IST-2000-25350 - SHAMAN

Deliverable Number	**D06**
Deliverable Title	**Status report on standards bodies**
Date of delivery	**30-Nov-01**
Document Reference	**SHA/DOC/TNO/WP6/D06/1.0**

Contractual Delivery Date	**30-Nov-2001**
Actual Delivery Date	**30-Nov-2001**
Editor	**Peter Windirsch (TNO)**
Participant(s):	**Vodafone, Royal Holloway, Nokia, Ericsson, T-Nova, Giesecke & Devrient, Siemens AG**
Workpackage	**WP6**
Est. person months	**1.0**
Security	
Nature	
Version	**1.0**
Total number of pages	**23**

Abstract:

The objective of this report is to identify standards and industry bodies as well as other projects which may work in technical fields related to SHAMAN and therefore be candidates where to the SHAMAN project results might be disseminated for influencing their further work.

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

Table of contents

Executive summary

The main objective of this report is to identify standards and industry bodies as well as other projects that may work in technical fields related to the SHAMAN project activities. Such bodies and projects are therefore potential places that the SHAMAN project results can be disseminated to and where the SHAMAN project results may be of influence. In addition to that main purpose, this report also helps to identify work in related fields which has already been performed and which may be used as input to the SHAMAN project.

In the first sections, relevant formal standards bodies are listed. In these standards bodies, various partners from international organizations, governments, industry, and academia are involved in specifying future standards in the area of telecommunications. These standards are intended to enable interoperable user devices as well as infrastructure components for use over a large number of countries if not world-wide.

In addition to the formal standards bodies enumerated in the first sections of this document, we also include a number of industry forums defining quasi- and de-facto standards that are supported at least by the participants working in the specific consortia. In these consortia, a large number of international partners from industry and sometimes from academia share work in generating these technical specifications.

We also describe research and development programmes, the latter mainly with European focus, which are performing work on future telecommunication systems.

For all three cases, the relevance of the different standards bodies and projects with respect to the outcome and dissemination of SHAMAN results is discussed. By identification of the standardization or project schedules, the possibilities of forwarding results from the SHAMAN project activities can be evaluated.

List of contributors

Name		Affiliation	Email	Phone
Boman	Krister	Ericsson AB (ERIC)	krister.boman@emw.ericsson.se	+46 317476045
Bücker	Wolfgang	Siemens AG (SAG)	wolfgang.buecker@mchp.siemens.de	+49 89 636 43697
Chandrasiri	Pubudu	Vodafone Group (VOD)	pubudu.chandrasiri@vodafone.com	+44 1635 682986
Ertl	Hubert	Giesecke & Devrient GmbH (GD)	hubert.ertl@gdm.de	+49 89 4119 2796
Garefalakis	Theo	Royal Holloway University of London (RHUL)	theo.garefalakis@rhul.ac.uk	+44 1784 414160
Gehrmann	Christian	Ericsson Mobile Platforms AB (ERIC)	christian.gehrmann@ecs.ericsson.se	+46 46 232904
Niemi	Valtteri	Nokia Group (NOK)	valtteri.niemi@nokia.com	+358 40 5331438
Windirsch	Peter	T-Systems Nova GmbH (TNO)	peter.windirsch@t-systems.de	+49 6151 833821
Wright	Timothy	Vodafone Group (VOD)	timothy.wright@vodafone.com	+44 1635 676456

The contributors are listed by name in alphabetic order.

Abbreviations

3GPP	Third Generation Partnership Project
AAA	Authentication Authorization and Accounting
API	Application Programming Interface
CA	Certification Authority
CDMA	Code Division Multiple Access
DAB	Digital Audio Broadcasting
DVB	Digital Video Broadcasting
EG	Expert Group
ETSI	European Telecommunications Standards Institute
GERAN	GSM / Edge Radio Access Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
IC	Integrated Circuit
IETF	Internet Engineering Task Force
IMS	IP Multimedia System
IP	Internet Protocol
IRTF	Internet Research Task Force
ITU	International Telecommunication Union
JCP	Java Community Process
JSR	Java Specification Request
MExE	Mobile Execution Environment
MIDP_NG	Mobile Information Device Profile – Next Generation
MT	Mobile Terminal
MWIF	Mobile Wireless Internet Forum
OO	Object oriented
OCSP	Online Certificate Status Protocol
PAN	Personal Area Network
PKIX	Public Key Infrastructure X.509
QoS	Quality of Service
SCP	Smart Card Platform
SIG	Special Interest Group
SIM	Subscriber Identity Module
SSL	Secure Socket Layer
TDMA	Time Division Multiple Access
TE	Terminal Equipment
TLS	Transport Layer Security
TSG	Technical Specification Group
UE	3G User Equipment
UMTS	Universal Mobile Telecommunication System
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network

WAP	Wireless Access Protocol
WCDMA	Wideband Code Division Multiple Access
WIM	WAP Identity Module
WLAN	Wireless Local Area Network
WSG	WAP Security Group
WTLS	Wireless Transport Layer Security

1 Introduction

1.1 Scope and purpose

The purpose of this report is to identify standards and industry bodies working in fields related to the SHAMAN work. It shall serve as input for the future SHAMAN result dissemination activities. The report lists the areas and the status of work in the standards and industry bodies. In addition, other research projects working in related fields and their possible relations to the SHAMAN project are listed.

