Source: **Chairman, Secretary SA3**

Title: **Status Report of SA_WG3 (Security)**

Document for: **Information and Decision**

Agenda Item: **7.3.1**

TSG SA3 STATUS REPORT

1 General Overview of Progress

The TSG_SA3#38 meeting was held in Geneva, Switzerland from the 26th to 29th April 2005. It was chaired by Mr Valterri Niemi (Nokia). The secretary was Mr Michael Clayton from the MCC. The host was EF3.

2 Lawful Interception

2.1 Correction on the use of identities for I-WLAN lawful interception (33.107) (Rel-6)

In the current version of TS 33.107, it is assumed that the IMSI is always available at the Packet Data Gateway (PDG), while the MSISDN is not. This is not according to the 3GPP WLAN specifications, which do not foresee the IMSI at PDG. Therefore, the MSISDN is recommended as an identity for I-WLAN Lawful Interception, instead of IMSI. It is also clarified that the NAI can be encrypted or based on temporary identities at the PDG and in those cases cannot be used for interception at that node.

Moreover, 3GPP TS 29.234 is added as reference.

The CR is presented in document **SP-050256** for approval.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050256	33.107	052	-	Rel-6	F	Correction on the use of identities for I-WLAN lawful interception	6.4.0	6.5.0	S3-050199

2.2 Lawful interception architecture and functions (33.107) (Rel-7)

Traditionally Lawful interception was based on telecommunication services allocating a dedicated channel for the data, which is primarily the voice data. Therefore, the telephony was the most common service. However, for a packet data network it is not so easy to determine that voice is being carried by the packets and which ones they are.

In order to set up a multimedia session, the UE and SCSF exchange SIP messages via the SGSN. For the SGSN these are mere IP packets and the SGSN cannot tell SIP message from any other type of data. Once the session is established the given application (e.g. VoIP) end points will start exchanging user plane data (RTP/IP packets) via SGSN. Once again, for SGSN these are mere IP packets, and SGSN has no knowledge what kind of data is inside these IP packets. The reason is that SGSN provides only IETF IP layer service, which routs IP packets for the given IETF application layer (e.g. VoIP service). Hence, in order to meet LI requirements SGSN must provide interception for network layer service only. By doing that SGSN operator would provide LI for e.g. VoIP application layer service as well, because there is no VoIP server node anywhere in the network.

The second CR provides some correlation of LI within IMS.

The two CRs are provided in **SP-050257** for approval.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050257	33.107	051	1	Rel-7	F	Clarifications for the usage of the notion of a service in distributed IP networks	6.4.0	7.0.0	S3-050316

SP-28	SP-050257	33.107	053	-	Rel-7	C	Correlation for IMS interception	6.4.0	7.0.0	S3-050201

2.3 Correction on IMS correlation for LI (Rel-6) (33.108)

Document SP-050258 contains a CR to 33.108 on IMS correlation for LI. In TS 33.108 there are some ambiguities between the correlation number which is used in the PS domain and the correlation number provided by the CSCF.

The CR is presented in **SP-050258** for approval.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050258	33.108	072	-	Rel-6	F	Correction on IMS correlation	6.8.2	6.9.0	S3-050202

2.4 Handover interface for Lawful Interception (Rel7) (33.108)

Document SP-050259 contains some CRs to 33.108 for LI

The first CR relates to how precise an IRI timestamp should be, which has been a discussion in the LI group for some time. That is to say, how many digits after the decimal dot should be included to represent the timestamp value?

The matter is further complicated by different interpretations of legislations in different countries. However, recent discussions have yielded an important common understanding that a single approach to resolving the problem is not appropriate. Therefore, separate timing requirements should be defined for each network type.

Partial consensus can be summarized as follows:

- One-second precise IRI timestamp generated by an intercepting GSN is sufficient to accurately report the sequence of events for the given LI target. Implementation may opt to have higher precision, of course.
- Concerning the IRI timestamp generated by an intercepting CSCF, one-second precise IRI timestamp may not be sufficient. In order to accurately report the sequence of events for the given LI target in a given CSCF, implementation should use higher precision timestamp than one second. This requirement however is subject to national regulations.

