# SHAMAN initial results

Tim Wright
timothy.wright@vodafone.com

## project participants

| | |
|---|---|
| Vodafone | UK |
| Royal Holloway | UK |
| Siemens Atea | BE |
| Nokia | FIN |
| Ericsson | SE |
| T-Systems Nova | DE |
| Giesecke & Devrient | DE |
| Siemens | DE |

# network security

- IP-based
- seamless global roaming
- connection to the networks and services through variety of heterogeneous access networks
  - wireless LAN
  - Bluetooth
  - enhanced cellular methods
  - legacy networks

# future mobile terminals

- multi-function
- distributed components
- dynamically configurable
  - some worn about the body
  - some in local environment
  - local wireless communications among themselves
  - secure communication
  - secure application environments
  - secure access to programs, information and services

# SHAMAN goals

to develop extensions to the security architecture for future mobile telecommunications systems to provide

- secure global roaming and secure access over heterogeneous radio networks
- security for highly configurable mobile terminals

# Workpackage descriptions

- WP1 – heterogeneous access to the core network
- WP2 – distributed and flexible terminals
- WP3 – PKI for the above
- WP4 – security modules
- WP5 – demonstrator
- WP6 – dissemination (*Workshop on July 25th, Royal Holloway, near London, "Security for mobile systems beyond 3G"* )

# WP1 - technical approach

- review
  - security features in candidate radio access networks
  - remote access procedures for mobile users
- identify consequent requirements on post-3G systems
- investigate suitability of current post-3G approaches as SHAMAN reference architecture
  - BRAIN
  - MWIF
  - ETSI BRAN (shorter term)

# WP1 – results

*D02: Intermediate Report:*

- review, requirements and reference architecture

*M1.2: Intermediate architectural and functional specification*

- separation of micro- and macromobility issues
- examination of key establishment algorithms
- secure initial access
- definition of a reference architecture for the *first hop*
- examination of issues and possible solutions for the security of the first hop

# WP3 - goals

- provide PKI solutions to needs of WP1 and WP2
- propose appropriate protocols and mechanisms
- address major PKI issues for future mobile systems
- feed results into ongoing appropriate standards developments for PKI.

# WP3 – ongoing & future work

- **ongoing work includes:**
  - **'clustering' of identified requirements from WP1 and WP2.**
  - **research on identified PKI issues:**
    - PKI for very limited devices
    - client revocation checking (certificate status issues)
    - certificate extensions and authorisation
- **work to be included in D07 (FEB-02) will also include**
  - **preliminary specification of protocols and mechanisms to address 'clustered' security requirements**
  - **research on the other identified PKI security issues**
- **after D07**
  - **final specification, complete research, support WP5**

# WP4 - goals

- specification of a security module providing high security for future developments in mobile communications

Year 1

- technology status and review
- future trends for SM technology
- identification of requirements on security modules for 4G systems

# WP4 - Future Work

- specification of a Security Module
- cross check with demonstrator work
- cross check with emerging standards
- final specification of Security Module

# WP5: Goals

to prototype ***critical components*** & ***novel functionality*** of future mobile communication networks.

- functionalities defined from WP1, WP2
- covers the WP1 issues of **roaming security** in heterogeneous access networks and the related issues in IP-based core networks
- covers the WP2 issues of user terminals:
  - secure communication between components and between components and the access network
  - privacy and protection of end-to-end traffic and access to networked applications and services

# WP5: Technical progress

- decision to make only one demonstrator
- identification of the features to demonstrate
  - roaming in one wireless technology and handover between two wireless technologies
  - key distribution/management in PAN
  - secure communication between different PAN components
- initial definition of the hardware platform based on the BRAIN architecture
- study of implementation tools – value & availability

# WP6 - goals

- establish, co-ordinate and maintain relations with relevant standards bodies and industry forums
- dissemination of project results
- collaboration with relevant EC projects
- SHAMAN workshop - July 25th 2002, Royal Holloway, near London

# WP2 - goals

**unified security architecture for future wireless, dynamically configured and distributed terminals including the service and application environment**

- distributed terminal reference model
- trust model
- communication security for the “local” network including application protocols
- secure configuration
- secure execution environment

# WP2 - technical requirements

- a simple and practical trust model
- simple security configuration mechanisms (e.g. semi-automatic key management)
- high level of cryptographic strength (using state-of-the-art, generally accepted cryptosystems)
- high quality security protocols
- usability
- mechanisms that can be easily analysed and evaluated
- low complexity implementations for devices with limited resources
- use of standard solutions whenever possible

