
**3rd Concertation Meeting of
Mobile/Wireless/Satellite IST projects
Brussels, 11 December 2000**

SHAMAN IST-2000-25350

Nigel Jefferies, project co-ordinator



SHAMAN Project

SHAMAN

Secure **H**eterogeneous **A**ccess for **M**obile **A**pplications & **N**etworks

- 8 partners
 - 1 academic
 - 2 operators
 - 5 suppliers
- 24 months
- 255 MM
- started 01-DEC-00
- pre-emptive kick-off meeting held in November



SHAMAN Project

MWS Concertation #3, 09-DEC-00, [2]

SHAMAN partners

- **Vodafone (co-ordinator)** (UK)
- **Royal Holloway University of London** (UK)
- **Siemens ATEA** (B)
- **Nokia Corporation** (FIN)
- **Ericsson Radio Systems** (S)
- **T-Nova** (DE)
- **Giesecke & Devrient** (DE)
- **Siemens AG** (DE)



SHAMAN Project

MWS Concertation #3, 09-DEC-00, [3]

Project goal

- to develop extensions to the security architecture for future mobile telecommunications systems to provide**
- **secure global roaming**
 - **secure access over heterogeneous radio networks**
 - **security for highly configurable mobile terminals**



Overview

security for *next generation* mobile

- two main areas of R&D
 - heterogeneous access networks and seamless roaming
 - dynamically configurable mobile terminals
- two supporting areas
 - PKI and key management R&D
 - R&D in secure H/W & S/W modules based on smartcard
- prototyping and demonstration
 - implementation of critical/novel components
- dissemination
 - appropriate standards and industry forums



Main Objectives

- extend the security architecture for ‘next generation’
- secure global roaming
- secure access over heterogeneous radio networks
- security for highly configurable mobile terminals
- define comprehensive security features
- define security mechanisms, protocols and procedures
- define supporting public key infrastructure
- define security modules and features

