TDOC TSG SA#191

3GPP TSG-SA WG3 (Security)

Report to SA Meeting # 3,

Yokohama, Japan

26-28 April 1999

Michael Walker

Chairman 3GPP TSG-SA WG3

vodafone

Document List,1

- SP-99117 Report of SA WG3 meeting
  - Michael Walker elected chairman
  - Stefan Peutz & Adam Berenzweig Vice-chairmen
- SP-99141 Status of SA WG3 deliverables - for information
- SP-99142 Acquiring cryptographic algorithms - for short discussion
- SP-99143 Interchanging SIM & USIM - for clarification

Document List,2

- SP-99144 Security Architecture - for approval
- SP-99145 Security Threats and Requirements - for approval

Status of 3GPP Security Deliverables, 1 SP-99141

3GPP security specification	Rapporteur	Milestones	Status
Objectives and principles	Tim Wright		1st release approved by WG3 and TSG SA # 2
Threats and requirements	Per Christofferson	For approval SA # 3	1st release approved by WG3
Architecture	Bart Vinck and Stefan Puetz	For approval SA # 3	1st release approved by WG3

Status of 3GPP Security Deliverables, 2 SP-99141

3GPP security specification	Rapporteur	Milestones	Status
Integration requirements	Colin Blanchard	1st release end of May	Outline completed
Cryptographic algorithm requirements	Takeshi Chikawaza	1st release end of may	Outline completed
Cryptographic algorithm specifications	Gert Roelofsen	1st release end of may	Method for acquiring algoritms approved by WG3

Status of 3GPP Security Deliverables, 3 SP-99141

3GPP security specification	Rapporteur	Milestones	Status
Lawful interception requirements	Berthold Wilhelm	1st release end of May	Outline completed, work joint with SMG10 WPD
Lawful interception architecture and functions	Berthold Wilhelm	Scope by end of June	
Guide to 3G security	Charles Brookson	Scope by end of June	

Cryptographic Algorithm Specification SP-99142

- SA3 agreed position for acquiring algorithms:
  - SA3 to generate algorithm requirements
  - Requirements to algorithm design group (e.g. ETSI SAGE)
  - Design or select algorithm, internal evaluation and commission a closed external expert evaluation
  - Publish design for public evaluation - possibly running in parallel with implementation phase
- Process for responding to public criticism needed

SIM as an Access Module in 3G?
SP-99143

		Mobile type	
		GSM	3G
Card type	SIM	OK	**GSM level of service and GSM level of security**
	USIM with SIM installed	If GSM application is available and visible, GSM service will be offered with GSM level of security	OK, enhanced 3G security

vodafone

Security Threats and Requirements, 1
SP-99145

- Starting point is aspirations for 3G security described in *Principles and Objectives*
- Sets the context for threat analysis and requirements capture (sec. 5)
- Threats analysed and evaluated as part of a risk assessment in accordance with ETSI ETR 332 (sec. 6 & 7)

Security Threats and Requirements, 2
SP-99145

- Identifies range of threats to mobile systems
  - Acknowledges active attacks, especially (but not exclusively) on the radio interface
  - Attention focused on core network as well as access and radio interface security
- List of security requirements derived from security objectives and threat analysis (sec.8)

Categories of Security Requirements,1 SP-99145

- Service requirements
  - Service access - eg *verify authority of SN*
  - Service provision- eg *IST by HE*
- System integrity- eg *modification of signalling*
- Terminal requirements
  - USIM security- eg *security data restricted to HE*
  - Terminal security- eg *secure identity against change*