# WP2 - technical approach (I)

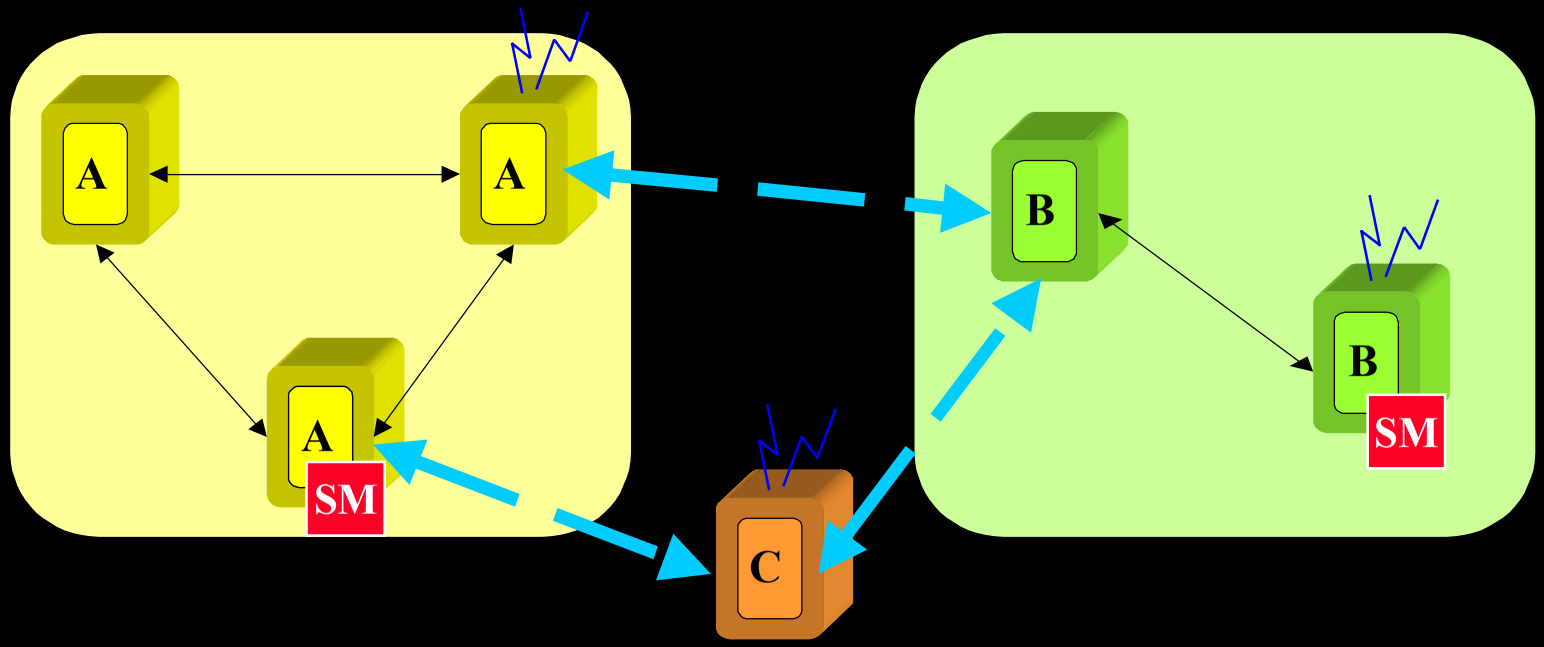
- build on *Personal Area Network* (PAN) reference model
- perform a comprehensive state-of-the-art study (covering both existing standards and academic research)

# WP2 - technical approach (II)

- add a trust model to the PAN model
- develop security initialisation solutions based on the trust model
- study communication security mechanisms based on the trust model
- develop an application and service authorisation model for the PAN reference model
- add policy management, access control and secure configuration mechanisms

# WP2 - technical approach (III)

PANs - abstract model



# WP2 – results (1) – D03 (public)

*Interim Report - Security Architecture for Future Mobile Terminals and Applications*

- security requirements
- preliminary PAN reference model
  - Abstract PAN model
- usage scenarios and threat analysis
- survey study
  - research papers
  - PAN internal communications
  - selected applications
  - programming languages and general purpose service discovery applications
- challenges for the security architecture

# WP2 – results (2) - MS 2.2

*Intermediate requirements and functional specification for security architecture for distributed mobile applications and service access*

- new PAN reference model including:
  - detailed definition of a PAN and the entities in the PAN
  - new PAN trust model
  - abstract descriptions of PAN configurations and usage scenarios
- new “personal” Certification Authority (CA) approach for PAN components

# WP2 – results - MS 2.2 (continued)

- proposals for intra PAN initial authentication and key establishment for
  - user assisted procedure
  - automated procedure based on ownership
- preliminary results on the secure execution environment covering
  - policy management and authorization principles
  - access control mechanisms

# WP2 – future work

- develop the “personal CA” concept together with WP3
- study authentication and key establishment protocols that provide location privacy
- evaluate the different authentication and key establishment procedures
- develop the access control and policy management mechanisms and adapt them to the rest of architecture
- study secure configuration principles
- write a detailed specification of the architecture