PIN verification takes place. When this happens, sensitive card functions can be performed even though the PIN is unknown to the perpetrator of the attack. A combination of a physical attack with a logical attack will reveal the private key.

Trojan Horse Attacks.

A trojan horse attack involves planting malicious code on a user's workstation without the user's knowledge. When the user submits a valid PIN, the trojan horse presents rogue data to be signed using the private key. The user is never aware that the rogue data has been signed. There are two ways of counter-attacking the trojan horse. The first is to use "single-access device driver" architecture. The operating system allows only one "trusted" application to have access to the smart card (if that one application can be compromised, of course, then even this approach can be circumvented). Not using a multi-application smart card both reduces the number of parties involved and creates a simpler operating environment with less complexity and potential for bugs. Although this reduces the possibility of attack, the benefits to be derived from multi-functionality are, of course, lost. Another way to prevent this type of attack is to require one private key entry per PIN entry; the user must then use the PIN every time the private key is to be used, thereby disallowing the trojan horse access to the key.

Social Engineering Attacks.

This kind of attack exploits the vulnerabilities inherent in human beings. For example, a hacker could pose as a network technician and request PIN and passwords in order to hack the system. This attack is not as effective when smart cards are involved because people are less likely (or even able) to share their smart card than a PIN or password.

When a decision to proceed with smart cards is made, it is essential to understand that "eternal vigilance" is not only expensive, but impossible. The risks associated with smart card tokens must be understood and bound and balanced against associated benefits. The

benefit of cost savings from increased efficiency or compliance should be weighed against the associated threats resulting from the fact that data will be exposed to remote access by users who hold the appropriate PKI credentials. Incremental steps to cost effectively control and leverage the demand for smart cards should be undertaken. The most appropriate system needs for PKI-enabled security services are unique to each set of specified security requirements of an organization.

10.6.2 Risks of PKI

PKI has recently become a popular solution for achieving electronic security and digital-based trust, but it does engender risks that vary in accordance with how the PKI is implemented and what user community it serves. Among the key risks are concerns over the maturity of PKI technology as well as key management itself.

10.6.2.1 Value Definition

Any PKI implementation should commence with an study of what data would benefit from increased exposure that PKI-enabled security services could address. The study includes evaluating the monetary or other value of the information and the associated savings that can be realized by allowing remote access. The determination of appropriate PKI-enabled security services is also needed.

10.6.2.2 Lack of Standards

Although in existence for more than 10 years, commercial products implementing PKI technology, have had limited use. Because of its limited use, standards have been slow to emerge. Some PKI standards are not mature or remain in fact because vendors must differentiate their products to justify procurement and the additional cost associated with implementing PKI. Fortunately, this situation is improving due to the efforts of vendor-sponsored organizations like the PKI Forum (http://www.pkiforum.org). However, PKI standards that apply to enterprisewide use of PKI are quite stable.

Standards that apply to PKI interoperability are still evolving and have been demonstrated to be sufficient for many applications that require interoperability; but they are not yet ubiquitously or consistently implemented, and thus are likely to evolve further.

10.6.2.3 Certificate Authority Issues

Among the most critical components of a good PKI is a reliable CA. Without proper certificate authority, the entire PKI process can be compromised. The CA and associated certification practices/policies are the root of trust by which PKI technology is currently deployed. Credibility, represented through the issuance, revocation, and management of certificates, is supplemented by the good will of the issuing organization or service (i.e., how firmly the issuer is willing to stand behind the product).

A lack of credibility resulting from poor certicate authority can break the trust necessary for an effective PKI as the CA component provides the trusted binding between a subscriber’s public key and his or her identity through the issuance of a certificate.

10.6.2.4 Registration Authority Issues

The introduction of human error in the RA process presents a risk to PKI. The RA works in conjunction with the issuance process to securely transmit the X.509 data about the individual and validate the identity of the individual when generating certificates, but is not an authority on the contents of the certificates. A human being is required for identity proofing. Sometimes, due to timing constraints, the verifying person may not always be as vigilant as he or she should be. A recommended solution is to require the maintenance of a log of every person identified, recording their name, identification credentials, and time of verification.

10.6.2.5 Relying Party/Subscriber Issues

Root certification substitution

The root certificate is a certificate self-signed by a CA, containing the CA's public key. The root certificate is usually placed into a browser's trust list of CAs, that is, a list of CAs whom the user wants to trust. Careful management of this trust list is very important because if a malicious party can surreptitiously place a new root certificate into the list (for a CA that should not be trusted), the user will be relying upon it inappropriately. Thus, centralized management of such a trust list is usually required. In an enterprise PKI, however, only a single root certificate is required—that of the enterprise's "trust anchor" or highest level CA. Managing this approach is much easier because the single root certificate can be placed into the enterprise users' software in such a fashion that malicious alteration of that certificate would be very difficult.

Malicious digital signatures

If a malicious party is able to insert code in a user's computer, he or she can get the user to digitally sign documents or material that the user did not intend to. This can be done without stealing or seizing control of the private key. The malicious code would appear to the user as if he or she is digitally signing something he or she intended to sign. In actuality, the document or material provided to the software that makes the signature occur is actually different from that appearing on the user's screen. However, if a malicious party can insert code in a computer, there is no security approach that will protect the user. Generally, the best way to guard against this type of attack is to protect the user's computer from insertion of malicious code. This however can be difficult to achieve. Furthermore, users should require receipts to be sent for each transaction. Such a protocol makes it very difficult for malicious parties to respond in a timely and effective manner.

Name space control

Certificates contain a public key and the name of the subject to whom the certificate is issued. If that name is ambiguous, such as only a common name, there are opportunities for malicious parties to impersonate the putative holder of the certificate. Additionally, it can be difficult to disambiguate (i.e., distinguish among) the many people who may have the same names as the person cited in the certificate. To minimize the potential for problems,

certificates generally should express names using a distinguished naming convention such as that prescribed in the X.500 standard, or that set forth using Internet domain components.

Theft of private key and PIN

If a malevolent party can steal the user's private key (which is usually encrypted) and the PIN or password or other identifier used to decrypt the private key, the user can be impersonated. Doing this, of course, may be very difficult, especially if the private key was generated on and protected on hardware tokens like a smart card. Moreover, such an attack is effective only against the targeted individual—it is not a more generalized attack effective simultaneously against a wide variety of users.

