IST-2000-25350 - SHAMAN

Deliverable Number	**D05**
Deliverable Title	**Intermediate report on the role of security modules in heterogeneous networks, distributed terminals and PKI**
Date of delivery	**31-OCT-2001**
Document Reference	/SHA/DOC/GD/WP4/D05/1.0

Contractual Delivery Date	31-OCT-2001
Delivery Date	31-OCT-2001
Editor	Hubert Ertl (hubert.ertl@gdm.de)
Participant(s):	G&D, NOK, VOD
Workpackage	WP4
Est. person months	
Security	Public
Nature	report
Version	Issue 1.0
Total number of pages	34

Abstract:

The purpose of this report is to provide the necessary background to support the work on the development of Secure Modules within Shaman WP4.

The main focus of WP4 is the development of a concept for trusted hardware and software modules to provide and support security for heterogeneous access networks (WP1), a unified security architecture for future distributed mobile terminals (WP2), and the public key infrastructures (WP3) they require.

Keyword list: security module, smart card, cryptography, PKI

Contributors

Name		Affiliation	Email	Phone
Ertl	Hubert	Giesecke & Devrient (G&D)	Hubert.ertl@gdm.de	+49 89 4119 2796
Heinrich	Hans-Jürgen	Giesecke & Devrient (G&D)	Hans-Juergen.Heinrich@gdm.de	+49 89 4119 2625
Niemi	Valtteri	Nokia Group (NOK)	valtteri.niemi@nokia.com	+35 840 5331438
Sovio	Sampo	Nokia Group (NOK)	Sampo.Sovio@nokia.com	+358504837440
Howard	Peter	Vodafone Ltd. (VOD)	peter.howard@vodafone.com	+44 1635 676206
Howker	Keith	Vodafone Ltd. (VOD)	keith.howker@vodafone.com	+44 1635 682216
Papadoglou	Nick	Vodafone Ltd. (VOD)	nick.papadoglou@vodafone.com	+44 1635 685653
Sondh	Jagjeet	Vodafone Ltd. (VOD)	Jagjeet.Sondh@vodafone.com	+44 1635 682927

The work described has been supported in part by the European Commission through the IST Programme under Contract IST-2000-25350.

Executive Summary

The SHAMAN project addresses the protection and security required for users, information and services as the next generation of mobile communications moves into new fields. The project is conducting R&D on the security infrastructures for two major aspects of mobile telecom following on from Releases 4 and 5 of 3GPP specifications for third generation mobile telecommunications.

The work concerns the provision of security for

- **global roaming** and **heterogeneous access networks;**
- **dynamically reconfigurable distributed mobile terminal systems.**

We are developing security architectures that will provide specifications of interfaces, protocols and mechanisms that are needed to deliver required levels of protection. We are also developing related supporting technologies based on public key infrastructure (WP3) and security modules based on smart cards (WP4).

This document provides a report on the work of SHAMAN Workpackage 4 (WP4) concentrating on the role of security modules in heterogeneous networks (WP1), distributed terminals (WP2) and PKI (WP3). It is the first deliverable of WP4 and acts as a starting documents for future work within WP4.

Security modules are a flexible and secure mechanism to allow for secure and personalised mobile communication within todays mobile communication infrastructure. Beside providing the basis for individual phone numbers and accountability of phone time recent moves in technology make use of security modules for secure transmission of data (e.g. OTA servers), storage of data (e.g. SMS), and digital signing procedures (e.g.WIM). A tamper resistant implementation of security modules is a precondition for easy administration of removable and exchangeable security modules, since they are faced with various tamper attacks during their life time.

The hardware of security modules is based on single chip micro controller technology and will continuously increase it's capabilities regarding processing power, storage sizes and interface bandwidth in future since it's directly linked to the reuse of existing memory and processor technology with approx. 8 years in delay and directly scales with the investment in the modules. A similar situation exists with software technology for security modules, since community is planing now to switch from proprietary operating system technology to open systems technology in future. Again the same scenario than general purpose systems did years before. Thus from basic technology development there is clear picture which devices will be available in future. As a result future devices will not be dependent on what's feasible from technical point of view, but from requirements put on them regarding standards, functionality and cost.

Thus the essential question is on the functional requirements for security modules and how standardisation of devices will evolve in future. Therefor this deliverable primarily collects and identifies the most important requirements on security modules generated from heterogeneous access, distributed mobile terminals and PKI. This list is successfully collected within this document but there is still a need to finally rank the requirements and to generate a specification from this list. Additionally these requirements need to be updated in parallel while the originating work packages evolve during project time and generate more detailed individual requirements.

Based on this analysis a rough layout of future security modules technology for the next few year can be given, but the real challenges on future work results from the analysis of the individual updated requirements and the progress made with standardisation in future.

Therefore the main focus of follow on work is on requirements analysis and detailed specification of future security modules, which is seen as an input for future standardisation work within international standards working groups.

Table of contents

List of abbreviations

3DES	Triple DES
3G	Third Generation
API	Application Programming Interface
ASP	Application Service Provider
CPU	Central Processing Unit
DES	Data Encryption Standard
DPA	Differential Power Analysis
DRAM	Dynamic Random Access Memory
EEPROM	Electrical Erasable Programmable Read Only Memory
FERAM	Ferro-Electic Random Access Memory
GSM	Global System for Mobile Communications
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
ISDN	Integrated Services Digital Network
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local Area Network
LEA	Law Enforcement Agency
MAC	Message Authentication Code
MMU	Memory Management Unit
MSISDN	Mobile Subscriber ISDN Number
OTA	Over the air
PAN	Personal Area Network
PDA	Personal Digital Assistant
PKCS#15	Public Key Cryptographic Standard No. 15
PKI	Public Key Infrastructure
RAM	Random Access Memory
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman
SIM	Subscriber Identification Module
SM	Security Module
SPA	Simple Power Analysis
UMTS	Universal Mobile Telecommunications/Telephony System
USB	Universal Serial Bud
USIM	Universal SIM
WAP	Wireless Application Protocol

WIM	Wap Identity Module
WTLS	Wireless Transport Layer Security

1 Introduction

1.1 Scope and purpose

Scope and purpose of this report is to provide the necessary background and foundations for future work on the development of a viable concept of a security model for UMTS comprising hardware and software. This model will provide high security features for future developments in mobile communications as investigated in work package 1 (heterogeneous access) [1], work package 2 (wireless terminals and applications)[2] and work package 3 (PKI)[3]. Additionally it provides input to work package 5 (specification of a prototype) and feedback to the other work packages mentioned.

1.2 Contents of this report

An overview on the state of the art and emerging use of security modules in mobile telecommunications comprising smart cards and other devices is given first. Outlining the functionality and services provided by current security modules shows up how security modules are used today. A technology outlook on future smart cards with respect to hardware and software capabilities is given in the following section. The outlook is based on knowledge about todays devices and provides the basis for future discussions.

In the main part of the document requirements on the security modules are collected from the other work packages on heterogeneous access, distributed terminals and PKI. These requirements are analysed, synthesised and extended by requirements originated from the security module concept itself.

Based on these findings challenges for the security models have been found as well as requirements identified which provide a basis for the future work on the specification of security models as well as an input to the other work packages on their future security module integration work.

1.3 Definition of SM

A security module is a tamper resistant device that is both physically and logically secure and has the ability to contain data and/or perform functions for certain security systems. Security module is capable of storing secret data and executing security functions in such a manner that no information about the secret data that could be efficiently used to break the security system is leaked out from the security module.

For example, smartcards are regarded as suitable devices to be used as SM. It is not necessary that the module must perform alone all functions that use secret data. In fact, in some cases execution of security functions can be distributed between SM and some other devices without revealing information about the secret data outside the SM.

The module can be a single smartcard, but does not have to be. It can as well consist of multiple smartcards or a smartcard and a special server functionality it communicates with. To be tamper-proof, those communication channels must be trustworthy. All this means that the security module does not have to be a single physical entity: It can be distributed across several locations or at least be accessible from several locations. Therefore, secure communication between the locations must be granted, like in a PAN (Personal Area Network, see Deliverable 3[2], chapter 2).