The CR proposes necessary modifications to the packet data domain clause.

Therefore, CR 70r1 proposes to add to the multi-media domain the missing sub clauses: “Performance, reliability, and quality”, “Security aspects”, “Quantitative aspects”.

CR 71 relates to the text on Intercept Related Information (IRI) only cases. It is not clear with respect to what information should be deleted before reporting the SIP message to law enforcement. Some might interpret the current statement to mean that all SIP bodies are to be deleted. Doing this, however, would also cause SDP (Session Description Protocol) information to be deleted. SDP, which could carry potentially valuable information about the media streams established by the user, should be considered connection control information and not user content. Thus, the information should be provided to law enforcement even for IRI-only cases.

Finally, CR 76 a correction to Annex B.6 regarding the import statement for the **hi3CircuitLISubDomainId**. An Object Identifier which is intended for the same purpose is

defined within the module itself. Therefore this import should be deleted.

The CRs for Rel-7 are provided in document **SP-050259** for approval.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050259	33.108	070	1	Rel-7	B	Clarifications to the timing issue	7.0.0	7.1.0	S3-050317
SP-28	SP-050259	33.108	071	-	Rel-7	B	Clarification pertaining to the filtering of SDP for IRI-only cases	7.0.0	7.1.0	S3-050200
SP-28	SP-050259	33.108	076	-	Rel-7	D	Obsolete Import Statement in Annex B.6	7.0.0	7.1.0	S3-050207

2.5 CRs to 33.108 on an Inconsistency in Annex B.5 for LI (Rel-6, Rel-7)

Document SP-050260 contains two CRs to 33.108 for Rel-6 and Rel-7. Annex B.5 contains an inconsistency for the Handover Information Management or 'him' object identifier. The Object Identifier Definition (OID) is not defined in the 3GPP module as specified in the tree and the module header but instead imported from the ETSI security domains definition. This CR in **SP-050260** deletes the import and the OID is defined in the 3GPP module.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050260	33.108	074	-	Rel-6	F	Inconsistency in Annex B.5	6.8.2	6.9.0	S3-050205
SP-28	SP-050260	33.108	075	-	Rel-7	A	Inconsistency in Annex B.5	7.0.0	7.1.0	S3-050206

3 Other CRs

3.1 CR to 33.203 on Description of 2xx Auth_Ok message (Rel-6)

In the subclause of Authentication of an IM-subscriber, the Description of 2xx Auth_Ok message is missing in the IMS registration flow. Document **SP-050261** contains the CR to include it.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050261	33.203	080	1	Rel-6	F	Description of 2xx Auth_Ok message	6.6.0	6.7.0	S3-050302

3.2 CRs to 33.220 on Generic bootstrapping architecture (Rel-6)

There are two CRs on Generic bootstrapping architecture in 33.220.

The first is on the local policy usage in the case where the Network application function (NAF) does not use User Security Setting (USS). This is extended and a missing option added to prevent possible ambiguity and interoperability problems

The second contains a correction to figure 4.4, which indicates that the first message would be protected by a MAC. The use of the term MAC in the figure might be confusing and no corresponding text explaining the MAC is included in the body. It might not even be possible to protect the first message using a MAC with all Ua protocols.

The CRs are provided in **SP-050262** for approval.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050262	33.220	050	1	Rel-6	F	Usage of USS for local policy enforcement in BSF	6.4.0	6.5.0	S3-050288
SP-28	SP-050262	33.220	051	1	Rel-6	F	Correcting figure 4.4	6.4.0	6.5.0	S3-050287

3.3 CRs to 33.220 on GBA User Security Settings (GUSS) transfer optimisation (Rel-7)

Document **SP-050263** contains a CR on the GBA User Security Settings (GUSS). The CR adds a timestamp to each GUSS indicating when the GUSS was last changed by the HSS.