10.6.2.6 Potential Risk of Implementing PKI

Essentially there are two methods of implementing a PKI; one is to contract for the service and the other is to implement the operation in-house. Both approaches have potential risk, however, these risks are managable.

Deciding whether to outsource the service or implement it in-house must be done not only by comparing costs, but most important, by considering the implementing organization's overall security policy and its requirements. That is, should the organization retain full control of its PKI, or should the organization let someone else execute that aspect of its security?

Other considerations include the degree of control desired by the organization, the availability of trained staff to implement and maintain the technology, etc…

Although neither way is inexpensive, many companies, lacking sufficient knowledge of security principles, firewalls, and network topologies, find that contracting the implementation is easier.

Specialized network engineering firms with trained resources can help setup the network elements and recommend reputable CA firms to handle the PKI authentication process. In any case, a carefully thought-out PKI implementation can help ensure satisfactory operation of a virtual private network (VPN) that assists the business with its goals.

PKI provided in-house from vendors, such as Entrust Technologies, Baltimore Technologies (both explained in detail in previous section), and Xcert, give an organization greater control. The organization can set its own certificate and key management policies and engineer infrastructure to comply with these policies. In addition, in-house PKI products are more feature-rich, and thus more flexible, than outsourced PKI services.

Outsource PKI services from vendors such as VeriSign (explained in detail in previous section), Thawte, and GTE also offer advantages. Costs and schedules are more predictable because the organization can leverage existing expertise. The organization is subject to an outsource PKI service provider's policies but can gain improved interoperability by joining the provider's trust network.

Cost is obviously a concern as well. In-house PKIs cost less per user than outsource PKIs, but overall support costs are higher. Usually, it is expected that an organization will have to issue a significant number of certificates before in-house PKI investment begins to pay off.

A third method of implementing PKI involves procuring services that are customized for the user. The user owns the PKI, but services are provided by a contractor that tailors services to the needs of the owner.

10.6.2.7 Risks of Digital Signatures

The risks of using digital signatures are broadly covered under three areas: fraud, service failure, and liability.

Fraud.

If a person defrauds an organization and a paper signature was used, it is possible in a court of law to prove or disprove that signature. This is not possible with a digital signature. If applied properly, however, the use of digital signatures reduces the risk of fraud. Safety can be assured only if the private key is safe and not subject to compromise. Creating and storing private keys on hardware tokens (like smart cards) make it more difficult for malicious code to remain undetected.

Service failure.

It is important to incorporate electronic services using digital signatures within the scope of an organization's disaster recovery plans. Organizations should also consider establishing backup sites for their CA, RA, and directories that supply the services necessary for applications programs to use certificates.

Liability.

As with other interactions that an organization has with outside parties, it has to consider how its actions make it legally liable to affected parties.

10.6.2.8 Barriers Faced by organizations in Implementing PKI

In addition to the risks associated with the lack of maturity of the technology and the fact that use of PKI/smart cards represents a culture shock to some organization employees, there are some other barriers to entry that an organization faces.

Infrastructure.

Public key infrastructure follows a three-step path to functionality.

Step one involves ascertaining that directories are consistent, compatible, and integrated.

Step two is the development of procedures to issue certificates that meet accepted standards. Building this infrastructure usually takes a long period of time. Depending on the size of the organization, several RAs may have to be created because they could be distributed. This means procedures have to be taught and certified.

Step three is the deployment of the certificates.

The complexity of the process and length of time required to put the infrastructure in place is often a significant challenge that may be a discouraging factor to organizations.

Software Compatibility.

In the final analysis, building a PKI provides only an infrastructure but challenges may still exist when trying to interface PKI with existing and future planned applications. How that infrastructure is used is ultimately what interests organization program personnel. Determining how applications programs employ certificates and access the infrastructure to determine whether to trust the certificates requires that applications programs be enabled to accept and use certificates.

The process of enablement can be very difficult, depending on which application programs are being enabled, how the organization's directory infrastructure is designed and deployed, and other factors.

It is not uncommon that the cost of using a PKI—making applications PKI-aware—can exceed the cost of implementing the PKI itself; although the more applications that are enabled, the greater the utility of the PKI and the long-term savings that are realized.

10.7 Conclusion

PKI/smartcards in conjunction with the NAME&NAME.ES modules are a very good business investment when they are used to satisfy security and business needs as they provide the means for secure online transactions. Compared to other technologies, PKI/smart cards offer tremendous security benefits through the encryption of transactions using PKI to offer non-repudiation, authentication, data integrity, and confidentiality. Organizations that require this level of security benefit are most suitable candidates for this technology.

By placing PKI certificates on a smart card, scalability, portability, interoperability efficiency, and data storage capacity are possible. PKI/smart cards can be used for logical access to computer networks as well as physical access to buildings.

In an organization of 10 000 users, the cost of PKI/smart cards hardware is shown to only be about 140€ per user (excluding the operational and maintenance costs required to operate these systems).

Return on investments calculations help to make equitable comparisons of alternatives to the current situation by evaluating their individual economic impact. Cost alone should not be the sole basis of an investment decision but rather a composite of factors like benefits, risks, and costs should be evaluated.

11 Interoperability of Services

NAME module must permit other useful services in the e-commerce environment to interwork with it. It should give cryptographic support for those services. Specifically, NAME module should provide support and interoperability to different methods of importance in the world of m-commerce and m-banking. These methods are:

- EMV
- SET
- Etc.

11.1 EMV

EMV (Europay-MasterCard-Visa) is a joint industry working group created to facilitate the introduction of chip technology into the international payment systems environment by developing joint specifications for smart cards (Integrated Circuit Cards/ICC) and terminals for Payment Systems. EMV is a standard providing a common framework for a chip-based credit/debit card system, and which basically allows cards and terminals to talk together.

NAME can support security requirements for EMV about integrated circuit cards and terminals to ensure correct operation and interoperability.

Cryptographic functions that could be supported by NAME module are:

- Data authentication
- PIN enciphering
- Application cryptogram generation and issuer authentication
- Secure messaging

11.2 SET

SET (Secure Electronic Transaction) is the electronic payment protocol selected by VISA, MasterCard and other major credit card companies as the new global standard for ensuring security and confidentiality when linking credit card holders, merchants, and financial institutions conducting business over the Internet.

NAME module should provide interoperability with SET protocol. Since the standard specifies the mechanisms to process orders for a credit card, but it does not specifies the way to implement it, SET could be supported by NAME module to secure transactions.

