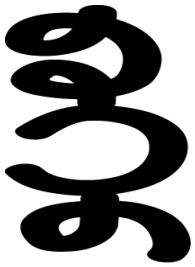

IST-2000-25350 - SHAMAN

Security for Heterogeneous Access in Mobile Applications and Networks
(01-NOV-2000 to 27-MAR-2003)

Deliverable Number	D14
Deliverable Title	Dissemination and use plan
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	13

Abstract:

Intentions for use and dissemination of SHAMAN results and experience.

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 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 SHAMAN project has been completed successfully. The results of the project are contained in the final technical report, deliverable D13. The intentions of the participants for exploitation and dissemination of the results following the completion of the project are outlined here.

This document summarises the intentions of the project members for the exploitation and use of the results of the SHAMAN project. The common intention is to support the contribution of the results to the appropriate standards bodies relating to mobile/wireless communications.

As the stated intention of the project was to carry out advanced research, the results are outside current product development timescales. The original scenario for realisation as product is still valid but, due to slow deployment of the early releases of UMTS and also to global economic effects, the intermediate dates for development of standards are already later than we foresaw at the beginning of the project.

Specific statements are included from each of the members.

Project summary

Participation in collaborative R&D and in standards work provides benefits to participants in addition to the obvious financial help received from the Community. For industrial participants, there are benefits and advantages in working together in developing early know-how and understanding of future directions, together with insights into the challenges and issues arising. For the academic participant there is the benefit and satisfaction in pushing forward the frontiers of theory and engineering knowledge with confidence in the likelihood of economic relevance. For all participants there is the benefit of being part of a community working together over extended periods in advanced R&D. In turn there are duties to ensure that results are made available to the wider community through publications and submissions to the standards bodies.

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 main work for the two areas was conducted by Workpackages WP1 (network) and WP2 (terminal). 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 final technical report D13 (see [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

WP6 Dissemination, external relations and liaison

The complete WP6 report is published as D12 (see [2]), and the specification of the WP5 demonstrator is published as D11 (see[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:

- 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 was to provide the architectural framework together with appropriate mechanisms and protocols to ensure the security of networks with these features.

We provided specifications of interfaces, protocols and mechanisms that are needed to provide required levels of protection. We have also developed important 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, WP2) 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 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 were 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 did not plan to add 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 related to exposure or compromise over the radio links and the core networks, others 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.

1.2 Project partners and contacts

Vodafone Group Services Limited	UK	Nigel Jefferies
Royal Holloway, University of London	UK	Chris Mitchell
Siemens Atea n.v.	BE	Jef Dankers
Nokia Corporation	FI	Valtteri Niemi
Ericsson AB	SE	Rolf Blom
T-Systems Nova GmbH	DE	Peter Windirsch
Giesecke & Devrient GmbH	DE	Hubert Ertl
Siemens AG	DE	Günther Horn

2 Outline of project results and conclusions

(for details see reference [1])

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

The following issues have been identified as requiring R&D and standardisation attention

WP1

in addition to further supporting R&D work, all these need to be taken up in the standards bodies

- EAP-based authentication methods;
- 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 Future action

3.1 General benefits

The principal impact of the network and terminal R&D results on products and services will be through the standardisation processes. The whole field of mobile communications is dependent on standards to support interoperability: there is little benefit in individualist developments which would set apart a product or seek to establish it as having unique advantage. The market place is substantially level, with no monopolistic positions to defend. The history of the industry is of co-operation and collaboration between operators and between suppliers in standardisation organisations like 3GPP and R&D undertakings such as SHAMAN, working towards standards and conventions for the benefit of the whole industry.

Participation in collaborative R&D and in standards work has to provide benefits to participants. For industrial participants, there are benefits and advantages in developing early know-how and understanding of future directions together with insights into the problems and issues arising. For the academic participant there is benefit and satisfaction in pushing forward the frontiers of theory and engineering knowledge with confidence in the likelihood of economic relevance. For all participants there is the benefit of being part of a community working together in ongoing R&D.

3.2 Outline of participant plans

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

Table 1 – Standardisation and exploitation

SHAMAN Project	NOV-2000 – OCT-2002
Project Workshop	JUL-2002
Prepare New Work Items in standards bodies or industry forums	AUG-2002 – DEC-2002
Standards activity on NWIs	JAN-2003 – JUN-2004
Availability in Major Standards Release	SEP-2004
Availability of derived products	JUN-2005

3.2.1 Vodafone Group Services Limited

During the lifetime of SHAMAN, the Vodafone R&D community has been integrated into a single entity: Vodafone Group Research and Development. This ensures that results from projects such as SHAMAN are available across the company and can be promoted regionally.

Vodafone is active in developing security standards within 3GPP and OMA and the SHAMAN results will provide valuable guidance in support of this work.

SHAMAN also establishes a valuable baseline for subsequent collaborative European research in this area proposed under FP6. More generally the work in SHAMAN will help Vodafone understand and address security issues in future mobile systems so that it can design, build and operate secure mobile products and services.

Following on from the SHAMAN Project Vodafone is already starting to exploit many of the concepts developed in the project in order to address security requirements in future mobile terminals and networks.

