Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSGS#4(99)284

Source: **3GPP TSG SA WG3 (Security)**

Title: **Status of 3GPP security deliverables and priorities of work items**

Document for: **Information**

Agenda Item: **5.3.1**

Status of 3GPP security deliverables

	3GPP security deliverable	Rapporteur	Doc #	Milestones	Status
1	Security principles and objectives	Tim Wright	33.120	V3.0.0 approved at SA#3	
2	Security threats and requirements	Per Christoffersson	21.133	V3.0.0 approved at SA#3	
3	Security architecture	Bart Vinck & Stefan Pütz	33.102	V3.0.0 approved at SA#3	CRs presented to SA#4 for approval
4	Integration guidelines	Colin Blanchard			V1.0.0 presented to SA#4 for information
5	Cryptographic algorithm requirements	Takeshi Chikazawa	33.105		V2.0.0 presented to SA#4 for approval
6	Criteria for cryptographic algorithm design process	Gert Roelofsen	33.901	Method for acquiring cipher algorithm approved by SA#3	V2.0.0 presented to SA#4 for approval
7	Lawful interception requirements	Berthold Wilhelm			V2.0.0 presented to SA#4 for approval
8	Lawful interception architecture	Berthold Wilhelm			First draft presented to SA3
9	Guide to 3G security	Charles Brookson			

Priorities of work items

	Work item	Security issues addressed	Priority
1	Ciphering mechanism	Confidentiality protection required to protect against unauthorised disclosure of user traffic and signalling information between UE and RNC. Ciphering also helps to protect against channel hijack.	Essential for R99. GSM ciphering mechanism cannot be used in the new access network. A new ciphering mechanism must be developed and integrated with the UTRAN architecture.
2	Ciphering algorithm	Algorithms for ciphering in the UTRAN must be standardised for interoperability reasons.	Essential for R99. GSM algorithms are unsuitable for the new access network. A new algorithm must be developed.
3	Integrity protection algorithm	Message authentication and relay inhibition of critical signalling messages required to guard against active attacks on the radio interface (so called false base station' attacks).	Essential for R99.
4	Integrity protection mechanism	Algorithms for integrity protection in the UTRAN must be standardised for interoperability reasons.	Essential for R99.
5	Authentication and key agreement mechanism	Assurance towards user that access link keys used in ciphering and integrity mechanisms are fresh. Helps guard against active attacks on the radio interface which use compromised authentication vectors (a type	Essential for R99. A mechanism based on the use of sequence numbers is currently being specified. However, a fallback'mechanism is also available should the sequence numbers

		of false base station'attack).	mechanism become unsuitable.
6	Authentication and key agreement algorithms	Algorithms do not need to be standardisation if sequence numbers scheme is used. If fallback'mechanism is adopted, some algorithms do require standardisation for interoperability reasons.	The specification of algorithm requirements is essential for R99. The algorithms themselves do not need to be specified. However, should the sequence numbers mechanism become unsuitable, the fallback'mechanism will be used and some algorithms will have to be standardised.
7	Core network signalling security mechanism	Sensitive signalling messages require protection to guard against various attacks. Confidentiality protection required to protect against unauthorised disclosure of authentication vectors.	Although this is a high priority item, it is recognised that implementable specifications might not be achievable in R99.
8	Core network signalling security algorithms	Algorithms for core network signalling security must be standardised for interoperability reasons.	A cipher algorithm designed by ETSI SAGE for this purpose called BEANO is already available. Off-the-shelf algorithms are likely to be suitable for the data integrity and authentication functions.
9	Network-wide encryption mechanism	Encryption should be extended as far as possible into the core network to provide enhanced confidentiality services towards users. Network-wide encryption involves extending encryption across the entire network.	Appropriate hooks'must be provided in the R99 specification so that the introduction of network-wide encryption in later releases is not precluded. This may be the only new security feature in UMTS which will provide direct benefit to end customers.
10	User identity confidentiality	Enhanced mechanism required to guard against attacks against user identity confidentiality.	Although enhanced mechanism is operator specific, it does rely on specification of a standard transport mechanism. Specification of this transport mechanism is essential in R99.
11	GSM/UMTS intersystem operation	Intersystem operation must not compromise the UMTS security architecture.	This work item is driven by service requirements for GSM/UMTS interoperation. It is currently believed to be feasible to specify secure procedures for GSM/UMTS interoperation in R99. Secure roaming between systems is assumed to be the highest priority, while procedures for secure intersystem handover are judged to be less important with handover within a single core networks being higher priority than handover between different core networks
12	Lawful interception architecture	Lawful interception is a regulatory requirement which must be satisfied. Specification required now to ensure that lawful interception capabilities are available from the outset. Interception of packet services is a concern.	Essential for R99. Can be largely based on GSM/GPRS architecture.
13	USIM application security	Secure messaging is required between applications on the USIM and applications in the network.	Essential for R99. Can just refer to GSM SIM Application Toolkit security. Enhancements will be considered in later releases.
14	Fraud information gathering system	Measures for exchanging appropriate and timely fraud information must be implemented from the outset to help guard against roaming fraud.	Essential for R99. Can just refer to GSM FIGS. Enhancements will be considered in later releases.
15	Visibility and configurability	Although in general security features should be transparent to the user, in certain	An encryption indicator should be included in R99. Other items are of

		situations the user should be given greater visibility and control over the operation of security features.	lower priority and will be considered in later releases.
16	Mobile Execution Environment Security	The download and execution of applications on a mobile terminal presents a wide range of security concerns currently being considered in GSM MExE.	Essential for R99. Can just refer to GSM MExE security. Enhancements will be considered in later releases.
17	Location services	User location confidentiality needs to be carefully controlled when location services are invoked.	Essential for R99 if location services are specified in R99. However, the priority of this work item is unclear. May be possible to refer to GSM Location Services. Enhancements will be considered in later releases.
18	IP security	The use of Internet security technologies in 3G systems should be deemed appropriate for use before being adopted	The priority of this work item is unclear. Impact of IP technologies, such as mobile IP, not yet fully understood.
19	Terminal security	The exact security issues addressed are unclear.	The priority of this work item is unclear. Item is currently being raised with SA.