IST-2000-25350 - SHAMAN

Deliverable Number	D12
Deliverable Title	Report on standards and external liaison
Date of delivery	30-November-2002
Document Reference	SHA/DOC/TNO/WP6/D12/1.0
Contractual Delivery Date	30-Nov-2002
Actual Delivery Date	22-Nov-2002
Editor	Peter Windirsch (T-Systems Nova) (for a list of authors, see page 4)
Participant(s):	ATEA, Ericsson, Giesecke & Devrient, Nokia, Royal Holloway, Siemens AG, T-Systems Nova, Vodafone
Workpackage	WP6
Est. person months	
Security	Public
Nature	Report
Version	1.0
Total number of pages	24

Abstract:

The document D12 contains a summary on all standards and external liaison activities of the SHAMAN project with respect to the dissemination of the project results. This is the main result of SHAMAN workpackage 6.

Keyword list: dissemination of SHAMAN results, cooperation with standards and industry bodies, cooperation with other research projects.

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.

Executive Summary

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

The work concerns the provision of security for

global roaming and **heterogeneous access networks;**

dynamically reconfigurable distributed mobile terminal systems

We are developing components for security architectures that will provide specifications of the interfaces, protocols and mechanisms that are needed to deliver the required level of protection. We are also developing related supporting technologies based on public key infrastructure (WP3) and security modules based on smart cards (WP4). At the end of the report we show how the architecture can be applied to a set of example scenarios taken from the demonstrator work of SHAMAN WP5.

This document in particular provides a report on the liaisons of the SHAMAN project with standardisation bodies as well as with research oriented cooperations and describes the steps taken to disseminate the results of the SHAMAN project.

Liaison with international standards bodies will proceed through existing channels and relationships of the SHAMAN partners and will continue beyond the formal end of the SHAMAN project as already mentioned in the Technical Annex of the project contract.

Authors

Name		Affiliation	Email	Phone / Fax
Blom	Rolf	Ericsson AB (ERIC)	rolf.blom@era-t.ericsson.se	☎ +46 (8) 5853 1707 🖷 +46 (8) 4047020
Chandrasiri	Pubudu	Vodafone Group (VOD)	pubudu.chandrasiri@vodafone.com	☎ +44 1635 682986 🖷 +44 1635 676147
Dankers	Jozef	Siemens Atea n.v. (ATEA)	Jozef.Dankers@siemens.atea.be	☎ +32 14 25 3218 🖷 +32 14 25 3339
Ertl	Hubert	Giesecke & Devrient GmbH (GD)	hubert.ertl@de.gi-de.com	☎ +49 89 4119-2796 🖷 +49 89 4119-2921
Gehrmann	Christian	Ericsson Mobile Platforms AB (ERIC)	Christian.Gehrmann@emp.ericsson.se	☎ +46 46 232904 🖷 +46 46 193455
Günther	Christian	Siemens AG (SAG)	Christian.Guenther@siemens.com	☎ +49 89 636 49655 🖷 +49 89 636 48000
Horn	Günther	Siemens AG (SAG)	guenther.horn@mchp.siemens.de	☎ +49 89 636 41494 🖷 +49 89 636 48000
Jefferies	Nigel	Vodafone Group (VOD)	nigel.jefferies@vodafone.com	☎ +44 1635 673883 🖷 +44 1635 233440
Mitchell	Chris	Royal Holloway University of London (RHUL)	c.mitchell@rhul.ac.uk	☎ +44 1784 443423 🖷 +44 1784 430766
Niemi	Valtteri	Nokia Group (NOK)	valtteri.niemi@nokia.com	☎ +358 5048 37327 🖷 +358 9 4376 6850
Tschofenig	Hannes	Siemens AG (SAG)	Hannes.Tschofenig@siemens.com	☎ +49 89 636 40390 🖷 +49 89 636 48000
Windirsch	Peter	T-Systems Nova GmbH (TNO)	peter.windirsch@t-systems.com	☎ +49 6151 833821 🖷 +49 6151 834464
Wright	Tim	Vodafone Group (VOD)	timothy.wright@vodafone.com	☎ +44 1635 676456 🖷 +44 1635 31127

The authors of this report are listed by name in alphabetic order.