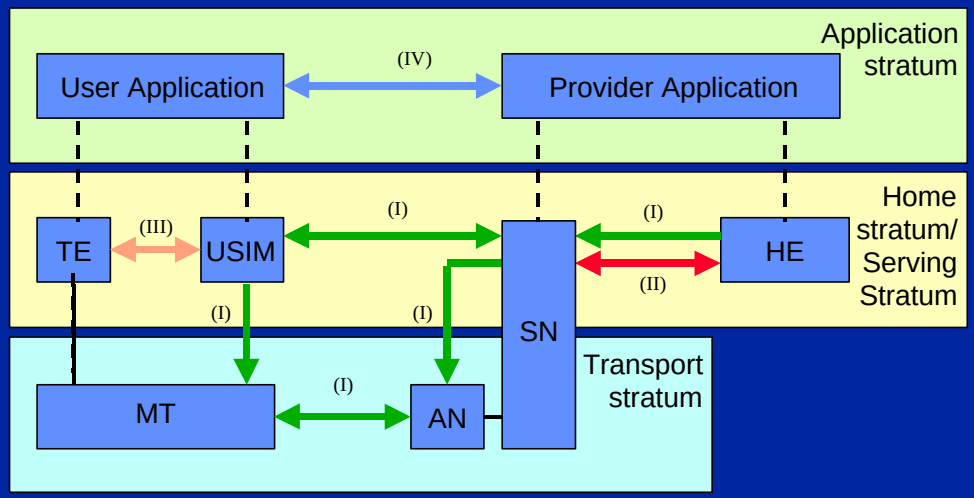
Categories of Security Requirements,2 SP-99145

- Protection of personal data - eg *protection of user location information*
- Lawful interception

Security Architecture SP-99144

- Definition of security features to address requirements - what will be provided
- Specification of mechanisms to provide security features - how it will be provided
- Architecture defined in three security layers and four security domains
- Builds on GSM security mechanisms

Security Layers & Domains SP-99144, sec.4



Security architecture composed of security domains (labelled I to IV)

vodafone

Security Features
SP-99144, sec.5

- Network access (I) - *eg user authentication*
- Network domain (II) - *eg HE-SN authentication*
- User domain (III) - *eg user-USIM authentication*
- Application domain (IV) - *eg data origin authentication, network wide confidentiality, IP sec*
- Visibility and configurability *eg transparency & being informed; rejection of non-encrypted links*

Network Access Mechanisms, 1
SP-99144, sec.6

- User identity confidentiality
  - GSM temporary identity & encrypted enhancement
- Authentication
  - User & network
  - GSM challenge- response, enhanced with signed sequence numbered challenge
  - DECT/TETRA local authentication key method retained in case security/synchronisation problem
  - Cipher & integrity key generation

Network Access Mechanisms, 2
SP-99144, sec.6

- Confidentiality of user traffic & signalling
  - similar to GSM but further back in network
  - cipher location, protected bits, synchronisation, switch-on, key length to be finalised
  - handover to be specified
  - operation with GSM SIM
- Integrity of user traffic & signalling
  - MAC based mechanism

Network Domain Security Mechanisms
SP-99144, sec.7

- Secure signalling links between nodes
  - Network element authentication
  - Confidentiality & integrity of exchanged data
  - public key based authentication with MAC integrity and block ciphering confidentiality using PNO algorithm likely
- Fraud information gathering

Application Domain Mechanisms
SP-99144, sec.9

- Secure USIM - network messaging
  - likely to be based on SAT with WIM enhancements
- Network-wide user traffic confidentiality
  - goal is to extend encryption to edge of network & provide user-to-user encryption within network
- Mobile IP security

Focus for next Meetings, 1

- Finalise details of cipher mechanism
- Produce requirements specification for
  - cipher algorithm
  - integrity algorithm
- Agree algorithm design authority and deliver requirements specifications

Focus for next Meetings, 2

- Funding for algorithm specification?
- Complete specification of signalling system security mechanisms
- First release of integration requirements- details of transport & storage requirements for security vectors

Meeting Schedule

May	11-12	Bonn
June	17-18	London
August	3-6	Sophia Antipolis (with SMG10)
October	26-27	The Hague
November	16-19	TBD (with SMG10)
December	7-8	Helsinki

vodafone