The SET protocol provides the mechanisms for the cardholder to securely transmit payment instructions as well as for the merchant to obtain authorization and receive payment for an order. Message data is encrypted using a randomly generated symmetric encryption key "signature" to create "digital envelope" for the exchanged information. Within SET, dual signatures are used to link an order message sent to the merchant with the payment instructions containing purchaser account information sent to the Acquirer.

Cardholders must register with a Certificate Authority (CA) before they can send SET messages to merchants.

Specifically, supported functionalities by NAME provided to SET are to be:

- Confidentiality: SET is only involved for security in the payment information, specially for the credit card number, and it does not try to secure the order information. SET specifies RSA public-key ciphering algorithms that can be supported by the NAME module to encrypt the credit card number, such a way that only the transaction-processing centre can understand. Fraud is avoided because the merchant cannot access the credit card number.
- Data integrity: NAME module can support facilities for signing a SET hashed message, providing integrity.
- Client authentication: the merchant should be able to confirm that user is the legitimate cardholder. A user's digital certificate stored in the NAME module can be used to verify that s/he is authorised to use that credit card. The user must obtain the digital certificate from the financial institution issuing that credit card and it should be saved onto the NAME module. The digital certificate is signed by the financial institution and it contains the user's identity and his/her public key. The user is in charge of sending the merchant his/her digital certificate to be identified.
- Server authentication: Consumer also needs to authenticate the merchant. It is also accomplished by means of digital certificates. No NAME module implications are required.

12 Interoperability with programming languages

In this point, we are going to explain the interoperability NAME and NAME.ES must provide to integrate themselves in a generic smart card and its own operating system.

12.1 Java Card

GSM architecture requires two components, on the one hand the mobile telephone, and on the other a SIM (Subscriber Identity Module). The latter stores subscriber's authentication information.

Sun's Java Card technology has been adopted by GSM standards and included in the usage of SIM Toolkit, and therefore it should be taken into account when implementing NAME and NAME.ES modules.

The Java Card Application Programming Interface for SIM Toolkit was developed with the collaboration of the main vendors with Java Card license, including Bull, De La Rue (Oberthur), Gemplus and Schlumberger. Java Card version 2.0 already included a JCRE specification. The more recent version is 2.1.1., which includes besides the API, the virtual machine and a JCRE specification. There are also available applet samples, and a development kit with a debugging environment, and a tool to intelligently download the applets into the smart card (or other device implementing Java Card 2.1 or above). This can be interesting to implement NAME and NAME.ES modules as applets and to download them into a smart card.

Java is a Sun Microsystems programming language that has two aspects interesting for the development of NAME and NAME.ES security modules for smart cards:

- The strong Java security model that enables the coexistence of many applications on the same smart cards, a very important aspect when storing confidential information in a smart card. This is the case of our security modules.
- Applications can be developed and validated quickly with Java, so that the time to market of new programs is shorter.

The Java Card Technology is composed of three parts:

- The Java Card Virtual Machine, which defines a subset of the Java programming language and a specification of the Virtual Machine desirable for smart cards.
- The specification for the Runtime Environment –Java Card Runtime Environment- that describes the behaviour of the development environment. This includes memory management, applications management, security commitment and other runtime aspects.

The specification of the programming application –Java Card API- that describes the classes and packages conforming the core and the programming extensions for applications in smart cards.

This three components provide a secure platform, independent from vendor, for smart cards. The platform isolates applications –called applets- from the proprietary

technologies, and provides a standard system besides the API for the development of these applications. By means of the API, applications are easier to write and it guaranties portability between different card architectures.

Java Card Technology is compatible with the existing card technology. To be exact, it is ISO 7816 compliant about the memory model, communication protocol and application execution model.

A Java card communicates with a terminal with the APDU protocol defined inside. Java Card Technology is also compatible with the existing terminal technology.

12.2 Windows for Smart Card

Windows for Smart Card is a 8-bit Microsoft operating system that permits the development of applications written in Visual Basic or Visual C++.

Unlike Java Card, interoperability with GSM networks is not defined by ETSI, and it turns in a specific Microsoft programming environment to furnish capabilities for smart cards.

The Microsoft operating system is composed of six blocks, and they can vary depending on the needs of the applications required by the end-user and are the following:

- I/O Block: it is in charge of managing the external communication protocol based on the standard ISO 7816-3.
- Cryptographic Block: it offers security services (algorithms, control access mechanisms…)
- File System Block: it is in charge of managing the card memory by using the File Access Table.
- Authentication and Authorization Layer: it controls the access to data verifying firstly the user's identity doing an action and checking all the realizable actions upon data or card services.
- API Windows for Smart Card Layer: it offers access points to data and card services. The main access points to the API are referred to access to files and security services.
- RTE (Run Time Environment) Block: it is the Microsoft Virtual Machine for Smart Card. The role of the virtual machine is executing the applets downloaded onto the smart card.

Windows for Smart Card enables the download of applications called applets. Applets are the base of the services offered by Windows for Smart Card.

There are two development modes for Windows Smart Card: the native mode and the interpreted mode.

The native mode is used for basic applications required by the smart card. This mode is reserved for the card mask extension, associated to open standards such as EMV, SIM. Features proposed by GSM 11.11 and 11.14 supported by the cards are developed using this native mode.

The applet mode (or interpreted mode) is used for the development of end-user's applets on the Run Time Environment (the virtual machine). These applets can be downloaded and executed in the cycle of life of the smart card.

Therefore, NAME and NAME.ES modules implementation has to take into account also this possibility to be developed.

Some issues must be regarded in relation with this operating system:

Windows for Smart Card already has a cryptographic module. This module is an abstraction layer that integrates different security functions implemented by the hardware of the card. The basic cryptographic modules supports the following algorithms: SHA-1 for hashing, DES and Triple DES with two and three keys, RSA is only present in the case of crypto-chips (the RSA algorithm requires a cryptographic accelarator and an additional library) and COMP128.

13 WIM

WAP Identity Module is a tamper proof device such as a smart card, which provides certificate-based authentication and digital signature applications for WAP services. WIM contains a digital certificate that authenticates a WAP customer and enables him/her to electronically sign transactions, based on wireless public key infrastructure (PKI)

Whereas the SIM card plays a role in the GSM standard to identify the subscriber, the WIM implementation is introduced to identify buyer and seller.

The WAP Identity Module is used in performing WTLS and application level security functions, and to store and process information needed for user identification and authentication. This means that sensitive data, such as keys, can be stored in the WIM, and all operations where these keys are involved can be performed in the WIM.

