IST-2000-25350 - SHAMAN

Security for Heterogeneous Access in Mobile Applications and Networks

Deliverable Number	D13
Deliverable Title	Final technical report - results, specifications and conclusions
Document Reference	SHA/DOC/PMN
Contractual Delivery Date	30-NOV-2002
Actual Delivery Date	30-NOV-2002
Editor	Keith Howker, Vodafone
Participant(s):	Vodafone, Royal Holloway, Siemens ATEA, Nokia, Ericsson, T-Nova, G&D, Siemens AG
Workpackage	WP1, WP2, WP3, WP4, WP7
Est. person months	
Security	Public
Nature	Final version
Version	1.0
Total number of pages	36

Abstract:

This report contains the specifications and conclusions arising from the work of the four technical development workpackages, covering security architecture for future mobile telecommunications systems. These address the provision of secure global roaming, secure access over heterogeneous radio networks and security for highly configurable mobile terminals, together with supporting technologies applying public key cryptography and a *secure module* based on smart card concepts.

Keyword list:

Security Architecture, Personal Area Network (PAN), Distributed Terminal, Communication Security, Security Initialisation, Imprinting, Authentication, Confidentiality, Encryption, Integrity Protection, Key Exchange, Public Key Infrastructure (PKI), Personal CA, Identity Privacy, Key Distribution, Trust Model, PAN Security Domain (PSD), Access Control, Security Policies, Secure Execution Environment, Link Layer Security, Network Layer Security, Security Associations, Usage Scenarios

Management summary

The technical development work of SHAMAN has been successfully completed. The results are included in this final technical report.

The project set out to provide security for the next generation of mobile communications in two distinct areas:

the network:	the mobile user will be able to roam globally, and connection to the networks and services will be through a variety of heterogeneous access networks, based on, for instance, wireless LAN and Bluetooth, in addition to enhanced cellular methods;
the terminal:	future multi-function mobile terminals will consist of dynamically configurable components, some of which may be worn about the body, that may use local wireless communications among themselves; these terminals will require secure applications environments to support their communications and their access to programs and information.

The technical development work of the project is organised into four workpackages, the results of which are the subject of this report.

WP1 Security for global roaming in IP-based mobile networks with heterogeneous access networks

WP2 Unified security architecture for future mobile terminals and applications

WP3 Public Key Infrastructure for next generation mobile telecommunications

WP4 Security modules

The main work for the two areas was conducted by Workpackages WP1 and WP2. The job of Workpackages WP3 and WP4 was to provide expert support in two important contributing technologies:

public key	development of PK technologies and related infrastructure issues;
secure modules	the use of trusted hardware and software, based on smart card concepts, to provide secure environment for storage and processing of critical information, in particular cryptographic material.

The complete deliverable consists of this overview document containing a technical summary of the whole project at the end of the eighth quarter, together with an extended annex for each of WP1 to 4. This overview is based on material included in the annual Project Review Report.

Two further workpackages complete the technical content of the project. For completeness, the summaries of WP5 - *Prototypes and demonstrations* - and WP6 - *Dissemination, external relations and liaison* - are included in this overview. The complete WP6 report is published as D12 [http://www.isrc.rhul.ac.uk/shaman/docs/d12v1.pdf], and the specification of the WP5 demonstrator is published as D11 [http://www.isrc.rhul.ac.uk/shaman/docs/d11v1.pdf].

In addition to summarising the results and achievements of the project, a number of open issues are identified which require further attention in the imminent FP6 research programme.

Table of Contents

1 Project Overview

Introduction

SHAMAN addresses the protection and security required for users, information and services as the next generation of mobile communications moves into new fields.

The main topics we address are:

- the mobile user will be able to roam globally, and connection to the networks and services will be through a variety of heterogeneous access networks, based on, for instance, wireless LAN and Bluetooth, in addition to enhanced cellular methods;
- future multi-function mobile terminals will consist of dynamically configurable components, some of which may be worn about the body, that may use local wireless communications among themselves; these terminals will require secure applications environments to support their communications and their access to programs and information.

Our goal is to provide the architectural framework together with appropriate mechanisms and protocols to ensure the security of services using the two areas we have identified.

We plan to maintain the sort of influence and impact on standards achieved by the earlier ACTS projects USECA and its predecessors. Some of the success of USECA – the global impact of project results – is attributable to a tight working relationship with urgent standardisation work and a sharp focus on its immediate requirements; this may also be seen as a limitation, leading to a restricted depth of vision and outlook. SHAMAN takes a definite forward-looking position and will carefully manage the relationship with standards, spearheading moves into the new areas of technology and services that we cover.

Summary

We conduct R&D on the security infrastructures for two major aspects of the next generation of mobile communications following on from Releases 4 and 5 of 3GPP specifications.

We develop security architectures providing specifications of interfaces, protocols and mechanisms that are needed to provide required levels of protection. We are also developing necessary supporting technologies based on public key infrastructure and smart card security modules.

The work concerns the provision of security for

global roaming and heterogeneous access networks;

dynamically reconfigurable distributed terminal systems.

Description of Work

The work addresses the development of security services and architectures that enable the above features to be integrated into the future overall security provision for mobile communications. Two independent tasks operate in parallel on these topics, supported by two common tasks that provide essential support for security solutions. One addresses the public key infrastructure that will allow this seamless integration and operation to take place; the other provides security modules based on smart card technology that will protect kernel security functionality and security-critical data and parameters. A further task takes the technical results of these four workpackages and validates them through system design and prototyping.

Project results will fall into two categories:

- technical and architectural specifications and reports destined for adoption in European and international standards;
- validation and demonstration of the functionality and feasibility of novel, critical or salient results.

1.1 Objectives - Overall goals

The future directions post 3G give rise to new security issues for UMTS, which need to be addressed. This leads to the main objective of the project:

To develop extensions to the security architecture for future mobile telecommunications systems in order to provide secure global roaming, secure access over heterogeneous radio networks and security for highly configurable mobile terminals.

In order to support this main objective the following sub-objectives are defined:

- to review the security requirements arising from the identified security issues and define a comprehensive set of additional security features to be provided by the UMTS security architecture
- to define a comprehensive set of additional security mechanisms, protocols and procedures required to provide the necessary security features
- to specify a public key infrastructure to support security mechanisms, protocols and procedures defined to address the identified security issues
- to define the security features and procedures involving smart cards and other security modules
- to demonstrate the technical feasibility and the functionality of salient or critical aspects of the results and to validate the specifications
- to disseminate the results of the project for adoption in the standards bodies and industrial forums, and in particular to provide a sound and validated technical basis for the definition of extensions to the UMTS security standards
- to build on the work of and collaborate with relevant EC projects.

A further objective which is not specific to SHAMAN is the study of developments relating to privacy of users. Although SHAMAN adds no new generic issues over and above those relating to second and third generation networks, the project will maintain a watch on concerns about legitimate privacy and anonymity with respect to identity and location. Some of the issues relate to exposure or compromise over the radio links and the core networks, others relate to information maintained or derived in network services and databases. The project will concentrate on privacy of user identities transmitted over the network and on possible privacy issues arising from new developments on smart cards and their utilization. It is not within the scope of the project to develop generic solutions to other broader concerns, however these will be monitored and reported.

1.2 Objectives - Second year goals

The goal for the remainder of the project was stated in the Current DoW as

> ***to complete the development of extensions to the security architecture for future mobile telecommunications systems in order to provide secure global roaming, secure access over heterogeneous radio networks and security for highly configurable mobile terminals.***

Specific goals for the second period correspond to the milestones and goals set out in the workpackage descriptions in Section 9.4, below.

Specific workpackage goals

WP1
- completion of definition of a reference functional architecture·
- specification of requirements on secure access procedures·
- specification of (a set of) secure access procedures satisfying the requirements·
- technical support for standardisation of selected solutions

WP2
- to develop the detailed model of the distributed terminal ·
- to develop a security architecture, based on the requirements and high-level functional specification produced during the first year

WP3
- to develop a public key infrastructure to support the requirements of the other WPs, covering network, terminal and SM developments, together with other generic requirements arising from identified areas of research into 3G and beyond.

WP4
- to develop an architecture for the security module (SM) based on the requirements identified in Year1;·
- to specify an SM, to be demonstrated in WP5, that meets the needs of the network, terminal and PKI;

WP5
- to develop the specification for a prototype covering the work of WPs 1, 2, 3 & 4,· to build a working model·
- to demonstrate and to evaluate the critical and novel aspects developed by the project

WP6
- to establish, co-ordinate and maintain relations with relevant standards bodies and industry forums;·
- to disseminate the information gained during the project by making inputs to the standardisation process, contributing technical papers to scientific conferences, and organising workshops.·
- to build on the work of and collaborate with relevant EC projects

WP7
- to ensure the smooth and effective running of the project, and successful completion with high quality results·
- to ensure efficient and effective internal communication and communication·
- to provide communication and liaison with the Commission and Concertation activities

2 Work and Achievements

The following sub-sections summarise the work of the SHAMAN workpackages, identifying their results and some of the open issues they have identified. For WP1 to WP4, these summaries are derived from the extended annexes to this report. The WP5 summary is derived from deliverable D11; the WP6 summary is derived from deliverable D12.

2.1 Work Package 1 - Security for global roaming in IP-based mobile networks with heterogeneous access networks

Work package 1 (WP1) is one of the two major technical work packages of the Shaman project. This section gives an overview of the results achieved in this work package, with emphasis on the results from the second year. Earlier results were presented in the following SHAMAN Deliverables:

D02 - *Intermediate report containing results of review, requirements and reference architectures (M06)*;

D09 - *Detailed technical specification" (M18);*

The material in D09 has been refined and extended in D13. So, the reader gets the complete picture of SHAMAN WP1 results by reading D02 and the WP1-related part of D13.

2.1.1 Scope of WP1 work

SHAMAN work is about security for mobile systems beyond the third generation. There is no common understanding of what a "post-3G" mobile system precisely is, but there seems to be widespread agreement that such systems will be characterised by an all-IP based core network to provide global connectivity (the use of IPv6 was assumed in SHAMAN), and a variety of heterogeneous access networks (e.g. WLAN, Hiperlan, Bluetooth, GSM, UTRAN and others) connected to this core network. A user in a post-3G mobile system should be able to use services from anywhere in the system (global roaming), and the use of a particular access network technology should be transparent to him when using these services. A distinction can be made between application layer services (e.g. web browsing) and network services (e.g. IP connectivity, mobility management, Quality of Service, session control). It seems to be generally accepted now that a future mobile system should, as much as possible, separate transport from applications, so as to reduce the complexity of the overall system and allow for an independent evolution of transport networks and applications.