1.4 References

[1] 'Intermediate Report: Results of Review, Requirements and Reference Architecture', Deliverable D02, IST-2000-25350-SHAMAN

[2] 'Interim Report – Security Architecture for Future Mobile Terminals and Applications', Deliverable D03, IST-2000-25350-SHAMAN

[3] 'Initial report on PKI requirements for heterogeneous roaming and distributed terminals', Deliverable D04, IST-2000-25350-SHAMAN

2 Functionality and services provided by Security Modules

2.1 Introduction to the current use of Security modules

The use of security modules for holding sensitive data is already wide spread in a variety of applications supporting a number of services. Security modules have evolved and are now capable of doing more than just holding data securely. Many security modules are depended upon to do cryptographic computations, generate encryption keys, carry out authentication etc. as well as to just hold data.

Having become an integral part of the GSM world, the security module is required to authenticate itself to the network on the behalf of the owner of that module before access to network services can be granted. The security module is also used to generate and store encryption keys, which are used to protect user traffic and signalling data on the radio interface.

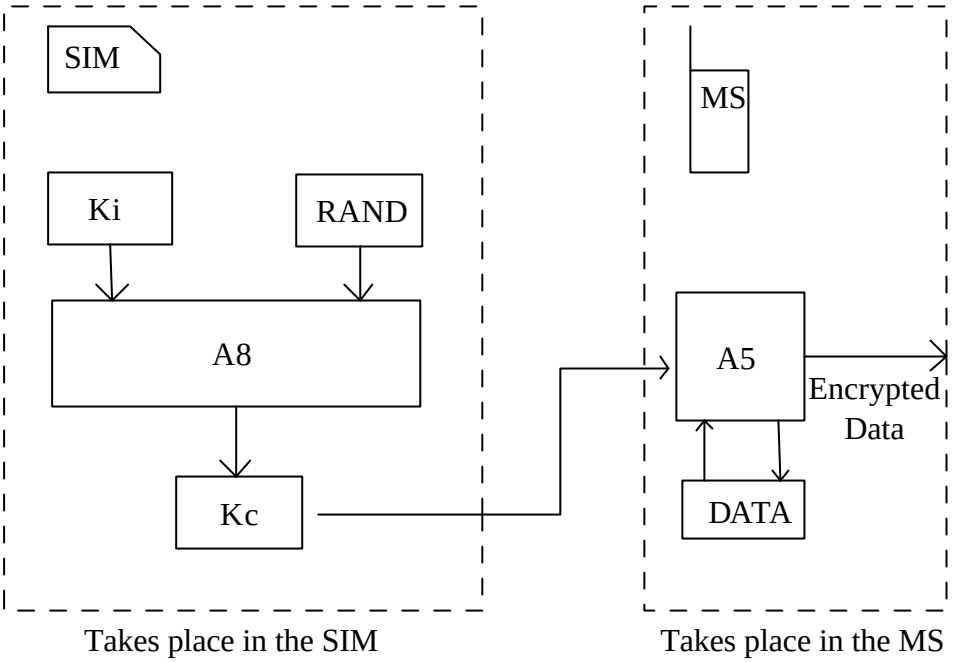
In the financial sector, banks are now issuing cards to their customers which contain a security chip for enhanced security as well as the ubiquitous magnetic strip. There are many other applications of security modules, e.g. for access control to buildings and computers (single sign on)

2.2 Support for services

2.2.1 To the Terminal

Security modules are defined to be tamper resistant devices that can perform data processing and store confidential information. A terminal (PDA, Mobile handset) is generally not as physically or logically secure as a dedicated security module when it comes to performing specific security operations. It is typically easier to extract data from a terminal than from a security module. However, on the other hand a terminal can hold more data, is more powerful and is capable of supporting a larger range of security functionality.

It is therefore often necessary to split security functions between the security module and the terminal to insure an adequately secure yet efficient implement. In this case the security module has to support some security functionality and the terminal may use the result of this computation. An example of such integration is the WAP Identity Module (WIM) [1] within the WAP forum. The WIM has support for processing and storing security data, it is able to do digital signing and will soon support encryption where the signed (and encrypted) data is then passed to the terminal and additional security mechanisms can be applied (e.g. transport layer encryption using WTLS [2]). For example the WIM is used for signing data with a users private key which is stored in the WIM, the terminal carries out the verification of digital signatures where the root certificates can be stored on the terminal or in the WIM. Another example is the GSM encryption method. The terminal is required to use the session key generated by the SIM to encrypt the voice data.



The diagram shows that the session (encryption key) is generated in the SIM by inputting the master encryption key Ki and a random that has been received from the Mobile switching centre (MSC). The session key is then passed to the mobile station (MS). The mobile station uses this session key to encrypt the voice data using the A5 encryption algorithm, which the MS must support. The session key is inputted into the A5 encryption generator along with the voice data, the outcome being scrambled data. The master encryption key Ki never leaves the SIM, but is used to generated a session key Kc.

2.2.2 To the Network

Providing services to networks is the most common use for security modules today. The wireless world, in particular GSM, relies on the security module (or Subscriber Identity Module) for authentication to the network based on a long-term subscriber authentication key before a user is allowed to use any service from that network. The security module is required to encrypt the voice call with the symmetric key generated in the Subscriber Identity Module (SIM). The SIM therefore is an integral part of the GSM architecture, providing security data storage and cryptographic processing.

The Universal subscriber identity module (USIM) is the 3G version of the SIM to work with the Universal mobile telecommunications system (UMTS) network. It supports 3G protocols and is backward compatible to support 2G authentication methods for access to 2G networks +[3]. Although the USIM is not regarded as a physical entity, it is seen as a logical application that resides on a Universal integrated circuit card (UICC). The UICC contains one or more USIMs and possibly other applications (e.g. credit card functionality or WIM). By inserting the USIM-card into a UMTS terminal the user is recognised by the UMTS network and can be addressed on this terminal either via his personal telephone number (MSISDN).

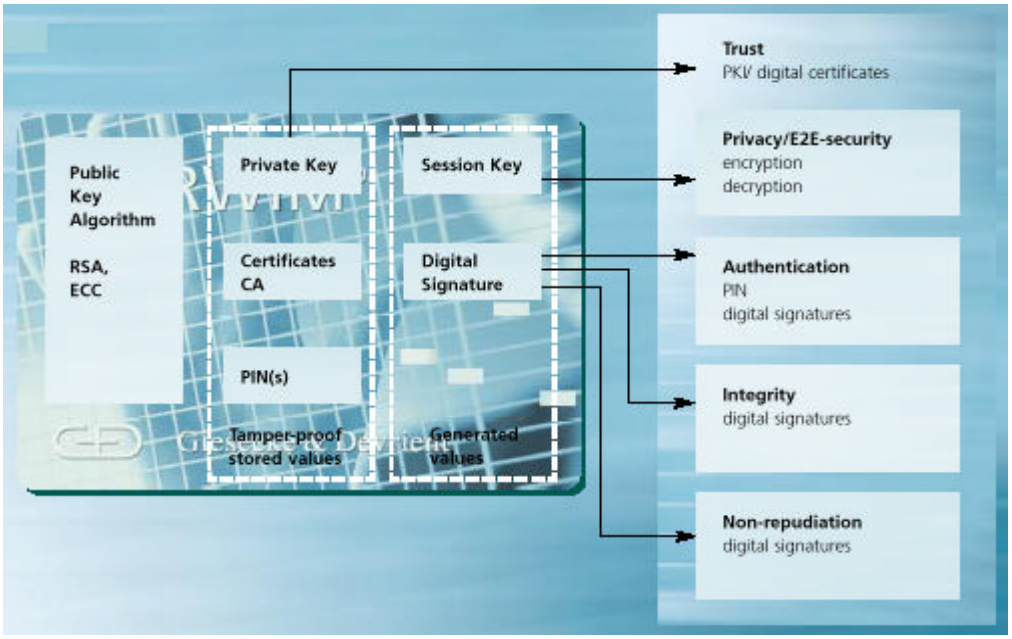
In contrast to GSM there will be a multitude of different types of terminals in UMTS, e.g. multi-mode or multi-band handsets, notebook-like communicators or UMTS-laptops with camera, speakers and microphone all equipped with a USIM-card. There will be terminals too where more than one USIM-card can be inserted. This means that some terminals (e.g. fax terminals) shall be used by several UMTS-customers simultaneously. The USIM stores the identity of the subscriber (user), operator and service provider and (at least one) user service profile. This service profile defines the services that a customer is subscribed to, the time and the network where he can use them.