There are four types of technical solutions for m-commerce in WAP technology, but they are actually more, so that they state the fight to get part of the market and its many revenues:

- The first choice is to combine SIM and WIM in a single chip. The advantage is that telephones only need a connector for a single chip. Even though this could be expensive, it cannot be forgotten that it permits subscribers to be buyers and the operator a seller of services.
- Another choice is installing WIM in the telephone memory. Mobile vendors are working on a standard to advance this option, because it could be the simpler option for them. However, this solution would be very vulnerable to hackers' attack.
- The third option is the double connector telephone, where SIM and WIM would have its own card reader. In this case, the position of the network operator would be less important, being more important the presence of financials and other organizations – for example, alimentary chains- that provide phone cards. Ericsson, Nokia and Motorola have announced the development of these terminals.
- The last alternative is using a external WIM reader that can communicate with a mobile phone using Bluetooth, for example.

WIM is present in the WTLS layer and is used to:

- Perform cryptographic operations during the handshake such as those operations required for client authorisation;
- Secure WTLS secure sessions.

WIM is used to protect private keys. The keys are stored on WIM and provide an environment for operations such as:

- Signing for client authentication;
- Key exchange using fixed client keys.

The WIM may also store certificates such as Certificate Authority and user certificates.

In reality, there is no need to store user certificates in a tamper proof environment. It is possible to store a certificate URL within the WIM as well as the actual certificate, but

permanent key pairs may be stored or indeed generated in the WIM. The WIM is used to protect secure sessions in addition to private keys, and supports the following functionality:

- calculation or generation of the pre-master secret;
- calculation and storage of the master secret key for each secure session;
- derivation and output of key materials based on the master secret key;

meaning that the master secret and pre-master secret never leave the WIM.

The WIM may need to 'unwrap' a key if an application receives a message key enciphered with a public key corresponding with a private key in the WIM. The wrapped key is sent to the WIM where it is deciphered using the private key, wherein the unwrapped key is returned. The unwrapped key may then be used to decipher the message.

For authentication and non-repudiation purposes, digital signatures are normally used. In the case of non-repudiation, a separate key is used with the user being requested to input authentication information such as a PIN for each signature that is made. In order for non-repudiation to be valid and secure, the signature key must never leave the tamper proof device. To sign data, the mobile device must first calculate a hash of the data then format the hashed data taking into account the requirements of the application, then send the hashed and formatted data to the WIM. The WIM then calculates the digital signature using the private key and returns the digital signature.

The WIM stores the following data:

- Information on properties of the module.
- Two key pairs: the first for authentication and key establishment, the second one for digital signature.
- A certificate or a "certificateURL" for each key pair.
- The certificate of each trusted CA.
- Data related to WTLS sessions.
- Information on protection of the data with PIN numbers.

Some more information related to the WIM module can be seen in the Annex 2, Business Survey.

14 Technical constraints

We will try to explain what the technical constraints of implementation are, in particular in regards to the actual standards implemented by the network operators.

Some of these constraints refer to relationships among smart cards and readers, applications, interface standards that are going to be explained:

- Hardware interoperability: traditionally, there has been a lack of interoperability between smart cards and readers. This is a problem when implementing NAME and NAME.ES modules because any kind of readers must be able to access them. The standard ISO 7816 has been developed for integrated circuits cards with contacts. From this standard, the following initiatives have been reached:
  - Europay, MasterCard, and VISA (EMV)—In 1996, EMV defined an ISO 7816-based smart card specification with a focus on the financial services industry.
  - Global System for Mobile Communications (GSM)—The European telecommunications industry adopted the ISO 7816 standards for their smart card specification to enable identification and authentication for mobile phone users.

  The problem with these two initiatives is that they fail to address interoperability, limiting the conjunct usage of NAME and NAME.ES modules between applications used, by instance, in a ATM and a mobile phone.

  Most of smart cards should implement several standards in order to be accessed by different readers:
  - PC/SC: PC/SC is a standard for integrating smart cards and smart card readers.
  - PKCS#7: The PKCS#7 Public Key Cryptography Standard describes a general syntax for data that may be cryptography applied to it, such as digital signatures and envelopes. The values produced according to the PKCS#7 standard are BER-encoded, which means that the values are represented as octet strings.
  - PKCS#11: The PKCS#11 Public Key Cryptography Standard specifies an API, called Cryptoki, to devices that hold cryptographic information and perform cryptographic functions.
  - PKCS#15: The PKCS#15 Public Key Cryptography Standard defines how keys, certificates, and application-specific data may be stored on a ISO/IEC 7816 compliant smart card. PKCS#15 allows multiple applications to be stored on a single smart card.
- Application interoperability: there are many different types of signing methods, many different types of hashing methods, and different types of encryption… different applications have different methods to access the NAME and NAME.ES modules. Therefore, NAME and NAME.ES modules have the limitation of their own signing methods, their own encryption methods… they are not going to provide full encryption facilities for every type of imaginable application.
- In relation with the previous point, it is more than possible that our security modules have to live together with other applications in the same smartcard. Therefore, there should be an interoperable layer supporting multiapplication. There should be a multiapplication system supporting many different applications in the same smartcard.

- The lack of smart card enabled desktop applications is a technical constraint, since NAME and NAME.ES modules will not be supported by applications in some cases, which makes interoperability between components and applications difficult. Many programs do not have native support for smart cards. Anyway, they usually support programming interfaces such as MSCAPI and PKCS#11 that allow other applications to provide this functionality.
- Difficulty to set up a system utilizing smart cards.
- Storage constraint. A smart card is a limited storage medium, and therefore, it cannot keep too much information. Digital certificates to trust must be of a small size, and besides, it is possible that not too many certificates may be stored in the security modules.