Table of Contents

1 Introduction

1.1 Scope and purpose of this report

The purpose of this report is to summarize the activities related to cooperation with and SHAMAN results dissemination activities to standards and industry bodies working in fields related to the SHAMAN work.

1.2 List of abbreviations

3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AH	Authentication Header
EAP	Extensible Authentication Protocol
ETSI	European Telecommunications Standards Institute
GPRS	GSM General Packet Radio Services
GSM	Global System for Mobile Communications
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystems
IPSEC	IP Security
IPSRA	IP Security Remote Access
IRTF	Internet Research Task Force
ISO	International Standardisation Organisation
IST	Information Society Technologies
ITU	International Telecommunication Union
MANA	Manual Authentication
MExE	Mobile Execution Environment
MIDP_NG	Mobile Information Device Profile – New Generation
MIND	Mobile IP based Network Developments
NSIS	Next Steps in Signaling
OCSP	Online Certificate Status Protocol
OMA	Open Mobile Alliance
PANA	Protocol for carrying Authentication for Network Access
PIC	Pre-IKE Credential Provisioning
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
SEG	Security Expert Group
SIG	Special Interest Group
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless LAN

1.3 References

The first deliverable in WP6 has been published at the end of the first year of the SHAMAN project:

[1] *IST-2000-25350 SHAMAN D06 – Status report on standards bodies*, November 2001, available online at http://www.ist-shaman.org/publicDocs/docs_index.htm

2 Standardisation liaisons

The subsequent section reports on the activities in the SHAMAN project taken to forward results and information from the SHAMAN project to standardisation bodies. It has already been recognised in the SHAMAN Technical Annex 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 did groundwork to prepare for future standards.

2.1 3GPP

2.1.1 Relation of SHAMAN work to 3GPP SA WG3 (Security)

The 3rd Generation Partnership Project (3GPP) is a joint effort of several standardization organizations around the world. The aim is to ensure harmonization of the 3rd generation mobile communication technologies in order to enable global use of the same techniques. One of the key standardization organizations in the project is ETSI.

So far 3GPP has released three sets of specifications. Release 99 was frozen in the spring of 2000, release 4 was frozen in the spring of 2001 and release 5 was frozen in the summer of 2002. Current work is targeting on release 6 specifications that are targeted to be frozen in the mid-2003.

The main work item in 3GPP Release 5 was IP Multimedia Subsystem (IMS).

The security working group of the 3GPP is called SA3. It has many work items for release 6.

From SHAMAN perspective the following work items are most relevant:

- PKI-based key management for network domain security: results of WP3 may turn out to be relevant in this context. At the moment 3GPP work is in the feasibility study phase, hence no definite conclusions can be drawn yet. Network domain security mechanisms are also relevant for SHAMAN WP1 work, since the security architecture built in WP1 counts partly on them. However, it should be noted that it was not in the scope of WP1 to develop new mechanisms for network domain security.
- Support for subscriber certificates: this work item has connections to the SHAMAN work packages 1, 2 and 3. Certificates are used in many technical features developed in WP1. For instance, WP1 results about using 3GPP authentication and key agreement procedures tunnelled into another security protocol have already turned out to be useful in discussions about certificate request procedures in 3GPP. Use cases for subscriber certificates have been fed into 3GPP from WP2. Also, WP3 results are taken into account in 3GPP certificate work.
- WLAN interworking: this work item is the first step in 3GPP towards the scenarios studied in SHAMAN WP1. In release 6, however, the connection between WLAN access technology and WCDMA/GSM/GPRS access technologies is quite limited; the most important common denominator is unified charging and billing. It is yet to be seen, whether WP1 results can be usefully applied already in this limited case of heterogeneous access networks. It is anticipated that in later releases of 3GPP the concept of connecting heterogeneous access networks to one uniform core network is developed further. At the same time, WP1 results become better applicable also.

- User equipment functionality split: SHAMAN WP2 results can be applied in this work item of 3GPP. In release 5, only initial specification work about requirements for UE functionality split was done. In release 6, it seems that e.g. work referred above for WLAN interworking creates momentum for the functional split work. As a side effect, also SHAMAN WP2 results may be applied more widely.
- Mobile Execution environment (MExE). MExE specifications are developed in a specific subgroup inside 3GPP (under T2 group)- The security group S3 is reviewing the security part of the specifications. SHAMAN WP 2 results are clearly relevant here but, unfortunately, it seems to be that the volume of interest in MExE specification work is decreasing in 3GPP.