LAN services have also adopted the use of security modules for secure log on. The security module like in the GSM world authenticates the user to the network in order for the user to use the services offered by the network. The security module can also be used to sign e-mails and hold encryption keys to encrypt e-mails and other data. An example of this is the Windows for smart cards platform [4], it allows smart card authentication and encryption with the current windows operating systems. Windows for smart cards can be programmed for one or more users, a user can not have concurrent account usage, and smart cards will be used to authenticate a user on to a PC or a network. The security credential such as a password or a biometric value is stored on the smart card this is compared to the template stored on the network as with an ordinary secure log on system.

2.2.3 To the end User

The use of security modules for the end user is a must when storing private and confidential data. Presently security modules are used in various ways to hold different type of information for a user. Standards such as PKCS#15 [5] allow for storage and access to data in a secure manner.

The WAP Identity Module (WIM) is used in performing WTLS and application level security functions. It stores and processes information needed for user identification and authentication. Sensitive information such as private keys are stored on the WIM and all operations where these keys are used or involved can take place on the WIM. An example use case of the WIM can be in a generating a WTLS session key where, the WIM generates a random and takes the random generated from the server, applies a function and outputs a session key for encryption over a WTLS session.



Structure of a WIM

Other functions include SignText, which allows a user to sign any piece of text. A of the text to be signed is passed to the WIM from the terminal, the WIM then uses the stored private key and applies the signing algorithm and signs the hash, and this is then passed back down to the terminal; the private key never leaves the WIM. The WIM follows the PKCS#15 file structure in order for it to carry out its requirements to store the following data:

- Information on properties of the module: supported algorithms etc.

- Key pairs for authentication, key establishment and digital signatures
- Own certificates for each key pair
- Trusted CA certificates
- Data related to WTLS sessions (including master secrets)
- Information on the protection of data with PINs

Cryptographic Token Information Format (PKCS#15) specifies how keys, certificates and application-specific data may be stored on an ISO/IEC 7816 compliant IC card or other media. It provides a hierarchical directory structure for the storage of information with certain directories having access control rights put upon them. PKCS#15 allows for a security module to present security credentials such as a digital certificate to an end application in a standardised way. PKCS #15 has the following distinct characteristics:

- Allows multiple applications to reside on the card
- Supports storage of any type of objects (keys, certificates and data)
- Support for multiple PINs whenever the security module supports it.

PKCS#15 defines a directory structure that allows for the storage of particular security information. It does this by defining directories such as PrKDF (Private key directory file), PuKDF (Public key directory file) etc. These directories then can be accessed in a standardised way by PKCS#15 compliant hardware. An important file in the structure is the Authentication Object Directory File (AODF), this is the directory of where the authentication objects are kept (e.g. PINs). The WIM specification specifies at least one AODF must be present on a WIM. The first object in the AODF is considered as a general PIN (PIN-G), if not otherwise indicated, all relevant files (CDF, PrKDF) are protected with this PIN.

2.3 References

[1] WIM Specification, www.wapforum.org

[2] WTLS Specification, www.wapforum.org

[3] 3GPP TR 31.900, www.3gpp.org

[4] Windows for smart cards, www.microsoft.com/windowsce/smartcard/start/intro.asp

[5] PKCS15, http://www.rsa.com/rsalabs/pkcs/pkcs-15/index.html

3 Emerging uses of Security Modules in mobile telecommunications

When secure communication between parties is established, then security algorithms and keys for these algorithms are needed. Since security of communication is based on a fact that only authorised entities know secret keys, it is clear that these secret keys must not be revealed to any other entities. So there must be a secure way to store and use these secret keys, a solution for this problem is to use security modules which are tamper resistant devices, that provide storing and using secret keys safely. Security modules must be resistant to physical attacks.
In this chapter we examine different kind of security modules related to mobile telecommunications. Security modules that are chosen into consideration in this chapter are smart card (e.g. SIM, WIM, USIM), iButton, eToken and secure ID. This chapter contains also description of work that has been done by IETF.
Smart card solutions have very essential role in mobile telecommunications. There exist also several ongoing EU IST projects [9].
It is possible that in future mobile communications, there is a need for SM with USB interface. That is because USB interface may provide interoperability of the same SM with various devices. eToken is described in this chapter as an example of SM with USB interface. Since USB is not the only interface that can be used, iButton is presented here as an example of SM with different kind of interface. Secure ID is presented here because it is a widely used mechanism in remote access security.

3.1 Smart Cards

There are two general categories of smart cards: contact and contact less smart card. A contact smart card requires insertion into a smart card reader with a direct connection to a conductive micromodule on the surface of the card (typically gold plated). The chips used in all of these cards fall into two categories as well: microprocessor chips and memory chips. A memory chip can be viewed as small floppy disks with optional security. In mobile telecommunications contact smart cards, with microprocessor are used.

GSM is the major application of smart cards. Instead of a mobile phone being personalised to subscriber, as in analogue systems, the handset is generic to all subscribers and is personalised by means of a Smart Card SIM (Subscriber Identity Module). The SIM contains all the personalisation and encryption details relative to specific end user.

SIM contains microprocessor, capable of handling its own security and managing the flow of data within the chip and between the chip and the outside world. It requires an operating system to manage these functions, and this operating system must conform to international standards set by the SMG9 group of ETSI.

In UMTS subscribers are also personalised by smart card like in GSM. This smart card is USIM (Universal Subscriber Identity Module). USIM contains new security algorithms; for example it allows mutual authentication of subscriber and serving network.

Wireless application identity module WIM is used to provide security on application layer in WAP. WIM implementation can be any tamper resistant device, not necessary smart card. Most likely WIM is integrated on SIM or in USIM.

3.2 Other configurations and formats

3.2.1 iButton

The iButton is a 16mm computer chip armoured in a stainless steel can. Just like smart cards there are memory iButtons and iButtons with microprocessor. Java powered cryptographic iButton contains microprocessor and it adds its complete cryptographic circuitry to a Java Virtual Machine (VM) that is Java Card 2.0 compliant. JavaCard 2.0 has been loaded into its own portable memory device, the iButton, and mounted it on a ring. Much like a Smart Card, the Java-powered ring uses a unique digital signature to encode its owner's identification. Unlike the Smart Card, the ring is durable, wearable, and supports more memory replacing at least 10 cards in its ability to initiate multiple transactions. It reads at a touch and erases only on authorised occasions. Now, mobile phone users can wirelessly dial up their bank account with a touch of a ring.

3.2.2 SecureID

RSA SecurID hardware tokens provide tamper resistant two-factor authentication, based on RSA Security's patented *Time Synchronization* technology, this authentication device generates a simple one-time authentication code that changes every 60 seconds. To access protected resources, the user simply combines his secret PIN with the code generated by his token. The result is a unique, one-time-use code that is used to positively identify, or authenticate, him. If the RSA ACE/Server validates the code, the user is granted access to the protected resource. If it is not recognised, the user is denied access.

3.2.3 Credential carriers (see IETF work)

Credentials are cryptographic objects and related data used to support secure communications over the internet. Credentials may consist of public/private key pairs, symmetric keys, X.509 public key certificates, attribute certificates, and/or application data. Secured credentials are a set of one or more credentials that have been cryptographically secured, e. g. encrypted/MACed with passkey.

Credentials may be used in any end user device that can be connect to the Internet, such as:

- Desktop or laptop PC
- Mobile phone
- Personal digital assistant (PDA)
- Etc.

Since a credentials usually contains secret information, they must never be sent in clear text and they should be stored securily. Using SACRED (Securely Available Credentials) protocols, users will be able to securely move their credentials between different locations, different Internet devices, and different storage media as needed. IETF have SACRED Working Group, which is working on the standardisation of a set of protocols for securely transferring credentials among devices.

Using security modules will solve many goals of the SACRED WG, but according [6] hardware tokens are not appropriate for every environment. However, SACRED protocols can also complement hardware credential solution by providing standard mechanism for the update of credentials, which are stored on the hardware device.

3.2.4 EToken

eToken is a portable USB device the size of an average house key, which offers a cost-effective method for authenticating users when accessing a network, and for securing electronic business applications. Just like in RSA SecureID authentication in eToken is based two-factor authentication. User authenticates it self to eToken by entering PIN, when eToken is connected into USB port of some device that contains keyboard. Two different eTokens exisists; eToken R2 and eToken PRO. eToken

R2 contains secured and encrypted EEPROM memory chip and eToken PRO contains smart card chip with level ITSEC LE4 security level. Other portable USB devices like eToken exists too for example Rosetta USB (token) see [8].