We could categorise technical constraints depending on the different application fields that standards are applied:

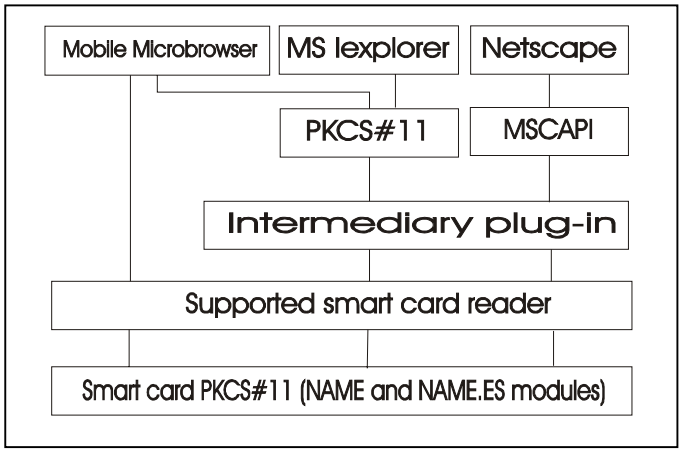
- Secure payment standards: there are a number of secure payment methods that could be supported by the encryption, signature and storage methods of NAME and NAME.ES modules. These are some examples of that:
  - SET
  - First Virtual
  - CyberCash
  - CAFE
  - Mondex
  - Visa Cash

  It is foreseeable that not all these types of payment standards are going to be operable with the NAME and NAME.ES modules. Anyway, some standards, like SET, do not define the implementations, but the behaviour of the process, facilitating the implementation of the security methods free to the developer of the application.
- Security standards
  - WTLS: WTLS supports the WAP Identity Module (WIM), which is a module similar to NAME module. The WIM stores sensitive information in a tamper-resistant device. The WIM, the same as the NAME and NAME.ES modules may be stored in a smart card, and it can live together with the SIM (the same as NAME and NAME.ES modules). Besides, the WIM can perform cryptographic functions that can be used by WTLS and the application layer. Therefore, similar efforts could be done to integrate the NAME and NAME.ES modules in WTLS.
  - SSL and TLS: The NAME and NAME.ES enhance the public-key authentication process by serving as a secure store for the private-key material, and as a cryptographic engine for performing a digital signature or key-exchange operation. The secure session is established by using public-key authentication with key exchange to derive a unique session key that can then be used to ensure data integrity and confidentiality throughout the session. Anyway, at the moment, no efforts are known to be done to adapt these layers to natively access smart cards. Instead, they support APIs to access them through other applications, which are developed to access smart cards, on the other hand. These plug-in applications offer

a transparent interface to browsers to access smart cards, and to be exact, to the NAME and NAME.ES modules.

Figure 18 shows this situation. Browsers providing with e-commerce and m-commerce services need to access NAME and NAME.ES facilities. This is a constraint, because such browsers usually implement built-in software solutions to provide security functions. Two solutions are found: the first is to program these browsers to access directly to NAME and NAME.ES facilities using those APIs to access smart cards. The second solution could be create an independent plug-in program that interfaces between the browser and the modules to give signing and encryption facilities. Some browser like Netscape and MS Internet Explorer already supports this.

Figure 18 Architecture for accessing security modules



- Transport standards: About transport standards, in the sense of data bearing standard protocols, we can find some of the following constraints when implementing NAME and NAME.ES modules:
  - HTTP: obviously, the HyperText Transfer Protocol is an unsecured protocol, since it has no implications with NAME and NAME.ES modules.
  - HTTPS: See SSL constraints.
  - WAP:
    - Before WAP 1.2 no characteristics had been foreseen for interoperability with a cryptographic module for signing and secure storage of information. Mobile devices intended to use NAME and NAME.ES modules must support WAP 1.2.
    - NAME and NAME.ES modules should storage credential using PKCS#15 in the WAP environment.

15 Requirements for PKI in UMTS

In this chapter we first give a survey of requirements relevant for PKI in UMTS. Then we address PKI in end-user application context and for UMTS system internal use respectively.

15.1 Survey of UMTS security requirements relevant for PKI

15.1.1 3G TS 21.133: Security Threats and Requirements

This specification contains an evaluation of perceived threats in the UMTS environment and produces subsequently a list of security requirements to address these threats. It describes the context in which the 3G security features are designed.

15.1.2 3G TS 33.102: Security Architecture

This specification defines the security architecture for the third generation mobile telecommunication system.

15.1.3 3G TS 33.106/107: Lawful Interception Requirements/Architecture

TS 33.106 “Lawful Interception Requirements” and TS 33.107 “Lawful Interception – Architecture and Functions” describe requirements and architecture for an interception service in UMTS.

15.1.4 3G TS 33.200: Network Domain Security; MAP application layer security

TS 33.200 and TS 33.210 define the security architecture for the UMTS core network domain control plane communications. The scope of the UMTS network domain control plane is to cover the control signalling in the UMTS core network with extension to cover the Iu-interface towards RNC. This includes both the SS7- and IP-based signalling protocols. Because of significant technical differences between the SS7 and the IP architecture, distinctions between SS7 and IP based protocols are made. SS7 and mixed SS7/IP based security protocols are referred to as legacy protocols. In R4 the only protected legacy protocol is MAP. MAP is protected on the application layer by a protocol called MAPsec.

15.1.5 3G TS 33.210: Network Domain Security; IP network layer security

This document defines the security architecture for the IP-based UMTS core network domain control plane communications and is part of R5. For native IP-based protocols, security shall be provided at the network layer. The security protocols to be used at the network layer are the Ipsec security protocols as specified in RFC-2401. All network entities supporting native IP-based control plane protocols shall support IPsec. The UMTS network domain control plane is sectioned into security domains and typically these coincide with operator borders. The borders between security domains are protected by Security Gateways (SEGs).A security domain may typically correspond to the core network of a single operator.

15.2 Requirements for PKI to support end-user applications in a UMTS environment

Since the introduction of GSM technology in Europe, the market for mobile services has grown extremely quickly. By the end of 2000, 252 million people in Europe used a mobile phone (63% of the population). The number shows that Europeans enjoy 'mobility' and embrace the fundamental benefits that can be offered: Mobility, Immediacy and Ubiquity.

With the introduction of UMTS these three characteristics will not only apply to verbal communication, but also to a lot of newly developed data services that will be offered by lots of different service providers. These are new players in the telecommunication market.

In this chapter a description will be given of these roles and new services in a UMTS environment. In general it can be said that these services are in need of more serious security functionalities. It will be explained why PKI, in conjunction with the NAME/NAME.ES module, is the most likely and suitable solution in the UMTS environment, and which requirements this new environment imposes on PKI and NAME/NAME.ES module. The requirements will be stated in quite general terms, as there are a lot of dependencies of the specific kind of applications and the parties (roles) involved in enabling that application.

15.2.1 UMTS end-user applications

In this chapter we first explain the traditional roles in a UMTS environment. Then we move on to look at which services we can expect in such an environment. Both the roles and the services have an impact on the level of security that should be required. The PKI in conjunction with the NAME/NAME.ES module is then proposed as a solution that will fulfil these requirements.

