USECA

UMTS Security Architecture

Inputs to Standards

Notes: (a) Impact Key: 0 = No impact; 1 = Low impact; 2 = Moderate impact; 3 = High impact
(b) all standards here are for future deployment therefor there is no *normal use* at this time
(c) all 3GPPwork will have European impact as ETSI plans to be fully compliant

Stdds Body/ Committee/ Subcommittee	**Date**	*Title of contribution*	**Impact on world standard**	**Impact on European standard**	**Impact on standard in normal use**
TIA/EIA TR45.2 & TR45.5	11Oct99	Questions and answer on the 3GPP authentication and key establishment mechanism	3		
TIA/EIA TR45.2 & TR45.5	11Oct99	Presentation on the 3GPP authentication and key establishment mechanism	3		
TIA/EIA TR45.2 & TR45.5.2	11Oct99	Presentation: Security interoperation between 3GPP and IS-41 systems	3	2	
TIA/EIA TR45.2 & TR 45.3	08Nov99	Brief analysis of network signalling load associated with the 3GPP mechanism	3		
TIA/EIA TR45.2 & TR45.3	08Nov99	Stage 2 descriptions for the 3GPP authentication and key establishment mechanism	3		
TIA/EIA TR45.2 & TR45.3	08Nov99	Stage 2 descriptions for the 3GPP authentication and key establishment mechanism	3		
3GPP TSG SA WG3	11May99	S3-99097: Formal analysis of 3G authentication and key agreement protocol	3	3	
3GPP TSG SA WG3	16Jun99	S3-99170: Results of formal analysis of the 3G authentication protocol with modified sequence number management	3	3	
3GPP TSG SA WG3	16Jun99	S3-99171: Modified sequence number management	3	3	
3GPP TSG SA WG3	16Jun99	S3-99179: Conditions on use of authentication information	3	3	
3GPP TSG SA WG3	16Jun99	S3-99180: Modified re-synchronisation procedure for AKA protocol	3	3	
3GPP TSG SA WG3	16Jun99	S3-99181: Sequence number management scheme protecting against USIM lockout	3	3	
3GPP TSG SA WG3	16Jun99	S3-99183: Formal analysis of the 3G authentication protocol with modified sequence number management	3	3	
3GPP SA 3	16Jun99	S3-99158: Interoperation between UMTS and GSM	3	3	
3GPP SA 3	16Jun99	Conversion functions for interoperation	2	2	

3GPP SA 3	16Jun99	S3-99262: Key selection for signalling	2	2	
3GPP TSG SA WG3	03Aug99	S3-99234: Enhanced window mechanism for sequence number management	1	1	
3GPP TSG SA WG3	03Aug99	S3-99235: Proposed response to LS statement 99231 fromN2 on Super-Charger concept	1	1	
3GPP TSG SA WG3	03Aug99	S3-99236: Response to doc. 99230 "A Possible Problem of the UMTS AKA Mechanism" from T-Mobil/Deutsche Telekom	2	2	
3GPP SA 3	25Aug99	S3-99263: Interoperation between UMTS and GSM	3	3	
3GPP TSG SA WG3	29Sep99	S3-99304: A generalised description of sequence number management options	3	3	
3GPP TSG SA WG3	29Sep99	S3-99322: Brief response to S3-99308 on the window mechanism for sequence number management	1	1	
3GPP TSG SA WG3	29Sep99	S3-99342: Over the air management of window and list sizes	2	2	
3GPP TSG SA WG3	29Sep99	TS 33.102 CR018: Support for window and list mechanisms for sequence number management in authentication scheme	3	3	
3GPP TSG SA WG3	29Sep99	TS 33.102 CR019: A generalised description of sequence number management options	3	3	
3GPP TSG SA WG3	11Oct99	TS 33.102 CRxxx: Modification of text for window and list mechanisms	1	1	
3GPP SA 3	26Oct99	S3-993876The 3GPP AKA as a candidate for ESA	2	2	
SMG4 MExE	12Jan99	4M99-008: Input document on 03.57 security section	1		
SMG4 MExE	12Jan99	4M99-016: Stage 1 security specification	1		
SMG4 MExE	12Jan99	4M99-038: Conclusions of Automatic Execution Workshop	0		
SMG4 MExE	12Jan99	4M99-040: 03.57 security table update	1		
3GPP T2 SWG1/SMG4 MExE	17Feb99	4M99-063: Additions to stage 1 security requirements	1		
3GPP T2 SWG1/SMG4 MExE	17Feb99	4M99-090: E-mail on certification	1		
3GPP T2 SWG1/SMG4 MExE	17Feb99	4M99-091: Network selection	1		
WAP PKI ad hoc	28Oct99	Contirbution on extensions to X.509 for signing of downloaded code	2		
WAP Forum, San Francisco	27Jun99	Contribution on bootstrap/provisioning root certificates	1		
WAP Forum, San Francisco	27Jun99	Contributions on certificate requirements for WAP and MExE	1		
3GPP TSG SA WG3 #1, London	02Feb99	S3-99021: Objectives and principles of 3GPP security	2	2	