The activity of WP1 was strictly limited to work on security for the transport network. It became increasingly clear during the project that work on security for applications would not be beneficial for transport network security. While it was recognised that leveraging an existing transport security infrastructure and user base (such as in GSM or 3GPP) for application security could be useful in a transitory phase, it was felt that for the target system application security and transport security should be treated independently. Transport security still being a vast area, SHAMAN WP1 decided to further focus their work. The primary focus of SHAMAN WP1 work was on the security features and mechanisms required to provide global IP connectivity and various forms of mobility to a globally roaming user in a post-3G mobile system. A secondary focus was on security for Quality of Service procedures in such a system.

2.1.2 Approach

The overall objective of WP1 was to define an initial security architecture and access procedures for post-3G mobile systems, based on a selected network reference architecture. In order to achieve this objective WP1 undertook the following steps:

- review of security features in candidate radio access networks and remote access procedures for mobile users;
- definition of a reference functional security architecture;
- specification of requirements on secure access procedures;

- specification of (a set of) secure access procedures satisfying the requirements;
- preparation of future standards work.

Any work on a security architecture for post-3G mobile systems faces the following challenges:

- heterogeneity;
- complexity;
- absence of generally agreed architecture for post-3G mobile systems;
- changing boundary conditions;
- unclear business relations and resulting trust models.

In order to cope with these challenges SHAMAN used the following approach: firstly, a security reference architecture was defined which was as generic as possible, making only the most basic and widely accepted assumption. Secondly, the complexity of the work to define security mechanisms in this security architecture was drastically reduced by identifying basic functional building blocks likely to be required in any type of post-3G mobile system. The different building blocks were selected in such a way that a change in one building block would have a minimal affect on the other building blocks and that it should then be easily possible to create the overall security architecture by suitably combining these building blocks. How a functional building block would be realised would depend on the boundary conditions, e.g. the trust relations resulting from given business relations or the particular network configuration chosen by an operator. This approach guarantees the flexibility necessitated by the fact that these boundary conditions are largely unknown today.

The five main building blocks identified are:

- Secure address configuration,
- Authentication and session key establishment,
- IP layer security,
- Link layer security, and
- Network domain security.

Protocols for IP-based networks are, in general, standardised by the IETF (Internet Engineering Task Force). The general approach taken for the work in SHAMAN was that any security architecture for post-3G mobile systems must be compliant with the IETF as far as applicable. However, the IETF (as opposed to e.g. 3GPP) does not standardise complete architectures. The challenge therefore remained to investigate how the protocols specified by the IETF can be used as (parts of) functional building blocks for a post-3G security architecture in a consistent and efficient way.

2.1.3 Network reference architecture

Security is not meaningful as a stand-alone feature. While general security requirements from the stakeholders' (users', operators', regulators' etc.) points of view can be formulated without reference to a particular communications system, security features and mechanisms are only meaningful in the context of a system to which they are applied. This system need not be specified in detail, but its major characteristics need to be known. As no generally accepted network reference architecture for post-3G mobile systems was – and is – available, SHAMAN undertook to survey existing activities in this area to select a suitable reference architecture. This work has already been done in the first year of the project, and its result has been reported in D02, but it is mentioned here again, because the selection of the reference architecture is fundamental for the understanding of the approach in SHAMAN WP1.

For each surveyed network reference architecture, security relevant network functional entities and the interfaces and information flows between them were investigated and the commonalties and differences of security functional architectures for the candidate network reference architectures were studied. Finally, it was decided that the architecture defined by the IST project BRAIN was a suitable basis for the SHAMAN work. It should be stressed, however, that security entities and mechanisms were chosen in such a way that the dependency on the particular characteristics of BRAIN were minimised. So, e.g. the SHAMAN security architecture does not depend on the particular micromobility protocol defined in BRAIN (BCMP), nor BRAIN specific nodes such as the anchor

point ANP nor the particular way in which BRAIN specified an interface between layers 2 and 3. How little is actually needed from the BRAIN architecture becomes apparent from the following subsection showing the basic functional security architecture of SHAMAN. However, the SHAMAN results are compatible with the BRAIN work and can be used to secure a system like BRAIN.

2.1.4 Basic functional security architecture

The following figure was adopted from BRAIN and then extended to show additional nodes in the radio access network.

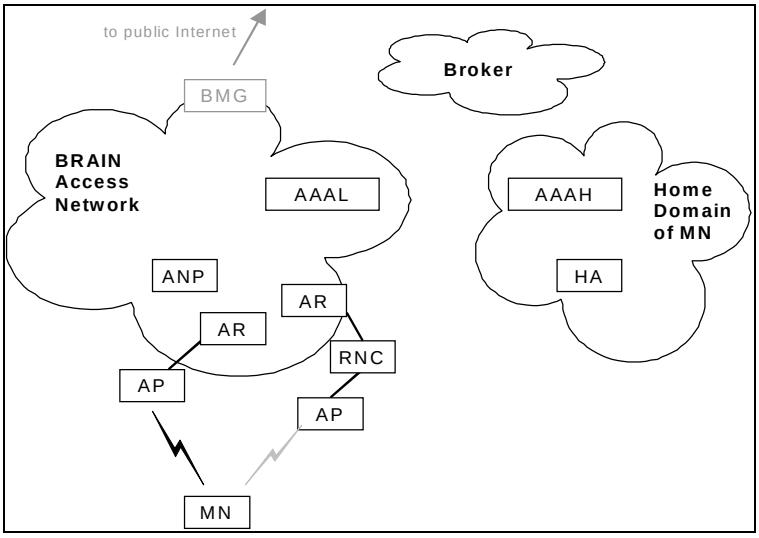

Figure 1 - Basic SHAMAN functional security architecture

The figure contains the following network entities:

MN: the Mobile node comprises all the security functionality on the user side, including possibly a smart card.

AP: the Access point terminates the radio link from the MN. It may terminate radio link layer specific security.

RNC: the Radio network controller is a UMTS-specific functional entity which is presented as an example of a radio-specific entity in the access network. It may also terminate radio link layer specific security.

AR: the Access router is the first router seen from the MN. The path between the MN and the AR is called the “first hop”. The AR may terminate network layer on the first hop. In general, the AP, the RNC and the AN will be different. This may create considerable complexity for the security in the access network realising the first hop (see pertinent subsection below).

ANP: the Anchor point is a BRAIN-specific entity realising certain mobility-related functions. It plays no essential role in the SHAMAN security architecture. It is presented here as an example of a network nodes whose communication interfaces have to be secured in a hop-by-hop fashion, see the subsection on network domain security below.

BMG: the BRAIN Mobility Gateway is also a BRAIN-specific entity separating the BRAIN-specific access network from the public Internet. It plays no essential role in the SHAMAN security architecture. As for the ANP, communication through the BMG has to be secured by applying network domain security

AAAL and *AAAH*: the authentication, authorisation and accounting servers in the local and the home domains are fundamental to the SHAMAN security architecture. They are well known from the IETF.

There function is to enable secure global roaming. A *broker* may be used as an intermediate between AAAL and AAAH.

HA: the home agent is an entity specific to Mobile IP, and, hence, may not be present in the architecture, depending on the use of Mobile IP for mobility.

The above architecture is complemented by other entities which are specific to certain scenarios, in particular:

CCC: a Cost Charging Centre is required when the access to network functions is based on means other than a subscription, e.g. on electronic payment.

2.1.5 Security requirements: privacy and anonymity

The work on security requirements occurred in the first year of the project, its results can be found in D02 and will not be dealt with here, with one exception: privacy and anonymity. This is for two reasons: firstly, the recognition of the importance of this requirement has been growing considerably over the past years. Secondly, it turned out in the course of the SHAMAN investigations that this requirement has a tremendous impact on the security mechanisms chosen. The seemingly subtle difference between the protection against passive attacks (eavesdropping) and active attacks (modification of messages) turned out to be all-decisive. With so-called secret key mechanisms, it seems possible only to protect against passive attacks, as is the case in today's GSM and UMTS systems. If the stronger requirement of protection against active attacks applies then, as far as can be seen, public key mechanisms are needed, and the protocols may be become more complex. As complexity implies cost, and the trade-off between such cost and the strength of anonymity protection which will be decided by the stakeholders is difficult to predict today, SHAMAN chose to explore the architectural implications of both variants of the requirement for privacy and anonymity. The implications are mainly reflected in the work on authentication and key agreement.

2.1.6 Trust Model

Before a security functional architecture can be defined a trust model is needed capturing the trust relationships between the parties involved. The need for certain security features may depend on these trust relationships. Trust models depend on business relationships and also on certain features of network deployment, such as the deployment of a node in an exposed or a protected environment. In spite of the fact that many determinants of a trust model are unknown today, a best guess at those determinants was made, and a trust model was elaborated. It is described in WP1's contribution to D13.

2.1.7 Building block "secure address configuration"

Since we want a mobile node to be provided with basic IP-connectivity, the mobile node has to acquire an IP-address. In the IPv6-world there are two options to automatically configure a node with an IP-address: stateless and stateful address autoconfiguration.

Results: when used unprotected both methods are susceptible to a variety of attacks. In the stateless case a published scheme (currently not standardised) is shown to effectively prevent relevant attacks. In the stateful case, message authentication is required which, however, need to be based on a shared secret between the MN and the DHCP server. But no standardised means to establish this shared secret is available for a roaming user.

Open issues: further standardisation work at the IETF on secure address configuration is needed.

2.1.8 Building block "Authentication and session key establishment"

When a mobile node attaches to a visited network it had never been in contact with before, the network wants to be assured to get properly paid for the services granted to the mobile node and the mobile node wants to be assured that the access network does not tamper with any data the mobile

node sends or receives via the access network. This requires some form of mutual authentication between the two, which can be carried out in a variety of ways.