The release 6 of 3GPP has a flavour of rather containing enhancements to earlier releases than creating major architectural changes. This implies that especially SHAMAN WP 1 results are better applicable to later releases where the concept of heterogeneous access networks is more thoroughly included into the system.

The results of the SHAMAN work package 4 may also be contributed into 3GPP later but this occurs probably in the context of the above-mentioned work areas.

2.1.2 3GPP MExE (Mobile Execution Environment) Security Group

Majority of the security work in MExE, particularly authentication (based on PKI) and authorization (a combination of security domains and user permissions) is complete. Nevertheless, it still lacks a reliable revocation solution and a workable administrator concept to manage third party roots on the terminal. Other areas that could potentially benefit from SHAMAN include security modules and the security of interfaces to local access networks.

However, to date there has been no direct contribution from SHAMAN to address these requirements. This is mainly because work in MExE has come to a standstill.

2.2 ETSI (European Telecommunications Standards Institute)

2.2.1 ETSI EP SCP (ETSI Project Smart Card Platform)

Due to the partner's strong interaction with EP SCP, the work on security modules, the specification of security modules and the general requirements from SHAMAN work packages have been discussed and the final results of SHAMAN are to be discussed with the company's representative working in EP SCP. This is intended to provide input for future standardisation efforts. The current contacts didn't result in new standards originating from pure SHAMAN work, but the requirements and issues discussed in SHAMAN have been reviewed and taken into account by the company representative and will be considered during future standardisation work in EP SCP.

2.3 IETF Internet Engineering Task Force

During the process of creating SHAMAN documents a number of Internet drafts have been read and reviewed. Comments have been submitted to the authors. However, no active participation (for example based on an own SHAMAN Internet Draft) in the IETF took place.

The following list briefly describes some of the IETF working groups with relevance for the work in SHAMAN:

2.3.1 AAA WG (Authentication, Authorization and Accounting)

The AAA working group tries to standardize a future AAA protocol based on Diameter. The documents in this WG are closely related to the EAP which offers different authentication and

key agreement methods. Various protocol proposals described in SHAMAN make use of these protocols.

2.3.2 EAP WG (Extensible Authentication Protocol)

As the charter of the working group says the work is currently restricted document and improve the interoperability of the existing EAP protocols. Currently the group is not chartered to review or standardize EAP methods.

2.3.3 PKIX WG (Public Key Infrastructure X.509)

The PKIX working group is partially of interest because it mainly develops Internet standards needed to support an X.509-based PKI.

2.3.4 IPSEC WG

In last few months the IPSec working group received special attention because the development of a successor of IKE (Son-of-IKE) and the related discussion about the properties of a key management protocol.

2.3.5 PANA WG (Protocol for carrying Authentication for Network Access)

The PANA working group is of interest for SHAMAN since it should provide a protocol for communication between an end host and the AAA attendant (i.e. the entity where a subsequent AAA protocol is started). Information exchanged between these entities is mainly determined by the EAP protocol. The work of PANA is therefore strongly related to the AAA and the EAP working group.

2.3.6 NSIS WG (Next Steps in Signaling)

The NSIS working group tries to develop a signaling protocol which allows to distribute quality of service information, middlebox (NAT bindings and firewall policies) and other information to a number of entities along the path between a data sink and a data source. Work in this group is by nature heavily influenced by the famous QoS signaling protocol RSVP (Resource Reservation Protocol).

2.3.7 IPSRA WG (IP Security Remote Access)

[2] The work in this group builds on the protocols produced in the IPSec group (IKE, IPSec AH, IPSec ESP) to better support road warriors i.e. access by remote users. The Pre-IKE Credential Provisioning Protocol (PIC) [3] is one of the protocol candidates which evolved from this work. IETF web site at http://www.ietf.org/

[3] Pre-IKE Credential Provisioning Protocol (PIC), http://www.ietf.org/internet-drafts/draft-ietf-ipsra-pic-06.txt

2.4 OMA Forum (Open Mobile Alliance)

There have been no direct SHAMAN contributions to the OMA security group. However, following the examination of the necessity of revocation within SHAMAN WP3, and the examination of different methods of client revocation checking (SHAMAN WP3 concluded that Online Certificate Status Protocol [OCSP] was the most suitable method for mobile devices), Vodafone have been promoting the specification of a mobile profile of OCSP for support by mobile devices. This profile is now in a relatively stable state and should be approved early in 2003.