3GPP TSG SA WG3 #2, Stockholm	23Mar99	S3-99040: Proposed LS to T3 on integrity on the USIM	1	1	
3GPP TSG SA WG3 #2, Stockholm	23Mar99	S3-99054: Some initial thoughts on end-to-end encryption	2	2	
3GPP TSG SA WG3 #3, Bonn	11May99	S3-99095: 3GPP Access interface ciphering algorithm requirements	2	2	
3GPP TSG SA WG3 #3, Bonn	11May99	S3-99098: Comments on authentication and key agreement protocol	2	2	
3GPP TSG SA WG3 #3, Bonn	11May99	S3-99101: Proposal for radio interface ciphering architecture	2	2	
3GPP TSG SA WG3 #3, Bonn	11May99	S3-99121: Addressing 2G weaknesses	2	2	
3GPP TSG SA WG3 #4, London	16Jun99	S3-99162: Proposed CR on key setting	2	2	
3GPP TSG SA WG3 #4, London	16Jun99	S3-99164: Key management for network wide encryption	2	2	
3GPP TSG SA WG3 #4, London	16Jun99	S3-99187: Proposed CR on 33.102 on Description of layer on which ciphering takes place	2	2	
3GPP TSG SA WG3 #4, London	16Jun99	S3-99189: Proposed LS to R2 on RLP PDU size	2	2	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99206: Proposed response to “CR to TS 25.301 - Integrity control mechanism”	1	1	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99216: Hooks for network-wide encryption	1	1	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99217: Location of integrity termination in the network	1	1	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99218: Synchronisation mechanisms for network-wide encryption	1	1	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99224: Proposed CR to 33.102 on Cipher keys on control and user planes	1	1	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99246: Proposed CR to 33.102 on Cipher key setting	2	2	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99248: Proposed CR to 33.105 on Cipher keystream block length	1	1	
3GPP TSG SA WG3 #6, Sophia Antipolis	29Sep99	S3-99297: Update on MExE security	1	1	
3GPP TSG SA WG3 #6, Sophia Antipolis	29Sep99	S3-99302: Support for multiple authentication algorithms and keys	2	2	

3GPP TSG SA WG3 #6, Sophia Antipolis	29Sep99	S3-99303: The use of Zero-Knowledge Identification mechanisms for 3G Terminal Identification	1	1	
3GPP TSG SA WG3 #7, The Hague	26Oct99	S3-99340: Keystream repeat attacks	1	1	
3GPP TSG SA WG3 #6, Sophia Antipolis	29Sep99	S3-99340: Proposed CR 33.102-016 on Network-wide confidentiality	2	2	
3GPP TSG SA WG3 #7, The Hague	26Oct99	S3-99385: Proposed response to LS from R3 on common identification of relocation co-ordination	1	1	
ETSI SMG10 WPC #1/99, Newbury	20Jan99	SMG10-99005: Draft security architecture 33.23 v0.0.2	2	2	
ETSI SMG10 WPC #1/99, Newbury	20Jan99	SMG10-99012: Draft security architecture 33.23 v0.0.3	2	2	
ETSI SMG 10	20Jan99	SMG10-99C013: Mutual authentication and key establishment for UMTS Release 99 based on random challenges and sequence numbers - MAC-based variant	3	3	
3GPP T2, London	15Mar99	T2-99070: Revised CR to 02.57 on security	1	see note, above	
3GPP T2, London	15Mar99	T2-99071: CR to 03.57 on security	1		
3GPP T2, London	15Mar99	T2-99224: CR to 02.57 security	1		
3GPP T2, London	15Mar99	T2-99227: CR to 03.57 Security Sections	1		
3GPP T2, London	15Mar99	T2-99229: Revised CR to 02.57 11.3 Security	1		
3GPP T2, Yokohama	12Apr99	T2-99342: Stage 1 Security section CR	2		
3GPP T2, Yokohama	12Apr99	T2-99430: Stage 1 Security section CR	2		
3GPP T2, Helsinki	06Sep99	T2-99725: LS to WAP Forum on Support of root keys storage on SIM for MExE Release 99	1		
3GPP T2, Helsinki	06Sep99	T2-99727: Draft LS to S3 on MExE security	1		
3GPP T2, Helsinki	06Sep99	T2-99729: LS to WAP EFI	1		
3GPP T2, Helsinki	06Sep99	T2-99730: A brief guide to certificate formats	0		
3GPP T2, Korea	06Oct99	T2-99803: Discussion of pros and cons of storing certificate descriptors on SIM in one CDF or three	1		
3GPP T2, Korea	06Oct99	T2-99806: Proposal for use of same certificate for Administrator and operator roles	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99065: CR to 23.057 to re-organise security section	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99066: CR to 23.057 on APIs (not treated in Tampere) next meeting	1		