15.2.1.1 Roles

When talking about traditional end-user applications, three roles can be identified in the UMTS environment:

- **User**: an entity that is authorised to use UMTS services because of its association with an operator. In UMTS a user is identified and authenticated through the use of a Universal Subscriber Identity Module (USIM).
- **Operator (Home environment)**: the role that has overall responsibility for the provision of a network connection to users with which it has an association. This includes the provision, allocation and management of user accounts and the mechanisms required to bill users for charges and to pay serving networks for user charges. It also includes negotiation with networks for the capabilities needed to provide UMTS services to its users, including off-line agreements to allow service provision, and on-line interaction to ensure that users are properly identified, located, authenticated and authorized to use services before those services are provided to them.
- **Service Provider (SP)**: the role that provides applications/services to users over UMTS bearers. Service providers may be third party, who may have some association with a home environment for charging and billing purposes, or they may be provided by the same organization that provides the home environment. The Service provider

may also act independently of any UMTS home environment. In this case the user would pay the SP directly.

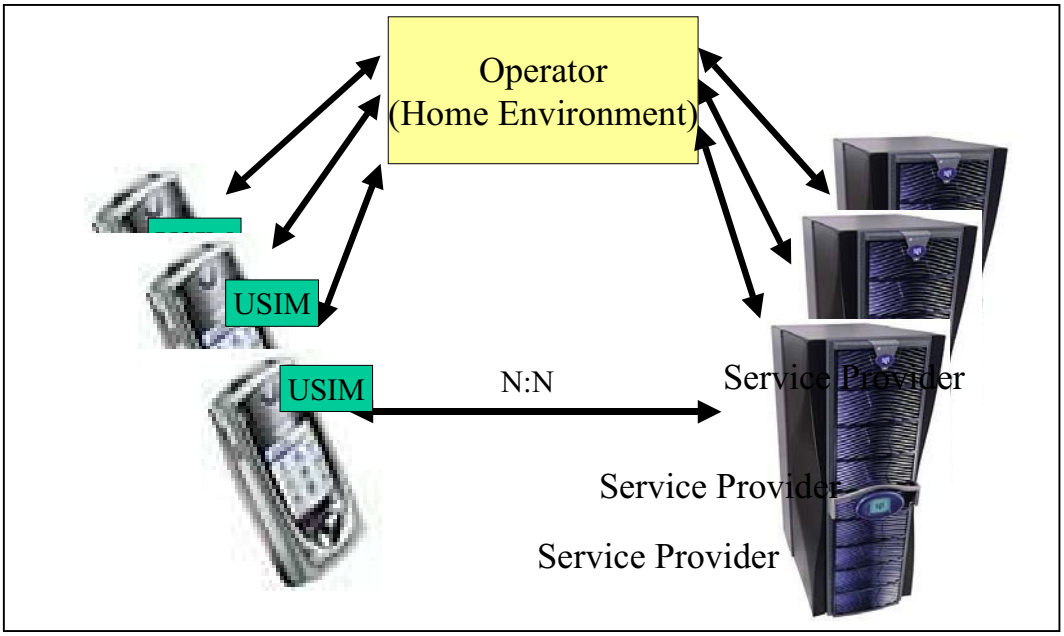


Figure 19 : Roles identified in the UMTS environment

The roles of service provider and operator (which could be filled in by the same entity) can have different (sometimes opposite) security demands. Every co-operation will have its specific solution. The security infrastructure will need to be very general and flexible.
Another issue that makes a flexible solution necessary is the fact that there are a lot of different users (for operator 1:N relation) and there are lots of different service providers (for operator 1:N relation). Several dynamic relations exist between those users and service providers that should be served by the security functions offered.

15.2.1.2 UMTS mobile services

Next to the kind of roles and the way these are realised, the kinds of services offered also imply some security requirements. Overall, UMTS end-user applications will not differ substantially from those already established for WAP applications. Basic application categories (See below) are not likely to change.

Table 14: Mobile Services Overview

Consumer segment	
Information	Communication

Dynamic Content • news • weather… **Reference Content** • phone books • catalogues • dictionaries…	**M–messaging** • SMS • e-Mail… **M–Advertising** • sponsored alerts • mobile promotion • permission marketing **M–Emergency Service** • child tracking
Entertainment	Transaction
M–Games & Gambling • Stand-alone games • M-betting… **M–Audio** • Ringtones • MP3… **M–video** • Photographs • Video-clips	**M–tailing** • M–auctions • M–sales • M–ticketing… **M–Finance** • M–brokerage • M–banking… **M–Payment** • Micro • Macro

Business segment

	Information	Communication	Transaction
External	**M–Supply Chain Management** • Fleet management • Track & Execute…	**M–Customer Relation Management** • M–sales • M–service…	
Internal	**M–Workforce** • M–Calender • M–Email • M–Groupware • …		

In essence, the progression from WAP to UMTS will manifest itself in gradually richer information contents, greater interactivity, and in some new application features such as location dependence, personalisation and immediacy (immediate access to information). These will enhance the usability of many existing and new applications and services.

The environment in which new services will be developed can be characterised by the following aspects:

- There will be new and different providers of services. For example: content providers, data service providers.
- UMTS will be positioned as the preferred means of communication for users. They will be preferable to fixed line systems
- There will be a variety of prepaid and pay-as-you-go services, which may be the rule rather than the exception. A long-term subscription between the user and a network operator may not be the paradigm.
- There will be increased control for the user over their service profile and the capabilities of their terminal.
- Non-voice services will be as important as, or more important than, voice services.
- The terminal will be used as a platform for e-commerce and other applications.

15.2.1.3 Security Aspects of UMTS services

One of the issues with these applications is the needed level of security. Security requirements are comprised of a combination of:

- Identification and authentication,
- Confidentiality,
- Integrity,
- Non-repudiation, and
- Availability

For the different application categories described above, different levels of security are required and a different subset of the security functionalities described above. Some examples are given below.