1.2 Contents of this report

This reports summarizes the activities in the identified standards and industry bodies working in fields related to the SHAMAN work. Information about the timeframe of the activities which may be relevant for providing SHAMAN results in time for inclusion in the standards and industry bodies work and standardization processes is given where available.

2 Standards bodies

2.1 ETSI (European Telecommunications Standards Institute) and 3GPP

ETSI is a non-profit organization whose mission is the production of telecommunications standards to be used throughout Europe and beyond. More than 880 members from more than 50 countries world-wide like public administrations, network operators, manufacturers, service providers, research bodies, and users participate in ETSI's activities. These activities are structured in work programmes, which are determined by the ETSI members, who are also responsible for approving its results. Therefore, ETSI's activities are maintained in close alignment with the market needs expressed by its members.

ETSI plays a major role in developing a wide range of standards and other technical documentation as Europe's contribution to world-wide standardization in the areas of telecommunications, broadcasting, and information technology. ETSI's prime objective is to support global harmonization by providing a forum in which all the key players can contribute actively.

Additional information:

[1] http://www.etsi.org .

[2] The annual report of ETSI for the year 2000 summarizing the main activities within ETSI can be downloaded from http://www.etsi.org/literature/annual_report.html .

2.1.1 3GPP - Third Generation Partnership Program

In 3GPP, many partners from around the world (including ETSI) have agreed to co-operate in the production of globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support, particularly a new radio access technology based on CDMA.

The participating partners have further agreed to co-operate in the maintenance and development of the Global System for Mobile communication (GSM) Technical Specifications and Technical Reports including evolved radio access technologies.

For the SHAMAN project,

- the working group "Security" (TSG SA WG3) from the Technical Specification Group "Service and System Aspects" (TSG SA) with respect to security aspects and
- the working group "Universal Subscriber Identity Module USIM" (TSG T WG3) from the Technical Specification Group "Terminals" (TSG T) with respect to the standardization of the security tokens used by the mobile device for various purposes

are considered as candidates for disseminating results and to be influenced for the process of standardizing future mobile systems.

2.1.2 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 two sets of specifications. Release 99 was frozen in the spring of 2000 and release 4 was frozen in the spring of 2001. Current work is targeting on release 5 specifications which will be frozen in the spring of 2002. Also, work towards release 6 has already started.

The main work item in Release 5 is inclusion of IP Multimedia Subsystem (IMS). This is built on top of the packet switched UMTS (or GPRS) network and it is designed in a way which also allows other transport networks to be used. In particular, several access technologies may be taken into use.

The security working group of the 3GPP is called SA3. Its main work areas for release 5 work are

- access security to the IMS;
- network domain security.

From the SHAMAN perspective the first is more relevant, since the possibility of heterogeneous access network structure is built into the concept of IMS. In practice, the first release of IMS (i.e. release 5 of 3GPP) has almost exclusively concentrated on the case where the underlying transport network (of IMS) is UMTS Release 99 PS and the access network is either GERAN (using TDMA technology) or UTRAN (which uses WCDMA technology). The developments in 3GPP in this area have been closely followed in the course of SHAMAN WP 1 work. On the other hand, the SHAMAN WP 1 results have not yet been fed into the 3GPP release 5 work. The reason for this is two-fold:

- the scope of 3GPP IMS work in rel. 5 is only a small subset of the scope of SHAMAN WP 1;
- the freezing date of 3GPP rel.5 is too early; in practice all major decisions for rel. 5 were made in 3GPP before SHAMAN WP 1 begun to produce results.

The first target release of SHAMAN WP1 results in 3GPP is release 6. The exact scope of release 6 is yet to be defined but it is quite probable that rel. 6 does not introduce any major architectural changes. If this turns out to be the case then SHAMAN WP 1 results are also applicable to later releases where the concept of heterogeneous access networks is more thoroughly included into the system.

There are two areas in the current 3GPP work which are directly relevant to the SHAMAN WP 2 activities. These are

- "UE functional split" work item;
- Mobile Execution environment (MExE).

The UE functional split issue is handled in several work groups in 3GPP and the security part shall be specified in SA3. In the release 5 time frame the issue may not be covered very well. The simplest case is the following. The user equipment contains two parts: a TE (e.g. a laptop) and a MT (e.g. a mobile phone) where only the latter has a radio connection to the wide area network. Since only some preliminary work has been done on SA3 so far, it is conceivable that SHAMAN WP 2 results are contributed to 3GPP in this work area. However, the most probable target for this is release 6 or later specifications.

The 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. Also in this case, release 5 specs cannot be affected by SHAMAN WP 2 work but the situation for further releases is different.