3GPP T2 SWG1, Tampere	15Jul99	T2X99067: Converged certification requirements for WAP and MExE	0		
3GPP T2 SWG1, Tampere	15Jul99	T2X99068: Provisioning certificates for WAP and MExE	0		
3GPP T2 SWG1, Tampere	15Jul99	T2X99071: CR to 23.057 to re-organise security section II	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99072: CR to 23.057 to re-organise security section III	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99087: revised T2X99071 - CR to 23.057 to re-organise security section II	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99090: revised T2X99072 - CR to 23.057 to re-organise security section III	1		
3GPP T2 SWG1, Newbury	11Aug99	T2X99106: CR to 23.057 on User Preference permissions	1		
3GPP T2 SWG1, Newbury	11Aug99	T2X99107: CR to 23.057 on permissions for actions not listed in the security table	0		
3GPP T2 SWG1, Newbury	11Aug99	T2X99109: CR to 23.057 on SIM certificate			
3GPP T2 SWG1, Newbury	11Aug99	T2X99110: Discussion doc on SIM certificate principles	1		
3GPP T2 SWG1, Newbury	11Aug99	T2X99111: LS to SMG9/T3 and accompanying CR to 11.11	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99112: LS to SUN on User Preferences	0		
3GPP T2 SWG1, Newbury	11Aug99	T2X99115: LS to SMG9, T3, SMG9 ad hoc on WAP-SAT interaction work item, on indication of terminal MExE capabilities in SAT TERMINAL PROFILE function	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99124: CR to 23.057 on SIM certificate (update of tdoc 109)	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99125: LS to SMG9/T3 and accompanying CR to 11.11 (update of tdoc 111)	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99126: LS to WAP Forum on SIM card support of MExE	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99129: LS to SMG9, T3, SMG9 ad hoc on WAP-SAT interaction work item, on indication of terminal MExE capabilities in SAT TERMINAL PROFILE function	1		
3GPP T2 SWG1, Newbury	11Aug99	T2X99131: CR to 23.057 on SIM certificate (update of tdoc 124)	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99133: LS to SMG9/T3 and accompanying CR to 11.11 (update of tdoc 125)	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99134: CR to 23.057 on SIM certificate (update of tdoc 131)	2		
3GPP TSG SA WG3	Nov99	S3-99416: CR 33.102-027 clarification of re-authentication during PS connections	1	1	
3GPP TSG SA WG3	Nov99	S3-99420: Evaluation of alternatives for sequence number management	2	2	