3.2.2 Royal Holloway, University of London

The Information Security Group at Royal Holloway will continue to provide an editor to support the completion of international standard ISO/IEC 9798-6 containing the MANA protocols developed within the SHAMAN project. This will be part of a long term commitment by Royal Holloway towards the development of international security standards. The benefits from this activity include not only the dissemination of research results into the wider community but also the acquisition of knowledge which is fed back into the large scale security-based masters degree teaching that Royal Holloway undertakes.

Using the expertise developed in SHAMAN, Royal Holloway will continue its research work in fields relating to the security of wireless communications, both in existing national and international collaborative research programmes, and as a basis for future bids for such research funding. The knowledge gained in SHAMAN will also be of direct benefit in informing postgraduate student teaching, both at the research (PhD) level, where around 10 students are currently involved in mobile-security related projects, and in masters-level courses.

3.2.3 Siemens Atea n.v.

Siemens Atea, will be active in the development of solutions for fixed and mobile networks in the domains of voice, data and multimedia applications, and this in the framework of their own projects as well as for the Siemens group world-wide. It will continue its research and support for and contributions to standards related to its activities.

3.2.4 Nokia Corporation

Nokia will work together with other companies and academia in creating new standards for mobile telecommunications relating to networking and the to the mobile terminal. An important goal is the creation of open standards. This supports faster development of the industry for the benefit of consumers.
In the areas related to SHAMAN, Nokia Research Center plans to contribute into various standardization bodies, including 3GPP, OMA, IETF and Bluetooth SIG.

3.2.5 Ericsson Radio Systems AB

Ericsson is a world-leading supplier of equipment for telecommunications systems and related terminal platforms. The Company produces advanced systems and products for wired and mobile communications in public and private networks with a strong commitment to IP technology supporting both voice and data.
The successes of Ericsson are largely owing to long-term investments in research and massive development endeavours. The new telecoms world coming to life requires new and innovative security solutions to provide all the services expected by users, the any-where/any-time access over different access networks and users utilising more and more sophisticated terminals in PANs.
The work within SHAMAN provides components and system concepts to secure our long-term competitive product provisioning. The project has delivered key security concepts and developed new security architectures and mechanisms which we will use as input to our product development, further internal as well as collaborative research work and as a basis for standards proposals and initiatives.

3.2.6 T-Systems Nova GmbH

Following restructuring of Deutsche Telekom AG, the role of T-Systems has become more focussed on the development of product solutions for the Deutsche Telekom group and for external clients, so for the immediate future, emphasis tends to be on development and consulting rather than on pure research activities. Nevertheless, the results of SHAMAN will be used and further developed by the T-Mobile branch (mobile communication and services provider) of Deutsche Telekom. Historically,

the SHAMAN team from T-Systems Nova and T-Mobile have strong cooperation sharing activities in the development and standardisation of security for mobile communication and T-System Nova's work in SHAMAN has been performed on behalf of T-Mobile. Therefore, T-Mobile will continue its support for and contribution to standards, and will be active in the development of mobile products and services for the mobile sector in the future. These activities are also based on the results created within SHAMAN.

3.2.7 Giesecke & Devrient GmbH

G&D is active in contributing to new standards and in developing new security products for mobile telecommunication. We are actively contributing to ETSI, SCP, OMA and the recently established WLAN Smartcard Consortium. The results of SHAMAN provide valuable guidance on the various security options to be selected by those standardisation committees.

G&D's participation in EU funded consortia like RESET and WITNESS allows us to share the results with European partners outside the SHAMAN consortium.

The development of the EAP AKA demonstrator was already helpful to visualise EAP authentication protocols to customers. Those protocols are expected to be used for WLAN authentication. For EAP AKA and EAP SIM we expect products within the next few months. Additionally the smartcard-based implementation of the Diffie-Hellman key agreement protocol acts as a reference for advanced smartcard solutions at G&D.

3.2.8 Siemens AG

Siemens has already started to exploit the results of SHAMAN in the form of standards contributions, in particular to the IETF (see deliverable D12), and will continue to do so in other standards bodies also (see table below). The standards that will be established with the help of SHAMAN contributions will enable innovative networking and terminal products by Siemens. In a more general sense, the results of SHAMAN have helped Siemens to shape and to consolidate the vision of mobile systems beyond 3G in the area of security, and to get a better understanding of the technical problems involved. This will help Siemens to develop secure products for mobile systems beyond 3G.

3.3 Publications

The participants will contribute SHAMAN results to appropriate publications, conferences and workshops as and when the opportunity arises.

The Institution of Electrical Engineers (IEE) plans to publish a book based mainly on the results of the project provisionally entitled *Security for mobility*. The editor is Chris Mitchell and contributors are members of the SHAMAN project.

3.4 Summary of future action

	International and Industry standards					Products and services				Collaborative R&D	
	3GPP	IETF	ISO/IEC	BT, IEEE etc.	OMA etc.	Network components	Network services	Terminals & components	Terminal services & applications	FP6 IP or STRP	FP6 NoE
Vodafone	✓	✓			✓		✓		✓	✓	✓
Royal Holloway			✓							✓	✓
Siemens ATEA	✓					✓		✓	✓	✓	✓
Nokia	✓	✓		✓	✓	✓		✓	✓	✓	✓
Ericsson	✓	✓		✓	✓			✓	✓	✓	✓
T-Systems Nova	✓					✓	✓		✓		
G&D	✓		✓		✓				✓	✓	✓
Siemens AG	✓	✓	✓			✓		✓	✓	✓	✓