# IST-2000-25350 - SHAMAN

## Security for Heterogeneous Access in Mobile Applications and Networks

| | |
|---|---|
| **Deliverable Number** | D15 |
| **Deliverable Title** | Evaluation report |
| **Document Reference** | SHA/DOC/PMN/VOD/D15/1a |
| **Contractual Delivery Date** | 27-MAY-2003 |
| **Actual Delivery Date** | 27-MAY- 2003 |
| **Editor** | Keith Howker, Vodafone |
| **Participant(s):** | Vodafone |
| **Workpackage** | WP7 |
| **Est. person months** | |
| **Security** | Public |
| **Nature** | Final version |
| **Version** | 1.0/a |
| **Total number of pages** | 17 |

**Abstract:**

Conclusions and assessment of the results of SHAMAN.

**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

The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

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

# Management summary

The technical development work of SHAMAN was completed successfully. The results are contained in the final technical report, deliverable D13. A summary of the results and an assessment of their impact is given here. In addition, a number of open issues are identified that will require attention in the FP6 research programme.

The assessment by the project is that its objectives have been met in terms of relevance and originality. The results are judged to be innovative and to match the original subject and scope of the project. As the declared intention was to conduct advanced research into two areas judged to be of future importance, it was not possible to set down precise, measurable success criteria. In addition to the development of security results themselves, it was necessary to firm-up the underlying related architectural options concerning future networks and terminals.

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 was organised as four workpackages:

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 work for the two main areas was conducted by Workpackages WP1 (network) and WP2 (terminal). The tasks 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 final technical report D13 [1]consists of an overview document containing a technical summary of the whole project, together with an extended annex for each of WP1 to 4.

Two further workpackages complete the project.

WP5 Prototypes and demonstrations

W6 Dissemination, external relations and liaison

The complete WP6 report is published as D12 [2], and the specification of the WP5 demonstrator is published as D11 [3]

**Table of Contents**

## References

[1] D13 Summary http://www.isrc.rhul.ac.uk/shaman/docs/D13_V1.pdf
together with
WP1 - Annex 1 - http://www.isrc.rhul.ac.uk/shaman/docs/d13a1v1.pdf
WP2 - Annex 2 - http://www.isrc.rhul.ac.uk/shaman/docs/d13a2v1.pdf
WP3 - Annex 3 - http://www.isrc.rhul.ac.uk/shaman/docs/d13a3v1.pdf
WP4 - Annex 4 - http://www.isrc.rhul.ac.uk/shaman/docs/d13a4v1.pdf

[2] D12 - http://www.isrc.rhul.ac.uk/shaman/docs/d12v1.pdf

[3] D11V2 - http://www.isrc.rhul.ac.uk/shaman/docs/d11v2_0.doc

# 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.

Two features of the next generation are seen as significant, as we move on from Releases 4 and 5 of the 3GPP specifications, for instance:

- 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 networks with these features.

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

To summarize, the work concerns the provision of security for:

- global roaming and heterogeneous access networks (WP1);
- dynamically reconfigurable distributed terminal systems (WP2).

**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 (WP1, PW2) 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 (WP3); the other provides security modules based on smart card technology that will protect kernel security functionality and security-critical data and parameters (WP4). A further task (WP5) takes the technical results of these four workpackages and validates key aspects of 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 led 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 was not specific to SHAMAN was 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 maintained 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 concentrated 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 was not within the scope of the project to develop generic solutions to other broader concerns.

# 2 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 below. Open issues are given in section2.2. These are all discussed at greater length in the respective workpackage annexes to D13.

## 2.1 Major technical results

**WP1**

- a flexible security architecture for post-3G mobile systems;
- for each building block in the architecture, an evaluation of candidate protocols;
- sound engineering knowledge about the selection and combination of candidate protocols according to the evolving needs and requirements of post-3G mobile systems.

**WP2**

- development of the 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 service-specific 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 on PK revocation and code authorisation in secure execution environments in mobile context.

**WP4**

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

## 2.2 Open issues

**WP1**

in addition to further supporting R&D work, all these 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.

## 2.3 Contributions to 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. Results from SHAMAN WP2, the MANA I and II manual authentication protocols, were forwarded to Bluetooth SEG by the respective members as they developed.

- 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.

