3GPP TSG SA WG3 Security — S3#29 **S3-030468**
15 - 18 July 2003
San Francisco, USA

Title: LS on Profiling of RFC3325 for IMS
Response to:
Release: Rel-6
Work Item: IMS-ASEC

Source: SA3
To: SA2, CN1
Cc: SA1

Contact Person:
Name: krister.boman@ericsson.com
Phone: +46 31 7474055

Attachments: S3-030372, S3-030456, S3-030377

---

1. Overall Description:

SA3 has within the work item for Presence Security progressed the work on profiling the RFC3325. SA3 has discussed the possibility to include a profile into TS33.203 for Release 6. The attached documents were discussed in deep and it was concluded that more feedback from CN1 and SA2 is required before approval of the CRs.

SA3 is aware of that CN1 has profiled RFC3325 for Release 5 already. There were concerns expressed at SA3#29 that the in the CR S3-030377 included priv-value types which are not yet supported in CN1 specifications could cause unnecessary workload on CN1.

Following an email discussion on the openness of the IMS for Release 6 at the SA3 reflector the definition of a SPEC(T) defined in RFC3325 for IMS was discussed in SA3-030372 where for our purposes T:=3GPP-IMS. The attached CR S3-030456 was postponed since SA3 agrees that at this point of time it is necessary to get standpoints on this issue from SA2 and CN1. In particular bullet point 4. of the SPEC(T) highlight some potential alternatives for implementation where it is important for SA3 to get more guidance in particular from SA2 on their requirements related to Internet-based SIP entities. Based on the information from SA2 and CN1 SA3 will take a decision on what standardisation effort is required and in particular evaluate if the S3-030456 shall be captured in an Informative Annex which is the current working hypothesis of SA3.

2. Actions:

CN1 and SA2: Study the attached documents and provide with comments to SA3 on which SA3 can take a decision what standardization effort is required from a security point of view.

3. Date of Next SA3 Meetings:

SA3#30	6-10 October 2003	Porto, Portugal
SA3#31	18-21 November 2003	London, UK

3GPP TSG SA WG3 Security **S3-030372**

July, 2003

San Fransisco, USA

Agenda Item: Presence/IMS

Source: Ericsson

Title: Profiling of RFC3325

Document for: Discussion/Decision

1. Introduction

On the SA3 email reflector there have been some discussions on the increased openness of Rel 6 version of the IMS. This paper aims to discuss on the Trust Domain and the SPEC(T) concepts as defined by IETF or the use of p-asserted-identity and as incorporated in the TS24.229 in CN1. A CR to TS33.203 is attached to reflect how SPEC(T) is implemented in 3GPP. It is proposed that this is captured in an Informative Annex.

It should be noted that this input paper defines the trust domain T to be equal to 3GPP-IMS i.e.

T := 3GPP-IMS

2 Discussion

In RFC 3325 [1] a private extension mechanism that makes it possible for nodes in the network to assert identities of users is defined. Clearly the user needs to be authenticated by a node in the system before an identity could be asserted. If a node has authenticated a user it can then assert the identity. All nodes belonging to the same system and are all included in the same Trust Domain can therefore trust that the identity belongs to the claimed one. As soon as an asserted identity is received from or sent to the complement to the trust domain the identity can no longer be asserted.

An example of such a system is a closed network as exemplified in the RFC 3325, which emulates a circuit switched telephone network.

SA3 has earlier discussed the problems with a UE that bypasses a P-CSCF after successful registration. It was then concluded that cf. TS33.203 Annex J "….if neither inter-CSCF traffic nor CSCF-SEG traffic can be trusted and if this traffic is not protected by the NDS/IP [5] mechanisms, then physical protection measures or IP traffic filtering should be applied. This is anyhow not in the scope of 3GPP specification.".

Furthermore this seems to be inline with the SA2 requirement from TS23.228 that an operator should based on the operator policy decide whether a S-CSCF may forward the SIP request/response to the open Internet, cf. Clause 5.4.2 in TS23.228. However no exact mechanism how this requirement could be implemented has been defined by 3GPP. One conclusion could be then that SA2 has had the view similar as SA3 on the bypassing P-CSCF problem that the exact mechanism is out of the scope of 3GPP. Clearly an operator has the choice to exclude all SIP traffic towards the Internet, which is one way of achieving this technically, but this choice might not be attractive for all operators considering the business implication of such an implementation.