The classical approach is the case where a subscription-like relation exists between the user of a mobile node and a home network, which also comprises the prior set-up of security information like keys, algorithms etc. The cryptographic mechanisms used in the authentication procedure could be based on symmetric or asymmetric techniques. Whereas the former requires the involvement of the home network during the initial authentication process between mobile node and visited network the latter allows for architectures that avoid an on-line involvement of the home network since the authentication may then be based on certificates. In this case, however, a public key infrastructure is required which has to be involved on-line for the verification of the certificates.

There might exist means of payment other than those relying on a subscription-like relation between the user of a mobile node and some home network (alternative access). This could be achieved by credit cards, various forms of electronic money or other means, leading to quite different system and security architectures.

Results: The alternatives for authentication and key agreement were analysed and developed in detail down to the level of information flow (stage 2 specification). A distinction was made between one-step and two-step approaches. The two-step approach uses two separate authentication protocols, one for network authentication and the second for authentication of the mobile node. Typically the network authentication protocol is executed first and it is used to create a protected tunnel through which the step-two authentication protocol is run. In particular, such a tunnel provides protection of user identity and other access negotiations against active attacks at the initial access phase. In general, it was found advantageous to use EAP as a format to carry authentication information. For a subscription-based symmetric-key approach, the one-step approach using EAP-AKA and “AAA for IPv6” (currently not specified as an EAP method) were found suitable in principle. For public-key based approaches, particular attention was given to the candidates for the son-of-IKE protocol. In contrast to today’s Internet Key Exchange Protocol (IKE), son-of-IKE is more lightweight and therefore suitable for use in a mobile environment. A cryptographic analysis of these protocols was performed as part of WP3. For the two-step approach, it was discovered that the use of PEAP, EAP-TTLS or PIC in the first step together with legacy client authentication protocols in the second step was flawed for important application scenarios, and a fix was proposed. For alternative access, new ground was broken with the definition of a suitable charging architecture. In addition, results were achieved on session key derivation and methods to ensure that no access to valuable resources can be gained by a user before authentication is completed (secure initial access).

Open issues: the completion of the IETF PANA work on the definition of a transport-independent protocol to carry authentication information.

2.1.9 Building block “IP layer security“

The various alternatives for the protection of the first hop (e.g. protection at link layer vs. protection at network layer) are discussed and analysed in a section below. However, if protection is implemented at the network layer we assume that IPsec is used, since it is the "natural" candidate to protect IP-traffic. In this case an IPsec security association has to be set up between the mobile node and an appropriate entity in the access network in the course of the initial access procedure. Although there exist methods to establish an IPsec security association based on a pre-shared secret (like the Internet Key Exchange protocol IKE), they are quite inefficient in our scenario, so that there seems to be a need for a more efficient, symmetric key based IPsec security association negotiation protocol. There are various ways how mobility can be handled and the specific design has a strong influence on the security issues involved. If we assume that the protection of the first hop is implemented using IPsec and that in the course of a handover the mobile node changes its point of attachment to the access network, the IPsec security association has to be newly established between the mobile node and the new point of attachment. This could be done by either running a new negotiation or by transferring the

IPsec security context from the previous point of attachment to the new one. Since the former is assumed to be too time-consuming, we focus on the latter approach.

Results: a complete new protocol for IPsec security association negotiation was developed which takes a shared secret resulting from any mutual authentication protocol as input and produces an IPsec SA as an output, using only very lightweight methods. IPsec SA handling in handover situations was studied.

Open issues: the work on security context in handover situations is not complete as it depends on output from the SEAMOBY group.

2.1.10 Building block "Link Layer security"

When considering link layer security, the terminating point at the network side as well as the used protection mechanism is dependent on the link layer technology. One can note that currently there are very few similarities between the protection mechanisms in the different technologies. It was therefore investigated how applicable the current protection mechanisms are when it comes to protecting the network access in the Shaman reference model and also what changes would be needed. The results of this investigation have been used together with the results from the IP layer security part to try to come to a conclusion of what methods that is needed to secure the first hop.

As for the IP layer security, an important part for the link layer security is the security association negotiation. Today, different techniques are used for various systems. The SA negotiation is closely related to the authentication and key establishment procedure. An interesting problem to investigate is how to perform SA negotiation that can work in the Shaman model. As the MN is mobile, the issue of context transfer also arise.

Results:

It can be concluded that that by tampering with an unprotected wireless link, undesirable damage can be caused to the victim mobile devices and the victim networks. The disabling of the security mechanisms for the signalling and control messages opens up for many different attacks, such as false network access points, link hi-jacking by a mobile station, and other kind of tampering of signalling data that may e.g., cause channel deterioration. Mechanisms for confidentiality protection of the traffic have been specified for all systems.

Providing adequate message authentication mechanisms on the signalling channel can prevent some of these threats. It is also necessary to provide message authentication and confidentiality protection for the IP traffic as well. However, message authentication (integrity protection) is only provided in UMTS, with a clear purpose of providing integrity protection to the radio control signalling messages only. The keys for these security mechanisms are derived at the network level authentication procedure when the network access connection is set up. Hence the protection of the link level can be provided only after the initial authentication.

Open issues: One of the issues that may need further study is what is the optimal selection for the cryptographic mechanisms to be used to protect the link layer. Further, a general framework for link layer SA negotiation may be desired as well as a standard way of doing context transfer.

2.1.11 First hop security options

Several options exist for the protection of user and signalling data on the first IP hop between the mobile node and the access router. One may use IP layer protection only, link layer protection only or a combination of both.

Results: a thorough threat analysis was performed. It resulted that optimal performance of the wireless communication cannot be guaranteed without protecting the basic signalling messages at the wireless link. On the other hand, authentication, integrity protection, QoS, and access control issues are most efficiently dealt with at the network layer. This shows that a combination of link- and network layer security mechanisms seems to satisfy the relevant security requirements best. This has to be traded off against complexity, however. One level of complexity is provided by the heterogeneity of link layer

security solutions, and the fact, that the first hop may be a mix of radio (e.g. WLAN) and fixed (e.g. Ethernet) link layer elements.

Open issues: the optimal solution depends on influencing factors such as the precise nature of the access networks which are not known today.

2.1.12 Building block " Network domain security"

Network domain security is about securing the communication between network internal nodes, beyond the first hop. It is just as important as access security issues. Fortunately, the problem seems easier to solve.

Results: It was found that the solutions which are about to be developed for IP-based core networks in 3G systems are also expected to be suitable for systems beyond 3G. These solutions provide IPsec tunnels between network entities. There is no need for a full mesh of such tunnels, as communication between two networks may be directed through security gateways which establish tunnels between them. Security association set-up is assumed to be handled through an authentication framework based on the use of a public key infrastructure, and using state-of-the-art certificate management tools.

Open issues: the principles of the solution seem to be well understood. However, the completion of the standardisation process and in particular the deployment of network domain security for 3G systems are not complete and may lead to many detailed practical questions.

2.1.13 Security for Quality of Service procedures

The main threats toward QoS include DoS (both against users and networks), manipulation of QoS level, and hijacking of QoS reserved flows. Without security, a specific QoS level (except best effort) cannot be guaranteed. It is not only important to protect QoS signalling, but also the QoS reserved flows so that these cannot be e.g., hijacked or in some other way misused. The main requirement that needs to be fulfilled to create a good level of protection is that integrity protection on both the QoS signalling and the QoS reserved flows must be applied.

Results: instead of creating new specific security mechanisms for QoS signalling and QoS reserved flows, the preferable approach have been to re-use existing security solutions defined in SHAMAN. The network domain security model can be reused to protect signalling within the network. The first hop security mechanisms defined at the network layer between MN and BAR can be used to protect all traffic at network layer and above. Due to the trust model, this protection will be enough for the protection of QoS at layer 3 and above.
Open issues: the layer 2 QoS protection is still an open issue, as the existing technologies do not offer the required link layer protection of the QoS signalling (with UMTS as an exception). This is of course very much related to the open issue in the link layer security building block.

2.1.14 Support for standardisation

It has already been recognised in the SHAMAN Technical Annex that the actual standardisation activity making use of SHAMAN results would lie beyond the end of the project. Due to the well-know developments in the mobile industry over the past two or three years, the estimated time for the introduction of systems beyond 3G has been moved further into the future, and consequently, standardisation efforts to specify the architecture of such systems have not started yet. Nevertheless, several areas can be identified in which SHAMAN WP1 has prepared groundwork to for future standards:

- a draft specification for the negotiation of security associations for IPsec based on lightweight authentication and key agreement mechanisms is in a quite advanced state. Its suitability for the submission to the IETF is currently under investigation;
- further standardisation work on EAP-based authentication methods may be desirable; requirements for such authentication methods have been elaborated;

- the work on the security of the first hop is suitable as a basis for the selection of the appropriate mix of link layer and network layer security in future mobile access networks, which may be standardised in future releases of 3GPP;
- the work on the charging infrastructure, in particular the Cost Charging Centre (CCC), may be used as a basis for standardised architectures allowing for access by means of electronic payment. While this is clearly seen as an important option for the future, and standardisation will be clearly required for interoperability, currently, no standardisation activity seems to be under way, as the economic push for alternative means of network access does not seem strong currently;
- the manual authentication (MANA) protocols developed in WP2 for Personal Area Networks may also be suitably used in hot spot areas for access to wide area networks. Inputs to standardisation is being considered for the Bluetooth SIG and ISO SC27.

2.2 Work Package 2 - Unified security architecture for future wireless terminals and applications

In this section we give a summary of the technical achievement during the second year in work package 2. We give a brief background to the work package results. Next we outline the main results of the security architecture for distributed terminals specification work. In Section 2.3.2.3 a short description of the interactions with and dependencies of the reset of the SHAMAN work packages is given. Finally we discuss the standardisation contributions from WP2.

2.2.1 Background

The WP2 work main goal during the second year has been to develop a detailed specification of security architecture for a distributed terminal environment, or as we call the concept, Personal Area Networks (PANs). During the first year we performed a pre-study with several security surveys of relevant technologies. Requirements and challenges for a distributed terminal environment were identified. The pre-study defined the scope and goal of our work and became the foundation of the distributed terminal security architecture specification work. The work has been carried out starting from a simple PAN model and a set of PAN usage scenarios. The model defines the basic PAN entities, the components, and the terms we use to describe communication between components and PAN formation. The focus of the architecture specification work is on the security of the local communication and the local services provided by components. The main architectural building blocks are: PAN trust model, component initialization, manual authentication, PAN communication security, access control and PAN security domains. In additions, we covers delegated authorizations and secure execution environments for distributed terminals.

