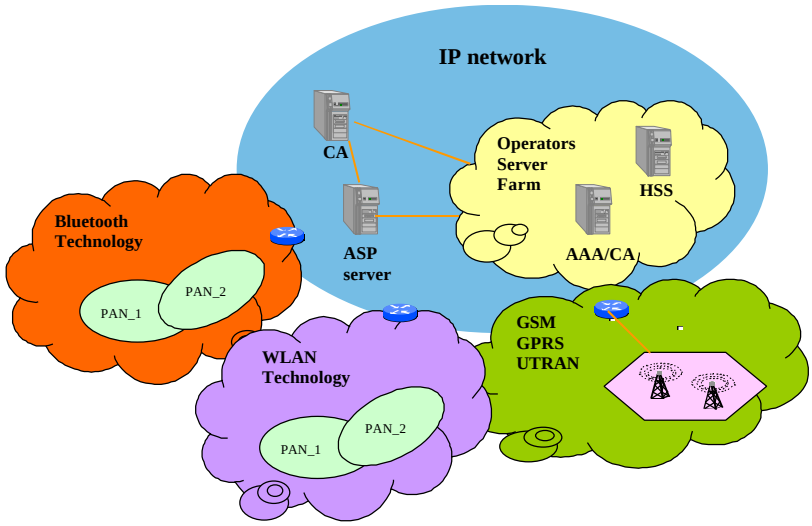
SHAMAN

SHAMAN IST-2000 25350 Security for Heterogeneous Access in Mobile Applications and Networks



Scope of project

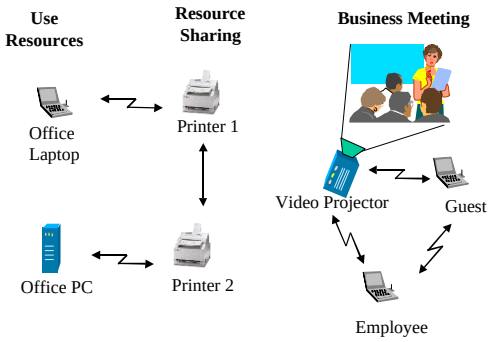
SHAMAN addresses the protection and security required for users, information and services as the next generation of mobile communications moves into new fields. The main topics which are addressed within SHAMAN are:

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

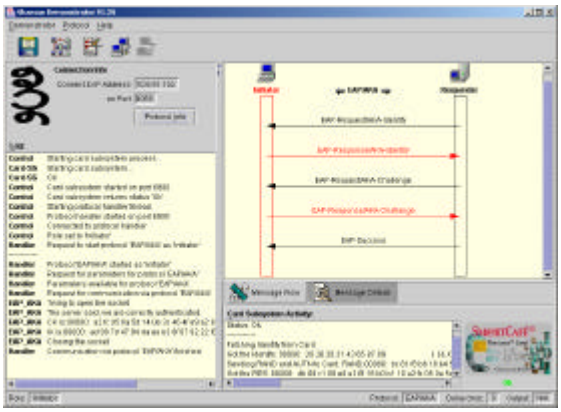
Approach for security

Four work packages have been defined within the project to provide the architectural framework together with appropriate mechanisms and protocols to ensure the security of services using the two areas

- Security for global roaming in IP-based mobile networks with heterogeneous access networks.
- Unified security architecture for future wireless terminals and applications.
- PKI for next generation telecommunications.
- Advanced security modules



The SHAMAN Demonstrator

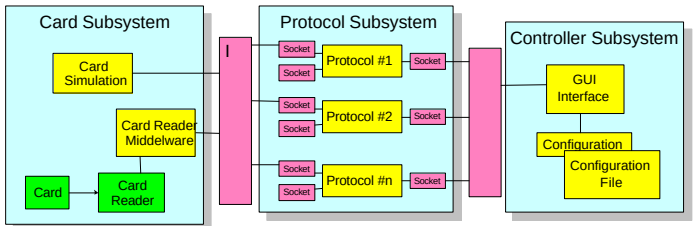


As one of the final results a demonstrator was set up, to show key features needed for authentication, security and roaming with in the underlying scenario. The key features to be demonstrated are imprinting and key agreement protocols.