This timestamp is then used to optimise the GUSS transfer policy between the HSS and the BSF. When a new authentication vector (AV) for the subscriber is required, it will also include the GUSS timestamp to the request. Upon receiving the GUSS timestamp, the HSS will compare it to the time of the GUSS it has in its databases.

If the timestamps are equal, the HSS does not send the GUSS to the BSF as the BSF already has a copy of the GUSS. If the timestamps are not equal, the HSS sends the GUSS as the BSF has an invalid GUSS, which needs to be updated. If the HSS has no GUSS, then it will send a no GUSS message to the BSF and the BSF will delete the old GUSS.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050263	33.220	052	-	Rel-7	B	GBA User Security Settings (GUSS) transfer optimisation	6.4.0	7.0.0	S3-050286

3.4 CR to 33.222 to remove editor's note in Generic Authentication Architecture (Rel-6)

Document **SP-050264** contains a simple CR to remove an editor's note left in.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050264	33.222	019	-	Rel-6	F	Removal of editor's note	6.3.0	6.4.0	S3-050301

3.5 CRs to 33.234 on Wireless Local Area Network (WLAN) interworking security (Rel-6)

Document SP-050265 contains three CRs on I-WLAN.

CR 64r2 specifies the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access. There are no security holes in using multiple IPSec SAs per IKE_SA, so release-6 specifications should not carry text that suggests that it does. Besides, when re-keying to avoid session interruption, at some point in time, two IPsec SAs need to coexist if there is only one IPsec SA per IKE SA.

CR 65r1 relates to the termination of WLAN sessions by the Authentication Authorisation Accounting (AAA) server. To support the control of simultaneous WLAN direct IP access session numbers, the AAA server needs to be able to send termination message to WLAN AN. SA2 has agreed the immediate purging of a user from the WLAN AN shall be supported by all WLAN ANs, and will provide the necessary changes in TS23.234 clause 6.3.1.2 making this function mandatory.

Finally, an analysis by CT4 on the text in TS 29.234 related to Wn has led to the conclusion that the specific method to implement this Reference Point is out of scope of 3GPP. CT4 have agreed a CR to 29.234 removing the description of the Wn reference point from Stage 3. The change proposed in this CR brings 33.234 in line with CT4's analysis and the changes made to 29.234.

The CRs are provided in document **SP-050265** for approval.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050265	33.234	064	2	Rel-6	F	Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access	6.4.0	6.5.0	S3-050314
SP-28	SP-050265	33.234	065	1	Rel-6	F	Terminate WLAN session by AAA server	6.4.0	6.5.0	S3-050312
SP-28	SP-050265	33.234	066	-	Rel-6	F	Correction to the definition of the Wn Reference Point	6.4.0	6.5.0	S3-050266

3.6 CRs to 33.246 on MBMS (Rel-6)

Document **SP-050266** contains ten CRs to 33.246 on MBMS.

It is hoped that with these, MBMS is completed with respect to SA3.

There are however, two outstanding items in conjunction with SA4. The first is stream bundling and it should be noted that there are two solutions. These solutions have been sent to SA4 for a choice and, if one particular one is chosen, then a further CR to 33.246 will be required.

The second relates to MBMS User Service finalization. Once again a liaison statement has been sent to SA4, but an assumed solution to this has been provided in the package below (CR 60r1).

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050266	33.246	058	1	Rel-6	C	MKI and authentication tag length in User Service Description	6.2.0	6.3.0	S3-050296
SP-28	SP-050266	33.246	059	1	Rel-6	C	Clarification of Key domain ID in service announcement	6.2.0	6.3.0	S3-050295
SP-28	SP-050266	33.246	060	1	Rel-6	F	Key usage clarification	6.2.0	6.3.0	S3-050298
SP-28	SP-050266	33.246	061	1	Rel-6	C	Omitted MTK Update Error Message	6.2.0	6.3.0	S3-050292
SP-28	SP-050266	33.246	062	1	Rel-6	D	Editorial corrections to TS 33.246	6.2.0	6.3.0	S3-050318
SP-28	SP-050266	33.246	063	1	Rel-6	C	Clarifications on MBMS key management	6.2.0	6.3.0	S3-050294