USB tokens have advantage, that no card reader is not required, because modern information and communication equipment (like PC, Laptops or future mobile phones) have already a fast and easy to use USB connector with the according drivers an SW support. There is ongoing IST project IST-1999-20323 SMART_USB, that is working on this task.

3.3 References

[1] Smart Card News Ltd, http://www.smartcard.co.uk

[2] Bart Preneel, Vincent Rijmen, "State of the Art in Applied Cryptography", Course on Computer Security and industrial Cryptography Leuven, Belgium, June 1997 Revised Lectures

[3] iButton Homepage, http://www.iButton.com

[4] RSA security inc., http://www.rsa.com

[5] "Securely Available Credentials – Credential Server Framework", Internet draft draft-ietf-sacred-framework-02.txt

[6] "Securely Available Credentials – Requirements", RFC 3157

[7] Aladdin Knowledge Systems, http://www.ealaddin.com/etoken/

[8] http://www.allusb.com/products/P11398.html

[9] http://www.cordis.lu/ist/cpt/2000cpa5r.htm

4 Smart card and Security Module Technology outlook

4.1 Tamper resistance of security modules

One of the essential concepts and concerns in security device technology is tamper resistance. The general definition is, that devices as well as their data and algorithmic behaviour can not be manipulated, copied or revealed to or by any unauthorised person. Tamper attacks can be started from third parities as well as from inside the system. The attack can be started at any one of the following access levels of a device:

- physical access to device with damaging analysis tools
- physical access to device with non-damaging analysis tools
- direct access to device during operation
- passive access to device during operation
- direct or passive access to external operations or protocols of a module

Basic tamper attacks to SM devices by damaging analysis are for example done as physical attacks to the devices. This can happen in unwrapping any packaging or analysing the physical structure of the device by hardware manipulation, by tapping signal lines, by contacting areas on a chip, by analysing electromagnetic radiation or by willingly inducing effects or errors (by light, laser, radiation, ...) into the operating module. Results or any different behaviour after manipulation can give useful information for analysis of the entire devices. There exist examples [1] of incidents with devices analysed and manipulated by this approach. Most of these successful attacks are on offline systems like pay-tv descrambler or similar systems. Up to date technology of security modules provide means to successfully prevent such attacks.

Older attacks based on timing analysis aimed to detect timing differences for selected operations like checking wrong or correct PINs, theses attacks have already been know from early mainframe architectures and are successfully solved now. In recent years a new class of attacks has showed up: Differential Power Analysis (DPA) and Simple Power Analysis (SPA). Both SPA and DPA try to analyse data and behaviour of algorithms by detailed measurement of the power consumption of devices in use. They are based on the finding, that different operations, different data sets and different algorithmic behaviour causes differences in the power consumption of a microprocessor executing any code. In measuring the detailed power consumption during operation one can easily detect loops and cycles as well as different kind of memory accesses and differences if zero or non-zero values are written or read. A close differential analysis of the power consumption can even reveal secret keys of a device if no guards against such attacks are implemented in hardware or software of the security module.

Today's technology of security modules targets to disallow the analysis of the modules to prevent the production of visual, functional and operational identical copy of the devices. While some of this features is reached by secured packaging including manipulation detectors, similar techniques are applied at logical level in using secure operating systems on smart cards, or to design algorithms to make SPA/DPA impossible.

Secured operating system can for example repeatedly check for internal consistency and authenticate with and against external devices during any external communication, to detect potential manipulations, while carefully designed algorithms disallow SPA/DPA and hardware sensors prevent from physical manipulations of the devices.

Beside the high efforts needed for producing and implementing tamper resistant security devices any certification of a security device for tamper resistance is a time consuming and expensive process as well. Limiting the certifications process to a smaller device allows for a easier and less complex

verification process and for reuse of the security modules within multiple devices later on. Additionally it also allows for easy adoption to local law requirement, which is essential for signature or encryption functionality in most countries.

Using a removable and exchangeable device allows to reuse certified technology within new or updated but not yet evaluated environments or devices. Additionally removable tamper resistant devices allow for secured transfer of secured information within possibly insecure environments by simply transferring the plug in module.

4.2 Hardware of security modules

4.2.1 General

Telecom security modules for mobile equipment are currently based on SIM cards containing standard low cost and low power microprocessors equipped with ROM, RAM, EEPROM storage and hard wired security algorithms. The security algorithms are based on symmetric key cryptography with individual permanent secret keys securely stored on both the SIM cards contained in the mobile device and the operators centralised databases.

While the operators centralised data processing centres can easily be protected and secured by standard means, the secret keys stored in the mobile device need to be protected by a tamper resistant and protected SIM card device against various attacks (e.g. spying out the key) and potential abuse (grabbing other persons identity).

SIM cards are tamper-resistant and trusted devices, produced by certified and trusted companies following agreed standards and state of the art in technology. SIM cards act as proxy for an individual user identity subscribed for the service and can be easily transferred on other devices by this single person. Beside this the SIM card is property of the operator and all security features and services are set up, guaranteed and certified by the individual operators.

Hardware technology of smart cards as a low cost, embedded consumer product can be estimated to follow the hardware technology of high end standard off-the shelf microprocessor technology with a delay of approx. 8 years. Production technology is at least 2 generations behind current state of the art in semiconductor production. First generations high end productions are used for memory components, second generation fabs are in use for standard microprocessor products, while third and forth generation fabs are used for telecom and embedded devices. Despite this delay in semiconductor core technology of approximately 8 years this gives a clear outlook what can be expected from core technology during the next years. Additionally specialised and standardised components are introduce faster than 8 years delayed into smart card technology. This effect can currently be seen with additional interfaces (e.g. USB), crypto-coprocessors (e.g. for RSA [2] or PKI) or soon to be released Java byte code interpreters.

4.2.2 Processing power

High end devices for smart card products are currently projected for 33 MHz CPU operation in 2002 by various chip suppliers and will reach 100Mhz by 2005. Restrictions from the mobile equipment and by the telecommunications standards limit the clock rate to 8 MHz or selected multiples to reduce noise on critical frequencies. Especially independent processor clocks adapting the CPU clock rate to the individual processing power needed during peak times and allowing slower low power operation during off-peak times are not permitted today but already available from today's chip technology. Fixed multiples of selected frequencies are allowed, but additional restrictions arise from heat dissipation and power consumption of individual devices. Currently 8 bit processor technology is replaced by 16-bit RISC technology and the transition to 32-bit technology can be foreseen within the next 2 years.

4.2.3 Storage

Today's standard devices are still using 32kB ROM, 2kB RAM and 32kB EEPROM. While low cost products are still using smaller amounts of memory there are high end smart card products available providing 128kB of ROM, 4kB RAM and 64kB EEPROM. Any scale in memory size directly scales to the chip area needed for the device and therefore scales the price for the product. This especially holds for high volume production periods like in year 2000, but is an major impact on prices in current low production volume period too.

The roadmaps of various chip suppliers show new products during next 2 years mainly increasing the size of RAM (up to 10KB), while retaining the ROM and EEPROM sizes at today's high end sizes (128kB ROM, 64KB EEPROM). As a new feature the FLASH ROM technology will be introduced in 2002 with additional 192kB of memory available in FLASH technology during the next 2 years. Beside the additional memory space available the devices can now be programmed and used more individually. Updates, enhancements or replacement of operating systems and services can be completely done after initial chip production without the need of an additional ROM mask redesign and chip production cycle. But a complete update of operating systems during smart card lifetime can not be expected during the next few years for security reasons as well as for technical reasons.

Additionally memory management and protection units (MMUs) are currently introduced to the consumer market allowing for hardware based protection and mapping of individual memory areas to the applications and operating systems needs. Up to now these protections are assured by a secured operating system implementing access restrictions by software means, which is technically feasible, but causes a large overhead in verification of the mechanisms. By using MMUs the operating system can now make use of individual hardware protection mechanisms to protect certain memory, code and interface areas from program access at operating system or applications program level.