## 2.4 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 real smart cards.

The SHAMAN demonstrator from workpackage 5 implements concepts developed in the SHAMAN project. It implements a number of protocols for critical security aspects of the two major technical topics using important results from the two supporting task. The possibility of securely partitioning certain memory or computing-hungry tasks between the smartcard and its host environment in the terminal was investigated and shown to be a practical solution to the technology constraints of the smartcard.

## 2.5 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 can be used and then asking the user or device to compare expected with received hash. 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, it allows 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.

# 3 Objectives and results

The objectives of the SHAMAN project, as laid out in the Description of Work Amendment 1, are listed together with a summary of how the project has achieved these objectives, together with references to the appropriate project deliverables.

## 3.1 WP1 Objectives and results

**Objective 1: completion of definition of a reference functional architecture**

This is provided in the WP1 contribution to D13, Section 2.1.

**Objective 2: specification of requirements on secure access procedures**

This is provided in D02, Sections 4 and 5. A review of how the requirements are met by the proposed solutions is provided in the WP1 contribution to D13, Annex A.

**Objective 3: specification of (a set of) secure access procedures satisfying *the requirements***

The WP1 contribution to D13, Sections 3 to 9, provides such procedures.

**Objective 4: technical support for standardisation of selected solutions**

The basis for future standards contributions has been laid in D13. Please note that "technical support" is required, not the standardisation work in itself, see also comments on Paragraph B.c in the response.

## 3.2 WP2 objectives and results

**Objective: Based on the requirements and high-level functional specification produced during the first year, to develop the detailed model of the distributed terminal and a security architecture.**

The WP2 work has targeted most problems listed in the original workpackage description for distributed terminal systems. Obviously, it is not possible at the defining phase of a research project to foresee all areas of importance or to give a complete picture of a problem space. Consequently, in the SHAMAN project, WP2 developed the research areas and focus along with the project development. Quite early, we decided not to work with the WAP or MExE environments or end-to-end security issues. The reason for not working with WAP and end-to-end security was that these problems already were taken care of by the OMA (Open Mobile Alliance) and regarding MExE, that the work had come to a standstill in standardisation. Apart from this, everything listed in the original work item description for WP2 has been covered, and the results can be seen in D13 Annex 2.

## 3.3 WP3 objectives and results

**Objective: to develop a specification of 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 our research into 3G and beyond.**

The primary objective of WP3 was to address all the PKI research issues needed to support the work of WP1 and WP2. Section 2 of the WP3 contribution to D13 (Annex 3) addresses "Public Key Based Network Access", evaluating the son-of-IKE protocols JFK (versions "i" and "r") and IKEv2 against sets of cryptographic requirements that are relevant in two different network access scenarios. The first scenario is the "traditional" subscription case and the second scenario is the alternative access case that has been developed within WP1. This work was done in the context of WP1.

Regarding WP2, Section 4 of the WP3 contribution to D13 addresses "The Personal PKI" and examines PKI issues that arise from the concept of personal PKI. The other sections in the WP3 contribution to D13 address generic PKI research issues that we considered relevant for future mobile telecommunication systems. While the work on "PKI for Limited Devices" was motivated in the WP3 work package description, we deemed work on revocation and secure execution environments necessary. Although PKI interoperability issues were not addressed to the expected extent, the problem was identified and ID-based cryptographic schemes compared to "traditional" certificate based approaches.

## 3.4 WP4 objectives and results

**Objective: Based on the requirements identified in D05, to develop an architecture for the security module and to specify an SM that meets the needs of the network, terminal and PKI as prototyped and demonstrated in WP5.**

WP4 investigated the envisaged road maps of smart card technology and produced an outline of technology trends. Additionally a generic SHAMAN reference model was produced and presented in our Annex 4 to deliverable D13. Detailed analysis of requirements has been done by a detailed study of IKE first and was continued with JFK.

A detailed investigation on the functionality split between mobile node and smart card showed that it is feasible and worth implementing. There are several options for the way in which the functionality split can be implemented and their pros and cons have been analysed.

This provides a sound basis for the partners' work on EAP SIM, EAP AKA and EAP smart card, where the functionality split between network protocol software and smart card hardware is currently under investigation, but IETF standardisation is still in the early stages, especially for the EAP smart card specifications.