SP-28	SP-050266	33.246	064	1	Rel-6	F	Use of IMPI in MBMS	6.2.0	6.3.0	S3-050293
SP-28	SP-050266	33.246	065	-	Rel-6	F	Clarification on CSB ID and SP payload use	6.2.0	6.3.0	S3-050297
SP-28	SP-050266	33.246	066	-	Rel-6	F	MIME type adjustments according to LS S3-050192	6.2.0	6.3.0	S3-050290
SP-28	SP-050266	33.246	067	-	Rel-6	F	Results of mapping the MBMS security requirements into security functions and mechanisms	6.2.0	6.3.0	S3-050319

3.7 CR to 33.978 on Correction of use of 401 Unauthorized and 399 Warning headers (Rel-6)

It would appear that the error codes "*401 Unauthorized*" and "*399 Warn-code*" are not used everywhere according to RFCs. Therefore, in interworking case 5 of section 6.2.6, it is proposed to use "*403 (forbidden*)" instead of 401 and 399. This seems adequate as a correctly implemented UE should always check first whether a USIM or ISIM is available before starting IMS procedures fully compliant with TS 33.203.

It is presented in SP-050267 for approval.

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050267	33.978	001	-	Rel-6	F	Correction of use of 401 Unauthorized and 399 Warning headers	6.0.1	6.1.0	S3-050305

4 Work Items

4.1 Lawful Interception in the 3GPP Rel-7 architecture

The 3GPP Rel-7 architecture continues to develop IP-based Services, which need to be addressed by lawful interception. SA WG3-LI will study advanced IMS services, Multimedia Broadcast and Multicast Services, Subscriber Certificates, and I-WLAN for possible lawful interception systems.

It is presented for approval in SP-050237.

4.2 New WID proposal: IMS security extensions

Release 5 and 6 IMS access security solution was mainly designed for UMTS access networks. Even though the access security solution is access network independent, there are still important use scenarios in which the current solution is difficult or even impossible to use.

An example is an access networks that include NATs, such as fixed broadband access as currently specified in ETSI and ITU-T in the framework of next generation networking (TISPAN-NGN).

TISPAN stated that "TISPAN NGN Release 1 priority is for securing IMS for a fixed network, and is independent of any discussion of what mobile operators may or may not mandate for interconnection to their IMS services i.e. the fixed operator has a commercial relationship with the customer, and deploys terminal, network, IMS service and HSS." However, for 3GPP operators running IMS, the authentication of the IMS subscriber must be based on access to physical UICC.

TSG-S3 has prime responsibility for all security-related specification work in 3GPP. The unity of the security extensions to the IMS security specifications must be preserved and handled in 3GPP SA3. TSG-S3 needs to study if IMS access security solution needs to be extended in order to solve the above problems, and how potential extensions are done.

5 Other issues

5.1 Vice chairmanship

The first term of Chairmanships and Vice Chairmanships for SA WG3 finishes in May 2005 and consequently a call for nominations has been sent out to the leader's list and SA3 mailing list.

At this time, there is only one candidate, however, SA3 should be prepared for a vote at the next meeting.

6 Meetings of SA3

6.1 Meetings since last SA

Meeting	Date	Location	Host
S3#38	25 - 29 April 2005	Switzerland (TBC)	Orange (TBC)

LI meetings

Meeting	Date	Location	Host
SA3 LI-#17	5 - 7 April 2005	Sophia Antipolis, France	ETSI

6.2 Planned meetings

Meeting	Date	Location	Host
S3#39	28 June - 1 July 2005	Montreal, Canada (possibly with SA WG2)	NAF
S3#40	13- 16 September 2005	ETSI or EF3 / TBD (possibly Slovenia co-located with TISPAN)	ETSI or EF3 / TBD
S3#41	15 - 18 November 2005	TBD	Qualcomm / TBD

LI meetings

Meeting	Date	Location	Host
SA3 LI-#18	28 June - 1 July 2005	Montreal, Canada	
SA3 LI-#19	12 -16 October 2005	TBD	TBD