2.1 SPEC(T)

The RFC 3325 requires that a SPEC(T) is defined from the template given below:

1. The manner in which users are authenticated
2. The mechanisms used to secure the communication among nodes within the Trust Domain
3. The mechanisms used to secure the communication between UAs and nodes within the Trust Domain

4. The manner used to determine which hosts are parts of the Trust Domain T
5. The default privacy handling when no Privacy header field is present
6. That nodes in the Trust Domain are compliant to SIP
7. That nodes in the Trust Domain are compliant to RFC 3325
8. Privacy handling for identity as described in Section 7 in RFC 3325

The RFC is only applicable for a defined Trust Domain T trusted by end users and end systems. It is worthwhile to mention that the RFC does not specify any security measure for protection of the asserted identity in terms of confidentiality, integrity and replay protection or any other mechanism. It is not possible to verify who has asserted the identity meaning that it is the responsibility of the Trust Domain. As indicated in the RFC there are sufficiently many type of networks where this is useful where this can be used although the limitations associated with it such as a closed network. A 3GPP network and the IMS network in many aspects are viewed as closed networks but this requires that the owners of the networks implement what is required in 3GPP standards as well as security measures not visible in the standards like Firewalls and Physical protection.

2.2 How does it work?

There are many cases covered in RFC3325 but at high level it works like as briefly described in this clause.

A node inserting p-asserted-identity performs an authentication of the user utilizing e.g. Digest.

Assume $N_i \in T$ and $N_j \in T$ and $N_k \notin T$ i.e. $N_k \in T'$ (i.e. the complement to T):

1. If N_i receives an asserted-id from N_j since both belong to T it can be accepted and no authentication of the subscriber is necessaryIf N_i receives an message from N_k, which is not trusted then if N_i wants to add an asserted identity to the message the N_i has to authenticate the user e.g. using DigestIf N_i receives a message from N_k, which is not trusted, and an asserted id is present then N_i must remove the header. This could be the case when an I-CSCF receives a message from the Internet, which could claim that the identity belongs to an IMS subscriber. Clearly 3GPP has not specified any means to authenticate a user form the Internet so this identity cannot be trusted.If N_i is about to forward an asserted identity to the N_k, which is not trusted. If the UE has required Privacy i.e. priv-value=id then N_i shall remove the asserted identity

2.3 What has been implemented in IMS?

Here we describe what has been implemented already in the TS33.203 and the Presence TR and indicates where there are some open issue left for study.

We can assume the following definition of the Trust Domain T for IMS (i.e. by definition T := 3GPP-IMS):

a) Nodes belonging to the same administrative domain and consequently, belonging to the 3GPP-IMS Trust Domain T (e.g., nodes under the control of the same operator);

b) Nodes belonging to other administrative domains and belonging to the 3GPP-IMS Trust Domain T (e.g., nodes belonging to other 3GPP networks); and

c) Nodes belonging to other administrative domains and not belonging to the 3GPP-IMS Trust Domain T (e.g, nodes that do not belong to any 3GPP network).

It is clear that we have that P-CSCF∈T, I-CSCF∈T and S-CSCF∈T. It is also clear that all other nodes in the architecture as specified in TS23.228 are trusted. However a node outside the 3GPP domains such as SIP server cannot be trusted.

The following aims to discuss the SPEC(T) from a 3GPP and IMS perspective:

1. How users are authenticated

The Authentication of subscribers takes place in the S-CSCF using IMS AKA as specified in TS33.203. Based on this authentication a Security Association can be created between the UE and the P-CSCF based on IK and CK

derived form IMS AKA. The P-CSCF will be able to verify the claimed identity and also able to assert identities based on the integrity protection using IK and applying either HMAC-MD5 or HMAC-SHA1 of the SIP message.