2.2.2 Specification of security architecture for distributed terminals

Below we give a short summary of the main results of the different parts in our security architecture for distributed terminal specification. All details can be found in the WP2 parts in the annex to this report.

2.2.2.1 PAN reference model

During the first year of the project we decided to work with a PAN model as reference model for the distributed terminal. The original model turned out to be a too broad definition and in order to narrow the WP2 scope we made a slightly revision of the reference model. Our PAN model relies to a great extent on existing PAN definitions like those provided by IEEE 802.15 and Bluetooth SIG. However, we work with generic technologies and we do not restrict ourselves to any particular local PAN interface, i.e., the interface used to connect components. We uses the following PAN definition:

A PAN is a collection of fixed, portable, or moving components within or entering a Personal Area, which form a Network through local interfaces. A Personal Area is a sphere around a person (stationary or in motion) with a typical radius of about 10 meters.

In addition to this basic definition we also define the basic terminology used in the security architecture.

2.2.2.2 PAN trust model

The trust model is the basis on which the security architecture is built. The trust model describes the different security relations we consider between PAN devices. Trust as such is a concept that can have very different meaning for different people. We have investigated the concept of trust and we explain how we treat the concept. The trust model we have chosen is a component centric model where all trust relations are viewed in relation to each component. Given one particular component in a PAN, what we call the *reference component*, we view the trust relation this component has to all other components in the PAN. Three trust classes have been defined:

- Untrusted component
- Second party component
- First party component

The untrusted class is all components for which the reference component does not share any security associations, while it does with first and second party components. The difference between first and second party components is in the amount of trust the reference component put into the components. First party components are in principle allowed to access all PAN services offered by the reference component and are hence considered as "highly trusted".

In addition to the three-class trust model we also use the concept of Personal Security Domain (PSD). A PSD is a group oriented trust model where all components in a group are given the same amount of trust when in comes to the right of accessing different PAN services.

2.2.2.3 PAN security requirements

We reviewed the role model developed at the start of the project for accuracy and continuing relevance of the roles defined. Suggested changes to the role model for use in future studies were made. The requirements described for each role were also reviewed for continuing relevance and whether or not they were met by the security architecture defined by Shaman WP2. Requirements that were still considered relevant but not met were identified, as input to future security research work.

2.2.2.4 Component initialisation

A prerequisite for secure communication and authentication of components is a procedure for equipping the component with a secure value of a cryptographic parameter and the necessary access policies. The initialisation procedure consist of three main steps: the establishment of an authenticated/secure channel to protect the rest of the initialisation, the establishment of cryptographic parameters for subsequent use in PAN security, and the configuration/negotiation of policies for service/resource access. Our architecture contains novel methods for initialisation. SHAMAN's manual authentication protocols are recommended for initial secure channel establishment; especially, for first-time primary initialisation. Several options for internal PAN security are possible using symmetric or public key techniques. In particular, public-key-based methods are interesting and together with WP3 we have developed the new *Personal PKI* concept, which is suitable for creating public key based security associations in the PAN environment. We conclude that component policy settings for first party components should be configured at the initialisation. While second-party configuration can be "negotiated" via a central PAN policy-controlling unit.

2.2.2.5 Manual authentication

Proving the identity of a component is part of the initialisation. We work with a PAN model where we can assume physical proximity between two components and in most cases that a user controls one or both components. Consequently, it will be possible to transfer information over a secure human channel between the components. This additional channel can be used to authenticate cryptographic information and other information transferred as part of the component initialisation. Authenticated key exchange is part of for example the Bluetooth standard. In Bluetooth the user is asked to enter the same *passkey* value into both components. The manual authentication is then based on this passkey. The manual authentication procedure is called *bonding* according to the Bluetooth terminology. If short passkeys are used (and the user do not want to enter long string values) the Bluetooth bonding algorithms are sensitive to passive eavesdropping or active man-in-the-middle attacks. Highly secure manual authentication using long passkeys or check values are well known but not special user-friendly. Hence, there is a need for new user-friendly secure manual authentication procedures. WP2 investigates three different manual authentication protocols. We call the protocols MANA I, II and III. MANA III is based on a proposal presented at a conference one year ago, while MANA I and II are developed by the SHAMAN project. We describe the protocols in details and we also gives a theoretical analysis of the security of MANA I and II. In addition, construction examples are given. We show that it is possible to achieve a fairly high security level using passkeys or check values not larger than 8 hexadecimal digits.

2.2.2.6 PAN communication security

Architectural building blocks for secure internal communication within PAN were basic requirements for the work. The final report contains an extensive treatment of protocols, analysis of existing layer 2 and 3 solutions and recommendations for the future.

We analyse to what extent the existing technologies and protocols, that are suitable for wireless intra-PAN communication, are appropriate for securing internal PAN data transfer. Based on this analyse we can recommend protection methods for the security architecture. Our analysis of Bluetooth and IEEE 802.11 WLAN shows that a solid security architecture cannot be based exclusively on the security services of them. The two main problems we have identified are the shortcomings of the current WLAN technology and the lack of integrity protection mechanism in Bluetooth. Our recommendations for the internal PAN communication security can be summarised as:

- Authentication can be provided at the link layer for direct communication between PAN components if the available link-layer authentication mechanism is reliable. Alternatively and in all other cases, IPsec with ESP in transport mode should be used to authenticate the links between PAN components.
- Confidentiality must be provided at layer 2.
- Integrity for both signalling and user data should be provided at layer 2.
- Identity and Location Privacy must comprise user identity confidentiality, component identity confidentiality, user location confidentiality and user untraceability. These services are not supported by the existing wireless technologies, which should therefore develop this functionality.

2.2.2.7 Access control

Access control is necessarily present at different levels in our PAN security architecture. Some form of authorisation is required if certain components attempt to use services offered by other component. The authorisation given to different components are given by the component access rules/policies. We discuss the requirements for expressing the authorisation policies. Access control is closely related to our PSD concept and we describe how access control can be achieved when using symmetric and public keys as basis for the PSD. The PSD specify common security and authorisation policies applicable to all members of that specific security domain. We provide formats for describing objects and permissions used for the access control mechanisms. We investigate three different approaches for how the permissions can be given:

- Access Control List (ACL)
- Symmetric key PAN tickets
- Public key PAN tickets

The different approaches are evaluated and compared. For the implementation of access control together with the PAN security domain concept in the SHAMAN demonstrator, the use of the access control list approach has been recommended.

2.2.2.8 PAN Security Domains (PSDs)

We use an approach where a common access security policy is applied to a set of component, called the PAN Security Domain (PSD). The purpose of the PSD is being able to run applications on a set of components in a secure and uniform way. An application might require a certain set of resources in a set of components in order to run properly. Then these resources must be available to all components in a PAN that utilize this application. Forming a PSD can do this. The following steps are part of the PSD set up procedures:

- Selecting a "PSD controller" component in the PAN
- Distribute available resources to potential PSD members
- Negotiation of resources and members in the PSD
- Key exchange with the PSD controller
- Generation and distribution of member-to-member (MTM) keys

We describe the format to use in order to negotiate shared resources and describe security policies. Based on the policies access control is provided through access control lists. Each member in the PSD must be able to authenticate each other member in the PSD and set up protected PAN links between themselves. This is done using the MTM keys. We describe both symmetric key and public key methods for generating and distributing MTM keys.

2.2.2.9 Delegated authorisation

Our security architecture is dependent on secure storage. Sometimes we also need to give some security sensitive functionality to one particular component in the PAN. This gives us high requirements on the physical security on the components. The vulnerability decreases if we are able to delegate cryptographic capabilities to other components in the PAN. Hence, we investigate PAN delegated authorisation. We introduces the problem of sharing authorisations and the notion of an authorisation domain, which allows authorisations to be granted to the domain, but used from any physical device that is part of the domain. We present improvements to a recently published protocol for capture-resilient devices and shows how the improved protocol can be used to realise the concept of authorisation domains. Our notable improvements are allowing delegation of authorisations from (a) a device of one user to a device of a different user, and (b) from one member of the authorisation domain to another.

2.2.2.10 Secure PAN execution environment

As part of the WP2 work we have examined secure execution environment solutions. We consider both execution environments contained solely within one component and distributed execution environments. We recall the requirements identified during the first year of the project and discuss how and if we have been able to meet the requirements. We describe secure delegation of software verification for the distributed environment and give an example of how it can be implemented in a Bluetooth PAN.

2.2.3 Other workpackages interactions and dependencies

WP2 have worked in close co-operation with WP3 on the work with defining a personal PKI for PANs. The personal PKI concept is one nice option of how to create the necessary security associations between the different PAN components. The WP2 requirements on key management and generation can be fulfilled with a design based on security modules. The requirements and possible

smart card solutions have been investigated by WP4. In particular, a security module preferably provides the core personal PKI functionality, the personal CA. In WP5 a demonstration implementation showing component initialisation using manual authentication protocols according to the WP2 security architecture. Furthermore, the local communication between the two components in the demonstrator show one the options described in the WP2 recommendations of how to secure the local wireless link. WP2 also contributed to WP1 by proposing MANA protocol to be used in the setting of network access for the provision of initial authentication of the network access point to the mobile node. Many of the results in WP2 have been presented at external conferences and at the SHAMAN workshop. The manual authentication protocols developed and evaluated by WP2 has been proposed as ISO and Bluetooth standards The WP6 deliverables describe all the details of the WP2 dissemination work.

2.2.4 Standardisation and industry forum contributions

The WP2 MANA work is most suitable to use in all kind of PAN component security initialisation situations. The MANA procedure has been submitted to ISO. The proposal has been discussed in the recent Warsaw meeting of ISO/IEC JTC1 SC27/WG2 meeting and received a high level of support from the working group delegates. It will be sent out for National Body ballot and it is therefore very likely that the work will proceed as part of the new entity authentication standard (probably becoming standard ISO/IEC 9798-6).

The MANA protocols have also been submitted to the Bluetooth SIG security expert group where it is under evaluation. The MANA I protocol is currently the main candidate for replacing the weak pairing procedure in Bluetooth and it is being proposed as a Bluetooth improvement.