Annex 1: Documents provided to this Plenary

Tdoc	Title	Source	Agenda	Doc for
SP-050255	Presentation of SA WG3 to TSG SA #28	SA WG3 Chairman	7.3.1	Information
SP-050236	Draft Report of SA WG3 #38	MCC	7.3.1	Information
SP-050256	CRs to 33.107 on Correction on the use of identities for I-WLAN lawful interception (Rel-6)	SA WG3	7.3.3	Approval
SP-050257	CRs to 33.107 on Lawful interception architecture and functions (Rel-7)	SA WG3	7.3.3	Approval
SP-050258	CRs to 33.108 on Correction on IMS correlation for LI(Rel-6)	SA WG3	7.3.3	Approval
SP-050259	CRs to 33.108 for Handover interface for Lawful Interception (Rel7)	SA WG3	7.3.3	Approval
SP-050260	CRs to 33.108 on an Inconsistency in Annex B.5 for LI (Rel-6, Rel-7)	SA WG3	7.3.3	Approval
SP-050261	CR to 33.203 on Description of 2xx Auth_Ok message (Rel-6)	SA WG3	7.3.3	Approval
SP-050262	CRs to 33.220 on Generic bootstrapping architecture (Rel-6)	SA WG3	7.3.3	Approval
SP-050263	CRs to 33.220 on GBA User Security Settings (GUSS) transfer optimisation (Rel-7)	SA WG3	7.3.3	Approval
SP-050264	CR to 33.222 to Remove editor's note in Generic Authentication Architecture (Rel-6)	SA WG3	7.3.3	Approval
SP-050265	CRs to 33.234 on Wireless Local Area Network (WLAN) interworking security (Rel-6)	SA WG3	7.3.3	Approval
SP-050266	CRs to 33.246 on MBMS (Rel-6)	SA WG3	7.3.3	Approval
SP-050267	CR to 33.978 on Correction of use of 401 Unauthorized and 399 Warning headers (Rel-6)	SA WG3	7.3.3	Approval
SP-050237	Lawful Interception in the 3GPP Rel-7 architecture	SA WG3	7.3.3	Approval
SP-050238	New WID proposal: IMS security extensions	SA WG3	7.3.3	Approval