The results of the supporting (technical) SHAMAN work packages 3 and 4 may be contributed into 3GPP later but this occurs probably in the context of the above-mentioned work areas.

Additional information:

[1] http://www.3gpp.org/TSG/SA3.htm .

2.1.3 3GPP T3 (USIM)

API definitions, language bindings, USAT and USAT interpreter are the main working packages currently under heavy discussion in T3 USIM. Since the core work on USIM has already settled down and additional features like API and USAT interpreter are considered now, there might be minor chance to bring SHAMAN results to the T3 USIM standards body. Due to the close interaction to the T3 USIM body the dissemination of SHAMAN results is guaranteed, but without impact on the detailed specification process as expected from today point of view, but this might change as work continues.

Most activities within T3 are currently transferred to ETSI EP SCP (see below), which provides a common IC card platform for all mobile telecommunication systems. Therefore, possible cooperations and exchange of results will primarily be directed towards ETSI EP SCP (see Section 2.1.5).

Additional information:

[1] http://www.3gpp.org/TSG/T3.htm .

2.1.4 MExE Security Group

The Mobile Execution Environment (MExE), which is a 3GPP standard, is essentially a special case (a monolithic terminal) in SHAMAN. MExE provides a secure standardised execution environment to which 3rd party software developers could write services to execute directly in the MExE handset. In addition to the use of standardised network services, MExE provides additional capabilities to control telephony events and manipulate standardised network services in a user-friendly manner. MExE does not define any new technologies itself, however it identifies existing and emerging technologies that could be incorporated into the MExE framework through standardization.

Currently three different MExE Classmarks have been defined. MExE Classmark 1 being handsets based on WAP technology while Classmark 2 devices are based on PersonalJava. Classmark 2 terminals support security architectures to authenticate operator, manufacturer and 3rd party applications on the handset using digital certificates. Classmark 3 terminals are based on KJava (K for Kilo, a compact implementation of Java) together with MIDP (Mobile Information Device Profile).

As part of Release 5 there is a new Classmark based on CLI (Common Language Infrastructure) that is been standardised. CLI is a standardised execution platform developed by ECMA (European Computer Manufacturers Association) based on the Compact .NET framework from Microsoft.

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

3GPP Release 5 closes in March 2002. It is therefore unlikely that SHAMAN will have impact on MExE release 5 – the main impact is expected to be in Release 6 (March 2002 to June 2003).

Additional information:

[1] http://www.mexeforum.org .

2.1.5 ETSI EP SCP (ETSI Project Smart Card Platform)

The ETSI Project for Smart Cards, EP SCP, was recently approved by the ETSI Board, replacing the SMG Technical Sub-Committee, SMG9. The first reason for the change to SMG9 is to create a central focus point for the standardization of a common IC card platform for 2G and 3G mobile telecommunication systems. A second reason is to allow the participation from companies involved in standardization work for mobile communication systems in 3GPP, 3GPP2, GAIT, T1P1, TR45 and others yet to be identified.

The main responsibilities of SCP are:

- development and maintenance of a common IC card platform for all mobile telecommunication systems;
- development and maintenance of the application independent specifications for the Integrated Circuit Card/Mobile Equipment interface of those telecommunication systems under the responsibility of ETSI;
- development and maintenance of IC card standards for general telecommunication purposes;

- development and maintenance of IC card standards employing advanced security methods for telecommunications applications such as financial transactions over Mobile Telecommunication Networks ("mobile commerce").

The main tasks of SCP are:

- maintenance of the common platform standards developed by the committee;
- specification of enhancements to the common platform to allow the addition of innovative features and functions;
- specification of generic issues for IC cards for Telecommunications, these include but are not restricted to:
  - interface enhancements such as new commands and improved speed,
  - generic application download and load mechanisms,
  - electrical parameters and protocol issues,
  - advanced security mechanisms and related protocols,
  - advanced functionality for use by applications supported by the common platform standards;
- specifications for the use of low voltage technology for telecommunications cards;
- elaboration and maintenance of IC card related test specifications for the common platform in collaboration with the respective groups of 3GPP and other mobile smart card specification bodies.

SCP has direct liaisons with the relevant bodies of all committees involved in elaborating the common platform. In particular, SCP has direct liaisons with ETSI TC SEC which is involved in the specification of security matters.

In addition, SCP has liaison with CEN TC224 and other regional / national bodies. Some informal liaison is handled by delegates attending international standardization meetings and forums, for example ISO TC68 SC6, ISO/IEC JTC1/SC17, the Java Card Forum and the WAP forum.

Due to the strong interaction with EP SCP, the work on security modules, the specification of security modules, and the general requirements from other SHAMAN work packages as well as the final results of SHAMAN will be discussed with selected members of EP SCP, to identify regions of interest for future standardization efforts.

Additional information:

[1] http://portal.etsi.org/scp .