2. The protection mechanisms among nodes within the Trust Domain

The security protection that has been defined for IMS in 3GPP relies upon underlying hop-by-hop security and the use of IPsec and TS33.210. It is mandatory to apply confidentiality protection and integrity protection between security gateways i.e. SEGs for SIP signalling between a VN and a HN. However it is optional for implementation to use the Zb interface inside the VN or the HN. According to TS33.203 it is also stated that if neither inter-CSCF traffic nor CSCF-SEG traffic can be trusted and if this traffic is not protected by the mechanisms defined in TS33.210, then physical protection measures or IP traffic filtering should be applied, which is outside the scope of 3GPP specifications.

3. The mechanism to secure communication between the UAs and nodes within the Trust Domain

The UE and the P-CSCF is utilizing IPsec for integrity protection as specified in TS33.203 and optionally the confidentiality protection as defined in TS33.102 between the UE and the RNC.

Since the AS's that reside within the HN are trusted it is up to the owner of the HN to apply IPsec as defined in TS33.210. All other SIP servers/proxies residing outside a 3GPP network is not considered in the 3GPP standards in terms of what security mechanisms should be applied.

4. The manner to determine which hosts belong to the Trust Domain

SIP nodes that receive or send traffic to other SIP nodes may take different actions (e.g., removal of P-Asserted-Identity header field) before forwarding the SIP message to the next node as described above.

Prior to forwarding a SIP message, a SIP node belonging the 3GPP-IMS Trust Domain must determine whether the next hop is part of the 3GPP-IMS Trust Domain or not. Similarly, when a SIP node in the 3GPP-IMS Trust Domain receives a SIP message, it must determine whether the previous node belongs to the 3GPP-IMS Trust Domain T or not.

The trust model in 3GPP has implicitly assumed what nodes belong to T however nothing has been stated in the specifications on how to determine that a node belongs to the complement to T i.e. T'. This could be accomplished in several ways at high level and here is an example list. The list is not exhaustive and does not exclude that the solutions can be combined:

I. The use of certificates and TLS

II. The operator implements the Zb interface and IPsec

III. Dedicated I-CSCF's for the Internet access

IV. 'Trusted' and 'untrusted' interfaces in I-CSCF

V. Physical protection measures or IP traffic filtering is applied. This is anyhow not in the scope of 3GPP specification.

VI. The 3GPP network is from a standardization point of view assumed to be a closed network i.e. there is no need for 3GPP to extend the existing standards further to verify that a message came from or is being sent to a trusted or untrusted node i.e. NDS/IP applies

In the following text some more details are given on some of the technical solutions however it does not aim to be an exhaustive review and many other possibilities are assumed to exist.

When a SIP node is receiving or sending a SIP message from/to another SIP node, it needs to determine whether it is a trusted node or not in the general IETF sense.

The manner to determine if the previous or next host is part of a the Trust Domain T is considered separated from incoming than outgoing traffic.

Incoming traffic:

These are SIP messages received by a SIP node. The SIP node must determine whether the previous node was part of T or not.

This can be achieved in many ways e.g. through:

1) A node can do a reverse DNS query (Note: one could perhaps argue DNS security could apply here but that is FFS) to find out if the source IP address belongs to a node of the same administrative domain or not. If the node belongs to the same administrative domain it belongs to T. Otherwise, it is uncertain whether the node is trusted or not i.e. it may or may not belong to T since it may or may not belong to 3GPP IMS. Hence this is not a complete solution.

2) A SIP node can implement TLS an operator apply suitable PKI. If a message is received over TLS, the SIP node possesses a certificate of the remote node. The management of the PKI in this case is out of scope for 3GPP. This solution does not work when the message is received without TLS as the sender of the message does the decision whether to use TLS or not.

3) The solution is based on differentiating trusted and not trusted traffic. This could be done at the Security Gateway or at an I-CSCF. It would require two logical SIP nodes, one processes trusted traffic and the other processes untrusted traffic. The Security Gateway is provisioned with rules that routes traffic received over the Zb interface to the logical trusted node, and traffic received outside the Zb interface to the node, which is not trusted. Differentiation of the trusted/untrusted traffic may be done in several ways, such us forwarding to a specific IP address or port numbers.