## 3.5 WP5 objectives and results

**Objectives:**

**·(1) to develop the specification for a prototype covering the work of WPs 1, 2, 3 & 4,·**

This was delivered as D11.

**(2) to build a working model**

The demonstrator implementation is still in progress and is due for completion at the end of the project.

**(3) to demonstrate the critical and novel aspects developed by the project**

The demonstrator uses the PC-to-PC set-up (connected by WLAN or Bluetooth) to show a general authentication and key agreement situation which occurs multiple times between multiple parties in the SHAMAN scenario. This is not restricted to a PC-to-PC situation, but this set-up was selected to allow the respective protocols to be implemented by the parties involved in the demonstrator work.

Demonstration of the newly designed functionality split between smart card and mobile node and demonstration of variants of the functionality split is only possible with this demonstrator set-up. Additionally the JAVA based implementation allows for flexibility and implementation within a single infrastructure and makes the demonstrator a future proof investment to be re-used for other demonstrator projects.

Other demonstration set-ups would have required modifications to existing commercial equipment such as GSM mobile software and their SIM card interfaces as well as their individual network access point.

We demonstrate the feasibility of smart-card support for protocols enabling security for global roaming over heterogeneous access networks, by implementing the functional split between the smart card and the terminal developed in SHAMAN. It is considered inappropriate because of the amount of resources required to build a demonstrator which would have to rely on a test-bed for the mobile communication infrastructure and would entail spending much resource on non-security related tasks.

Please also note in this context that implementations of some of the access network technologies assumed to be most relevant for post-3G systems, in particular IP-based UMTS radio access networks are not widely available.

While for pure application-oriented projects a real life demonstrator is mandatory for proof of concept, for security and network level projects, the results can be shown by implementing those security and network protocols standalone. The benefit of implementing them is that the protocols can be directly visualised and studied within the JAVA environment.

# 4 Innovation

## 4.1 WP1

Innovation in the project occurred at two levels:

1) at the building block level, where solutions for missing building blocks in a security architecture were provided or existing solutions were enhanced;

2) at the architecture level where (existing or new) solutions for building blocks were evaluated against the requirements for "post-3G" security, and were combined in a novel way.

Examples of both types of innovations are listed below. We would draw attention to second class of innovation, which may be less obvious, although it probably constitutes the major task in designing a "post-3G" security architecture. The emphasis on building blocks/protocols may be the view of the IETF and perhaps also of many research organisations, whereas the strength of the European mobile industry rests on the specification of complete architectures.

*re 1): innovation at the building block level*

a) IPsec security association negotiation protocol: this is a lightweight protocol, based entirely on symmetric-key methods, which is used to establish an IPsec SA after a successful authentication and key agreement (AKA) procedure (using any AKA protocol). Such a lightweight protocol is missing today, but is very desirable for a mobile environment. A complete specification in the form of an IETF draft is provided in the WP1 contribution to D13, section 5.1 and Annex B.

b) Two-step approach in access authentication: Two-step approach means that authentication of the access service network is separated from the authentication of the mobile node. Such a separation might offer significant advantages in increased flexibility particularly for heterogeneous access. The existing IETF proposals (PEAP, PIC; PoTLS) were analysed and found to be susceptible to man-in-the-middle attacks. Suitable countermeasures were designed. We contributed the SHAMAN findings to relevant IETF working groups where work has been initiated to make the technical and policy refinements needed to fix the problem. One of the proposed countermeasures has found entry into IKEv2.

*re 2): innovations at the architecture level*

a) different elements, some existing, some new, of secure access procedures were combined into information flows in a secure and efficient way; this is shown in the information flows in the WP1 contribution to D13, section 4.2..

b) For network access based on means other than a subscription, e.g. electronic purses, new ground was broken with the definition of a suitable charging architecture, including the new functional elements "credit control centre" and "cost charging centre". A protocol sequence chart was provided for the secure access procedure, cf. WP1 contribution to D13, section 4.6.

c) Model and steps of initial access: the steps in initial access were defined. The vulnerabilities in each step were identified. The existing solutions were analysed.

d) First hop security: the first hop is the connection between the mobile node and the first router in the network and may comprise different communication technologies. WP1 developed a model of the first hop. The role of the link layer security was analysed in detail for UTRAN and Bluetooth as example cases. It was concluded that for full security, both network layer and link layer security mechanisms are needed. This may result in double protection, which in some cases must be traded off with performance. The conditions for such trade-off were discussed.