In long term (5 years) FERAM technology will replace the EEPROM technology and provided larger memory sizes with characteristics only known from toady's RAM technology. This includes memory access cycles of 1 micro second compared to today EEPROM access cycle time of 1-3 micro seconds.

4.2.4 Interfaces and Bandwidth

While there are several attempts to provide faster interface for other use of cards (e.g. USB Interface for signature or computer logon cards) the standardisation of mobile equipment restricts to the available serial transmission rates on the existing contact pads of GSM smart cards. The serial line of state of the art smartcard processors can be programmed to provide up to 115.2 kbit/sec and as an extension one existing but commonly unused pad on the external interface can be re-used for a second serial I/O-channel. Hereby the I/O bandwidth can be significantly increased for special usage without violating the standard interfaces definitions for the regular I/O line.

Of additional importance is the memory bandwidth if larger amount of data (e.g. key sets) have to be stored into secured memory areas. Currently the memory bandwidth is low compared to exiting DRAM technology and no significant improvement can be expected for the very near future. Storing single byte or single page data currently takes some milliseconds with today's EEPROM technology. In fact even the existing processing power of most recent smart card CPU can not be fully used, since both the external serial interface and the internal memory interface are slow compared to today's demand from data streaming format. For example full data stream encryption is only possible for slower streams by today's technology. The external I/O bottleneck will be removed soon by USB like interfaces, but GSM specifications not yet allow to use in practice. The memory bandwidth will be significantly increased by FERAM technology in the longer run (5 years), allowing smartcards to make use of their already existing processing power.

4.2.5 Architectural support for software

Architectural support for software is provided by various means. The already mentioned memory management units as well as basic segmentation concepts support the implementation of access checks in operating systems software. Another important area is the provision of architectural support of cryptographic algorithms by implementing cryptographic co-processors for DES and consequently for 3DES. Recently RSA crypto engines have been introduced, which currently support 1024-bit key length and will support 2048 bit RSA keys in 2002. More elaborated and advanced crypto processors can be expected within the next 5 years as plain commodity products.

A more high level support of software concepts is the provision of so-called HW accelerators for selected operating systems or languages. The roadmaps of chip suppliers show HW accelerators for Java (HW byte code interpreter) to speed up Java code execution or to ease Java virtual machine integration by providing a large set of the basic virtual machine operations in hardware. Even operating systems like MULTOS or WINSC could gain from the provision of individually provided HW accelerators. While Java language is a currently agreed demand on future smart card systems it's not yet finally decided if Java is the open operating system platform for long term use on smart cards. At least it adapts well a an implementation, programming and interfacing language for scalable embedded devices for the next few year. In the long run even open source projects like LINUX could influence the smartcard industry. It depends if the development of embedded LINUX version gets really pushed and stability and security issues finally solved.

4.3 Software of security modules

The current state of the art in software technology and operating systems is very similar to 10 years ago UNIX consolidation, were some different implementations and many different branded products merged into a consolidated UNIX release, a newly rising OS windows NT and the upcoming LINUX hype later on.

While vendor specific OS still dominate the smart card market, so-called open operating systems are now discussed for some years and first trials have been successfully started in past. With the current situation important open platforms are MultOs, Windows for Smartcards and Java for Smartcards. While Java has already proved to be a viable concept for the future, Windows and Java platforms are still under heavy development and MultOs development has settled down. By open platform concepts the importance of standardised APIs is recognised as state of the art and standardised APIs replace the individual vendor specific APIs or clean up the existence of multiple API variants on smart card platforms.

Today's commercial systems are based on symmetric key algorithms and there is a clear understanding of the security concept based in a mutually known secret called a secret key, which can be compromised independently by each of the both parties knowing the secret key by unveiling the key willingly or by accident. Thus with the symmetric key concept even the security model is symmetric and can be broken from sides knowing the secret.

More recent systems start to make use of asymmetric schemes using different keys for the different directions of security relationship. This at least doubles the number of keys in use for centralised communications schemes, but exponentially increases the number of key in use if peer to peer communication and additional security features like signing and authentication are also used separately. This leads to so called public key systems, storing all recipients keys needed to send encrypted messages to them in a global public directory with various lookup mechanisms. The general assumption behind is, that using a public key does not allow for easy calculation on the private key needed for decryption.

PKI requires increased computational power of the SIM cards involved and has to store a larger amount of secret data on card as well as to handle more dynamic cryptographic data interfacing with

the crypto unit. Therefore PKI puts a load on storage, interface and computational power as well as on the clear and bullet-proof definition of a security model and an appropriate user interface.

Additionally PKI allows for “non-repudiation”, which means, that only a single person or entity can have performed a selected action (like a signature), since he is the only one knowing the key and nobody else holds a copy of it. This feature also has consequences for smartcards production process to have the keys and PINs only stored on card and nowhere else, while with symmetric approaches the key have also to be stored outside the card, for example to transfer the keys to the network operators. In contrast to the symmetric cryptography systems no second copy of a secret key exists in a PKI system, thus nobody can misuse any copy of a secret key. But on the other hand PKI systems fully rely on the complexity of the underlying crypto algorithms.

4.4 References

[1] Ross J. Anderson, Markus G. Kuhn: *Tamper Resistance - a Cautionary Note*, The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, pp 1-11, ISBN 1-880446-83-9

[2] RSA security inc., http://www.rsa.com

5 Requirements for Security Modules

5.1 Identification of requirements

5.1.1 Network (WP1) requirements for SM

The objective of this chapter is to review the requirements defined in the SHAMAN D02 [1] deliverable regarding unified security architecture. The purpose is to identify the requirements that are directly or indirectly associated with the requirements defined for the SMs. The following section summarises the specific SM requirements needed to be considered when designing an SM for heterogeneous

5.1.1.1 SM and SM-related requirements

This chapter identifies the requirements from [1] that applies to SM based mechanisms and/or the associated SM infrastructure, if these are to be used to provide the security services for next generation networks.

Req.	Related security features (Authentication/Authorisation/Confidentiality/Integrity/Non-repudiation)
1	Mechanisms shall be available to prevent or adequately minimise the misuse or misappropriation of network services
4	Mechanisms shall be available to directly and unambiguously attribute certain actions to those entities responsible.
10	It shall be possible for all critical security functions (e.g. where user-specific keys are involved) required for heterogeneous access within the same communication service provider domain to be implemented on a single physically and logically secure module. However, the use of multiple security modules within the same domain is not precluded, neither is it mandated that separate security modules should be used between different domains. The security module should be physically secure as well as logically secure. For security reasons, it may be desirable for the security module to be distributed and managed separately to the rest of the terminal, i.e. it may be desirable for a human user to insert and remove a security module after the terminal enters the distribution chain. This is for further study.
29	The terminal supplier requires strong authentication and authorisation to allow/restrict remote upgrade and management of the supplierware in the terminal components
30	The terminal supplier requires a reliable method for verifying the integrity of the supplierware in the terminal components, and disclaims any and all liability/guarantees in case said verification fails.
31	The security module supplier requires standardised interfaces in the terminal to support correct and secure functioning of the security module.
32	The security module supplier requires that the security functions running on the security module can easily be implemented such that the implementation is as much as possible resistant against hardware and side channel attacks. Preferably they should be composed out of standard security algorithms which are known to be resistant.
39	The subscriber requests the right to inspect and correct the stored personal data
43	The subscriber requests the right to inspect and correct the stored personal data

44	The user requests that his communication data, as well as the communication associated data (e.g. CDR´s), are transmitted, stored and processed in a secure way to ensure the privacy and integrity of his communication. Therefore, eavesdropping or traffic analysis of user traffic, signalling and / or data shall not be possible.
45	The user requests that no other user is able to perform operations or access services in place of him and at the user's cost. Masquerading as another user shall be prevented by appropriate authentication measures.
53	The subscriber requests the right to inspect and correct the stored personal data
56	The subscriber requests the right to inspect and correct the stored personal data

5.1.1.2 Derived SM requirements

This section describes the requirements derived from the requirements in 5.1.1.1.

Networks need to authenticate and agree session keys with users before granting them access to services. Authentication and key agreement is typically based on a private/secret key stored on the user's security module. The key must be guarded against unauthorised disclosure to prevent the subscription from being cloned to allow unauthorised calls to be charged to the target user's account. It is therefore advisable to use a tamper-resistant device to store authentication keys and operations so that information which may be used to determine the private/secret authentication key is not exposed outside the security module and so that an attacker cannot read the authentication key by tampering with the module.

