

CHANGE REQUEST

TS 33.203 CR CRNum # rev # Current version: **6.2.0**

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the # symbols.

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	#	SIP Privacy mechanism when IMS interworking with non-IMS network		
Source:	#	Nokia		
Work item code:	#	IMS-ASEC	Date:	# 14/5/2004
Category:	#	A	Release:	# Rel-6
		Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
		F (correction)	2	(G<SM Phase 2)
		A (corresponds to a correction in an earlier release)	R96	(Release 1996)
		B (addition of feature),	R97	(Release 1997)
		C (functional modification of feature)	R98	(Release 1998)
		D (editorial modification)	R99	(Release 1999)
		Detailed explanations of the above categories can be found in 3GPP TR 21.900 .	Rel-4	(Release 4)
			Rel-5	(Release 5)
			Rel-6	(Release 6)

Reason for change:	#	This CR adds the handling of user privacy feature in SIP, when the IMS interworking with a non-IMS network.
Summary of change:	#	The privacy handling is added with modification to Rel-5 handling for Rel-6 IMS.
Consequences if not approved:	#	It is impossible to guarantee IMS interworking security.

Clauses affected:	#	5.3, 6.5										
Other specs affected:	#	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">X</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;">X</td> </tr> <tr> <td></td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	X			X		X	Other core specifications	# TS 24.229, TS 24.228
		Y	N									
		X										
	X											
	X											
			Test specifications									
			O&M Specifications									
Other comments:	#											

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".
- [2] 3GPP TS 22.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for the IP Multimedia Core Network".
- [3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem".
- [4] 3GPP TS 21.133: "3rd Generation Partnership Project; T Technical Specification Group Services and System Aspects; Security Threats and Requirements".
- [5] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".
- [6] IETF RFC 3261 "SIP: Session Initiation Protocol".
- [7] 3GPP TS 21.905: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Vocabulary for 3GPP specifications".
- [8] 3GPP TS 24.229: "3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".
- [9] 3GPP TS 23.002: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, Network Architecture".
- [10] 3GPP TS 23.060: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, General Packet Radio Service (GPRS); Service Description".
- [11] 3GPP TS 24.228: "3rd Generation Partnership Project: Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".
- [12] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication".
- [13] IETF RFC 2406 (1998) "IP Encapsulating Security Payload (ESP)".
- [14] IETF RFC 2401 (1998) "Security Architecture for the Internet Protocol".
- [15] IETF RFC 2403 (1998) "The Use of HMAC-MD5-96 within ESP and AH".
- [16] IETF RFC 2404 (1998) "The Use of HMAC-SHA-1-96 within ESP and AH".
- [17] IETF RFC 3310 (2002): "HTTP Digest Authentication Using AKA". April, 2002.
- [18] IETF RFC 3041 (2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".
- [19] IETF RFC 2402 (1998): "IP Authentication Header".
- [20] IETF RFC 2451 (1998): "The ESP CBC-Mode Cipher Algorithms".

- [21] IETF RFC 3329 (2002): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".
- [22] IETF RFC 3323 (2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".
- [23] IETF RFC 3325 (2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network".

5 Security features

5.1 Secure access to IMS

5.1.1 Authentication of the subscriber and the network

Authentication between the subscriber and the network shall be performed as specified in section 6.1.

An IM-subscriber will have its subscriber profile located in the HSS in the Home Network. The subscriber profile will contain information on the subscriber that may not be revealed to an external partner, cf. [3]. At registration an S-CSCF is assigned to the subscriber by the I-CSCF. The subscriber profile will be downloaded to the S-CSCF over the Cx-reference point from the HSS (Cx-Pull). When a subscriber requests access to the IP Multimedia Core Network Subsystem this S-CSCF will check, by matching the request with the subscriber profile, if the subscriber is allowed to continue with the request or not i.e. Home Control (Authorization of IM-services).

All SIP-signaling will take place over the PS-domain in the user plane i.e. IP Multimedia Core Network Subsystem is essentially an overlay to the PS-domain. Hence the Visited Network will have control of all the subscribers in the PS-domain i.e. Visited Control (Authorization of bearer resources) since the Visited Network provides the subscriber with a transport service and its associated QoS.

For IM-services a new security association is required between the mobile and the IMS before access is granted to IM-services.

The mechanism for mutual authentication in UMTS is called UMTS AKA. It is a challenge response protocol and the AuC in the Home Stratum derives the challenge. A Quintet containing the challenge is sent from the Home Stratum to the Serving Network. The Quintet contains the expected response XRES and also a message authentication code MAC. The Serving Network compares the response from the UE with the XRES and if they match the UE has been authenticated. The UE calculates an expected MAC, XMAC, and compares this with the received MAC and if they match the UE has authenticated the Serving Network.