Table 15 : Examples of applications

Information applications	Members of the soccer club Madrid can get information about the situation on the field during an international game of their first team. They get the current score, and can view video fragments of the most exciting moments and of course all the goals. Secure requirements: These members should be identified (identification and authentication) properly, because they can use this service for free. Other interested soccer fans, can receive the same kind of information for one Euro. The possibility for secure mobile payment has to be offered in a UMTS environment.
Communication applications	Two colleagues are calling each other on their mobiles, while one is on holiday. He knew the board of directors had given a presentation about the vision and strategy for the next five years, and he is interested in finding out what important things were said. Secure requirements: His colleague will send him the presentation. But not before checking his

	identity (identification and authentication). He will also make sure it is sent encrypted (confidentiality) as it would be very interesting information for all the competitors, should it fall into the wrong hands.
Entertainment applications	There is a new mobile group game for over 20 people, which takes days to play. A serious competition has started. Secure requirements: It is important that the identification is done properly to determine the candidates and eventually the winner. Also the availability of the game is very important.
Transaction applications	With the development of m-commerce , contracts also have to be signed, so a digital signature should be offered. This immediately takes care of identification, authentication, confidentiality, data integrity and nonrepudiation of the document signed.
Business segment	For a mobile CRM application, availability will be very important to give customers a trustworthy impression. Furthermore the identity of the customer should be determined (identification) to build up knowledge about him.

From the description of the 3G environment and the above examples, it can be derived that:

- The security functions need to be very flexible as a lot of new and different providers will offer their services, and need to able to pick the function they need.
- Security functions need to be scalable, as there are a lot of dynamic relations between the service providers and the users.
- Secure payment solutions are required
- The security functions need to deal with a terminal that will have more and more PC-like functions as downloading of applications and configuration by the user.
- Security functions need to offer a high level of security because they will be used for m-commerce transactions.

15.2.1.4 Security Solution: PKI/NAME

Up to now, we have described the security needed for further development of 3G end-user applications. The next question is how this security is going to be realised and implemented.

A Public Key Infrastructure in conjunction with the NAME/NAME.ES module is the best security solution:

- As all the issues ‘demanded’ by the applications/services can be offered by a PKI
- As the PKI solution is flexible and able to handle the multi-user/multi service provider situation.

- As the PKI solution is scalable to lots of end-users and service providers.
- All the advantages of the NAME/NAME.ES modules are also provided.

15.2.2 Requirements for PKI/NAME for end-user applications

PKI is already used in an Internet environment. There are however several differences between PKI in an Internet environment and PKI in a mobile environment. Therefore it is not possible to copy the current situation 1 to 1 to the future UMTS situation. The main differences are:

- keys are stored on the (U)SIM card
- limited amount of data storage
- limited performance
- limited data rates
- links to the place where the certificates are the role of the operator (ISP vs. Mobile operator)

15.2.2.1 What must be provided by a PKI/NAME

A lot of things have to be accounted for before end-users can make use of the PKI security functionality. The user must have a certificate at his disposal. Some control issues have to be managed and securely written down in policies. For the final realisation of the security functionality, choices have to be made, etc. In this paragraph some issues are given.

The PKI "process"
1. The PKI certificate generating process:
    a. User registration
    b. Generating user key pair
    c. Distributing private user keys
    d. Generating user certificates
    e. Distributing user certificates
2. Maintaining and publishing the CRL
3. Root certificate
4. Cross-certification

The PKI-NAME/NAME.ES security functionality
5. Authentication (both user as SP)
6. Communication security: data origin authentication, confidentiality, and integrity
7. Digital signature (both signing and verifying)

15.2.2.2 Requirements and choices for PKI/NAME UMTS environment

The former roles, which were obviously different (User, Operator, Service Provider, and CA) become more diffuse when applying a PKI in a mobile environment, they now can mutually exchange tasks within the PKI process. Choices herein are depending on the kind of service (the acquired service level) and the type of role the different parties see for themselves. This means that findings can be discussed only in very general terms.

1a. User registration

Which party will fill in the role and tasks of the Registration Authority (RA)

- The operator can offer this as a (paid) service.
- A third party (can also be the CA) can offer this
- When the required level of security of an application is very high, the SP will not accept the CA registration, and will probably register the user himself

1b. Generating user key pair

- The keys can be generated by a CA (third party or operator)
- The keys can be generated by the operator.
- The keys can be generated on the smart card
- The keys can be generated by the smart card developer
- The keys can be generated by the Service Provider

More than one key pair may need to be generated, and this can be done by different parties.

1c. Distributing private user keys

- When generated by a CA, the private key can be put on the smart card by the CA himself or transported to the operator or smart card "company"; the public key can be distributed to the operator or the CA.
- When generated by the operator, they can put the private key on the smart card, or give it to the smart card company and they can either keep a list of the public key themselves or delegate this to the CA
- When generated on the smart card, the private key is already where it is supposed to be, the public key can be distributed to a CA or to the Operator
- When generated by the Service provider they can put it on the smart card, and publish the public key themselves or give it to the Operator.

More than one key pair may need to be distributed.

1d. Generating certificate

- The CA can generate a certificate
- The operator can generate a certificate

1e. Distributing certificate

2 Maintaining and publishing the CRL

3. Root certificate

- Some root certificates of broadly known CA's
- Only the root certificate of the operator, where the operator has the certificates of other CA's
- Every SP its own root certificate (will not be possible due to the limited amount of space on the smart card), but some SPs will need/want their own root certificate on the smart card.

  There must be some kind of control on the number of root certificates on the smart card and the parties that have their root certificate on the smart card. There also has to be a clear policy on how to renew an expired root certificate, how to put a new root certificate on the smart card, and how to delete a root certificate.

4. Cross-certification

For some applications it will be important that the application is also available to the end-users in other CA domains. In these cases cross-certification might be a solution.

5. Client Authentication

- The user needs a certificate with his public key signed by a CA.
- This certificate can be stored either
- on the USIM
- elsewhere with a link on the USIM
- on the mobile device

These are not security-based choices. For example storage on the USIM is more practical than on the device, because when buying a new device the user can keep his USIM with the certificate.

- For verification, the service provider needs the root certificate of the user's CA:
- Identical to server's CA
- Client's CA has a contract with the Server's CA
- It's the operators CA
- For verification a CRL check is necessary

Server Authentication

- The service provider needs a certificate with its public key signed by a CA
- For verification, the end-user needs the root certificate of this CA:
- Can be stored on the USIM
- Can be checked via the root certificate of the operator, which is on the USIM
- For verification a CRL check is necessary

6. Communication security.

- A symmetric encryption algorithm should be known both on the mobile device and by the service provider.
- The symmetric encryption key can be generated either:
- On the USIM and sent to the server encrypted with its public key, or
- On the service provider site and sent to the mobile device encrypted with its public key

This is not a security-based choice, but for performance reasons and the limited space on the USIM, we suggest the latter.