2.2 IETF Internet Engineering Task Force

The Internet Engineering Task Force (IETF) is a large open international community where network designers, operators, vendors, and researchers cooperate for new developments for the Internet architecture and the smooth operation of the Internet.

The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (application, general, internet, operations and management, routing, security, sub-IP, transport, user services). Work is performed based on the exchange of information via mailing lists and during IETF meetings held three times per year.

In addition to the activities of the IETF which are focused on engineering and standards making results which are to be achieved in short term, more long term oriented research activities are performed under the framework of the Internet Research Task Force (IRTF).

Additional information:

[1] http://www.ietf.org/rfc/rfc1602.txt The Internet Standards Process

[2] http://www.ietf.org

[3] http://www.ietf.org/rfc/rfc1603.txt IETF Working Group Guidelines and Procedures

[4] http://www.irtf.org

[5] http://www.ietf.org/rfc/rfc2014.txt IRTF Research Group Guidelines and Procedures.

2.2.1 AAA Group (Authentication, Authorization and Accounting)

The IETF Authentication, Authorization and Accounting Working Group focused their activities on the development of requirements for Authentication, Authorization and Accounting as applied to network access. Requirements were gathered from other IETF working groups. The developments are based on the DIAMETER protocol (a successor of the RADIUS protocol, also developed within IETF activities) and shall address the following issues:

- An accounting operational model for different types of network access.
- Compatibility with IPv6 and backwards to the RADIUS protocol.

Since the deadlines for outputs from that working group as published under [1] are in the past time only, it is expected that only the results of this working group might be used by SHAMAN and no contributions of SHAMAN to the working group are likely.

Additional information:

[1] http://www.ietf.org/html.charters/aaa-charter.html .

2.2.1.1 IRTF Authentication, Authorization and Accounting Architecture Research group

In addition to the IETF AAA group, there is also an IRTF Authentication, Authorization and Accounting Architecture Research group. Main goal of the IRTF AAAA research group is the development of a generic and widely applicable AAA architecture that includes issues of which multi organization interoperability, AAA transactions, application independent session management, and strong security mechanisms may give some input to the SHAMAN project. It closely cooperates with the IETF AAA group.

Additional information:

[1] http://www.aaaarch.org/home.html

2.2.2 PKIX Group (Public Key Infrastructure X.509)

The IETK PKIX works on protocols relating to the use of PKI technology within the internet. As part of the IETF, it is part of an open standards body. PKIX is in large part made up of certification authorities (CAs) and companies producing security software, though there is some attendance from mobile operators and terminal manufacturers.

PKIX's most well known output is its profile of X.509 certificates and certificate revocation lists for internet use, RFC 2459. Though not universally used, RFC 2459 is the profile that most new applications conform to. PKIX has also produced guidance for the production of Certification Practice Statements (CPSs) and the Online Certificate Status Protocol (OCSP), a method for obtaining a certificate's status in real time.

SHAMAN WP3 might interact with PKIX in making recommendations for adaptations to PKIX protocols for client revocation checking. SHAMAN should hopefully not require any changes to PKIX certificate profiles. However, RFC 2459 is currently being revised, so there is the possibility of SHAMAN making some recommendations or suggestions before this revision is approved.

PKIX, like all IETF groups, approves specifications as and when they are ready, and does not conform to any set timetable. Therefore, aside from individual specification timetables, SHAMAN does not have any timescales for inputs.

Additional information:

[1] http://www.ietf.org/html.charters/pkix-charter.html .

2.2.3 SIP Group (Session Initiation Protocol)

The IETF Session Initiation Protocol (SIP) working group is currently working on improving the existing specification of SIP (RFC2543) which is intended for initiating interactive communication sessions between users for voice, video, chat, interactive games, and virtual reality related communication. The analysis of potential application of the SIP is out of scope of the activities of that working group and will be handled by the Session Initiation Proposal Investigation working group (SIPPING).

The group will also maintain dialogues with other IETF working groups like the IP telephony (IPTEL) WG, whose Call Processing Language (CPL) relates to many features of SIP, will continue to consider the requirements and specifications previously established by the PSTN and Internet Internetworking (PINT) working group, and will consider input from the Distributed Call Signaling (DCS) Group of the PacketCable Consortium for distributed telephony services, and third-generation wireless network requirements from 3GPP, 3GPP2, and MWIF.

For both working groups (SIP and SIPPING respectively), the planned milestone dates as published at [1] and [2] are at the end of 2001 or the beginning of 2002, so that SHAMAN can expect some results as input for its work but no contributions from SHAMAN to the IETF working groups' activities would be ready in time.

Anyhow, there are still ongoing activities within 3GPP related to IMS (IP Multimedia System) to extend the existing SIP and SIPPING specifications as can be found under [3].

Additional information:

[1] http://www.ietf.org/html.charters/sip-charter.html

[2] http://www.ietf.org/html.charters/sipping-charter.html

[3] http://www.3gpp.org/TB/Other/IETF.htm .