Outgoing traffic:

Prior to forwarding a SIP message, a SIP node belonging to the 3GPP-IMS Trust Domain needs to determine whether the next node is a trusted or untrusted node. While 3GPP does not mandate a specific mechanism, operators must make sure that the SIP nodes support at least one of the mechanisms:

1) A node can do a reverse DNS query to find out if the destination IP address belongs to a node of the same administrative domain or not. If the node belongs to the same administrative domain it belongs to T. Hence this is not a complete solution.

2) A SIP node can implement TLS and set up a TLS session towards a remote node. The exact structure of the PKI system is out of the scope of 3GPP. This solution only works the SIP node forwards SIP requests, but not for the SIP responses since it can choose the transport protocol when forwarding a SIP request but not when forwarding a SIP response since that choice is made by the originator of the request. This is an issue since TLS only works with TCP and hence cannot provide with a full solution for UDP.

5. The default privacy handling when no Privacy header field is present

The elements in the Trust Domain must support the 'id' privacy service therefore absence of a Privacy header can be assumed to indicate that the user is not requesting any privacy. However the exact details of this is under consideration in the TR for Presence Security and there are some FFS's that need to be progressed to fully cover this part of the SPEC(T).

6. That nodes in the Trust Domain are compliant to SIP

It can be assumed by SA3 that all the IMS nodes in 3GPP are compliant with SIP RFC 3261 as specified in TS23.228 and TS24.229. The security parts are specified in TS33.203, which is SIP compliant.

7. That nodes in the Trust Domain are compliant to RFC 3325

All nodes in IMS are compliant with RFC3325 (however the work is still being progressed in SA3 for Release 6).

8. Privacy handling for identity as described in Section 7 in RFC 3325

The nodes in IMS act appropriately upon the Privacy "none" and "id" tags. This requires keeping the P-Asserted-Identity header or removing it according to the procedures described in RFC 3325 [23]. However the exact details of this is under consideration in the TR for Presence Security and there are some FFS's that need to be progressed to fully cover this part of the SPEC(T).

It can be seen that from the definition of the SPEC(T) above there are some open issues still in the TR for Presence in SA3 that need to be further progressed. Furthermore some of the issues in the SPEC(T) is not under the responsibility of SA3 only since it includes also SA2 i.e. there some architectural issues that need to be resolved.

3 Conclusions

Ericsson proposes that SA3 initiates an LS to SA2 asking SA2 on the need for creating standards in more detail in order to specify how a S-CSCF can decide if it is communicating with an node within IMS or with the external Internet and clarify what solutions they foresee in relation with Clause 5.4.1 in TS23.228 from a network implementation point of view. SA2 should consider the need to do standardisation as indicated in bullet VI in clause 2.

In order to progress the work on including material on this topic Ericsson asks SA3 to approve the attached CR to TS33.203. This CR contains material that covers these aspects however not in every detail as described in part 4 in this document. However depending on the outcome of the discussions in SA3 as well as answers from SA2 Ericsson will progress this in TS33.203 such that if necessary more details are defined. It should be noted that there ~~are two~~the attached CRs assumes that some other Ericssons CR to SA3#29 on Privacy is approved. ~~attached. One that assumes that another CR on anonymity is endorsed which makes references to new clauses in TS33.203 and another, which do not make these references.~~ In the case that the CR is postponed it is proposed to view this CR as a pseudo CR to the Presence TR and that SA3 endorses to put the relevant text into the TR.

4 References

[1] IETF RFC 3325 (2002): " Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network".

3GPP TSG-SA3 Meeting #28
San Fransisco, USA, July, 2003

Tdoc ⌘S3-030456

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **5.6.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Trust Doman and the definition of SPEC(T)
Source:	⌘	Ericsson
Work item code:	⌘	IMS-ASEC
Date:	⌘	01/07/2003
Category:	⌘	**D**
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	*(GSM 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:	⌘	There is no privacy mechanism for IMS from Stage 2 point of view for Release 5. However it is proposed in another CR from Ericsson that this is incorporated in TS33.203 since this mechanism exists in Stage 3 already in Release 5. Since the privacy RFC3325 specifies that a SPEC(T) is defined this CR aims to define such SPEC(T). It should be noted that T:=3GPP-IMS by definition
Summary of change:	⌘	Introduces the SPEC(T) for 3GPP IMS in an informative annex
Consequences if not approved:	⌘	Given that the Privacy CR related to RFC3325 is approved there will be a gap in the IMS TS since the concept of the SPEC(T) is missingin the TS