The PSD work could as well be a possible input to the Bluetooth SIG as a framework for service level security in current Bluetooth and in particular upcoming high rate mode. WP2 is currently evaluating a formal PSD input to the Bluetooth SIG.

2.3 Workpackage 3 – Public key infrastructure for next generation telecommunications

Work package 3 is one of the two supporting technical work packages of the Shaman project. In this section an overview of the main results of this work package is provided, with emphasis on the results from the second year of the project. The results of this work package have been presented in detail in the following SHAMAN deliverables:

- D04, *Initial report on PKI requirements for heterogeneous roaming and distributed terminals*.
- D07, *Intermediate specification of PKI for heterogeneous roaming and distributed terminals*.
- D13, *Final technical report* (WP3 part).

The material in deliverable D07 has been extended and refined in deliverable D13. Thus, to obtain a complete picture of the SHAMAN WP3 results, it is sufficient to read D04 and the WP3-related part of D13.

2.3.1 Scope of WP3 work

The primary goal of the work within this work package has been to address the PKI-related requirements arising from the two primary technical work packages (WP1 and WP2). This has motivated two large pieces of work conducted within WP3, namely

- the work on *public key based network access*, outlined in section 2.3.2 and motivated by the requirements of WP1, and
- research on the *personal PKI*, as described in section 2.3.4, which was motivated by the needs of WP2.

However, over and above research arising directly from the requirements of WPs 1 and 2, research was conducted in a number of other areas based on assessments of likely future requirements for PKI

to support security for mobile telecommunications. This work has focussed on the following main areas, each of which are described in more detail below.

- *Public key revocation in a mobile environment* – this work is based on an assessment of requirements performed during the first year of the project.
- *PKI for secure execution environments* – security issues for mobile code of all types are a major current concern, and PKI is expected to play a major role in supporting future solutions.
- *PKI for limited devices* – some, if not most, of the devices in current and future mobile networks are expected to have limited computational and/or memory capabilities; supporting PKI functions on such devices is a major challenge.
- *Authorisation* and *Authentication* are two fundamental services which can be supported through the deployment of a PKI, and mobile specific issues relating to their provision are explored.

2.3.2 Public key based network access

Access to foreign access networks is the main focus of WP1. Access can be based on either secret key or public key techniques. In WP3, the cryptographic requirements for public key based network access have been considered, and the two public key authentication protocols chosen for further consideration by WP1, namely JFK and IKEv2, have been evaluated. Based on this evaluation, recommendations for the network access case have been given.

The work considers the security and privacy requirements that a public key authentication protocol must provide for access to a foreign access network. There are two cases: the "traditional" subscription case, where a user has a subscription with a home operator and, as a consequence thereof, a long-term trust relationship with this home operator, and the alternative access case, where the user pays ad hoc (using e-payment mechanisms) for services received by the access network.

The requirements for the subscription case are first considered; the differences for the alternative access case are then discussed. The discussion of requirements was used to analyse the suitability of various candidate protocols. Finally an assessment of the protocols against the requirements formulated for the subscription and alternative access case has also been conducted.

Two public key authentication and key agreement protocols were reviewed, namely

- JFK (which comes in two variants JFKi and JFKr), and
- IKEv2.

The protocols were evaluated with respect to the requirements identified previously. The assessment for the subscription case suggests that JFKi fulfils all requirements for network access. However, JFKr and IKEv2 do not protect the user from active attacks from bogus access networks and cannot therefore be recommended for the network access scenario.

In the alternative access case, the set of requirements differs because the mobile node (MN) may remain anonymous initially. This implies that the requirements for "authentication of the MN towards the access network" and "MN confidentiality" are not an issue. Instead, the MN requires the access network to authenticate itself towards the MN. The assessment of the public key protocols for the alternative access case concluded that JFKi, JFKr, and IKEv2 are all suitable for the network access scenario.

2.3.3 PK revocation in a mobile environment

In the first year of the project (as reported in D04), the use of four methods for clients to check the revocation status of certificates was considered: Certificate Revocation Lists (CRLs), the Online Certification Status Protocol (OCSP), the Simple Certificate Verification Protocol (SCVP) and the XML Key Management System (XKMS). These four techniques/protocols were described but not compared to any great extent. In the second year of the project the two most promising of these four protocols, namely OCSP and XKMS, were subjected to further analysis, compared, and recommendations were then formulated as to which should be used for the applications under consideration within SHAMAN.

SCVP was excluded as progress on it within the relevant standards body (the IETF PKIX group) has stalled, and there is little support for its continuation. A major fault with CRLs identified in many places is that, in the mobile domain, CRLs cannot be used to provide up to date certificate revocation information because their size means that mobile bandwidth considerations prevent updates of CRLs, and infrequent CRL update considerably reduces the effectiveness of CRL use. These considerations motivated the focus on OCSP and XKMS.

To compare these two methods a set of criteria for the comparison were formulated. These criteria are:

- Security mechanisms (what security is provided and how?);
- Current support (standards and technologies implementing the method);
- Hardware and software support (can mobile handsets support the method? What are the implications?);
- Memory and bandwidth implications.

The conclusion from this comparison was that, overall, OCSP seems to be the preferable solution for certificate revocation in the near future due to the significantly smaller size of its messages compared to XKMS and the fact that it can be implemented more easily on the client side.

2.3.4 The personal PKI

The use of PKI and public key mechanisms in Personal Area Networks has been discussed in D07 and is extended for D13. The following issues have been investigated:

- General management issues in the personal PKI, such as the handling of keys and certificates.
- Requirements for the personal PKI have been listed and evaluated.
- The operation of a personal CA has been described and the concept of multiple personal CAs has been introduced. That is, because a CA hosted on a mobile device might not be constantly available in a PAN, other devices might act as secondary CAs. In this context synchronisation issues and root-key-distribution are of importance.
- Device initialisation is a subject already discussed in WP2 and earlier in WP3. In more recent work this topic has been addressed in more detail. A protocol was given and evaluated, and scenarios with very restricted devices have been investigated. Finally an analysis of a somewhat similar scheme, described in a Maher patent and dealing with device initialisation, too, has been given.
- The use by a CA of proof of possession, i.e. to obtain evidence that a party requesting a certificate for a public key is in possession of the corresponding private key, has been analysed. Several different mechanisms have been proposed and discussed, and comparisons made between the proposed methods and the contents of relevant standards.
- Over and above revocation mechanisms, as they are used in a conventional PKI, the PAN offers the possibility of introducing new revocation mechanisms. Such mechanisms are described and evaluated.
- A comparison of traditional PKI mechanisms with the concept of ID-based cryptography in the context of the PAN has also been performed.
- Finally, conclusions and further research topics arising as a result of the work have been given.

2.3.5 PKI for secure execution environments

This work has considered the use of PKI to address security issues relating to the download of executable code from outside of the PAN over a global interface. A detailed assessment of the security requirements has been performed. This led to an initial assessment of authorisation issues, based partly on a critical assessment of the approach followed by MExE.

This has been followed by a consideration of issues for authorisation and authentication that are raised by the presence of an execution environment on the device, whether secure or not. More correctly, it is not the execution environment that raises the issue but the presence of flexibility in terminal

behaviour in general. This issue was explored using two examples, Digital Rights Management and Bluetooth, and the general issues that these examples raise were considered. Finally, some ways that public key techniques can be used to resolve this issue have been examined.

Other work in this area has included consideration of whether it is really necessary to make execution environments on mobile devices secure.

2.3.6 PKI for limited devices

PK techniques are computationally more intensive than secret key techniques (especially hashing), even purportedly more efficient techniques such as those based on the use of elliptic curve cryptography. If certificates are used to transmit the public key to the verifying entity, then the following requirements apply:

- the provision of root and intermediate certificates at the entity;
- a reliable, resilient (and ideally, one that cannot be changed by the user) time source at the verifying entity to verify that the certificate has not expired;
- in some cases, long certificate chains are needed, which require extra bandwidth and processing;
- the client should ideally have access to revocation status information on the certificate.

These requirements are all significant for limited devices.

Further, an entity seeking to obtain a certificate for itself must go through a reasonably intensive registration procedure in order to gain a certificate from a public CA. This is because it is seeking to authenticate itself to an entity with which it has no existing trust relationship, that is, the RA of the public CA.

Ways of ameliorating these issues have been investigated and conclusions drawn.

2.3.7 Authorisation

The issue of authorisation, i.e. granting rights to certain people or instances, has been investigated. Authorisation with symmetric cryptographic mechanisms was only discussed briefly whereas several scenarios for authorisation supported by certificates has been looked at in more detail.

Several possible mechanisms have been considered.

- The use of different ‘certificate classes’ related to several sub-CAs. This scenario was discussed as a solution which is easy to implement.
- The use of extensions in X.509 certificates as a basis for authorisation. This solution is easy to implement, as X.509 offers the possibility of private extensions, containing ‘non-standard’ information.
- The use of attribute certificates. These certificates, usually not containing cryptographic keys, are bound to a public key certificate. Attribute certificates are used to certify certain roles or rights. Due to the linkage with the public key certificate the registration process is much easier.
- The use of SPKI certificates was introduced briefly.

2.3.8 Authentication

Authentication has been considered, with a focus on mechanisms using public key cryptography.

In the public key context requirements for a server and requirements for the mobile devices are listed and compared. Finally, several interoperability issues are investigated.

2.4 Workpackage 4 - Security Modules

2.4.1 Scope of work

The purpose of Workpackage 4 is the development of a concept for a security module (SM) which provides high security for future mobile communications in heterogeneous networks.

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. A 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 for this purpose. Security modules are a flexible and secure mechanism to allow for secure and personalised mobile communication within today's mobile communication infrastructure. They must be designed to be easily administrated and exchangeable.

The use of security modules for holding sensitive data is already widespread 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.

The most obvious example for an application making use of security modules is GSM. The security module for GSM is the SIM card; it is required to authenticate itself to the network on 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).