The AKA-protocol is a secure protocol developed for UMTS and the same concept/principles will be reused for the IP Multimedia Core Network Subsystem, where it is called IMS AKA.

The Home Network authenticates the subscriber at anytime via the registration or re-registration procedures.

5.1.2 Re-Authentication of the subscriber

Initial registration shall always be authenticated. It is the policy of the operator that decides when to trigger a re-authentication by the S-CSCF. Hence a re-registration might not need to be authenticated.

A SIP REGISTER message, which has not been integrity protected at the first hop, shall be considered as initial registration.

The S-CSCF shall also be able to initiate an authenticated re-registration of a user at any time, independent of previous registrations.

5.1.3 Confidentiality protection

Confidentiality protection shall not be applied to SIP signalling messages between the UE and the P-CSCF. It is recommended to offer encryption for SIP signalling at link layer i.e. between the UE and the RNC using the existing mechanisms as defined in [1].

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [5].

5.1.4 Integrity protection

Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signaling, as specified in section 6.3. The following mechanisms are provided.

1. The UE and the P-CSCF shall negotiate the integrity algorithm that shall be used for the session, as specified in chapter 7.
2. The UE and the P-CSCF shall agree on security associations, which include the integrity keys, that shall be used for the integrity protection. The mechanism is based on IMS AKA and specified in clause 6.1.
3. The UE and the P-CSCF shall both verify that the data received originates from a node, which has the agreed integrity key. This verification is also used to detect if the data has been tampered with.
4. Replay attacks and reflection attacks shall be mitigated.

Integrity protection between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [5].

5.2 Network topology hiding

The operational details of an operator's network are sensitive business information that operators are reluctant to share with their competitors. While there may be situations (partnerships or other business relations) where the sharing of such information is appropriate, the possibility should exist for an operator to determine whether or not the internals of its network need to be hidden.

It shall be possible to hide the network topology from other operators, which includes the hiding of the number of S-CSCFs, the capabilities of the S-CSCFs and the capability of the network.

The I-CSCF shall have the capability to encrypt the address of an S-CSCF in SIP Via, Record-Route, Route and Path headers and then decrypt the address when handling the response to a request. The P-CSCF may receive routing information that is encrypted but the P-CSCF will not have the key to decrypt this information.

The mechanism shall support the scenario that different I-CSCFs in the HN may encrypt and decrypt the address of the S-CSCFs.

5.3 SIP Privacy handling ~~in~~for IMS Networks

Privacy may in many instances be equivalent with confidentiality i.e. to hide the information (using encryption and encryption keys) from all entities except those who are authorized to understand the information. The SIP Privacy Extensions for IMS Networks do not provide with such confidentiality. The purpose of the mechanism is rather to give an IMS subscriber the possibility to withhold certain identity information of the subscriber as specified in [22] and [23].

NOTE 1: It is useful that the privacy mechanism for IMS networks does not create states in the CSCFs other than the normal SIP states.

Editor's note: the exact mechanism for building the trust relation for privacy handling is ffs.

*** NEXT CHANGE ***

6.5 CSCF interoperating with proxy located in ~~non-IMS~~a foreign network

SIP signalling protected by TLS specified in RFC 3261 [6] may be used for protecting the SIP interoperation between an IMS CSCF with a proxy/CSCF located in ~~non-IMS~~a foreign network. The CSCF may request the TLS connection with a foreign Proxy by publishing sips: URI in DNS server, that can be resolved via NAPTR/SRV mechanism specified in RFC 3263 [23]. When sending/receiving the certificate during the TLS handshaking phase, the CSCF shall verify the name on the certificate against the list of the interworking partners.

Editor's note: the definition of a foreign network is currently meant a non-IMS network. It may extend to also IMS network which is ffs.

The TLS session could be initiated from either ~~the CSCF or the foreign proxy~~network. A TLS connection is capable of carrying multiple SIP dialogs.

Applying this method is to prevent attacks on SIP level, but it does not prohibit other security methods to be applied so as to strengthen the security for IP based networks. This part is specified in Annex A of TS 33.210 [5].

NOTE 1: The key management and certificate management for TLS is out of scope of the present specification.

NOTE 2: The security mechanism between the CSCFs within IMS is covered by NDS/IP security specified in TS 33.210 [5].

*** END OF CHANGE ***