2.3 WAP Forum / WAP Security Group

The WAP Forum is a standards body that produces specifications covering the functionality required for wireless devices to access internet type content and services. It was founded by Ericsson, Nokia, Motorola and Openwave (then called Unwired Planet) in 1997 and opened out to public membership in 1998. The first version of the standards, WAP 1.0 was released in 1998. This has been followed by 3 subsequent version, including WAP 2.0, released in August 2001.

The WAP security specifications are produced by the WAP Security Group (WSG). The WSG has produced specifications for Wireless Transport Layer Security (WTLS, an adaptation of SSL for wireless communication), the WAP Identity Module (WIM, a specification of storage of sensitive cryptographic parameters and functions) and a function for requesting a wireless client to produce a digital signature (function *signText*). Within WAP 2.0, a profile of X.509 was produced and a profile of the IETF's Transport Layer Security (TLS, the standardised version of SSL).

There is possible interaction between the WSG and SHAMAN in a number of ways.

Many SHAMAN requirements for a device to perform public key based client authentication may take advantage of the WIM. Some changes to the WIM, and to functionality producing client authentication (*signText*, and the profile of TLS) may be required to support the client authentication requirements (e.g. inter- and intra- PAN, client authentication over wireless LAN) of SHAMAN. There may also be interaction concerning the WIM between the WSG and SHAMAN WP4. SHAMAN WP3 may make recommendations to WSG on how client revocation checking should be performed and other PKI functions. SHAMAN WP2 may make recommendations for how the WSG's generic Signed Content specification could be used in practice, for secure inter-PAN transmission of executables.

The WAP forum has decided not to produce specification releases on a fixed timetable but only when there are an appropriate number of individual approved specifications. There are therefore no fixed milestones for SHAMAN to meet.

Additional information:

[1] http://www.wapforum.org .

3 Industry forums and research projects

3.1 Bluetooth Consortium/ Bluetooth Security Expert Group

The Bluetooth Special Interest Group (SIG), comprised of leaders in the telecommunications, computing, and network industries, is driving development of the Bluetooth technology and bringing it to market. The Bluetooth SIG includes promoter companies 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia and Toshiba, and more than 2000 Adopter/Associate member companies.

The SIG performs specification work in different working groups focusing on particular use cases or parts of the specification. Membership in working groups is limited to active selected contributors from companies with significant vested interest in developing products. To enable broad industry and cross-industry feedback, expert groups have also been formed. The expert groups support working groups or other SIG entities like policy committees. The Bluetooth SIG security expert group provides the working and policy groups with expertise in a wide range of security issues. This includes suggestions for security solutions and improvements of existing and upcoming standards. The actual specification work related to security is performed in the relevant working groups. New and updated compete specifications are given in regular main releases.

There are several working groups that are relevant for the SHAMAN WP2, WP3 and WP4 work. SHAMAN will have the possibility of influencing both the security expert group and the relevant working group directly. SHAMAN has the opportunity to contribute to the security content of the next main release of the Bluetooth specification. The Personal Area Network (PAN) working group is working with communication scenarios that are applicable to the SHAMAN WP2 PAN reference model. The PAN group has so far not developed any advanced security architecture and the SHAMAN WP2 target is future releases. The Radio 2 (high rate) working group security architecture has not at all been settled and the WP2 internal communication security solutions as well as the WP3 non-certified PKI work will be useful input to this work. The Car working group is about to release a new SIM access profile. That profile follows the car scenarios that WP2 are working with. Although the WP2 and WP4 work will be too late to influence the first release of the specification, the work is targeted towards future releases. The WP3-related WP2 work as well as the WP2 work on key exchange might be fed into the possible new standardized higher layer key exchange work that has been suggested by the security expert group.

There are no deadlines known for providing results from SHAMAN as possible inputs to the Bluetooth activities.

Additional information:

[1] http://www.bluetooth.com .

3.2 MIDP_NG Group

Java is probably the most powerful programming language available to developers for web-based applications. Its platform independence and Object Oriented (OO) concepts mean that developers are able to write applications to a wide range of devices rapidly. However, these applications are not catering the vast number of resource-constrained devices, such as mobile phones.

The Mobile Information Device Profile-Next Generation (MIDP_NG) is a compact Java technology standard for mobile phones defined within the Java Community Process (JCP). The JCP is run by Sun to develop Java standards to address different niche markets by involving experts from those areas (more information at [1]). The specification work in JCP is done by different Expert Groups (EG) after a JSR (Java Specification Request) is approved. MIDP_NG is a result of JSR118 (more information at [2]).

MIDP_NG is currently defining a PKI based security framework for authenticating downloaded applications to terminals. The majority of the basic concepts behind the framework are now finalised. However the details remains to be worked out. For example the group still has not made a decision on certificate revocation, i.e. whether it should support revocation or not, and if so, which standard it is going to follow.