Annex 2: CRs provided to this Plenary

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers Current	Vers New	Doc-2nd-Level
SP-28	SP-050256	33.107	052	-	Rel-6	F	Correction on the use of identities for I-WLAN lawful interception	6.4.0	6.5.0	S3-050199
SP-28	SP-050257	33.107	051	1	Rel-7	F	Clarifications for the usage of the notion of a service in distributed IP networks	6.4.0	7.0.0	S3-050316
SP-28	SP-050257	33.107	053	-	Rel-7	C	Correlation for IMS interception	6.4.0	7.0.0	S3-050201
SP-28	SP-050258	33.108	072	-	Rel-6	F	Correction on IMS correlation	6.8.2	6.9.0	S3-050202
SP-28	SP-050259	33.108	070	1	Rel-7	B	Clarifications to the timing issue	7.0.0	7.1.0	S3-050317
SP-28	SP-050259	33.108	071	-	Rel-7	B	Clarification pertaining to the filtering of SDP for IRI-only cases	7.0.0	7.1.0	S3-050200
SP-28	SP-050259	33.108	076	-	Rel-7	D	Obsolete Import Statement in Annex B.6	7.0.0	7.1.0	S3-050207
SP-28	SP-050260	33.108	074	-	Rel-6	F	Inconsistency in Annex B.5	6.8.2	6.9.0	S3-050205
SP-28	SP-050260	33.108	075	-	Rel-7	A	Inconsistency in Annex B.5	7.0.0	7.1.0	S3-050206
SP-28	SP-050261	33.203	080	1	Rel-6	F	Description of 2xx Auth_Ok message	6.6.0	6.7.0	S3-050302
SP-28	SP-050262	33.220	050	1	Rel-6	F	Usage of USS for local policy enforcement in BSF	6.4.0	6.5.0	S3-050288
SP-28	SP-050262	33.220	051	1	Rel-6	F	Correcting figure 4.4	6.4.0	6.5.0	S3-050287
SP-28	SP-050263	33.220	052	-	Rel-7	B	GBA User Security Settings (GUSS) transfer optimisation	6.4.0	7.0.0	S3-050286
SP-28	SP-050264	33.222	019	-	Rel-6	F	Removal of editor's note	6.3.0	6.4.0	S3-050301
SP-28	SP-050265	33.234	064	2	Rel-6	F	Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access	6.4.0	6.5.0	S3-050314
SP-28	SP-050265	33.234	065	1	Rel-6	F	Terminate WLAN session by AAA server	6.4.0	6.5.0	S3-050312
SP-28	SP-050265	33.234	066	-	Rel-6	F	Correction to the definition of the Wn Reference Point	6.4.0	6.5.0	S3-050266
SP-28	SP-050266	33.246	058	1	Rel-6	C	MKI and authentication tag length in User Service Description	6.2.0	6.3.0	S3-050296
SP-28	SP-050266	33.246	059	1	Rel-6	C	Clarification of Key domain ID in service announcement	6.2.0	6.3.0	S3-050295
SP-28	SP-050266	33.246	060	1	Rel-6	F	Key usage clarification	6.2.0	6.3.0	S3-050298
SP-28	SP-050266	33.246	061	1	Rel-6	C	Omitted MTK Update Error Message	6.2.0	6.3.0	S3-050292
SP-28	SP-050266	33.246	062	1	Rel-6	D	Editorial corrections to TS 33.246	6.2.0	6.3.0	S3-050318
SP-28	SP-050266	33.246	063	1	Rel-6	C	Clarifications on MBMS key management	6.2.0	6.3.0	S3-050294
SP-28	SP-050266	33.246	064	1	Rel-6	F	Use of IMPI in MBMS	6.2.0	6.3.0	S3-050293
SP-28	SP-050266	33.246	065	-	Rel-6	F	Clarification on CSB ID and SP payload use	6.2.0	6.3.0	S3-050297
SP-28	SP-050266	33.246	066	-	Rel-6	F	MIME type adjustments according to LS S3-050192	6.2.0	6.3.0	S3-050290
SP-28	SP-050266	33.246	067	-	Rel-6	F	Results of mapping the MBMS security requirements into security functions and mechanisms	6.2.0	6.3.0	S3-050319
SP-28	SP-050267	33.978	001	-	Rel-6	F	Correction of use of 401 Unauthorized and 399 Warning headers	6.0.1	6.1.0	S3-050305