## 4.2 WP2

1) MANA protocols

Protocols for exchanging initial keys between two PAN components were designed. The initial authentication in these protocols relies on participation by the user. Three different versions of the protocols depending on the user interfaces were presented. The MANA protocols are user friendly without compromising security.

2) PAN trust model and PAN security domains

We worked on secure initialisation of PAN components. We defined how PAN security associations are created using for example the MANA protocols (see the item above). In order to be useful in different PAN contexts, a security association must be connected to authorisations. We developed a new three level trust model, which reflects the natural user demands on PAN connections. Furthermore, we invented the new PAN security domain concept where all components in the domain share a common security policy and have controlled access to each other's resources.

3) Personal PKI

User convenient PAN key management was one of our main goals. We invented the new *personal PKI* concept where one device acts as a "master device" that issues certificates to other personal PAN components. The concept was handed on to WP3, which further developed and extended the concept.

4) Delegated authorisations

A new cryptographic protocol for delegating usage of an RSA private key was designed. Using this protocol a master device can delegate the capability of using its RSA private key to other devices without either online connection to the master or risk to the security of the private key. The private key operation requires assistance of an external untrusted server. Further delegation by a device to another device is possible if permitted by the master.

The delegated authorisation protocol provides the PAN with shared private key capability. One application is that any PAN device can create digital signatures with the same private key. In particular such functionality can be used to establish back-up for the PAN CA. Another application of delegated authorisation we presented is fair DRM in the PAN, meaning that multiple personal devices can access the protected content by decrypting the content key.

5) Distributed download

Download to a distributed terminal may require allocation of different functions to different terminal components. As far as we can discover, this problem has not been studied previously. Scenarios and information flows for distributed download were developed, showing the communication between the terminal components and with the outside world.

## 4.3 WP3

The innovative character of the work of WP3 is as follows:

(1) For WP1, innovations include the identification of the cryptographic requirements that are essential in two different network access scenarios, namely the subscription case and the alternative access case, and the evaluation of a choice of PK authentication protocols against these requirements.
The achievements here do not lie in the choice of JFK and IKEv2, but in identifying the respective requirements. As a result of this analysis, it has became clear that active attacks are possible on the mobile node and that therefore user identity confidentiality (an important requirement for network access) cannot be guaranteed.

(2) For WP2, the “Personal PKI” concept has been developed. The main research contributions in this area have been the work on multiple CAs, revocation in a PAN, proof of possession, and

device initialisation. Further novel contributions relate to the possible use of ID-based cryptography in a PAN environment.

(3) The issues raised in "PKI for Secure Execution Environments" address highly relevant research topics for future telecommunication systems.

## 4.4 WP4

1) IKE functionality split

We presented how the Internet Key Exchange (IKE) protocol can be distributed in secure way between a tamper resistant module and a mobile terminal. IKE is still the only standard that IETF provides for internet key exchange. In the WP4 Annex of D13 it is explained how the security module can execute IKE with the help of the computation resources provided by the terminal.

2) JFK functionality split

We presented how the Just Fast Keying (JFK) protocol can be distributed in secure way between a tamper resistant module and a mobile terminal. The two son-of-IKE proposals, JFK and IKEv2 were merged into one protocol in Oct 2002. Many of the results of this work still apply to the new protocol.

3) Reference Model of a Security Module

Based on the requirements resulting from other workpackages a reference model of a security module has been designed and different levels have been specified to fully match individual requirements.

4) Private key usage without security module

The security requirements of the delegated authorisation protocols developed in WP2 were analysed. The main result is that the devices, *except* the master device, do *not* need security modules. However, the software has to be designed and configured carefully to take account of the relationships with the master device.

## 4.5 WP5

WP5 is not innovative in the sense of design tools and software tools used.