2.5 Bluetooth Consortium/ Bluetooth Security Expert Group

The Bluetooth SIG is about to enhance the Bluetooth industry standard. The standard is evolved in two main directions:

- Support of new applications through the introduction of new profiles
- Radio improvements and extensions

The latter includes improvements to the baseband, link manager and host controller layers in the Bluetooth stack. The current (Bluetooth 1.1) security is defined on all layers within the focus of the radio improvements. The weaknesses of the current link level security mechanisms are well documented. The two most serious concerns are the weak pairing procedure and the location tracking threat. The Bluetooth SIG radio 1 improvements sub-working group has already addressed the location tracking problem. The weak pairing procedure has been listed as one of the main obstacle for wide Bluetooth deployment in a recent NIST report. Hence, there is awareness within the Bluetooth SIG of that an improved pairing procedure is needed. However, so far nothing has been done to improve the weak pairing procedure.

The WP2 MANA work addresses secure manual procedures for authenticated key exchange, i.e., strong pairing procedures. Three different MANA protocols have been evaluated by WP2 and a theoretical security analysis of the MANA I and II protocols have been performed. The MANA I and II together with appropriate anonymous Diffie-Hellman key exchange are good candidates for replacing the weak pairing in Bluetooth. WP2 in co-operation with WP3 has sent in an improved pairing contribution to the Bluetooth SIG Security Expert Group (SEG). The contribution is based on section 6 of the WP2 D13 part. Anonymous Diffie-Hellman combined with MANA I is suggested as the primary option to replace the current weak pairing. MANA II is recommended as an optional strong pairing procedure. The SEG will study the SHAMAN input and based on the result of the internal evaluation give a proposal for improved pairing to the Bluetooth SIG radio 1 improvements sub-working group.

[4] Kaisa Nyberg (Ed.). *A Protocol for Enhanced Bluetooth Pairing*. Submitted to bt-sec-eg@bluetooth.org on Oct. 26, 2002

2.6 MIDP_NG Group (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.

2.7 ISO (International Organization for Standardization)

2.7.1 ISO/IEC JTC1/SC27 (Security techniques)

In October 2002 a New Work Item proposal was submitted to this ISO committee containing the MANA authentication protocols developed within SHAMAN WP2. Work is now under way on including these protocols in a new part of the ISO authentication protocol standard, ISO/IEC 9798. 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).

[5] *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 Liaisons with other research activities

3.1 IST Information Society Technologies

3.1.1 IST-2000-28584 MIND (Mobile IP based Network Developments)

MIND is the successor of IST-1999-10050 BRAIN. BRAIN was of particular interest to SHAMAN as SHAMAN decided to base the SHAMAN security architecture on the BRAIN network architecture. Many of the experts active in BRAIN also continued to work in MIND. An exchange of ideas was therefore considered very useful.

The cooperation occurred at three levels:

- Firstly, an important level of interaction occurred inside the partner organisations. This was possible as there was a substantial overlap in the consortium members of BRAIN and of SHAMAN, respectively. This provided a very efficient way to obtain clarifications and explanations on published documents of both projects.
- Secondly, an email list was set up, hosted by Vodafone, over which discussions relating to the ongoing security work in both projects took place and working documents were exchanged. This was useful, although the focus of the security work was different: MIND focused on scenarios for ad-hoc networking while the latter was not in the scope of SHAMAN.
- Thirdly, a MIND representative, Mr. Hu Wang from NTT DoCoMo, participated in the SHAMAN workshop on 25 July 2002 and gave a presentation on " Securing MANETS: mechanisms derived from the MIND scenarios".

[6] MIND web site at http://www.ist-mind.org

3.1.2 IST-1999-20117 INTERNODE (Interworking of Nomadic Multi-domain Services)

The interaction between INTERNODE and SHAMAN was mainly concentrated on providing information about the projects' activities and on giving presentations at the partner's workshops.

SHAMAN provided a presentation to the INTERNODE workshop held at Paris on January 18, 2002. Due to the case of illness of the speaker, the SHAMAN contribution was only included to the workshop proceedings in the form of presentation slides, but actually no presentation has been given [25].

