3GPP TSG SA WG3 Security — S3#34 **Tdoc ⌘S3-040559**
6 - 9 July 2004, Acapulco, Mexico

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 [X]

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 one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (G<SM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	This CR is an update of S3-040429, based on the companion discussion paper since SEG based security mechanism is inadequent to handle the authentication of SIP peer, and further handling of user privacy.
Summary of change:	⌘	- The traffic between CSCFs uses the TLS based solution specified in RFC3261 (the traffic over Cx interface remains unchanged, i.e. based on NDS/IP) throughout the specification; - Two pictures are re-drawn, because there are small errors and they are not word editable; - The privacy handling is added to Rel-6 IMS with modification of Rel-5 mechanism; - The NDS part is updated in section 6.5.
Consequences if not approved:	⌘	It is impossible to guarantee IMS interworking security.

Clauses affected:	⌘	2, 4, 5.3, 6.5				
		Y	**N**			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 24.229, TS 24.228
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

START OF CHANGE

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)".

[25] OMA WAP-219-TLS, 4.11.2001: http://www.openmobilealliance.org/tech/affiliates/wap/wap-219-tls-20010411-a.pdf.

NEXT CHANGE

4 Overview of the security architecture

In the PS domain, the service is not provided until a security association is established between the mobile equipment and the network. IMS is essentially an overlay to the PS-Domain and has a low dependency of the PS-domain. Consequently a separate security association is required between the multimedia client and the IMS before access is granted to multimedia services. The IMS Security Architecture is shown in the following figure.

IMS authentication keys and functions at the user side shall be stored on a UICC. It shall be possible for the IMS authentication keys and functions to be logically independent to the keys and functions used for PS domain authentication. However, this does not preclude common authentication keys and functions from being used for IMS and PS domain authentication according to the guidelines given in clause 8.

For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on a UICC. Further information on the ISIM is given in clause 8.

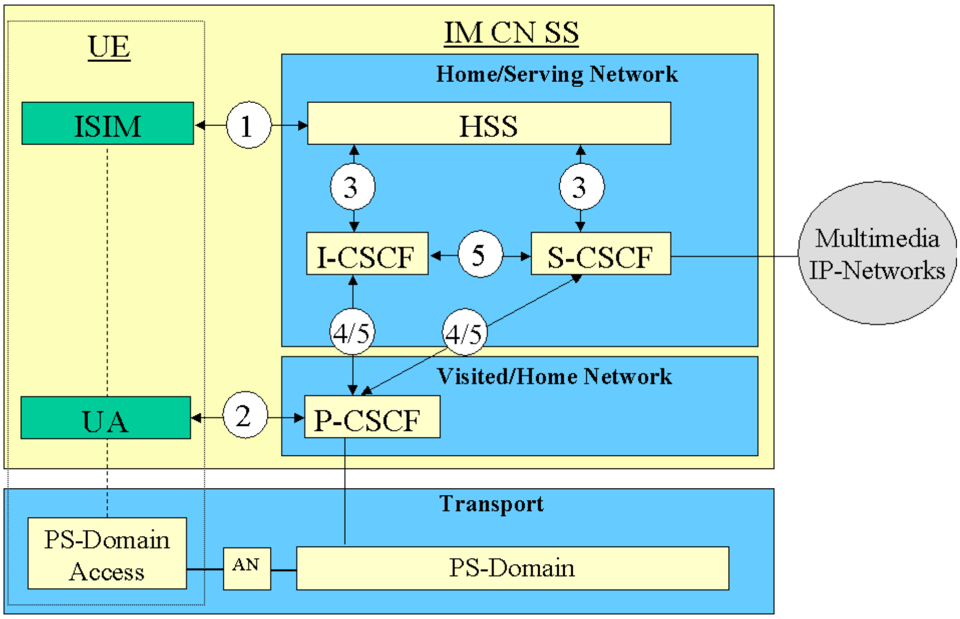


Figure 1: The IMS security architecture

There are five different security associations and different needs for security protection for IMS and they are numbered 1,2, 3, 4 and 5 in figure 1 where:

1. Provides mutual authentication. The HSS delegates the performance of subscriber authentication to the S-CSCF. However the HSS is responsible for generating keys and challenges. The long-term key in the ISIM and the HSS is associated with the IMPI. The subscriber will have one (network internal) user private identity (IMPI) and at least one external user public identity (IMPU).