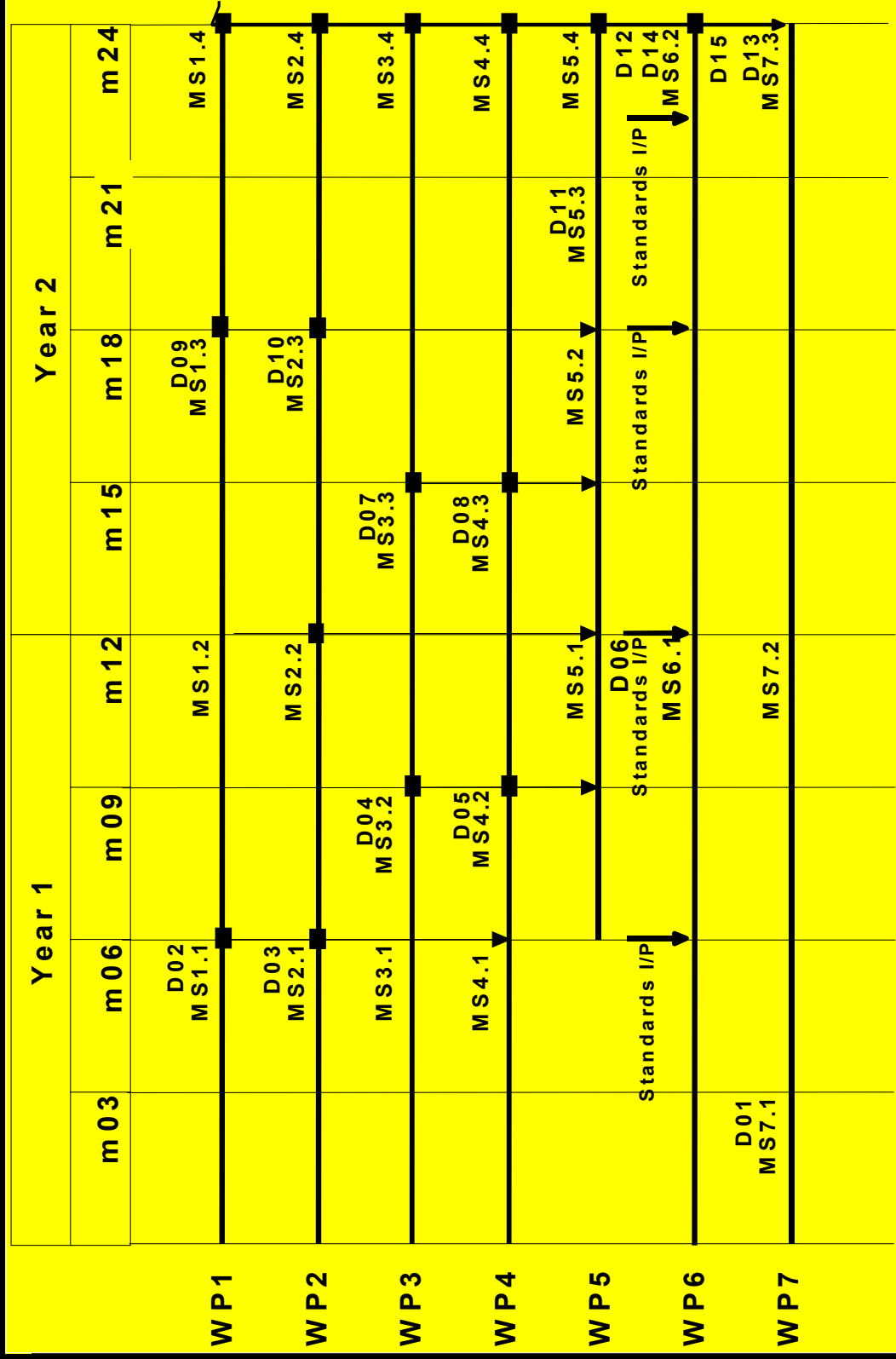


Objectives (2)

- **security features** for UMTS security architecture
- **security mechanisms**, protocols and procedures
- **public key infrastructure**
- **smart cards** and other security modules
- **demonstrate** technical feasibility and functionality
- **disseminate** results into standards bodies and industrial forums
- **validated** basis for **extensions to the UMTS security standards**
- **build on and collaborate with relevant EC projects.**



Project timescales



SHAMAN Project

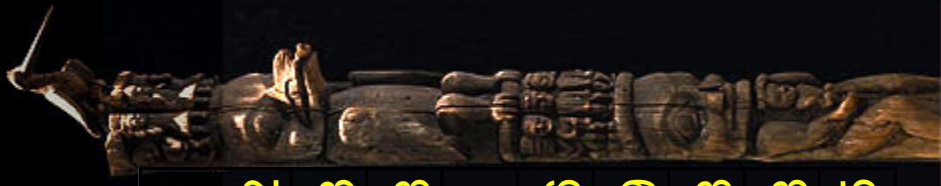
MWS Concertation #3, 09-DEC-00, [8]

Deliverables

1. Project Quality Plan M03
2. Intermediate report: requirements and reference architectures M06
3. Intermediate report: security architectures M06
4. Initial report on PKI requirements M09
5. Intermediate report: Security Modules M09
6. Status report on standards bodies M12
7. Intermediate specification: PKI for hetero-roaming and dist. terminals M15
8. Intermediate specification: Security Modules M15
9. Detailed technical specification: Security for heterogeneous access M18
10. Detailed technical specification: Dist. mob. terminal system security M18
11. Specification of prototypes M21
12. Report on standards and external liaison M24
13. Final technical report: complete results, specs. and conclusions M24
14. Dissemination and use plan M24
15. Evaluation report M26



Resources



	CO1	AC2	CR3	CR4	CR5	CR6	CR7	CR8
WP1	10	8	0	9	10	10	0	15
WP2	5	0	4	17	11	4	0	12
WP3	8	15	9	0	0	6	0	0
WP4	8	0	0	8	0	0	15	0
WP5	0	10	8	0	0	0	18	0
WP6	1	1	1	1	1	2	1	1
Tech coord	4	2	2	2	2	2	2	2
Proj Admin	8	0	0	0	0	0	0	0
Total	44	36	24	37	24	24	36	30
								255

SHAMAN Project

MWS Concentration #3, 09-DEC-00, [10]

SHAMAN linkages

- contributions to programme
- security for next generation
- secure modules
- PKI domains
- 4G
- reconfig radio projects
- BRAIN
- etc.



SHAMAN Project

MWS Concertation #3, 09-DEC-00, [11]