At the SHAMAN workshop at Royal Holloway, University of London, on July 25, 2002 (see also section 4.3), Peter Lonergan from National Electronics Technology Centre (NETC), Enterprise Ireland, gave a speech on the INTERNODE project's objectives related to providing an integrated solution for service providers to manage mobile virtual private networks (VPNs) [51].

[7] INTERNODE web site at http://www.mobile-ip.de/~crist/Data/

3.1.3 IST-2001-37763 PAMPAS (Pioneering Advanced Mobile Privacy and Security)

PAMPAS is a roadmapping project in the EC IST Programme. The goal of PAMPAS is to develop a roadmap for European research under 6th Framework Programme in the area of mobile privacy and security.

Several SHAMAN partners take part also in PAMPAS. Participation in SHAMAN has been useful for these partners as regards to PAMPAS work also, giving insight on research problems in certain areas of mobile security.

The first PAMPAS workshop was held in September 2002. Also those partners in SHAMAN that are not involved in PAMPAS itself were represented in the workshop and active contributions were provided.

[8] PAMPAS web site at http://www.pampas.eu.org/

3.1.4 IST-2001-34157 PACWOMAN (Power Aware Communications for Wireless OptiMised personal Area Network)

PACWOMAN aims to take a holistic view of (W)PANs (and WCANs) including all OSI layers from physical up to application. WP2 of SHAMAN has done something similar for PANs and distributed terminals, but with a strict security focus and a mandate to reuse existing components. The interaction between PACWOMAN and SHAMAN has mainly been by using results delivered by the projects. SHAMAN deliverable D3 "Security Architecture for Future Mobile Terminals and Applications" is one of the references used in the PACWOMAN delivery D5.1 "State-of-the-art of the WPAN networking paradigm" which in turn has been reviewed and served as reference documentation in the continued SHAMAN WP2 work.

[9] PACWOMAN web site at http://www.imec.be/pacwoman/

3.2 Wireless World Research Forum (WWRF)

The Wireless World Research Forum (WWRF) is a global organization whose aim is to encourage coordinated research towards the next generation of mobile communications. It was founded in 2001 by members of the European-funded WSI (Wireless Strategic Initiative) project, and now has over 100 members including manufacturers, network operators and academic institutions. The output has been a set of visions of the mobile future and the development of a reference model and further recommendations on research directions. The work of the SHAMAN project was presented at their fifth meeting in Arizona, USA during March 2002. However at this stage, SHAMAN is mainly focussed on carrying out research, rather than identifying future research priorities. It is anticipated that such recommendations will form the basis of a WWRF contribution at the end of the SHAMAN project.

[10] WWRF web site at http://www.wireless-world-research.org/

4 Dissemination activities

4.1 Public presentations and papers

The subsequent section collects references to all journal articles, scientific papers and project presentations which were derived from work originating from the SHAMAN project.

4.1.1 Journal articles

[11] K. Boman, G. Horn, P. Howard, V. Niemi, *UMTS Security*, IEE Electronics and Communication Engineering Journal, vol. 14 (2002), pp. 180 – 190.

[12] J. Dankers, T. Garefalakis, R. Schaffelhofer, T. Wright, *PKI in mobile systems*, IEE Electronics and Communication Engineering Journal, vol. 14 (2002), pp. 191 – 204.

[13] S. Schwiderski-Grosche and H. Knospe, *Secure Mobile Commerce*, IEE Electronics and Communication Engineering Journal, vol. 14 (2002), pp. 228 – 238.

4.1.2 Scientific papers

This section summarises all scientific paper publications given in the context of the SHAMAN project. For most of these papers, corresponding presentations have been given at the respective conferences.

[14] C. Gehrmann, G. Horn, N. Jefferies and C.J. Mitchell, *Securing access to mobile networks beyond 3G*, in: *Proceedings of the IST Mobile Communications Summit 2001, Barcelona, Spain, September 2001*, pp.844-849.

[15] Ch. Gehrmann, K. Nyberg. *Enhancements to Bluetooth Baseband Security.* Proceedings of the NordSec 2001 conference, Lyngby (DK), Nov. 1 – 2, 2001

[16] C. Gehrmann, K. Nyberg and C.J. Mitchell, *The personal CA - PKI for a Personal Area Network*, in: *Proceedings - IST Mobile & Wireless Communications Summit 2002, Thessaloniki, Greece, June 2002*, pp.31-35.