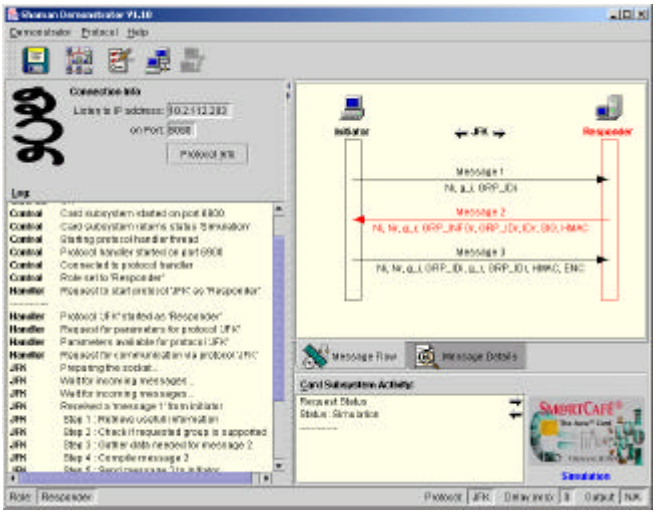
- For imprinting the MANA protocol has been selected, which allows devices to be imprinted by manual inter-action even on very limited devices.
- For key agreement a first draft of the EAP AKA authentication protocol has been implemented, which makes use of the symmetric 3G authentication algorithm (MILENAGE) for network infrastructures supporting the EAP authentication transport protocol.
- As a representative of asymmetric internet key agreement protocols the JFK protocol (Just Fast Keying) has been adopted, which was one of several candidates for IKE version 2.

The following features are provided by the demonstrator:

- Java™-based simulation and GUI environment
- a smart card as well as a smart card simulation can be used.
- several protocols can be used, added and replaced (plug-ins).
- Protocol implementations can be written in different programming languages.
- The architecture can be extended and reused.



Architecture of demonstrator

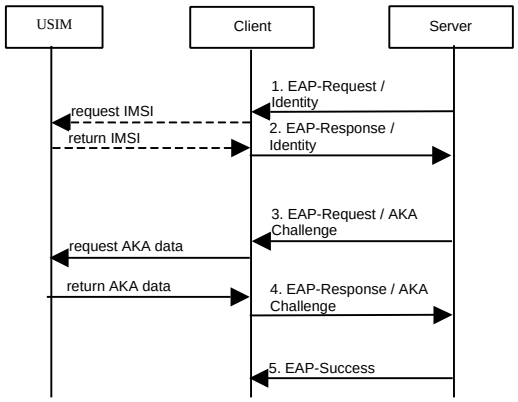


JFK Protocol

The principle GUI display of the demonstrator shows:

1. Message flow:
   - messages to/from a smart card
   - messages to/from the other protocol entity
2. Message details
   - All detailed protocol and timing information
   - The actual values exchanged between the protocol entities and the smart card
   - Message details are stored in a log file

The EAP AKA Protocol

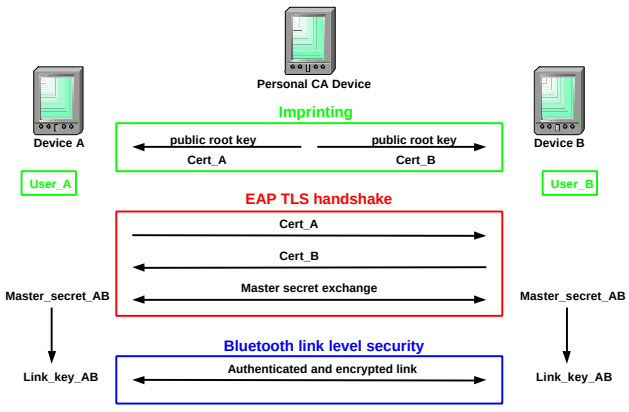


EAP AKA protocol

The Extensible Authentication Protocol (EAP) was originally designed to be used with PPP to provide a flexible means of authenticating hosts or users to network access servers. EAP does not define a specific authentication method but only the basic messages and protocol steps which could be used by many different concrete authentication mechanisms.

Within the demonstrator EAP AKA was implemented as this protocol can be used for 3GPP-based authentication over a non-3GPP access network, e.g. a Wireless LAN, thereby giving an example of heterogeneous access. EAP AKA makes use of the 3G AKA authentication algorithm provided by an UICC. Within the demonstrator EAP AKA was implemented making used of 3G AKA authentication algorithm provided by an UICC.

Beside showing how these protocols can be securely run for TCP/IP connections (e.g. based on Bluetooth or WLAN), advanced security module technology is used, to demonstrate how protocols can be split between terminal equipment and security modules. This split can be designed at various levels of the implementation. As a result the most security relevant parts (e.g. secret keys, hashes and signatures) are executed with the security module, while the rest of the protocol is executed on the mobile equipment for execution speed and flexibility reasons. Final timing measurements show, that the functionality split is a feasible way to improve security through the use of a smart card while maintaining a reasonable performance.



Imprinting and key exchange between two slave devices within a Personal Area Network (PAN).

SHAMAN Partners

Vodafone Limited, UK

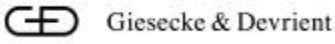
Royal Holloway, University of London, UK

Siemens Atea n.v., BE

Nokio Corporation, FIN

Ericsson Radio Systems, S

T-Systems Nova GmbH, DE



Giesecke & Devrient, DE

Siemens AG, DE

Giesecke & Devrient GmbH
Prinzregentenstrasse 159
P. O. Box 80 07 29
81607 Munich
Germany

Phone + 49 (0) 89 41 19-15 43
Fax + 49 (0) 89 41 19-15 40

www.gi-de.com
telecom@de.gi-de.com