2.4.2 Smartcard technology trends

Smartcards as tamper-proof devices are especially designed to minimise the probability of all kinds of attacks on its security features. Examples of attacks that a smartcard must withstand are SPA (simple power analysis) or DPA (differential power analysis), which could be used by an adversary to discover a secret key stored on the device. The downside of smartcards, as well as of all tamper-resistant devices, is the shortage of storage and processing power; security modules are therefore also "constrained devices". However, the technology evolves about at the same speed as standard microprocessor technology, it only follows it with a delay of about 8 years. For the following 5 years, a strong improvement of performance can be expected; the chip's clock rate will probably rise from typically 1-5 MHz today to 20-33 MHz, the storage capacity of the EEPROM from 16 kB to 32-96 kB and the transmission rate which is 9,6 kB/s across a serial interface will presumably reach 115 kB/s because of the ubiquity of USB interfaces. Equally, the power of coprocessors which are mainly used for numerous cryptographic algorithms will increase significantly.

2.4.3 Requirements on the security module

A security module must meet several requirements in the SHAMAN context. High-level requirements have been formulated and summarised for the individual workpackages 1-3 as well as from the workpackage 4 and user perspective.

The high-level requirements had to be refined in order to specify the low-level functionality that a SHAMAN-compliant security module must provide. The result is a number of basic functions (like storage of data or execution of cryptographic calculations) it must implement, as well as the support for certain protocols. The latter is also denoted as "functionality split" between a mobile node (a

terminal) and its security module (a smartcard). A subset of these protocols (and possible versions for the functionality split) are implemented in the SHAMAN demonstrator.

For WP1, the security module must support secure network access. The functionality split for one secret key (AAA for IPv6) and two public key protocols (IKE and JFK) was studied. In addition, the involvement of the security module in security mechanisms for protecting the confidentiality and integrity of the access link was investigated. It was assumed that the security module is not directly involved in the protection of the access link communications; instead the session keys are generated as part of authentication on the security module and then passed to the terminal where they are used.

For WP2, work focussed on secure PAN internal communication and distributed security modules. It was studied how the SM is involved in the imprinting process. Additionally, the SM needs an authentication algorithm for connection establishment, whereas confidentiality and integrity protection on the SM are not practical. The workload of security functions on a SM can be distributed either on a group of SMs or between a SM and an untrusted device. The distribution of a single private key operation between the SM and an untrusted device was described. In this way, the workload on the SM for an RSA computation can be reduced to about 7%. Delegated authorisation of the RSA private key was also studied. In delegated authorisation the use of the RSA private key can be delegated to other devices. Requirements for a SM providing delegated authorisations were identified.

For WP3, it was investigated how a SM can implement or support a personal CA (certification authority). Requirements for a SM in a CA client device and a CA server device have been identified. These have to be fulfilled in order to set up a PKI (public key infrastructure) within a PAN (personal area network).

2.4.4 Reference model

Altogether, the requirements from the workpackages lead to a multitude of functions which should be implemented on a smartcard. With today's technology, not all of these can be implemented on a single device. It is necessary to define the demands for security more clearly and to find a trade-off between high security on the one hand and feasibility as well as performance on the other hand. Therefore, three different levels of security have been defined which form the basis of a security module reference model.

The first two levels are called "intermediate" and "high security", whereas the third is called "personal-CA level"; the latter fulfils all requirements for the set-up of a PKI as defined in WP3. For the intermediate level, functions like random number generation, storage of long-term secrets and calculation of a one-way function are required, which are readily available on common smartcards of today. In addition, basic protocol support for a secret and a public key protocol must be present, which is not standard functionality. For high security, it is also demanded that the SM be able to store short-term secrets, compute Diffie-Hellman secrets, create public-private key pairs on card and store security contexts (for plastic roaming). Besides, some more advanced (and more secure) protocol options must be supported. For personal CAs, the smartcard should also be able to manage certificates, i.e. store, create and validate them, including revocation checks.

Today's smartcards already offer an appropriate basis for the realisation of a SHAMAN-compliant security module. All of the intermediate level and some of the high level functions (as defined above) can be provided. The rapid increase of storage capacity and processing power will allow more sophisticated solutions in the near future, offering the user a personalised token with high flexibility and maximum security.

2.4.5 Deliverables in WP4

In the project year 2001, the deliverable D5 was finished which provided a common understanding of the term "security module" and a set of requirements which a security module has to fulfil in the SHAMAN context.

The next deliverable D8, which was finished in May 2002, provided a detailed scenario for the low-level functionality of the SHAMAN security module. However, at this stage the functionality split between mobile node and security module for the crucial protocols of WP1 and WP2 was not yet determined. This was a task for the remaining work and will be included in the final deliverable D13.

2.4.6 Cooperation with other workpackages

WP4 is a supporting workpackage for WP 1-3: The security module must serve as a secure container or execution environment for critical data and processes. On the other hand, WP4 delivers input for WP5, the SHAMAN demonstrator. The demonstrator will implement a subset of the security module's functionality in order to investigate feasibility and performance of the respective features.

2.4.7 Issues arising

Issues emerged from the workpackages 1-3 as follows: In WP1, the problem of secure network access must be solved. Public as well as secret key protocols are candidate solutions for this problem. As an example for a secret key protocol, AAA for IPv6 was investigated. Among the public key protocols, the IETF work to develop a possible successor to the IKE protocol was monitored. Today, IKE is regarded as heavyweight and difficult to implement. Nevertheless, since the son-of-IKE is not yet finally determined, the functionality split for the IKE protocol was investigated. The JFK protocol, which is one promising candidate for an IKE successor, was investigated as well. As already mentioned, the role of the security module in protecting the first hop is not as crucial; it just creates short-term keys and passes them on to the terminal.

In WP2, solutions for internal PAN communication and secure initialisation of components have to be found. The secure initialisation can be achieved using a manual authentication protocol (MANA) and an imprinting mechanism for either an asymmetric system or a symmetric system. The subject of investigation in WP4 is which steps of these protocols must happen in the security module and which data must be stored therein. For other requirements like confidentiality and integrity protection it must also be investigated what kind of support a security module could provide. Another area of investigation was the distribution of workload across several entities with different security capabilities; since security modules are constrained devices, it may be beneficial to delegate part of its workload to more powerful devices, and the challenge is to find protocols which do this without a loss in security.

In WP3, the concept of a personal CA was introduced, and the question arose how a security module can fit in this scenario. The desired degree of security can only be achieved if certain tasks are done by a smartcard, on the server as well as on the client side.

All these requirements from the workpackages should be categorized and prioritised to form a unique model for a SHAMAN-compliant security module, the reference model.

2.4.8 Work and solutions

For the secure network access, two versions of the AAA protocol were presented: One basic version and one with an extra challenge from the home network. It turned out that two new commands for the smartcard are necessary, and that both protocol versions are stateful. A detailed message flow for the functionality split was given. The IKE protocol was thoroughly investigated with respect to functionality split. However, this won't be applied in the long run, so it was necessary to determine the functionality split for a son-of-IKE candidate, too; the chosen one was JFK. Five possible functionality split options have been presented. The most important task for the security module is the creation of a private/public key pair (creating them on card offers even higher security) and using the private key for signing operations. All other tasks were not regarded to be as critical, so that the 5 options don't differ substantially in the security they offer. In order to minimise the amount of data to be transferred to the smartcard, not the whole data to be signed will be transferred, but only their hash. In order to prevent chosen hash attacks on the private key, this hash value can be rehashed on the card. Additionally, the card must create a number of short-term secrets by applying a keyed hash function

(HMAC) to a formerly negotiated Diffie-Hellman key. For the demonstrator in WP5, two of these JFK split options will be implemented.

On behalf of WP2, protocols for component initialisation had to be investigated with respect to security module tasks and functionality split. It turned out that the security module must at least be able to perform a one-way function. In order to improve security, it could also optionally perform steps according to the Diffie-Hellman protocol, i.e. create a random number and carry out exponentiation and modulo divisions with big numbers. For confidentiality and integrity protection, the security module must derive short-term keys, which basically boils down to performing a one-way function again. The security module can also support secure download by storing certificates and verifying signatures, but this is not mandatory.

For WP3, it had to be investigated how a security module can enable the operation of a personal CA. Here, it has to be distinguished between the case of the device which itself acts as the CA (the server) and another device which wants to have its public key certified by the CA (the client). On both kinds of devices, the security module needs to fulfil certain tasks; on the client, it should be able to create a private/public key pair on card, store it and use it in subsequent calculations. On the server, it should be able to fulfil the same tasks as on the client plus the creation of certificates and possibly CRLs (certificate revocation lists); optionally, it could also support secure auditing, i.e. collect integrity-protected records of events, and messages from OCSP.

2.4.9 Feasibility of the features on common smartcards

Most of the requirements which have been identified as a result of the WP4 investigation work are already available today on common smartcards. Certain other tasks are specific to protocols and the corresponding functionality split, but can be implemented without major difficulty, including the introduction of new command APDUs. Diffie-Hellman calculations are not commonly available on smartcards, but can also be implemented with manageable effort.

However, some requirements, especially those which have to do with certificate handling, may impose a high workload (because of the sheer amount of data which has to be transferred and processed) on the smartcard which today's devices typically can't easily manage. Although the concept of server-aided RSA computation increases rather than decreases the amount of data which has to be transferred and processed, it could help to reduce the amount of work the security module has to do when signing the certificate using the RSA private key. In server-aided RSA, the amount of work to do by the security module for RSA signing can be reduced to about 7%.

However, in future smartcards all of the required features (including those for the personal CA level) may be available, due to increased storage capacity and processing power. An estimation about the necessary hardware features for a SHAMAN security module (at least for the intermediate and high security level) was given. Current state-of-the-art smartcards can already fulfil these demands.

2.5 Work Package 5 – Prototypes

In this section, we give a summary of the main results and technical achievements during the second year in work package 5. First, we give a small introduction detailing the scope of this work package and then, we will further elaborate on the use cases that will be worked out in the demonstrator. A brief overview of the hardware and software architecture will also be given.

Recent results of the workpackage are covered in deliverable D11; no annex of extended description of results is therefore attached. Full results of the demonstrator work will be included in the final project documentation.

2.5.1 Scope of the Work Package

The goal of the SHAMAN Demonstrator is to prototype critical components of future mobile security architectures, identified within the project by WP1 and WP2.

The demonstrator concentrates as much as possible on the mobile security aspects of various user scenarios and reuses existing implementations where possible. With respect to the mobile technology, 'real' technology will be used where possible, including smart card technology for implementing critical security components at the user side, Bluetooth for personal area network communication and IEEE 802.11 for network access communications.