2. Provides a secure link and a security association between the UE and a P-CSCF for protection of the Gm reference point. Data origin authentication is provided i.e. the corroboration that the source of data received is as claimed. For the definition of the Gm reference point cf. TS 23.002 [9].

3. Provides security within the network domain internally for the Cx-interface. This security association is covered by TS 33.210 [5]. For the definition of the Cx-interface cf. TS 23.002 [9].

4. Provides security between different networks for SIP capable nodes. This security association is covered by ~~TS 33.210 [5]~~TLS as specfied in RFC3261 [6], cf. section 6.5. This security association is only applicable when the P-CSCF resides in the VN and if the P-CSCF resides in the HN then bullet point number five below applies, cf. also Figure 2 and Figure 3.

5. Provides security within the network internally between SIP capable nodes. This security association ~~is~~may ~~covered by~~use TLS as specfied in RFC3261 [6], cf. section 6.5~~TS 33.210 [5]~~. Note that this security association also applies when the P-CSCF resides in the HN.

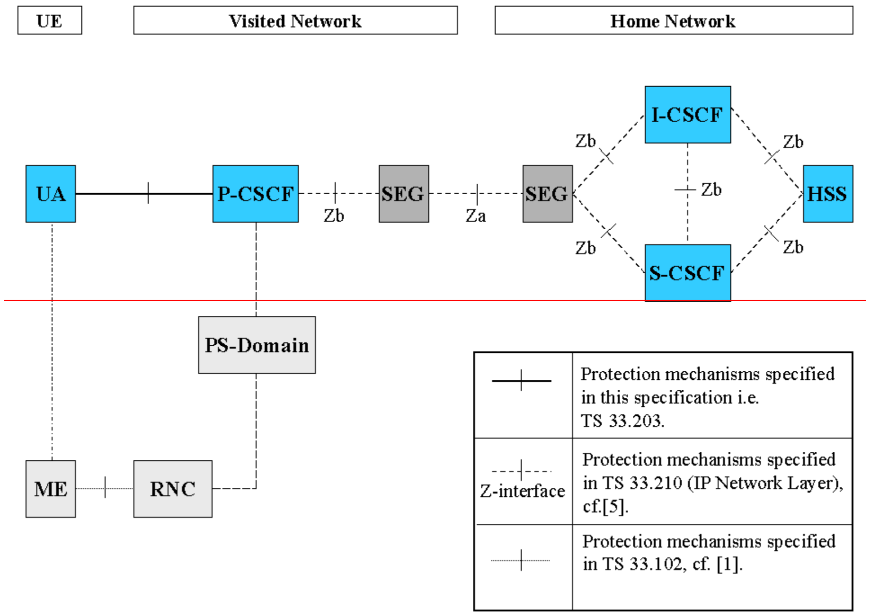
There exist other interfaces and reference points in IMS, which have not been addressed above. Those interfaces and reference points reside within the IMS, either within the same security domain or between different security domains. The protection of all such interfaces and reference points apart from the Gm reference point are protected as specified in TS 33.210 [5].

Mutual authentication is required between the UE and the HN.

The mechanisms specified in this technical specification are independent of the mechanisms defined for the CS- and PS-domain.

An independent IMS security mechanism provides additional protection against security breaches. For example, if the PS-Domain security is breached the IMS would continue to be protected by it's own security mechanism. As indicated in Figure 1 the P-CSCF may be located either in the Visited or the Home Network. The P-CSCF shall be co-located within the same network as the GGSN, which may reside in the VPLMN or HPLMN according to the APN and GGSN selection criteria, cf. TS 23.060 [10].