MIDP_NG is working towards very ambitious deadlines, the specification is expected to be ready for community review (a review by other groups in the JCP) by mid December 2001 and they expect the specification to be stable by end of January. Nevertheless the thinking in SHAMAN has influenced the work MIDP_NG in certain ways. The PKI work in WP3 has contributed to discussions on certificate revocation, in particular with respect to the OCSP (Online Certificate Status Protocol) standard. Also the discussions and thinking in WP2 has influenced in defining some fundamental concepts in the security framework in MIDP_NG. One example is the concept of a security policy files and its management.

Additional information:

[1] http://jcp.org/

[2] http://jcp.org/jsr/detail/118.jsp .

3.3 IST Information Society Technologies

The Information Society Technologies programme builds a framework for research activities funded by the European Commission. One area of supported projects within the IST programme contains advanced mobile communication systems and devices. All projects listed in the four subsequent subsections are members of the "Systems Beyond 3G" cluster, whose main goals are

- the development of evolutionary scenarios based on 3G systems and revolutionary scenarios deploying leading access technologies
- the integration of mobile and fixed communication networks
- allowing seamless transition and service provisioning across heterogeneous access technologies
- the consolidation of results of projects in relevant fields

Additional information on the "Systems Beyond 3G" cluster can be found at http://www.cordis.lu/ist/ka4/mobile/beyond3g.htm.

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

The IST-project MIND is a follow-up to the project IST-1999-10050 BRAIN (Broadband Radio Access for IP based Networks). BRAIN developed a framework for the deployment of high bandwidth access technologies, taking the example of HIPERLAN/2, that could be complementary to 3G cellular technologies. As its most salient results BRAIN developed a reference architecture for an access network (BAN – BRAIN Access Network) as well as concepts for handling micromobility issues within the BAN. Furthermore BRAIN developed concepts for end-to-end QoS provisioning.

MIND advances the approach taken by BRAIN through the extension of IP-based radio access networks to include mobile ad-hoc networks. The project will take as a starting point the concept of an IP core, accessed by a variety of technologies. It will develop this vision with business models and user considerations (including scenarios - which will look at the user side of ad-hoc networks). From this the project will derive the requirements on the network and air interface parts of the vision. In addition the project will conduct a trial - practical research - into the use of HIPERLAN/2 and an IP-based access network, using IP QoS and IP mobility management techniques, as a complement to UMTS and as a part of this vision.

The activities of the MIND project are divided in the following workpackages:

- WP1: definition and improvement of the mechanisms for the rapid creation and seamless provision of broadband IP services and applications, to develop new business and service models and to help specifying and evaluating application and service level trials conducted by WP6 Trials.
- WP2: Enhancement of BRAIN Access Routers (BARs) and BRAIN terminals with routing capabilities to operate in a MIND self organising wireless environment supporting ad-hoc mode.
- WP3: Refine, extend and validate the capabilities of the Air Interface proposed in the BRAIN project to facilitate broadband IP-based services for 4G mobile users.
- WP4: Standardisation contributions and dissemination of MIND results to organisations deemed important for the global deployment of MIND specifications as well as conferences, workshops, journals and the Internet.
- WP5: Project management work.
- WP6: Establishing a trial system to validate essential specifications defined by the BRAIN project as well as new studies dealt by WP1, WP2 and WP3.

3.3.1.1 Relevance to SHAMAN

SHAMAN WP1 studies the BRAIN Access Network (BAN) reference architecture as one promising candidate reference architecture based on which security issues for heterogeneous access could be investigated. Therefore SHAMAN will closely follow the activities of MIND since it (MIND) will built upon and advance the results of BRAIN. Security aspects have not been covered in-depth in BRAIN and, though considered important, are not a focus of MIND. Therefore it is expected that the results of SHAMAN will considerably contribute to MIND's work.

As a first step to initiate the cooperation between SHAMAN and MIND, SHAMAN WP1 will provide a document identifying open issues in the BAN reference architecture with respect to security by the end of 2001.

Additional information:

[1] http://www.ist-mind.org .

3.3.2 IST-2000-25394 MOBY DICK (Mobility and Differentiated Services in a Future IP Network)

The main objective of the MOBY DICK project is the development, implementation and test of end-to-end communications components based on IPv6. These components will support seamless vertical and horizontal hand-over mechanisms for and between different networks. The mechanisms for QoS and AAA functionality shall be based on the proposals developed by IETF and IRTF respectively. In the course of the project, a test scenario for validating the results, using UMTS, 802.11 Wireless LANs and Ethernet technologies, will be set up.