2.5.2 Demonstrator Scenarios

There are two main scenarios. The first scenario focuses on secure network access, based on public key techniques; this is one scenario identified in WP1. The second scenario reflects the work of WP2 on secure PAN communication. Both scenarios will briefly by explained below.

2.5.2.1 Secure access to heterogeneous networks, based on public key techniques

In this paragraph we describe WP1 network access scenarios, parts of which will be implemented in the WP5 Demonstrator.

Basically, there are two different cases where public key authentication can be used for network access. In the first case, the "traditional" case, the user of a MN is subscribed to a home network and requires access to an unknown access network that has a trust relationship (i.e. a roaming agreement) with the home network. In this case, the user can exploit his long-term relationship with the home network for gaining network access. The second case is the alternative access case where a user of a MN is not subscribed to a home network, or the home network is not trusted or not accessible by the current access network. Instead, the user aims at securing the wireless link between the MN and the AR using public key techniques.

There are two possibilities for employing a public key based approach. The following first step is performed in both approaches:

1. The MN pages for network APs that advertise services for its home operator or another trusted third party (e.g. a roaming broker). The MN announces the identity of this home operator or trusted third party. The access network has a number of public key certificates, at least one signed by each home network or trusted third party with which it has a roaming agreement. The AP selects the right public key certificate and sends it to the MN. By verifying this certificate the MN is assured that a roaming agreement exists between the MN's home network and the foreign network.

The next step involves the MN and the access network employing a public key based authentication protocol.

2. The MN directs its authentication request to the access network. This message authenticates the MN. There are two main possibilities here, depending on whether the MN's identity is encrypted with:
    a. *The public key of the home network*: In this case the access network is not able to authenticate the MN. Assuming that the message contains information regarding the MN's home network, the access network forwards the message to the MN's home network which is able to verify the MN's identity and sends a corresponding message to the access network. In this case, the MN remains anonymous towards the foreign network.
    b. *The public key of the foreign network*: In this case the access network is able to verify the identity of the MN. Hence, there is no necessity to involve the home network in the authentication process (except if revocation checking of the MN certificate is required).

So, the MN and the AR need to establish an SA (and generate a secret key from which other keys, for authentication and encryption, can be derived). On the network layer, IPsec provides a solution. Today, in IPsec, these SAs can be established by running the IKE protocol between the MN and the AR. However, IKE is considered a complex protocol. This issue has been recognised by the IETF

IPsec working group and two proposal son-of-IKE protocols are being discussed, i.e. JFK (Just Fast Keying) and IKEv2.

For the WP1 Demonstrator, the JFK protocol will be used to generate a secret key between a laptop representing a mobile node and a laptop representing the AP of an operator's access network. On the mobile node side, a real smart card will be used for security critical components.

2.5.2.2 Secure personal area network communications

In this paragraph, we describe a WP2 scenario, parts of which will be implemented in the WP5 Demonstrator.

In WP2, manual authentication or imprinting has been studied where the imprinted devices obtain a certificate on a public key (the private/public key has first been generated in the PAN component to be imprinted). In order to provide this functionality, WP2 and WP3 have developed a new PKI concept called a "Personal CA". The personal CA is used by an ordinary user for home or small office deployment. As with any other PKI, we would like all units in a communication network to share common root public keys and use certificates issued by a trusted CA corresponding to the public root key. One of the personal components must act as a "Personal CA". Such a component is able to issue certificates to all other personal components. Hence, since all the personal components can be equipped with certificates issued by the same CA, i.e. the personal CA, they will all share a common root public key. Consequently, the public keys in the certificates can be used to exchange session keys or authenticate personal components in a PAN.

Then, after being imprinted, two first party components can exchange any information authenticated and confidentiality protected, based on a derived shared secret or on their certificates and the public key of the personal CA. It is possible to run a higher layer authentication protocol based directly on the security association, and derive mutually known authenticated secret keys for confidentiality and integrity protection of the communication. Another possibility is to perform only the authenticated key exchange at the higher layer. The mutual authentication of the components is performed at the link layer, where the keys for integrity and confidentiality protection of the data are derived. This approach is favourable for devices running a wireless link technology with good authentication and key agreement functions. This is illustrated in the figure below, where after the imprinting step of both devices, a higher layer handshake protocol is run to exchange the certificates between the components, and create and exchange a secret key. In principle any higher layer key exchange/ key agreement protocol can be used. This secret key would then be used to derive the necessary link keys for authentication and confidentiality protection at the link layer.

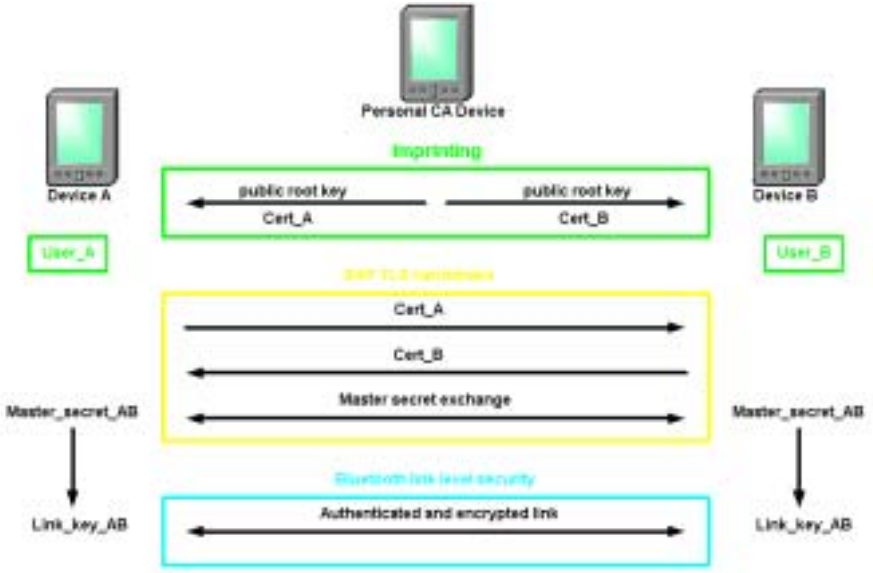

Figure: Schematic overview of the Imprinting protocol and subsequent authentication

The WP2 Demonstrator will focus on the implementation of the MANA I and the imprinting protocol. For the imprinting protocol, we have opted for “Imprinting for a public key system”, this to further illustrate the concept of a “Personal CA”. After this imprinting step (of two components), the JFK protocol, already been used for the WP1 Demonstrator will be reused as the protocol for key agreement. The derived secret key during this JFK run will be used further to establish the Bluetooth link layer keys. To this end, we use an external piece of software, originally not part of the demonstrator.

2.5.3 Demonstrator Architecture

2.5.3.1 Hardware Architecture

The demonstrator architecture is targeted towards the BRAIN (access) network. However, no attempt is made to build a real BRAIN network; instead, the BRAIN access and home network are software emulations on one or more PCs. For the mobile nodes, ‘real’ wireless technology is used, especially with regard to the link layer. However, higher layer functionality will be implemented and integrated on PCs, enabling the developer to implement the protocols in a way that allows the user to gain insight into their functioning. For the security-critical parts of the protocols, a real smart card will be used.

In the following figure, we represent the hardware set-up. A first laptop is connected to a card reader. A second laptop, possibly also equipped with a smart card, is connected to the first laptop via a wireless link. For the WP1 scenario, this wireless link will IEEE802.11, while in the WP2 scenario, the wireless link is based on Bluetooth technology.

Figure: Demonstrator hardware set-up

2.5.3.2 Software Architecture

The software architecture supports the use cases selected by the other SHAMAN work packages. Besides, the following design goals are also met:

- A smart card as well as a smart card simulation should be usable; it should be possible to switch to new cards and new card middleware without significantly changing the rest of the system.
- Several protocols could be utilised, added and replaced without significantly changing the rest of the system (plug-in-principle).
- It should be possible to use existing protocol implementations, eventually written in different programming languages.
- The architecture could be extended and reused in future projects.
- Portability and interoperability (e.g., usage of a heterogeneous environment like LINUX and Windows machines at the same time).

This generality can be achieved by choosing an architecture consisting of 3 building blocks where the different blocks communicate with each other via sockets. The information to be exchanged consists only of ‘protocol’ messages with a relatively simple structure, so a more high-level communication is not of much use. A socket interface is the best choice in terms of openness, portability and extensibility. Of course, a socket interface also has its drawbacks: It is low-level and therefore not very user friendly, and issues like thread handling may be tricky.

The software architecture consists of three building blocks, called the controller-, protocol- and card subsystem. The purpose of the controller subsystem is to start the whole system, read configuration information, offer the user some way of interaction and display all interesting events on a GUI. The protocol subsystem contains all protocol implementations. Those can be open-source implementations, which would in this case just have to be adapted to the architecture, namely supplied with the proper interfaces and breakout calls. The card subsystem consists either of the card itself with the corresponding card reader (hardware), the driver and the so-called “middleware“ (which provides an API for communication between application programs and a smart card), or of a card simulation that can be used in case there is no smart card or reader attached.

2.6 WP6 - Dissemination, external relations and liaison

The main objectives of WP6 are the establishment and coordination of relations with relevant standards bodies and industry forums in the area of mobile security. In addition, the technical results and achievements of the SHAMAN project are to be disseminated to a wider public by the means of publications and presentations as well as by electronic means like the Internet.

2.6.1 Dissemination of results from the SHAMAN project

During the report period, the dissemination of SHAMAN results was performed in the form of publications and presentations. Various scientific conference contributions have been prepared to inform the mobile security research community about the advances in the SHAMAN project. A detailed list of the second year SHAMAN publications can be found in Annex 2 of this report. The publications and presentations have been appended to the Annex. To give interested readers information about the work performed for deriving the results of the SHAMAN project which are more detailed than those based on the presentation slides or on the published scientific papers, also all the public project deliverables have been made available via the SHAMAN web site at http://www.ist-shaman.org .

As another major action within the dissemination efforts of the SHAMAN project a workshop was organised by workpackage 6. The one-day workshop was held on July 25, 2002 and was hosted by Royal Holloway, University of London, at Egham, Surrey. The event found widespread interest: 130 participants from many European countries attended the workshop. The participants came from commercial / industrial organisations (88), academia (31), government agencies (9) and two not further specified. At the SHAMAN workshop, the latest results from the SHAMAN project were presented and a number of invited speakers working in scientific fields related to the SHAMAN activities gave presentations about their views on specific mobile security issues. The workshop was finished with a panel discussion where the workshop speakers were discussing *"The way ahead – Security issues for future mobile systems"* with the workshop audience.