Req. 1. The SM must be capable of supporting advanced security mechanisms, thus offering high security levels for authentication and session key agreement

Req. 2. A single SM should be capable of implementing all the security mechanisms that are necessary to authenticate and agree session keys with multiple access networks

Terminal manufacturers and network operators may need to make software/functionality changes to the MT. It is important to be able to check that the data sent was not altered or tampered by an intermediate unauthorised source.

Req. 3. The SM must be capable assisting the terminal in verifying the integrity of downloaded software , e.g. by supplying root public keys which may be used to verify signatures on downloaded software

Terminal manufacturers and network operators may need to make software/functionality changes to the SM. It is important to be able to check that the data sent was not altered or tampered by an intermediate unauthorised source.

Req. 4. The SM must be capable of verifying signatures on software that is downloaded to the SM.

Req. 5. Sensitive information such as secret keys should be protected against unauthorised access via physical or electrical interfaces.

Req. 6. In the case where the user of a terminal abuses the services or the access that was granted from the network operator it should be possible to uniquely identify the user so that they can be held accountable of their actions. This unique identification for accountability purposes should be stored in a secure place and it should not be possible to modify it.

Users will be able to access different types of networks with the same SM. Network operators or system administrators may have access to the SM for manipulating certain data. However, it should not be possible for an operator or administrator to view, or more importantly to modify, any

credentials within the SM that do not belong to them with the only exception of the Law Enforcement Agency (LEA). In contrast the user should be able to access and modify personal data stored on the SM.

Req. 7. The SM should be capable of securely protecting against disclosure or modification of network information and credentials on the SM by unauthorised network operators and other parties.

Req. 8. The SM must be capable of allowing the users to access and modify stored personal data.

Req. 9. The SM should be capable of allowing the LEA to have access of the users personal stored data upon request based on a lawful authorisation.

5.1.2 Distributed Terminal (WP2) requirements for SM

This chapter reviews the requirements for security identified in [2] and relates them to requirements relating to SM.

5.1.2.1 Introduction

In [2] security requirements for distributed terminals have been presented. For each PAN component requirements are listed separately. That is because role models are considered to be significant. Chapter 5.1.2.2 presents those requirements that are associated to SM and requirements that are derived from these are presented in chapter 5.1.2.3.

5.1.2.2 SM and SM-related requirements

This chapter identifies the requirements from [2] that applies to SM based mechanisms and/or the associated SM infrastructure, if these are to be used to provide the security services for next generation networks. WP2 implies **potentially** SM-related requirements for PAN **internal** and **external** communications.

Req.	Related security features (Authentication/Authorisation/Confidentiality/Integrity/Non-repudiation)	Relevant for PAN internal communications	Relevant for PAN external communications
1	It shall be possible to provide confidentiality of user data and signalling data in transit to PAN component.	Y	Y
2	It shall be possible to provide integrity of user data and signalling data both in transit to PAN component and when stored in a PAN component.	Y	Y
3	It shall be possible to provide authentication of the source of applications downloaded by the user.	N	Y
4	It shall be possible for the user to determine whether an authenticated source is an authorised source of applications or not.	N	Y
5	It shall be possible for the user to be in control of which applications are downloaded to the user's PAN component, with regard to download from both remote servers and other components in the user's PAN.	Y	Y
6	It shall be possible for the PAN components to keep a log of all actions taken by applications downloaded to the PAN component and all actions of PAN components with which the PAN component interacts.	Y	Y

7	It shall be possible for the user to exercise complete control over the transmission of user input information from the user's PAN component to both remote servers and other PAN components.	Y	Y
8	It shall be possible for the PAN component owner to nominate a party to act as PAN manager with regard to their PAN component.	Y	N
9	It shall be possible for the PAN component owner to revoke the rights of the PAN manager with regard to their PAN component.	Y	N
10	It shall be possible for the PAN component owner to only grant access to use the PAN component to authorised parties.	Y	N
11	It shall be possible for the PAN component owner to only grant access to accrue charges to authorised parties.	N	Y
12	It shall be possible for the PAN component owner to only grant network access and use of any subscription module that the PAN component has to those parties authorised by the owner.	N	Y
13	It shall be possible for the PAN component owner to define the access policy and security policy with regard to their PAN component.	Y	N
14	It shall be possible for the PAN component owner to define the access policy for applications, and negotiate the security policy with the ASP with regard to their PAN component.	N	Y
15	It shall be possible for the ASP to authenticate the client receiving a downloaded executable.	N	Y
16	It shall be possible for the client to authenticate the source (by definition, the ASP) of a downloaded executable.	N	Y
17	It shall be possible for the downloaded executables to be sent from the ASP to the client with confidentiality.	N	Y
18	It shall be possible for the downloaded executables to be sent from the ASP to the client with integrity.	N	Y
19	It shall be possible for the ASP to obtain the clients terminal capabilities with integrity.	N	Y
20	It shall be possible for the ASP to obtain the client terminal capabilities with confidentiality.	N	Y
24	It shall be possible for the authorisation level conferred on an ASP to passed with integrity to the client.	N	Y
25	It shall be possible for the authorisation level conferred to an ASP to be passed with confidentiality to the client.	N	Y
26	It shall be possible for the client to obey the authorisation level received.	N	Y
27	It shall be possible for the AA to withdraw the authorisation level on ASPs and ensure that terminals are informed of this withdrawal of authorisation.	N	Y
28	It shall be possible for the PM to authenticate PAN component users requesting authorisation.	Y	N
29	It shall be possible for the PM to confer variable authorisation levels	Y	N

	on PAN component users.		
30	It shall be possible for the authorisation level conferred on a PAN component user to be passed with integrity to other PAN component users.	Y	N
31	It shall be possible for the authorisation level conferred to a PAN component user to be passed with confidentiality to other PAN component users.	Y	N
32	It shall be possible for the other PAN users to obey the authorisation level granted to the new PAN component user.	Y	N
33	It shall be possible for the PM to withdraw the authorisation level on PAN component users and ensure that other PAN components are informed of this withdrawal of authorisation.	Y	N
34	It shall be possible for the PM to disable authorisation capability of AAs.	N	Y

5.1.2.3 Derived SM requirements

From external communication requirements point of view nothing needs to be added to WP1 derived SM requirements. However it is possible to use SM to secure PAN internal communications. If this approach is chosen then there are also following requirements:

The PAN component that contains SM authenticates the owner of the the component for example by using PIN.

Req. 0. The SM should be able to authenticate the PAN component user.

According to requirements 8 and 9, owner of the PAN component should be able to nominate and revoke that component to act as PAN Manager.

Req. 1. The SM should provide mechanism to switch on and off the PAN Manager functionality, whenever owner of the PAN component wants it.

According to requirements 10 and 13 PAN component owner should be able to set access and security policies. It is important that only authorised entity can set these policies. Therefore SM should contain access and security policy database that can be modified by only authenticated parties. PAN Manager can also set acces and security policies for the components.

Req. 2. The SM should be able to store authorization information.

According to requirements 1 and 2 of the previous section SM may be needed for securing PAN internal communication. If this is the case, then the following applies:

Req. 3. The SM should provide mechanisms to provide security for internal communications: integrity, confidentiality, authentication.

5.1.3 PKI Requirements (WP3) for Security Modules

5.1.3.1 Introduction

Within SHAMAN the essential requirements from all involved parties in mobile communications have been collected in advance. Afterwards are they have been analysed for resulting requirements in work

package 1 (heterogeneous access) [1] and work package 2 (wireless terminals and applications) [2]. These requirements are evaluated in the previous two sections of this report with respect to security modules. Work package 3 (PKI)[3] evaluated these requirements itself in the same way as within the previous sections to identify requirements for PKI related issues. The final report on PKI requirements therefore does not produce a new list of strong requirements for security modules itself, but list single requirements and some optional solutions, some of them coming from special aspect of PKI.

5.1.3.2 SM and SM-related requirements

The requirements originated from future terminals and applications are condensed to the following list of requirements from PKI technology point of view:

- Authentication of one party against another
- Transport security, i.e. confidentiality and integrity
- Authorisation of parties:
  - PAN-internal authorisation issues
  - 'Global' authorisation issues
- Withdrawal of authorisation
  - PAN-internal withdrawal
  - 'Global' withdrawal
- Local policy enforcement

Beside these requirements organisational issues specific to PKI are identified that need to be solved by any security module in use by any means. This comprises key and certificate management issues as well as interoperability issues and results in the following list specific to PKI requirements on SM.