3GPP TSG SA WG3	Nov99	S3-99424: Optimising sequence number management	2	2	
3GPP TSG SA WG3	Nov99	S3-99425: Data integrity mandatory for UMTS subscribers only	2	2	
3GPP TSG SA WG3	Nov99	S3-99492: Proposed CR to 33.102 section 6.4.3 on USIM triggered authentication and key setting during PS connections	1	1	
3GPP TSG SA WG3	Dec99	S3-99501: CR to section 6.3 of TS 33.102 (security architecture)("L")	2	2	
3GPP TSG SA WG3	Dec99	S3-99502: CR to Annex C of TS 33.102 ("K")	2	2	
3GPP TSG SA WG3	Dec99	S3-99503: CR to Annex F of TS 33.102 ("M")	2	2	
3GPP TSG SA WG3	Dec99	S3-99504: justification of the proposed changes to section 6.3 and Annex F ("j")	2	2	
3GPP TSG SA WG3	Dec99	S3-99505: Adding BAN analysis of 3G authentication to TR 33.902	1	1	
3GPP TSG SA WG3	Dec99	S3-99523: Discussion on authentication algorithm requirements)	1	1	
3GPP TSG SA WG3	Dec99	S3-99535: SQN management options	2	2	
3GPP TSG SA WG3	Feb00	S3-00127: CR to 33.102: Restructuring of section 6.3	0	0	
3GPP TSG SA WG3	Feb00	S3-00128: CR to 33.102: Update of ciphering specification	2	2	
3GPP TSG SA WG3	Feb00	S3-00129: CR to 33.102: Update of data integrity specification	2	2	
3GPP TSG SA WG3	Feb00	S3-00130: CR to 33.102: Interoperation and intersystem handover/change between UTRAN and GSM BSS	2	2	
3GPP TSG SA WG3	Feb00	S3-00131: CR to 33.102: Local authentication and connection establishment	2	2	
3GPP TSG SA WG3	Feb00	S3-00132: CR to 33.102: User identity confidentiality	2	2	
3GPP TSG SA WG3	Feb00	S3-00133 CR to 25.301: Ciphering and Integrity	2	2	
3GPP TSG SA WG3	Feb00	S3-00134 CR to 33.105: Update of ciphering specification	2	2	
3GPP TSG SA WG3	Feb00	S3-00135 CR to 33.105: Update of data integrity specification	2	2	
3GPP TSG SA WG3	Feb00	S3-00136 Discussion on CRs on ciphering	2	2	
3GPP TSG SA WG3	Feb00	S3-00172: Presentation on USECA	1	1	

3GPP TSG SA WG3	Feb00	S3-00193 CR to 33.102 on Cipher key and integrity key lifetime	2	2	
3GPP TSG SA WG3	Feb00	S3-00194 CR to 33.102 on Cipher key and integrity key setting	2	2	
3GPP TSG SA WG3	Feb00	S3-00195 CR to 33.102 HE control over accepting non-ciphered connections	1	1	
3GPP TSG SA WG3	Feb00	S3-00207 CR078 to 33.102: Conversion functions	2	2	
3GPP TSG SA WG3	Apr00	S3-00222: Initialisation of COUNT-I and COUNT-C	2	2	
3GPP TSG SA WG3	Apr00	S3-00251: Review of TS 24.008	1	1	
3GPP TSG SA WG3	Apr00	S3-00253: CR to 33.102: Authentication and key agreement (editorial)	1	1	
3GPP TSG SA WG3	Apr00	S3-00254: CR to 33.102: Authentication and key agreement (minimal)	1	1	
3GPP TSG SA WG3	Apr00	S3-00255: CR to 33.102: Conversion functions for GSM-UMTS interoperation	2	2	
3GPP TSG SA WG3	Apr00	S3-00256: CR to 33.102: 3G-3G Handover	2	2	
3GPP TSG SA WG3	Apr00	S3-00257: CR to 33.102: 3G-2G and 2G-3G Handover for CS services	2	2	
3GPP TSG SA WG3	Apr00	S3-00258: CR to 33.102: Limitation and reduction of the effective cipher key length by the serving network	2	2	
3GPP TSG SA WG3	Apr00	S3-00259: CR to 33.102: Initialisation of synchronisation for ciphering and integrity protection	2	2	
3GPP TSG SA WG3	Apr00	S3-00268: CR to 33.102: Removal of enhanced user identity confidentiality	2	2	
3GPP TSG SA WG3	Apr00	S3-00269: CR to 33.102: Removal of network domain security	2	2	
3GPP TSG SA WG3	Apr00	S3-00275: 3GPP Security/AKA - Requirements and development (Presentation Slides)	1	1	
3GPP TSG SA WG3	May00	S3-00312 Independence of confidentiality and integrity in MAP Layer III and other layer III issues	2	2	
3GPP TSG SA WG3	May00	S3-00368: Replay protection for core network signalling messages	2	2	
3GPP TSG SA WG3	May00	S3-00378: CR to 33.102: Clarification on terminology in user domain	1	1	
3GPP TSG SA WG3	Aug00	S3-00406: CR to 33.102: Re-transmission of authentication request using the same quintet	2	2	

3GPP TSG SA WG3	Aug00	S3-00444: Core network security protocols	2	2	
3GPP TSG SA WG3	Aug00	S3-00445: Key management for core network security	2	2	
3GPP TSG SA WG3	Aug00	S3-00447: Overview of security mechanisms for access security for IP-based services	1	1	
3GPP TSG SA WG3	Aug00	S3-00467: Review of the integrity protection procedure	1	1	