P-CSCF in the Visited Network



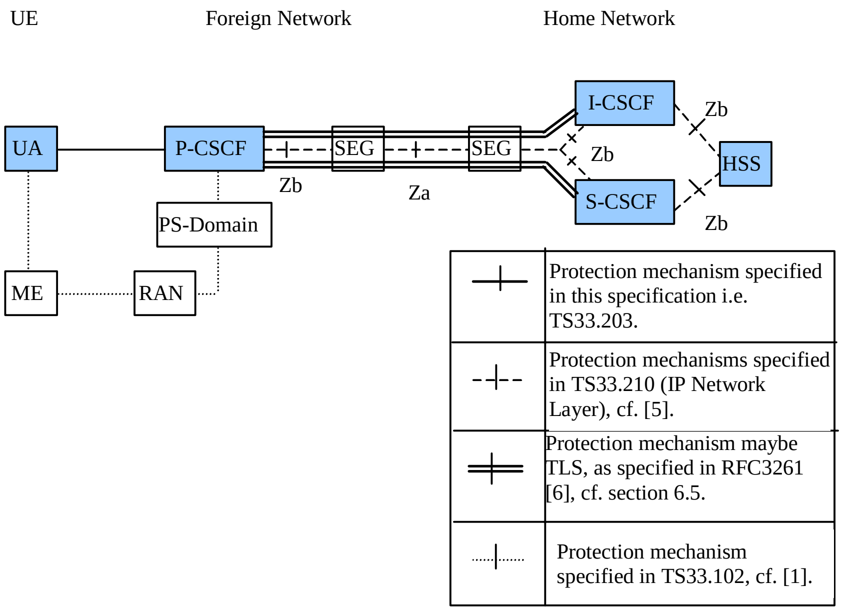
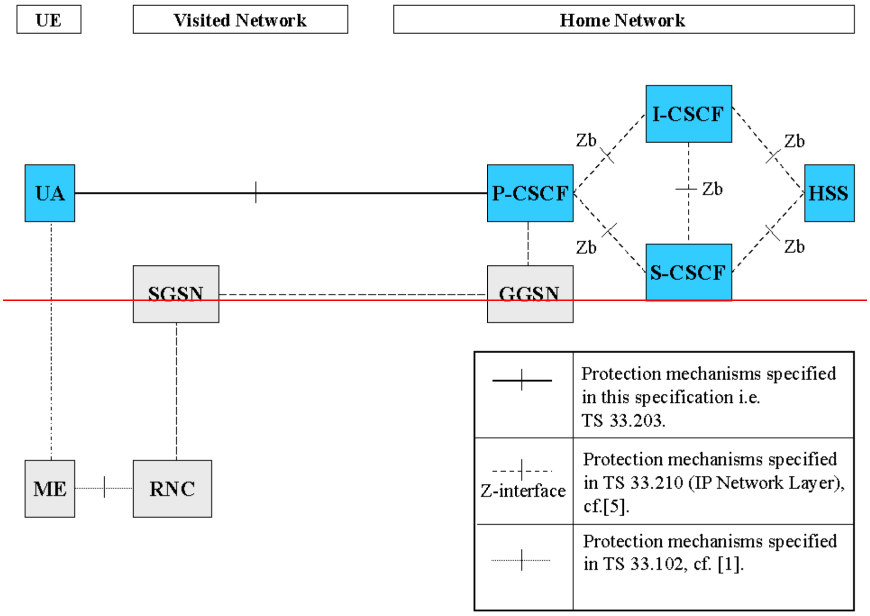