Annex 3: 3G&GSM TSs and TRs under SA3 responsibility

Spec	Title	Ph1	Ph2	R96	R97	R98	R99	Rel-4	Rel-5	Rel-6	Rel-7
01.31	Fraud Information Gathering System (FIGS); Service requirements; Stage 0					7.0.1	8.0.0				
01.33	Lawful Interception requirements for GSM					7.0.0	8.0.0				
01.61	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements				6.0.1	7.0.0	8.0.0				
02.09	Security aspects	3.1.0	4.5.1	5.2.1	6.1.1	7.1.1	8.0.1				
02.31	Fraud Information Gathering System (FIGS); Service description; Stage 1					7.1.1					
02.32	Immediate Service Termination (IST); Service description; Stage 1					7.1.1					
02.33	Lawful Interception (LI); Stage 1					7.3.0	8.0.1				
03.20	Security-related network functions	3.3.2	4.4.1	5.2.1	6.1.0	7.2.0	8.1.0				
03.31	Fraud Information Gathering System (FIGS); Service description; Stage 2					7.0.0					
03.33	Lawful Interception; Stage 2					7.2.0	8.1.0				
03.35	Immediate Service Termination (IST); Stage 2					7.0.1					
10.20	Lawful Interception requirements for GSM			5.0.1							
21.133	3G security; Security threats and requirements						3.2.0	4.1.0			
22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification						3.2.1	4.1.0	5.0.0	6.0.0	
22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1						3.0.0	4.0.0	5.0.0	6.0.0	
22.032	Immediate Service Termination (IST); Service description; Stage 1						3.0.0	4.0.0	5.0.0	6.0.0	
23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2						3.0.0	4.0.0	5.0.0	6.0.0	
23.035	Immediate Service Termination (IST); Stage 2						3.1.0	4.1.0	5.1.0	6.0.0	
33.102	3G security; Security architecture						3.13.0	4.5.0	5.5.0	6.3.0	
33.103	3G security; Integration guidelines						3.7.0	4.2.0			
33.105	Cryptographic algorithm requirements						3.8.0	4.2.0	5.0.0	6.0.0	
33.106	Lawful interception requirements						3.1.0	4.0.0	5.1.0	6.1.0	
33.107	3G security; Lawful interception architecture and functions						3.5.0	4.3.0	5.6.0	6.4.0	
33.108	3G security; Handover interface for Lawful Interception (LI)								5.9.1	6.8.2	7.0.0
33.120	Security Objectives and Principles						3.0.0	4.0.0			
33.141	Presence service; Security									6.1.0	
33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security							4.3.0	5.1.0	6.1.0	
33.203	3G security; Access security for IP-based services								5.9.0	6.6.0	
33.210	3G security; Network Domain Security (NDS); IP network layer security								5.5.0	6.5.0	
33.220	Generic Authentication Architecture (GAA); Generic bootstrapping architecture									6.4.0	
33.221	Generic Authentication Architecture (GAA); Support for subscriber certificates									6.2.0	
33.222	Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)									6.3.0	
33.234	3G security; Wireless Local Area Network (WLAN) interworking security									6.4.0	
33.246	3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)									6.2.0	
33.310	Network domain security; Authentication framework (NDS/AF)									6.2.0	
33.810	3G Security; Network Domain Security / Authentication Framework (NDS/AF); Feasibility Study to support NDS/IP evolution									6.0.0	
33.817	Feasibility study on (Universal) Subscriber Interface Module (U)SIM security reuse by peripheral devices on local interfaces									6.1.0	
33.900	Guide to 3G security								0.4.1		
33.901	Criteria for cryptographic Algorithm design process						3.0.0	4.0.0			
33.902	Formal Analysis of the 3G Authentication Protocol						3.1.0	4.0.0			
33.908	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms						3.0.0	4.0.0			

33.909	3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions							4.0.1			
33.919	Generic Authentication Architecture (GAA); System description									6.2.0	
33.941	Presence service; Security									0.6.0	
33.978	Security aspects of early IMS									6.0.0	
35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications						3.2.0	4.1.0	5.0.0	6.0.0	
35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification						3.1.2	4.0.0	5.0.0	6.0.0	
35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data						3.1.2	4.0.0	5.0.0	6.0.0	
35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data						3.1.2	4.0.0	5.0.0	6.0.0	
35.205	3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General							4.0.0	5.0.0	6.0.0	
35.206	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification							4.0.0	5.1.0	6.0.0	
35.207	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' test data							4.0.0	5.0.0	6.0.0	
35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data							4.0.0	5.0.0	6.0.0	
35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation							4.0.0	5.0.0	6.0.0	
41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0							4.0.1	5.0.0	6.0.0	
41.033	Lawful Interception requirements for GSM							4.0.1	5.0.0	6.0.0	
41.061	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements							4.0.0			
42.009	Security aspects							4.0.0			
42.033	Lawful Interception; Stage 1							4.0.0	5.0.0	6.0.0	
43.020	Security-related network functions							4.0.0	5.0.0	6.1.0	
43.033	3G security; Lawful Interception; Stage 2							4.0.0	5.0.0	6.0.0	
55.205	Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8									6.1.0	
55.216	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 1: A5/3 and GEA3 specification									6.2.0	
55.217	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data									6.1.0	
55.218	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 3: Design and conformance test data									6.1.0	
55.919	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report									6.1.0	