The activities in MOBY DICK are divided in the following workpackages:

- WP1: Project Framework (Requirements, Applications and System Integration) [M0 - M30]

The three implementation related workpackages for design, implementation and local testing of the solutions developed within the project are:

- WP2: Quality of Service [M4 – M28]: implementation and evaluation of QoS models in highly dynamic and heterogeneous network topologies.
- WP3: Mobility [M4 – M28]: the development of an architecture for wireless internet access by developing new mechanisms for seamless hand-over and QoS support during and after hand-over.
- WP4: Authentication, Authorization, Accounting and Charging [M4 – M28]: including the definition of a suitable charging concept to allow for permanent mobile IP based services

Two additional administrative workpackages are:

- WP5: Integration, Validation, Evaluation and Trials [M12 – M16, M20 – M24, M26 – M36]: for testing the implementations developed during the project at locations all over Europe for a period of six months based on exchange students as test-users.
- WP6: Project Management and External Relations [M0 – M36]:
  participation in the following activities is planned:
  - IRTF (Internet Research Task Force)
  - AAAArch (Authentication, Authorization, and Accounting Architecture) working group

  In addition, it is planned to monitor the following activities:
  - ETSI / 3GPP activities
  - MWIF
  - IEEE 802.11

Results in the following areas are planned as contribution to the "system beyond 3G" program:

- Solutions for mobile IPv6
- End-to-end QoS for mobile users
- AAA and charging mechanisms for access networks and backbone
- End-to-end architecture for all-IP based mobile communication supporting heterogeneous network (e.g. radio router with IP air interfaces)

The project is planned for a period of 36 months from 01. Jan. 2001 to 31. Dec. 2003.

3.3.2.1 Relevance to SHAMAN

The following issues in MOBY DICK may be of relevance for similar activities within SHAMAN:

- The integration of QoS, IPv6 mobility, and AAA.
- Working prototype of an AAA and charging server for interconnection of mobile nodes to the backbone network.
- Mobile enabled applications for mobile nodes.

Additional information:

[1] http://www.ist-mobydick.org .

[2] Information Society Technologies. *Draft proceedings of the 4th Concertation Meeting – IST Area IV.5 Mobile / Wireless / Satellite*, Brussels, 13. – 14. March 2001. p. 29 - 40

3.3.3 IST-1999-12515 DRiVE (Dynamic Radio for IP-Services in Vehicular Environments)

The main objective of the DRiVE project is to enable spectrum-efficient high-quality wireless IP in a heterogeneous multi-radio environment. As a result, in-vehicle (i.e. highly mobile) multimedia services, which ensure universally available access to mobile multimedia services for information and support for education and entertainment, will be possible.

To achieve this objective the DRiVE project addresses the convergence of cellular and broadcast networks to lay the foundation for such innovative IP-based multimedia services. The work in DriVE therefore is concentrated on the following two key issues:

1. Optimization of inter-working of different radio systems (GSM, GPRS, UMTS, DAB, DVB-T) in a common frequency range with dynamic spectrum allocation.

2. Co-operation between network elements and applications in an adaptive manner.

The approach to reach these goals within DRiVE is subdivided into four workpackages:

- WP1 (dynamic radio aspects): develops methods for dynamic frequency allocation and for co-existence of different radio technologies (GSM, GPRS, UMTS, DAB, DVB-T) in one frequency band to increase the total spectrum efficiency and reach.
- WP2 (IP-infrastructure): realises an IPv6-based mobile infrastructure that ensures the optimised inter-working of cellular and broadcast networks. The IP-infrastructure will provide support for asymmetric communication, for uni-, multi-, and broadcast, for quality of service and for continuous service in the presence of hand-over.
- WP3 (services, implementation, and trials): develops adaptive services for a multi-radio vehicular environment, integrates the key concepts of DRiVE developed in WP1&2 to demonstrate them and validate the benefits by user trials and field test.
- WP4 (project management and dissemination): manages the project and co-ordinates the dissemination of the results, e.g. contribution to standardization activities (ETSI, IETF, ITU).

The following results are expected from the DRiVE project:

- Specifications for the co-operation of cellular and broadcast networks in a common frequency range with dynamic spectrum allocation.
- An estimate for the increase of overall spectrum-efficiency by using dynamic radio systems.
- IP-based mobile infrastructure that ensures optimised inter-working of radio networks for spectrum efficient provision of high quality multimedia services.
- Demonstrations of key concepts of DRiVE and validation of the benefits of the technology by user trials and field tests.
- Influence on ongoing standardization using the consortium member's presence in the corresponding bodies 3GPP, (ETSI, IETF, ITU).

3.3.3.1 Relevance to SHAMAN

The following issues in DRiVE may be of relevance for similar activities within SHAMAN:

- Heterogeneous wireless access methods for IPv6 based communication (this will give additional insights into IPv6 related problems compared to IPv4 which shall be the current basic protocol platform within SHAMAN)
- DRiVE deliverable D04 "Roaming and Hand-Over for Intersystem Mobility" (Jan. 2001)

The project is planned for a period of 24 months from 01. Apr. 2000 to 31. Mar. 2002.

Additional information:

[1] http://www.ist-drive.org .

3.3.4 IST 1999-10669 Wine Glass (Wireless IP Network as a Generic Platform for Location Aware Service Support)

The Wine Glass project targets the move to an integrated seamless network that ensures global personal connectivity and enables access to wireless multimedia communications and services by anyone, from anywhere, at any time, with capabilities, quality and performance comparable to those of fixed network services.