[17] C. Gehrmann, T. Kuhn, K. Nyberg and P. Windirsch, *Trust model, communication and configuration security for Personal Area Networks*, in: *Proceedings - IST Mobile & Wireless Communications Summit 2002, Thessaloniki, Greece, June 2002*

[18] H. Knospe, S. Schwiderski-Grosche, *Online Payment for Access to Heterogeneous Mobile Networks*, in: *Proceedings - IST Mobile & Wireless Communications Summit 2002, Thessaloniki, Greece, June 2002,* pp. 748 – 752.

[19] T. Garefalakis and C.J. Mitchell, *Securing Personal Area Networks*, in: *Proceedings of PIMRC 2002, 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Lisboa, Portugal, September 2002*, IEEE, 2002, pp. 1257 - 1259.

[20] H. Knospe and S. Schwiderski-Grosche, *Future Mobile Networks: Ad-hoc Access based on Online Payment with Smartcards*, in: *Proceedings of PIMRC 2002, 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2002)*, pp. 197-200, September 2002.

4.1.3 Presentations

In this category, we summarize all remaining presentations related to SHAMAN given at workshops, scientific conferences, … without the requirement of publishing a scientific paper together with the presentation.

[21] B. Adams, N. Jefferies. *SHAMAN Presentation at 3GPP SA LI*. 3GPP SA LI meeting, Clearwater, 6 - 8 March 2001

[22] N. Papadoglou. *Contribution to poster session.* IST Mobile Summit, Barcelona, Sep-2001.

[23] Günther Horn. *Security in IP-based mobile networks and ad hoc networks: future challenges*. Presentation at IST Committee Working Group on Security and Mobility Meeting, Oct-2001.

[24] Nigel Jefferies. *Securing Mobile Networks – review of ASPeCT, USECA & SHAMAN.* Presentation at IST Committee Working Group on Security and Mobility Meeting, Oct-2001.

[25] Keith Howker, *Securing Future Mobile Communication Systems*, Internode Workshop, Paris, 18 January 2002 (submitted for inclusion to the proceedings, presentation has not been given due to illness of speaker)

[26] Tobias Martin, *Sicherheitsarchitekturen künftiger Mobilfunksysteme (in German language)*, CAST-Forum (http://www.cast-forum.de), Darmstadt, 21 Feb. 2002

[27] Nigel Jefferies, *Securing Access to Mobile Networks beyond 3G*, WWRF workshop, Tempe, AZ, March 2002

[28] K. Nyberg, *Link Layer Security for the First Hop - IST SHAMAN Project*, European Cooperation in the Field of Development of Mobile and Personal Communications - IST Projects, Moscow, 15-17 May, 2002

[29] Pubudu Chandrasiri, *Securing Access to Mobile Networks beyond 3G*, International Conference on Telecommunications ICT 2002, Beijing, China, 23 – 26 June 2002

4.1.4 Concertation meeting presentations

[30] Nigel Jefferies, *SHAMAN IST-2000-25350*, 3rd Concertation Meeting of Mobile/Wireless/Satellite IST projects, Brussels, 11 December 2000

[31] Timothy Wright, *Initial results from the SHAMAN project* - presented to the Reconfigurability and "Beyond 3G" clusters, 3rd Concertation Meeting of Mobile/Wireless/Satellite IST projects, Brussels, 11 December 2000

[32] Günther Horn. *"Securing network access in post-3G mobile systems (SHAMAN WP1)"*, Systems beyond 3G Cluster meeting, Brussels, 11 September 2002

4.2 SHAMAN web site

For dissemination of SHAMAN results via the Internet, the SHAMAN web site has been set up shortly after the beginning of the project. That SHAMAN web site is available at http://www.ist-shaman.org . It provides an overview on the activities and the work programme in the SHAMAN project. It also has been used for public announcements (e.g. call for participation for the SHAMAN workshop, programme information and registration

for the SHAMAN workshop, …) and it is used for distributing all public deliverables resulting from SHAMAN work listed below as well as the SHAMAN workshop booklet (see [46]) containing all presentation slides shown at the SHAMAN workshop. They are all available on-line for download (see http://www.ist-shaman.org/publicDocs /docs_index.html):