A number of comments were received in response to a follow up email to the registration list. All of them were positive about both format and content; our favourite was one that would have liked more SHAMAN material and fewer invited presentations.

2.6.2 Liaison with standards bodies, industry forums and other research projects

As part of the work in the SHAMAN project, ongoing activities in different standardisation groups and industry consortia are monitored with respect to their possible influence to the work of SHAMAN. Inputs from standardisation activities and other research projects in areas relevant for SHAMAN workpackages can be summarised by the following list:

- IETF (Internet Engineering Task Force):

  The IETF work on various authentication and key agreement protocols was considered in the activities performed in WP1 and WP2: EAP (Extensible Authentication Protocol), JFK (Just Fast Keying), IKE, IKEv2 (Internet Key Exchange protocol) and SRP (Secure Remote Password Protocol) have been evaluated for the SHAMAN security architecture components.

For securing the communication and for the enhancement of communication confidentiality, various alternatives of IPsec tunnels have been analysed.

That work our analysis has been based upon was performed by the following IETF working groups and published e.g. in the form of internet drafts: AAA (Authentication, Authorization and Accounting), EAP (Extensible Authentication Protocol), PKIX (Public Key Infrastructure X.509), IPsec (IP security), PANA (Protocol for carrying Authentication for Network Access), NSIS (Next Steps in Signalling), and IPSRA (IP Security Remote Access). It has been analysed for the SHAMAN work and comments have been sent to the authors of the respective internet drafts.

Within the quality of service (QoS) work performed in SHAMAN, resource reservation protocol (RSVP) and DiffServ (Differentiated Service) have been considered.

- 3GPP (3rd Generation Partnership Project):

  The 3GPP WG SA3 (Security) is working on the standardisation of next generation mobile network security features. Related to SHAMAN, the following work items were the most important for consideration in SHAMAN work: PKI based key management for network domain security (related to WP3 and WP1), the support of subscriber certificates (WP1, WP2, WP3), WLAN interworking aspects (WP1) and user equipment functional split (WP2).

  - ETSI (European Telecommunications Standards Institute)

    The EP SCP (ETSI Project Smart Card Platform) working group is active in the standardisation for smartcards as a common IC card platform for 2G and 3G mobile telecommunication systems. Their current discussions have also been evaluated within WP4 and results from the SHAMAN project will be forwarded to EP SCP for their future standardisation efforts.

- MIDP_NG (Mobile Information Device Profile – New Generation)

  Even though there were no direct inputs to MIDP 2.0 from the SHAMAN project, the time spent on developing and researching into various security requirements and mechanisms provided a good foundation to understand the requirements from the MIDP 2.0 specification. In particular, the concept of security policy used in MIDP 2.0 (as a secure execution environment) was influenced by some of the early work on PSDs that took place in SHAMAN WP2.

- Other IST (Information Society Technologies) projects:

  The BRAIN network reference architecture developed in the IST-1999-10050 BRAIN project (Broadband Radio Access for IP based Networks) has been selected as base for describing the components to build up a security architecture in SHAMAN. Some information exchange between the BRAIN successor project, IST-2000-28584 MIND (Mobile IP based Network Developments), and SHAMAN has been established.

  Information exchange by mutual workshop presentations has been performed with the IST-1999-20117 INTERNODE (Interworking of Nomadic Multidomain Services).

  Similarly, mutual review of project deliverables and consideration of the partner's results in the own work has been performed with the IST-2001-34157 PACWOMAN (Power Aware Communications for Wireless OptiMised personal Area Network).

Members of SHAMAN are also active in the mentioned standardisation groups. Therefore it is very likely that results from the SHAMAN project are integrated in future releases of the respective standards even after the termination of the SHAMAN project itself.

3 Conclusions

The project has to a very large extent achieved what it set out to do in the chosen areas:

the development of architectures and technical approaches for
heterogeneous network access and roaming and for
future mobile terminals, together with supporting technologies in the fields of
PKI and the *security module*.

The precise challenges were unknown at the outset, and could only be clarified as the work progressed. As a consequence, a number of open issues are identified which need to be addressed in future research and the development of standards. The main achievements with respect to those challenges are listed in section 3.1, below, and the open issues are given in section 3.2. They are discussed at greater length in the respective workpackage annexes.

3.1 Major results

This section summarises what are judged to be the more important results of the workpackages.

WP1

- a flexible security architecture for post-3G mobile systems;
- for each building block in the architecture, a list of evaluated candidate protocols;
- sound engineering knowledge about how to select and combine the most suitable candidates according to the evolving needs and requirements of post-3G mobile systems.

WP2

- development of a Personal Area Network (PAN) as a model for future mobile terminals;
- a comprehensive treatment of PAN security resulting in a novel flexible PAN security architecture; the architecture has broad coverage including PAN access control, policy handling, delegation of authorisation and software downloading;
- a new PAN security trust model;
- different PAN component security initialisation and internal PAN communication security alternatives developed, analysed and compared;
- new protocols for manual authentication of PAN components; the protocols have been submitted to ISO and the Bluetooth SIG as standards proposals.

WP3

- assessment of suitability of public key based authentication protocols for use in access authentication, for both subscription-based and ad hoc payment cases; selection of appropriate protocols;
  (Work motivated by WP1)
- novel techniques proposed for management of PKI in personal environment;
  (Work motivated by WP2)
- recommendations made on PK revocation and code authorisation in secure execution environments in mobile context.

WP4

- an analysis of requirements and identification of roles for SM in post-3G mobile systems;
- a reference model for the *security module*;
- identification of functionality split and partitioning of responsibilities between SM and its environment.

3.2 Open issues

WP1

- further work is needed on the following topics, all of which need to be taken up in the standards bodies
- EAP-based authentication methods;
- a transport-independent protocol to carry authentication information;
- secure address configuration;
- the combined use of link and network layer security in a post-3G architecture;
- standardised security context transfer;
- layer 2 Quality of Service protection.

WP2

- purely symmetric key based component initialisation methods,
- hardware and software complexity figures for different manual authentication and key exchange options,
- comparison between most recent PAN technology standards developments and our PAN internal communication security requirements,
- details of access control information exchange protocols and formats
- further development of our PAN security domain concept,
- elaborate usage scenarios and investigate partial authorisation and chained delegations for our delegated authorisations approach,
- standardisation proposals for verification and authentication for PAN software downloading.

WP3

- Consequences of lack of mobile node authentication in non-subscription case needs further investigation.
- Alternatives to use of PKI and code signing need to be investigated for secure execution environments in mobile domain.

WP4

- further examination of *Real World* and *End User* requirements and deployment
- research into advanced distributed protocols - beyond distributed RSA etc.
- extension of the scope of smart card standards, introducing protocol support etc.

3.3 Impact of current or emerging standards on work of project

Details about the affected SHAMAN workpackages and technical work items which received inputs from other standardisation activities have already been reported in section 2.6.2.

3.4 Impact on the Work of Standards Bodies.

The subsequent section reports on the activities in the SHAMAN project which have been or will be taken to forward results and information from the SHAMAN project to standardisation bodies. It has already been recognised at the outset of the project that the actual standardisation activity making use of SHAMAN results may lie beyond the end of the project. Due to the well-know developments in the mobile industry over the past two or three years, the estimated time for the introduction of systems beyond 3G has been moved further into the future, and consequently, standardisation efforts to specify the architecture of such systems have not started yet. Nevertheless, several areas have been identified in which SHAMAN could already contribute to standards bodies or has prepared groundwork for prepare for future standardisation efforts.

- 3GPP (3rd Generation Partnership Project):

  It is expected that SHAMAN WP1 results especially will be applicable to post-release 6 of 3GPP in the future. The respective information will be forwarded by SHAMAN members which are also active in 3GPP WG SA3.

- Bluetooth Consortium / Bluetooth Security Expert Group

  The SHAMAN work related to Bluetooth Consortium / SEG addressed secure manual procedures for authenticated key exchange for strong pairing procedures in distributed environments. As results from SHAMAN WP2, the MANA I and II manual authentication protocols, have been forwarded to Bluetooth SEG by the respective members.

[1] Kaisa Nyberg (Ed.). *A Protocol for Enhanced Bluetooth Pairing*. Submitted to Bluetooth Security Expert Group on 26-OCT-2002

- ISO (International Organization for Standardization)

  The MANA (manual authentication) protocols developed in SHAMAN WP2 have been submitted to become part of the new ISO authentication standard ISO/IEC 9798. The submission has been subject to discussion by the ISO/IEC JTC1 SC27/WG2 meeting and was sent out for National Body ballot.

[2] *National Body Proposal for a New Work Item on Entity authentication based on manual data transfer*, Document ISO/IEC JTC1/SC27 N3316, submitted on 02 Oct 2002, Secretariat ISO/IEC JTC 1/SC 27 . DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany

3.5 Practical experiments

It was never the intention to conduct user trials or experiments involving actual network access, but rather to prototype certain critical or novel developments using PC technology together with smart cards. The resulting SHAMAN demonstrator from workpackage 5, demonstrates concepts developed in the SHAMAN project. It will be available after the completion of the demonstrator in the first quarter of 2003.

3.6 Patents

SHAMAN has submitted a patent entitled "audible hashes". If you are sending a public key from one terminal to another, a PKI hierarchy can be used, or some sort of OOB integrity method such as sending a (truncated) hash of the key by a secure OOB method and then asking the user or device to compare expected with received hash can be used. The SHAMAN patent concerns sending such a hash from a terminal device or component that does have a display to a neighbouring terminal device without a display. Instead of displaying a hash of the received public key, the receiving terminal would use some text–to-speech functionality (which could be quite simple if just covering letters and digits) to just read it out to the user. The user could observe the hash in text on the terminal with the screen that sent the public key and check that expected hash (on the screen) = received hash (read out). This method does of course rely upon the user to some extent, but given this, does allow a public key to be securely transmitted to a low capability and screen-less device, such as a headset, without the need for provisioning of root public keys on the headset. This last task is often, because of the commercial negotiations required, very difficult to achieve.