1. **Key management Issues**
   - Key pair generation

     Distributed generation of the key pair in the mobile device by the user

     Distributed generation of the key pair on the SIM by the user

     Central generation if the key pair by the manufacturer of the device or the owner of the SIM, before delivering the device or SIM.

     Centrally organised generation of keys on request
   - Key storage

     On the SIM

     On an additional smart card

     In Software
   - Key backup and recovery

     Only needed for encryption keys
   - Key Update

     Possible reuse of key material if safely stored on tamper resistant devices
   - Key history and archive

2. **Certificate management issues**
    - Registration
    - Certificate generation and distribution
    - Certificate dissemination and retrieval
    - Certificate validation
3. **Interoperability Issues**
    - Signature Policies
    - Certificate Translation

5.1.3.3 Derived SM requirements

The condensed and derived requirements for security modules are:

- Safely generate, store and manage private keys
- Manage the corresponding public keys.
- Handle certificates, policies and interoperability
- Perform basic crypto functions based on stored private keys

Besides meeting these basic requirements tamper resistant security modules can even assist in the more efficient operation of PKI infrastructure. For example keys stored on a tamper resistant device are more secured against long term attacks and will finally produce less updates of key material as well as additionally allow for longer re-use of existing key material. As an example new certificates can be generated by re-using safely stored private keys again, if updated certificates are needed after expire or with new additional data provided. Sometime new certificates are also needed if new PIN values are generated and activated by the user. To successfully implement PKI in future on mobile equipment some external issues like the collision of trust models and commercial models needs to be solved. Finally the general user acceptance of a PKI scheme which is more complex than pure symmetric secret key needs to be achieved.

5.2 Requirements analysis and integration/synthesis

The requirements on SMs originate from heterogeneous access, distributed terminals and PKI as well as from requirements directly generated from SM technology itself. These requirements are collected in the following sections.

5.2.1 Requirements from other WPs

From other work packages basic requirements on security modules have been collected. In summary the detailed analysis produced the following list of requirements and most wanted features of security modules:

- Support of advanced security mechanisms, thus offering high security levels for authentication and session key agreement
- Provision of a single SM implementing all the security mechanisms that are necessary to authenticate and agree session keys with multiple access networks
- Providing assistance to the terminal in verifying the integrity of downloaded software (e.g. by MAC functions, integrity keys) which may be used to verify signatures on downloaded software
- Verifying signatures on software that is downloaded to the SM.

- Protecting sensitive information such as secret keys against unauthorised access via physical or electrical interfaces.
- In the case where the user of a terminal abuses the services or the access that was granted from the network operator there should be an unique identification of the user for accountability purposes.
- Secure storage of unique identification of users which can not be modified.
- Secure protection against disclosure or modification of network information and credentials on the SM by unauthorised network operators and other parties.
- Allowing the authorised users to access and modify stored personal data.
- Allowing the LEA to have access of the users personal stored data upon request based on a lawful authorisation.
- Mechanisms to switch on and off the PAN Manager functionality, whenever owner of the PAN component wants it.
- The SM should be able to authenticate the PAN component user.
- Store authorisation information for different components.
- Provide mechanisms for security of internal communications: integrity, confidentiality, authentication.

The requirements form the WP3 (PKI environments) are more detailed to the special requirements of PKI systems, since concrete functionality has to be provided for PKI. The basic requirements are:

- Safely generate, store and manage private keys
- Manage the corresponding public keys.
- Handle certificates, policies and interoperability
- Perform basic crypto functions based on stored keys

Later work on SM requirements will rank these requirements and decide which individual functionality will be included into a reference architecture or the specification of a SM.

5.2.2 Internally (SM) generated Requirements

Beside the requirements on SM technology from the heterogeneous access, distributed terminal and PKI level of a mobile system further requirements are directly raised to security modules (for example by local law) or generated from the SM technology itself.

- Comply with laws and regulations within the appropriate jurisdiction.
- Interoperation with mobile equipment as well as with other SMs.
- Exchangeable and replaceable SM implementation as an important feature of SM.
- Fixed device implementation for special usage of SMs (especially for low cost devices).

5.2.3 Requirements directly generated by user

Direct requirements from the end user of security modules have not been analysed up to now. Such requirements might include a direct interface for monitoring the security module activity, may include dual use of security modules for security functionality other then telecommunications or even for functionality other then security as for example notebook functionality. This investigation is for further study and requires a clearer understanding how security modules are handled in future.

5.3 References

[1] 'Intermediate Report: Results of Review, Requirements and Reference Architecture', Deliverable D02, IST-2000-25350-SHAMAN

[2] 'Interim Report – Security Architecture for Future Mobile Terminals and Applications', Deliverable D03, IST-2000-25350-SHAMAN

[3] 'Initial report on PKI requirements for heterogeneous roaming and distributed terminals', Deliverable D04 IST-2000-25350-SHAMAN

6 Conclusions

6.1 Introduction

For SMs in mobile Networks and Terminals two major independent but complementary roles are identified:

- as a subsystem or component trusted by other components to provide security services and supporting operations;
- as a security hub providing security supervision, monitoring and control over other components of a *security domain* (for example within a PAN or interfacing global access).

For both roles various kinds of modules are expected providing the necessary functionality according to the individual demands coming from the mobile communication itself as well as from direct user demands and from usage within other environments (dual used SMs).

6.2 Architectures for future Security Modules

Based on the analysis of the previous chapters the following architecture of a security module is expected for the 2 years or 5 years time from now. This is neither an official statement of the companies involved into the SHAMAN project nor a commitment on any development, but based on the expectations from a technical point of analysis from todays point of view.

A single module will still be based on single chip micro controller technology, but capabilities will scale up during time and single security modules will interact as a distributed security infrastructure.

For the pure single chip performance the following numbers are expected for the next years in lowest cost, mass marked and sophisticated application (and price) scenarios.

	lowest cost	mass market	sophisticated
Technology	0.8 µ	0.5 µ	0.25 µ
MHz	1	1 -5	10
RAM	0.25 kB	1 kB	2.5 kB
ROM	16 kB	32 kB	96 kB
EEPROM	8 kB	16 kB	64 kB
FERAM	None	None	None
Coprozessors	None	None	RSA, DES
External IF	Serial 9.6 kb	Serial 9.6 kb	Up to 115 kb
Storage cycle time	8ms	4ms	2ms

Table 1 current scenario

	lowest cost	mass market	sophisticated
Technology	0.35 µ	0.25 µ	0.18 µ
MHz	1 - 5	12	66
RAM	0.25 – 0.5kB	3 kB	12 kB
ROM/ Flash EEPROM	16 kB	128 kB	256 kB
EEPROM	8 kB	32 - 64 kB	128 kB
FERAM	None	None	None
Coprozessors	DES, AES	DES, AES, RSA, ECC	DES, AES, RSA, ECC
External IF	Up to 115 kb	Up to 115 kb	Up to 115 kb/ USB
Storage cycle time	3ms	2ms	2ms

Table 2 scenario expected for 2 years

	lowest cost	mass market	sophisticated
Technology	0.25 µ	0.18 µ	0.12 µ
MHz	1 - 10	20 - 33	120
RAM	0.5 kB	6 kB	(64 kB)
ROM/ Flash EEPROM	24 kB	256 kB	(512 kB)
EEPROM	8 - 16 kB	32 - 96 kB	(256 kB)
FERAM	None	None	1 MB*
Coprozessors	AES, ECC	AES, RSA, ECC, Hash	AES, RSA, ECC, Hash
External IF	Up to 115 kb	Up to 115 kb/ USB	Up to 115 kb/ USB
Storage cycle time	2ms	1ms	(1ms) – 100ns

Table 3 scenario expected for 5 years

* instead of RAM, ROM and EEPROM

6.3 Challenges for security modules

For a security module (SM) that meets all the requirements described above, it will certainly not be sufficient to think in terms of a traditional smartcard that just stores some rudimentary algorithms and user-specific data like keys. More functionality has to be implemented, but two conditions must be taken into account:

1. the inherent limitations of processing power and storage capacity of secure, tamper-resistant devices (such as a smartcard) which will always be more restricted than state of the art or specialised communications and computing components;

2. all communications between SM components in any form of federated (*multi-processor*) operation must be secured in terms of privacy, integrity and resilience.