[33] SHAMAN Deliverable D02, *Intermediate Report: Results of Review, Requirements and Reference Architecture*, 21 Dec. 2001

[34] SHAMAN Deliverable D03, *Interim Report - Security Architecture for Future Mobile Terminals and Applications*, 08 Nov. 2001

[35] SHAMAN Deliverable D04, *Initial report on PKI requirements for heterogeneous roaming and distributed terminals*, 10 Sep. 2001

[36] SHAMAN Deliverable D05, *Intermediate report on the role of security modules in heterogeneous networks, distributed terminals and PKI*, 31 Oct. 2001

[37] SHAMAN Deliverable D06, *Status report on standards bodies*, 30 Nov. 2001

[38] SHAMAN Deliverable D07, *Intermediate specification of PKI for heterogeneous roaming and distributed terminals*, 01 Mar. 2002

[39] SHAMAN Deliverable D08, *Intermediate specification of Security Modules*, 15 May 2002

[40] SHAMAN Deliverable D09, *Detailed specification of security for heterogeneous access*, 14 Jun. 2002

[41] SHAMAN Deliverable D10, *Detailed specification of distributed mobile terminal system security*, 31 May 2002

[42] SHAMAN Deliverable D11, *Specification of prototypes*, 16 Sep. 2002

[43] SHAMAN Deliverable D12, *Report on standards and external liaisons*, to be published (will be made available on the web site shortly after its release in Nov. 2002)

[44] SHAMAN Deliverable D13, *Final technical report comprising the complete technical results, specification and conclusion*, to be published (will be made available on the web site shortly after its release in Nov. 2002)

[45] SHAMAN Deliverable D14, *Dissemination and use plan*, to be published (will be made available on the web site shortly after its release in Feb. 2003)

4.3 SHAMAN workshop

As an action within the dissemination efforts of the SHAMAN project a workshop was organised by workpackage 6. The workshop was held on July 25, 2002 and was hosted by Royal Holloway, University of London, at Egham, Surrey.

Figure 1 Royal Holloway, University of London

Figure 2 Reception and Registration

Figure 3 SHAMAN posters exhibition

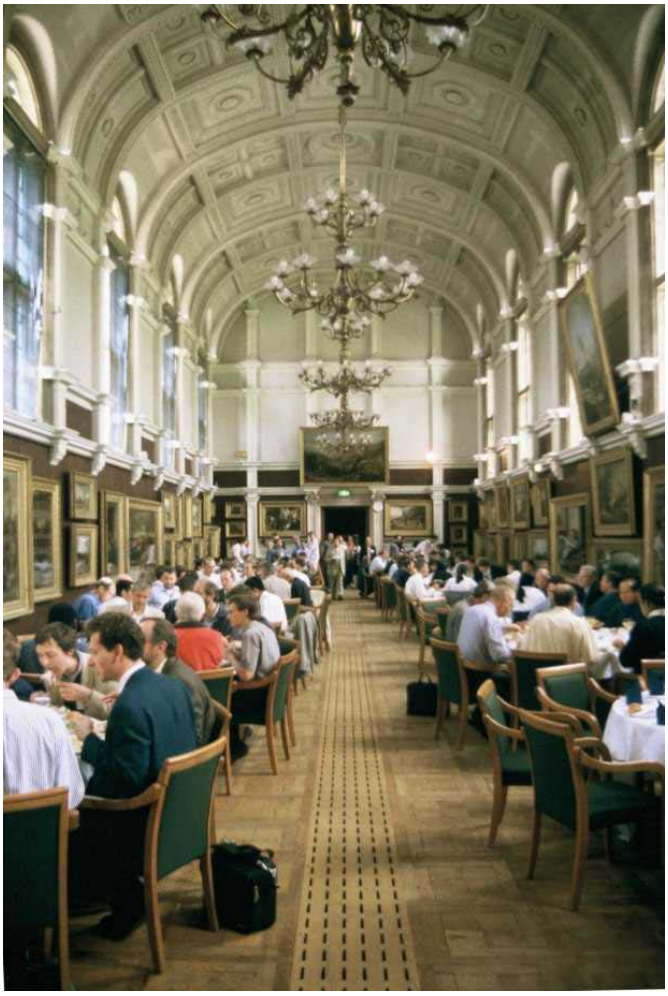

Figure 4 Participants' offline discussions in RHUL's picture gallery during the workshop breaks