The innovative character lies in the implementation of protocols on a real smart card. Instead of merely being a container for data, the smart card actively participates in selected protocols according to a functionality split which has been designed in WP4. In the JFK protocol, for example, the smart card is aware of the current protocol state, and reacts to incoming messages accordingly; in addition, the Diffie-Hellman key exchange and a keyed hash function have been implemented on-card. The functionality split aims for the best trade-off between speed and security which can be achieved between the smart card, a secure but limited device, and a mobile equipment, which may have high computational capabilities but limited security capability.

# 5 Standardisation

A clear distinction is be made between the commitment of the project to produce technical results which can be used in input documents to standards bodies, and the exploitation of project results in the actual standardisation work. The latter is not the responsibility of the project collectively. Rather it is the responsibility of individual partner companies participating in the standards bodies, and is driven by the standardisation strategies of the companies. These strategies are determined by many factors, including market analyses, product strategies, situation in the standards bodies, and efficient use of available resources, and are subject to change, depending on the evaluation of these factors. They are not determined by the need of research projects to demonstrate results. The SHAMAN Description of Work foresaw the main exploitation of SHAMAN results in standards work as taking place between Jan 2003 and Jun 2004. The project participants are working broadly to this schedule of our exploitation plan, but it should be noted that the market has undergone quite drastic changes since the Description of Work was written. Customer demand for *post-3G* systems, and hence the industry's need for corresponding standardisation work, is coming later than expected at the start of the porject. Nevertheless, the process of contributing SHAMAN results to the standards bodies has already begun.

1) The SHAMAN work on the two-step approach to access authentication has already had an impact on IETF standardisation. The existing IETF proposals (PEAP, PIC; PoTLS) were analysed and found to be susceptible to man-in-the-middle attack. Also countermeasures to this attack were designed. Nokia contributed the SHAMAN findings to relevant IETF working groups where work has been initiated to make the technical and policy refinements needed to fix the problem. One of the proposed countermeasures has found entry into IKEv2 (version 05, section 2.16).

2) In January 2003, i.e. after the audit, Siemens contributed a draft to the IETF PANA group entitled "PANA Framework Issues" (draft-tschofenig-pana-framework-00.txt) which is partly based on and explicitly acknowledges SHAMAN WP1 work. In March 2003, Nokia and Siemens co-authored draft-ietf-pana-pana-00.txt which takes the framework issues into account. PANA work is currently pushed by a PANA design team. The Nokia WG co-chair and design team members are in close contact with the SHAMAN participants of Nokia, the Siemens design team member worked in SHAMAN WP1.

3) The WP1 work on first hop security (link vs. network layer security) is of relevance to the current discussion on 3G-WLAN interworking security in 3GPP SA3 and has considerably helped the three SHAMAN WP1 members active in 3GPP SA3 to analyse the security problems involved. Several contributions to 3GPP SA3 by partners in SHAMAN WP1 have been made on this issue.

4) WP1 produced a complete draft for an IPsec security association negotiation protocol, in a form ready for submission to the IETF. Whether and when it is actually submitted is a matter of the standardisation strategies outlined above.

5) The WP1 work on alternative access to networks, based on electronic payment rather than subscription, is a good basis for future standards work. However, the market does not seem to be ready at the moment for this alternative access.

6)The MANA protocols (see 7) and 8) below) may be also used for public access, and hence become relevant to WP1, in situations where manual configuration is acceptable.

7) The WP2 manual authentication problem and solutions have been submitted to ISO/IEC JTC1 SC27/WG2 and have been accepted as a new work item (to become ISO/IEC 9798-6).

8) The new WP2 MANA protocols were also submitted to the Bluetooth SIG Security Expert Group where they have been well received and resulted in a new improved pairing work item proposal under preparation by the security expert group.

9) It is planned to send the PSD work as a standards contribution to the Bluetooth SIG.

10) WP3 work on multiple CAs, revocation in a PAN, and device initialisation will lead to a standards contribution to the Bluetooth SIG.

11) WP4 results have been discussed by the partners' representatives in EP SCP and 3GPP. Individual aspects have been informally input by SHAMAN but no new standards have resulted from that up to now. The functionality split between SM and ME as well as the EAP work stimulated participation in WLAN security work on EAP AKA/SIM as well as on EAP smart card, which will be in the scope of the *Wireless LAN smart card consortium*, which is to be established in 2003.

The anticipated overall timescale for emergence of our work as product is reproduced from the original Annex 1 to the Contract – Description of Work.