From the Wine Glass project, contributions shall be provided to technical innovation by exploiting the potential of IP-based wireless mobile multimedia networking with UMTS and WLANs. The objective of the project is to exploit enhanced and / or new IP-based techniques to support mobility and provisioning some level of QoS in a wireless internet architecture based on UMTS and incorporating WLANs, and to explore their potential in enabling location- and QoS-aware application services for

wireless mobile users. As a part of the results from the project, a wireless internet testbed incorporating an IP backbone, UTRAN access to IP-based core network, and WLAN access to intranets, as a way to investigate, develop, test, integrate, validate and evaluate such innovative techniques and applications will be provided. From the viewpoint of the participating organizations, currently proposed techniques, such as Mobile-IP, IntServ, DiffServ, H.323, etc., are either non-scaleable or immature. As a result of this project, more advanced techniques, together with ideas of their enabled location- and QoS-aware application services, should be submitted to 3GPP and IETF as contributions in UMTS and mobile multimedia internet respectively.

This project will be realised in two phases:

- Phase-1 technical activities will concentrate on technical requirements and expected results for the project; hardware and software development and integration requirements for the wireless internet testbed; assessment of intermediate research results with respect to mobility support in the wireless internet architecture and location-aware application services.
- Technical activities in project phase 2 will include final integration of the wireless internet testbed; assessment of final research results with respect to support of mobility and soft-guaranteed QoS in the wireless internet architecture, as well as location- and QoS-aware application services.

A more detailed workpackage description of the Wine Glass project is only available from deliverable D1 which can be accessed via the "Download" section on the project's web page http://domobili.cselt.it/WineGlass/). The workpackages are:

- WP1: Project management and dissemination;
- WP2: Requirements, integration co-ordination, validation and evaluation;
- WP3: IP-based network;
- WP4: 3G UTRAN;
- WP5: Location- and QoS-aware services and applications.

3.3.4.1 Relevance to SHAMAN

The following issues in Wine Glass may be of relevance for similar activities within SHAMAN:

- Mobility management integration (access, Mobile-IP)
- QoS

The project is planned for a period of 24 months from 01. Jan. 2000 to 31. Dec. 2001. It therefore may end too early to get input from SHAMAN, but the results of the project might be taken into consideration by SHAMAN.

Additional information:

[1] http://domobili.cselt.it/WineGlass .

Conclusions

In this section, the most significant opportunities for the dissemination of results from the SHAMAN project and possible inputs from other projects and activities are summarized.

Outputs from the following workpackages could be contributed to the **3GPP SA WG3** activities:

- WP1: access security to the IP multimedia subsystem
- WP2: UE functional split and Mobile Execution Environment (MExE)
- WP3 and WP4: results on PKIs and security modules could be contributed to 3GPP in the context of the above mentioned areas

In addition, results from WP4 can be contributed to **3GPP T3** and **ETSI EP SCP** activities.

Results of SHAMAN WP3 on recommendations on PKIX protocol adaptations for client revocation checking could be forwarded to the **IETF PKIX** group. The other IETF working groups mentioned in this report will mainly serve as source of information due to their advanced state in reaching their last milestones soon.

Interactions between SHAMAN and the **WAP forum / WAP security group** could be established for the following work items:

- WP2 may make recommendations on signed content specifications (e.g. for secure exchange of executable code)
- WP3 may make recommendations on client revocation checking and other PKI related functionality
- WP4 may make recommendations on WAP Identity Module (WIM) characteristics.

Within the **Bluetooth Consortium**, several working groups are relevant for SHAMAN, both for providing input to SHAMAN and for receiving results from SHAMAN work in WP2, WP3 and WP4 for future releases of Bluetooth specifications. Especially,

- WP2 may contribute to the *Personal Area Network (PAN)*, *Radio 2 (high rate)*, and *Car* working groups and
- WP3 may contribute to the *Radio 2 (high rate)* working group.

Cooperation links from SHAMAN with the **Mobile Information Device Profile-Next Generation (MIDP_NG)** activities within the **JAVA Community Process** have been established by active collaboration of a SHAMAN member. Results from WP2 and WP3 have already influenced the definition of concepts for a security framework in MIDP_NG and on PKI certificate revocation, respectively.

For a cooperation with **IST MIND** the selection of IST BRAIN's (BRAIN is the predecessor project of MIND) network reference architecture as a base for the development of a security architecture in SHAMAN is the key. Derivative work within SHAMAN WP1 on the additional security architecture might be contributed to the further activities in MIND. From **IST MOBY DICK**, SHAMAN may get valuable input on IPv6 mobility and AAA related issues. SHAMAN results on AAA and charging could be contributed to MOBY DICK. Due to its early end in 2002, SHAMAN could mainly receive input on inter-working of different radio access systems from **IST DRiVE** project while contributions in the other direction are rather unlikely. As for the IST DRiVE project, SHAMAN may only get inputs from **IST WineGlass** results on mobility management integration and QoS without a chance of contributing to the project due to its early end in 2001.

References

- No global references. All relevant references were added at the end of each section. -