7. Digital signature (both signing by user and verifying by SP)

- The signature algorithm is to be stored on the user's USIM.
- The private key, belonging to the certificate used and specific for digital signature (so a different key then used for (network) authentication), has to be on the USIM
- For verification, the SP needs to know the signing algorithm used.
- For verification, the SP needs to verify the users certificate (see user authentication)

Another possibility is to offer time stamping as an added functionality.

16 Conclusions

Telcoms companies and organizations use the Internet to transact business, effective user authentication, confidentiality, data integrity, and non-repudiation become critical security objectives.

The widespread use of the Internet necessitates information assurance improvements, These include the ability to verify that communicating parties are who they claim to be and the ability to accept forms that have been digitally signed and will be legally binding.

Further, telcoms organizations must be able to ensure the confidentiality of business transacted over the Internet and to protect this data from tampering. PKI facilitates e-commerce in that it can provide security services for electronic communications and the electronic exchange of information between parties, including those who do not have a previously established relationship.

This document represent a deep study in the secure and business requirements for a Telcom company, as well as the different possibilities to achieve them. Taking into account the Telcoms security requirements and needs we can conclude that the public key and smart cards technologies in conjunction with the NAME and NAME.ES modules is a very good option to accomplish all of these secure requirements demanded, remarking the relevance of the NAME and NAME.ES modules to achieve them.

INFORMATION SOCIETIES TECHNOLOGY
(IST)
PROGRAM

Contract for:

Smart.IS
Accompanying Measure

Annex 1 to D5.1: PKI cost and standards related

Project acronym: **Smart.IS AM**
Project full title: **Smart.IS AM, Accompanying Measure for accelerating Electronic Business and New Transactional Information Systems**

Contractor no.: CR-5 TELEFÓNICA INVESTIGACIÓN Y DESARROLLO
Related to other Contract no.: -

Date of preparation of deliverable : 29 May 2002

Proposal number: IST-1999-13114

Operative commencement date of contract: January 2002.

1- Cost for the PKI Infrastructures

Once we have explained in full detail the possible solutions for implementing a PKI, we have contacted with the providers in order to have the costs if its products. To estimate the costs of a PKI for a client is not possible without having some information related to its concrete requirements. In sections 6 and 7 we present possible configurations from different vendors to implement a PKI, all the technical information is presented on this section. This information presented in sections 6 and 7 y very useful to choose a PKI implementation. Choosing the required configuration that match with the client requirements, with the information provide in section 7, is easy to have the costs, you just have to contact the providers. In this section we provide the costs for a concrete implementation of PKI, just as an example, because for giving precise data the required configuration, the number of users… are needed. In section 10 the cost of a generic PKI are presented.

1.1 Entrust solutions

We have contacted with the Entrust providers in order to have the figures. The cost for a possible PKI Entrust implementation is provided in the Table 16: Cost for 250 users and Table 17: cost for 1000 users.

Table 16: Cost for 250 users

Product	Quantity	Unit Price	Discount	Discounted Unit Price	Extended Price (USD)
Entrust Authority Security Manager	1	25.000,00			25.000,00
Single Application ID	250	50,00			12.500,00
Web Plug-in Server	1	15.000,00			15.000,00
Web Plug-in	250	30,00			7.500,00
Self Administrator Server	1	15.000,00			15.000,00
Roaming Server	1	15.000,00			15.000,00
E-mail Plug-in	250	30,00			7.500,00
				Sub-Total	97.500,00
Support and Maintenance					
				Silver Level Support (18%)	17.550,00 USD
				TOTAL	**115.050,00 USD**

Table 17: cost for 1000 users

Product	Quantity	Unit Price	Discount	Discounted Unit Price	Extended Price (USD)
Entrust Authority Security Manager	1	25.000,00			25.000,00
Single Application ID	1000	50,00	15%	42,50	42.500,00
Web Plug-in Server	1	15.000,00			15.000,00
Web Plug-in	1000	30,00	15%	25,50	25.500,00
Self Administrator Server	1	15.000,00			15.000,00
Roaming Server	1	15.000,00			15.000,00
E-mail Plug-in	1000	30,00	15%	25,50	25.500,00
				Sub-Total	163.500,00
Support and Maintenance					
				Silver Level Support (18%)	29.430,00 USD
				TOTAL	**192.930,00 USD**

1.2 Comparing costs

We will take this Entrust costs as a reference. Comparing this cost with other commercial solutions, we conclude that this is one of the most expensive solutions.

The costs provided by the VeriSign providers are lower that the ones provided by Entrust for implanting a PKI with similar features, and the ones provided by Baltimore are almost similar to the Entrust ones.

Figuring out PKI costs involves a complex equation. An organization embarking on PKI has to figure in much more than just each vendor's stated software prices, based on per-seat charges and amortizing them over five years or so. PKI vendors sometimes charge based on the number of applications you want to PKI-enable. You may typically have two certificates per person, and you want encryption key recovery because people leave an organization and because 20% of users over five years forget their passwords for using their certificates. Companies should also have two certificate authorities systems that issue digital certificates - in case one has problems.

Other costs include hardware, the time of corporate lawyers involved in approving a licensing contract and vendor software maintenance fees. In addition, companies may need to pay for training users and technical staff, which could include help-desk personnel and people to validate users' identities before giving them certificates. Smart cards and readers will also be required if digital certificates are to be stored using such technology.

A common thing in all the PKI solutions is that the price decrease as the number of users is increased. It is estimated that deploying PKI as software managed in-house typically costs 150 € to 180 € per user for 5 000 to 25 000 seats. But that drops sharply for higher volumes, to an estimated 40 € per user for 100 000 seats and 30 € per user for 200 000 seats.

For example, to outsource PKI as a service from VeriSign or another such company costs roughly the same up to between 30 000 and 80 000 seats. Beyond that number of seats, it's less expensive to run the PKI system in-house,

2 Standards

This section presents a list of the different standards about electronic signature.

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

The different projects are mainly :

- EESSI The European Electronic Signature Standardization Initiative. The specification of standard are carried out by the European Standards Organizations CEN and ETSI.
- E-Europe SmartCard : 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.

We will only focus in the ones involving the EESSI.

EESSI

The standards-related work on the 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 Standardization 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, organizational 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 interoperate 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)