Figure 2: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the VN

P-CSCF in the Home Network



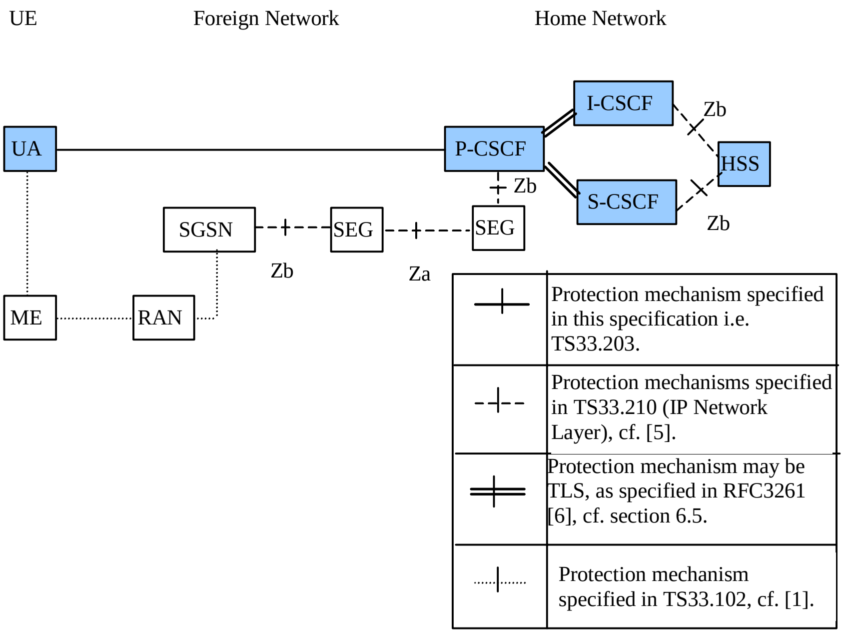


Figure 3: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security~~, cf. TS 33.210 [5]~~, when the P-CSCF resides in the HN

The confidentiality and integrity protection for SIP-signaling is provided in a hop-by-hop fashion, cf. Figure 2 and Figure 3. The first hop i.e. between the UE and the P-CSCF is specified in this technical specification. The other hops, inter-domain and intra-domain ~~are~~shall use the TLS specified in RFC3261 [6], cf. Section 6.5.~~TS 33.210 [5]~~.

*** NEXT CHANGE ***

5.1.3 Confidentiality protection

Possibility for IMS specific confidentiality protection shall be provided to SIP signalling messages between the UE and the P-CSCF. Mobile Operators shall take care that the deployed confidentiality protection solution and roaming agreements fulfils the confidentiality requirements presented in the local privacy legislation. The following mechanisms are provided at SIP layer:

1. The UE shall always offer encryption algorithms for P-CSCF to be used for the session, as specified in clause 7.

2. The P-CSCF shall decide whether the IMS specific encryption mechanism is used. If used, the UE and the P-CSCF shall agree on security associations, which include the encryption key that shall be used for the confidentiality protection. The mechanism is based on IMS AKA and specified in clause 6.1.

Confidentiality between CSCFs shall rely on the TLS specified in RFC3261 [6],; and confidentiality between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in TS 33.210 [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 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,shall rely on the TLS specified in RFC3261 [6]; and integrity protection between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in TS 33.210 [5].

*** NEXT CHANGE ***

5.3 SIP Privacy handling in IMS when interworking with foreign 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.

When a Rel-6 IMS interworking with a foreign network, the CSCF in IMS network shall decide the trust relation with the other end, based on whether 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 network is not trusted, the privacy information shall be removed from the traffic towards to the foreign network. When receiving SIP signalling, the CSCF shall also verify if any privacy information is already contained. If the interworking network is not trusted, the information shall be removed by the CSCF, and retained otherwise.

NOTE 2: A foreign network could be any network that does not belong to the same operator.

*** NEXT CHANGE ***

6.5 CSCF interoperating with proxy located in 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 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 inititiated 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 key management and certificate management for TLS is out of scope of the present specificatioshall be based on ncovered by TS 33.310 [24]. The TLS profiling is specfied in [25].

NOTE 2: The security mechanism between the CSCFs within IMS is covered by NDS/IP security specified in TS 33.210 [5].NOTE 2: A foreign network could be any network that does not belong to the same operator.

*** 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 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 int~~er~~ra-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 ***