Both, invited speakers from the mobile security community as well as speakers from the SHAMAN project presented recent results and perspectives into the future of security aspects for future post-3G mobile communication systems in their talks. In addition, posters on the main activities of SHAMAN were on display. The workshop found widespread interest and was attended by 130 participants from industry, government, and academia. Statistical details are given in the following tables:

Country	**Participants count (based on latest registration list)**
Belgium	4
Finland	3
France	1
Germany	15
Ireland	2
Israel	1
Netherlands	1
Sweden	4
United Kingdom	99
- total -	130

Table 1 Participants' country of origin

Out of the 130 participants, 22 are SHAMAN members.

Participants category	**Participants count (based on latest registration list)**
Industry / Commercial	88
Government	9
Academia (including students)	31
Other / unknown	2
- total -	130

Table 2 Participants' professional category

The workshop presentations have been combined in a booklet and were distributed to all participants. It is also available as a PDF file (for AcrobatReader V5.0) and can be downloaded from the SHAMAN web site [46].

[46] *Presentations and Posters of the IST-2000-25350 SHAMAN Workshop "Security for mobile systems beyond 3G"*, July 25, 2002, Royal Holloway, University of London, available online at http://www.ist-shaman.org/publicDocs/docs_index.htm

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.

The workshop presentations are listed in the subsequent paragraphs.

Invited presentations at the SHAMAN workshop:

[47] Michael Walker, *Security Challenges for the Next Generation of Mobile Communications*
Keynote talk

[48] Fred Piper, *PKI – Does it have a future?*

[49] Hu Wang, *Securing MANETs: mechanisms derived from the MIND scenarios*

[50] Günter Schäfer, *Network Denial of Service: One Major Challenge for the Next Years of Network Security Rersearch*

[51] Peter Lonergan, *INTERNODE: A Nomadic Source Secure VPN provisioning system*

Workshop presentations contributed by SHAMAN members:

[52] Nigel Jefferies, *Introduction to the SHAMAN project*, SHAMAN Workshop 2002, Royal Holloway, University of London, 25 July 2002

[53] Günther Horn, *Securing Network Access in post-3G Mobile Systems*, SHAMAN Workshop 2002, Royal Holloway, University of London, 25 July 2002

[54] Scarlet Schwiderski-Grosche, *Online Payment for Access to Heterogeneous Mobile Networks*, SHAMAN Workshop 2002, Royal Holloway, University of London, 25 July 2002

[55] Kaisa Nyberg, *PAN security issues and solutions*, SHAMAN Workshop 2002, Royal Holloway, University of London, 25 July 2002

[56] Christian Gehrmann, *The personal CA – PKI for a Personal Area Network*, SHAMAN Workshop 2002, Royal Holloway, University of London, 25 July 2002

[57] Timothy Wright, *Issues with the use of PKI for authorisation of code download*, SHAMAN Workshop 2002, Royal Holloway, University of London, 25 July 2002

[58] Hubert Ertl, *Security Modules in Future Mobile Communication Systems*, SHAMAN Workshop 2002, Royal Holloway, University of London, 25 July 2002

5 Conclusions

This section summarises the standardisation activities and external liaisons of the SHAMAN project. Key contributions to the respective standards bodies are listed.

For the framework of the 3GPP SA WG3 (Security) activities, results from the PKI and subscriber certificate work in SHAMAN workpackages 2 and 3 are forwarded through the SHAMAN members which are also active in 3GPP SA WG3. It is also expected that results from the security module work in SHAMAN workpackage 4 can be contributed to 3GPP in the future.

The MANA protocols developed in workpackage 2 have been submitted to the Bluetooth Consortium / Bluetooth Security Expert Group SEG for the application of device pairing and to ISO/IEC JTC1/SC27 to become part of the new entity authentication standard (ISO/IEC 9798-6) for further consideration in their standardisation activities.

It is expected that future research issues resulting from the current SHAMAN work could be forwarded to both the Wireless World Research Forum (WWRF) and the 3GPP WG SA3 activities for future consideration by the SHAMAN partners who are also involved in the mentioned activities. Details on the future dissemination of SHAMAN results will be reported in upcoming WP6 deliverable D14 [45].

6 References

- No global references. All relevant references were added in the respective sections. -