Challenges and future work

The distribution of security functionality over multiple smart cards, and how these communicate and inter-work will be investigated.

Earlier [TechAnnex], we have identified the possibility of distributing security functions between several co-operating SMs, or between the SM and less secure but higher-performance parts of, say, the terminal, balancing security and efficiency. A single component SM could be visualised as a secure *atom*; the challenge is to construct *molecules* – multi-SMs and SMs with other external components – that have identifiable and predictable security properties and characteristics.

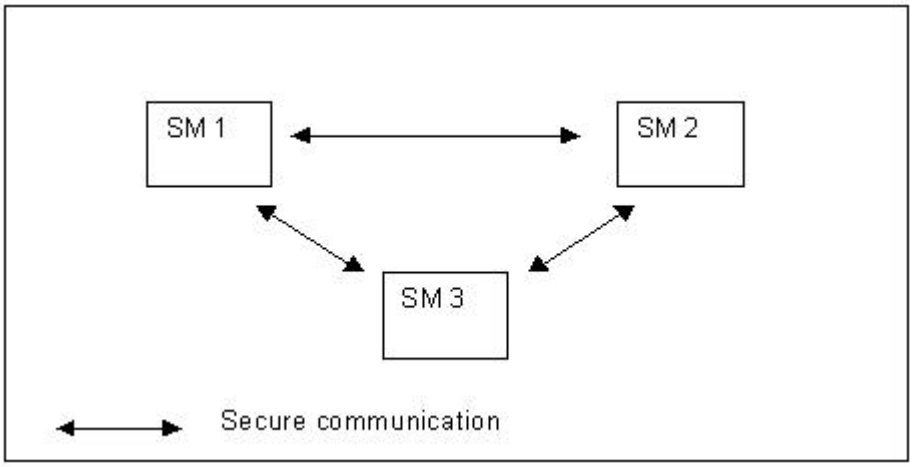


Figure 1: Distributed SM

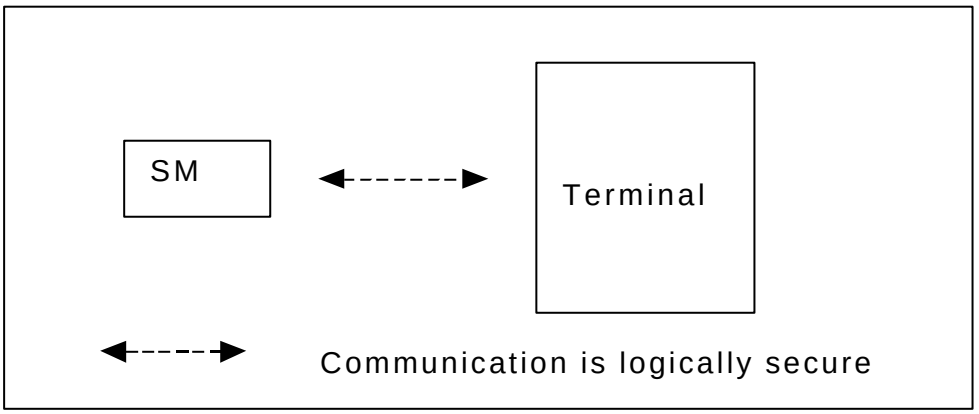


Figure 2: Distributed security functionality between SM and terminal

In figure 2 communication must be logically secure, it means that no information about the secret data that could be efficiently used to break security system is leaked out from the SM. Situation where SM is distributed may provide efficient solution for those security functions that requires parallel computation. When SM is distributed then some portion of resources in single SM *atoms* are needed to provide secure communication between SMs and for management of these SM components. It should be further study to investigate what kind of resources is needed when SM is distributed.

When security function is distributed between SM and less trusted terminal, it can provide great amount of processing power. Some security functions like Internet Key Exchange protocol [RFC2409] are quite complex and therefore require large amount of processing power. If IKE is performed in distributed SM, that consists smartcards, then number of these smartcards may increase unnecessary large. It may be better to distribute the IKE protocol rather than SM. Document [IKE] contains description of how IKE can be distributed securely between SM and less secure terminal.

It should be further study to investigate what kind of security functions can be distributed in this way, how this distribution should be done and which method is better distribution of SM or security function.

A further role for the SM is the provision of a trusted environment for trusted software. This might take the form of compartmentalised applications providing specific functions or services, or it might act as a trusted reference monitor (secure kernel, say) which would supervise the operation of less trusted application software in a less trusted environment offering higher processing performance, larger storage capability and higher bandwidth communication. Table 6.1, below, identifies where the SM may be deployed.

A further future requirement on the SM concerning its rôle as a trusted component may be the availability of a *trusted channel* that does not rely on the environment – so the user can ensure that she is not being spoofed by some malicious functionality, say. This might be no more that a couple of red/green LEDs to indicate go/no_go: – your system is OK/corrupt; the certificate is good/bad; etc.

The application of SM technology must contribute to and conform with legal and social needs concerning to the balance of personal anonymity and privacy against the requirements of law-enforcement.

6.4 Options and possibilities

The table below summarises the services and areas of application where SM can be of value. No ranking of importance (from '*might be nice*' to '*essential*') is given; this is seen as being for further investigation in conjunction with WP1, 2 and 3.

	own use	provides	Supports
Authentication			
Authorisation			
Integrity			
data protection			
access control			F
Cryptographic services			F
Trusted functionality			F
Communication security			
Trusted software			

Table 6.1 – SM exploitation

* - OK in principle, but only slow/small data, *signature* and MAC, say
F – future use – no interface at this time

The column headings should be self-explanatory:

own use — the SM uses this service or functionality for its own purposes: - to control access to itself; to ensure its own communication are secure; etc.

provides — the SM provides such (secure) security services to, or on behalf of, its client (or clients)

supports — the SM delivers some essential trusted aspect of a security service provided by another component to its clients which are not necessarily clients of the SM.

6.5 Conclusions for future Work

First of all, a clear understanding of what the SM must be capable of should be established: for example, is there a necessity to encrypt data in the SM? to what degree should one provide end-to-end security?

Secondly, the borderline of the SM may not be clear. If a mobile handset, e.g., performs crypto algorithms on its hardware, one may be tempted to consider it part of the SM; however, an SM is defined to be „tamper-resistant", so probably not every security task will be performed on the SM (because of efficiency reasons).

Since the SHAMAN framework in its whole generality encompasses a number of different technologies (different access networks and mobile standards), it will be a challenge to define an SM concept which is compatible with all of these. A definition of a 'SHAMAN-compliant' SM could provide the basis of a future standard in its own right, one which is compatible with the most common technologies of today (Bluetooth, IEEE 802.11). As time goes on, future technologies could be built to support this SM standard, so the manufacturers could declare their products to be 'SM-compliant'. This, of course, makes great demands on extensibility and scalability of the whole concept.

The SM must be able to support a variety of crypto algorithms to be future-proof, among these maybe elliptic-curve algorithms. It is also important to make no unnecessary limitations of key-lengths.

As former deliverables show, key management is always a delicate issue. The SM must offer an appropriate interface. One major requirement will probably be the generation of key pairs on a smartcard. Additionally first investigation on IKE [2] as the most common protocol currently used in IPSec implementations showed it to be a quite complex protocol. So it would be very hard task to run IKE just in smartcard, but even this will require for further investigation or protoype work.

It is not yet clear if all necessary interaction with the smartcard will be possible with the existing standards, like the SIM application toolkit. Eventually those standards would have to be extended.

The validation of certificates is still a problem, because of the limited processing power of today's tamper-resistant devices.

On the user-side, all security services should be efficient, fast and intuitive – and transparent, in certain cases. For example, if the user has a distributed terminal, for the usage it should play no role where the SM (or its different parts) are located.

In a distributed environment, tests will be certainly more difficult than for monolithic systems. It will be hard to prove the correctness of the system, especially with respect to security, because perhaps not every attack in every configuration can be tested.

6.6 References

[TechAnnex] Annex 1 to SHAMAN Contract - *Description of Work*

[IKE] Nokia, Distributing Internet Key Exchange protocol between tamper resistant device and mobile terminal