

CR-Form-v7

CHANGE REQUEST

TS 33.203 CR CRNum rev Current version: **6.3.0**

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 (foreign) network		
Source:	Nokia		
Work item code:	IMS-ASEC	Date:	28/6/2004
Category:	F	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:	Rel-6 IMS shall support interworking with non-IMS networks. IMS entities need to know whether a remote SIP entity is trusted, in order to apply screening policies, and further handling of user privacy.		
Summary of change:	Mechanisms to establish trust with non-IMS networks are added.		
Consequences if not approved:	It is impossible to guarantee security of interworking between IMS and non-IMS networks.		

Clauses affected:	2, 5.1, 5.3, 6.5, Annex J										
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 style="text-align: center;"></td> </tr> <tr> <td style="text-align: center;"></td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"></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 3602 (2003): " The AES-CBC Cipher Algorithm and Its Use with IPsec".
- [23] IETF RFC 3263 (2002): "Session Initiation Protocol (SIP): Locating SIP Servers".
- [24] [3GPP TS 33.310: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, Network Domain Security \(NDS\); Authentication Framework \(AF\)".](#)

*** NEXT CHANGE ***

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 clause 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 clause 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 TS 33.210 [5].

NOTE1: TLS is mandatorily supported by SIP proxies according to RFC3261 [6], and operators may use it to provide confidentiality and integrity inside their networks instead of or on top of IPsec, as the intra-domain Za interface is optional, and TLS may also be used between IMS networks on top of IPsec. It should be pointed out, that the 3GPP specifications do not provide support for TLS certificate management in a fashion similar to TS 33.310 (NDS/AF) [24] nor do they ensure backward compatibility with Release 5 CSCFs nor interoperability with other networks which do not use TLS, in case TLS is used by Release 6 CSCFs. These management and compability issues need then to be solved by manual configuration of the involved operators.

*** NEXT CHANGE ***

5.3 SIP Privacy handling in 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 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.~~

5.4 SIP Privacy handling when interworking with non-IMS Networks

When a Rel-6 IMS is interworking with a non-IMS network, the CSCF in the IMS network shall decide the trust relation with the other end. The other end is trusted when the security mechanism for the interworking (cf. section 6.5) is applied as well as the availability of an inter-working agreement. If the interworking non-IMS network is not trusted, the privacy information shall be removed from the traffic towards to this non-IMS network. When receiving SIP signalling, the CSCF shall also verify if any privacy information is already contained. If the interworking non-IMS network is not trusted, the information shall be removed by the CSCF, and retained otherwise.

Because absence of the security mechanism for the interworking (cf. section 6.5) indicates an untrusted non-IMS network, separate CSCFs are usually needed to interface with IMS and non-IMS networks. The CSCF interfacing with IMS networks implicitly trusts all IMS networks reachable via the SEG that establishes security according to TS 33.210 [5]. A Rel-5 CSCF always assumes this trust relationship and network configuration. For a Rel-6 CSCF, this implicit trust setting shall be a configuration option, that an operator can set according to his network and interface configuration.

*** NEXT CHANGE ***

6.5 CSCF interoperating with proxy located in a non-IMS 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 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: A "foreign network" is currently defined as a non-IMS network. It may extend to also IMS network which is ffs.~~

The TLS session could be initiated from either 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 NOTE 1 in section 5.1.4 on the use of TLS also applies here~~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].~~

*** NEXT CHANGE ***

Annex J (informative): Recommendations to protect the IMS from UEs bypassing the P-CSCF

After the UE does a successful SIP REGISTER with the P-CSCF, malicious UE could try to send SIP messages directly to the S-CSCF. This could imply that the UE would be able to bypass the integrity protection provided by IPSec ESP between the UE and the P-CSCF.

NOTE: The TS 24.229 [8] defines a trust domain that consists of the P-CSCF, the I-CSCF, the S-CSCF, the BGCF, the MGCF, the MRFC and all the AS:s that are not provided by 3rd party service providers. There are nodes in the edge of the trust domain that are allowed to provide with an asserted identity header. The nodes in the trust domain will trust SIP messages with asserted identity headers. The asserted identity information is useful as long as the interfaces in an operator's network can be trusted.

If a UE manages to bypass the P-CSCF it presents at least the following problems:

- 1) The P-CSCF is not able to generate any charging information.
- 2) Malicious UE could masquerade as some other user (e.g. it could potentially send INVITE or BYE messages).

The following recommendations for preventing attacks based on such misbehavior are given:

- Access to S-CSCF entities shall be restricted to the core network entities that are required for IMS operation, only. It shall be ensured that no UE is able to directly send IP packets to IMS-entities other than the required ones, ie. assigned P-CSCF, or HTTP servers.
- Impersonation of IMS core network entities at IP level (IP spoofing), especially impersonation of P-CSCFs by UEs shall be prevented.
- It is desirable to have a general protection mechanism against UEs spoofing (source) IP addresses in any access network providing access to IMS services.

If the traffic is between two non-IMS foreign CSCFs, it is recommended to use TLS mechanisms as specified in RFC3261 [6]. This will mitigate the problems caused by mis-behave of the UE. If neither inter-CSCF traffic nor CSCF-SEG traffic can be trusted and if this traffic is not protected by the NDS/IP, TS 33.210 [5] mechanisms, then physical protection measures or IP traffic filtering should be applied. This is anyhow not in the scope of 3GPP specification.

*** END OF CHANGE ***