Clauses affected:	⌘				
		Y	**N**		
Other specs affected:	⌘		**N**	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

Informative Annex X: SPEC(*T*)

The RFC 3325 mandates a network operator to define SPEC(*T*) that specifies the behaviour in the nodes of the network. This Annex is an informative annex which highlights how the SPEC(*T*) is implemented in 3GPP networks as well as examplifies how certain behavour could be implemented.

Note: By definition *T*:=3GPP-IMS

The nodes that beleong to the Trust Domain *T* include the P-CSCF, I-CSCF, S-CSCF, SEG the HSS and all other nodes and interfaces that belong to the operators within 3GPP IMS. Applications Servers that are provided by suppliers outside the 3GPP IMS do not belong to *T*.

1. The manner in which users are authenticated

The subscribers and users are authenticated in the S-CSCF as specified in Clause 6.1. Based on this authentication a Security Association can be created between the UE and the P-CSCF based on IK and CK derived form IMS AKA. The P-CSCF will be able to verify the claimed identity and also able to assert identities based on the integrity protection using IK and applying either HMAC-MD5 or HMAC-SHA1 of the SIP message.

2. The mechanisms used to secure the communication among nodes within the Trust Domain

The mechanism to use for SIP and IMS between nodes belonging to different security domains is the use of a SEG (Security Gateway) as specified in TS33.210 [5]. Optionally an operator could use IPsec over the Zb interface as specified in TS33.210 [5].

3. The mechanisms used to secure the communication between UAs and nodes within the Trust Domain

The UE creates a Security Association between itself and the P-CSCF as specified in Clause 7. It is mandatory to use integrity protection and the confidentiality mechanism, which is used, is between the UE and the RNC as specified in 33.102 [1].

[Editors Note: It has been agreed to put confidentiality protection into the Presence TR at IPsec level. This should be included later.]

4. The manner used to determine which hosts are parts of the Trust Domain *T*

Through the registration procedure the P-CSCF will get the name of the receiving SIP server e.g. the S-CSCF as specified in TS23.228 [3], which can be viewed as trusted, and belonging to *T* from a P-CSCF point of view. All similar mechanims as defined in TS23.228 [3] for determining hosts within 3GPP IMS are trusted and belong to *T*.

However the mechanims in TS23.228 [3] does not cover all cases e.g. when a node within *T* is receiving a SIP message, which does not belong to the same administrative domain e.g. originating from the Internet. Note: It is important to distinguish incoming traffic from outgoing traffic. There are several options possible in order to verify if a node belongs *T* or not e.g. the following approaches and/or a combination thereof (however this list does not aim to be an exhaustive list):

1. The use of TLS and a PKI
2. Implementation of the Zb interface as speficied in TS33.210 [5]
3. Dedicated I-CSCF's for the Internet access.
4. 'Trusted' and 'untrusted' interfaces in I-CSCF.
5. Physical protection measures or IP traffic filtering is applied as described in Annex J.

It is under the responsibility of the operator to choose adequate means to achieve the trust level required and ensure that the 3GPP network remains a closed network from the Trust Domain *T* point of view. The 3GPP specifications do not mandate any particular mechanism and is left as implementation and deployment choice.

5. The default privacy handling when no Privacy header field is present

The behaviour is specified in Clause 5.2 and Clause 6.5.

6. That nodes in the Trust Domain are compliant to SIP

All the IMS nodes in 3GPP are compliant with SIP RFC 3261 [6] cf. TS23.228 [3] and TS24.229 [8].

7. That nodes in the Trust Domain are compliant to RFC 3325

All nodes in IMS are compliant with RFC3325.

8. Privacy handling for identity as described in Section 7 in RFC 3325

The Privacy Handling is specified in in Clause 5.2 and Clause 6.5.

3GPP TSG-WG3 Meeting #29
San Francisco, USA, 15th–18th July 2003

Tdoc ⌘S3-030377

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.203** **CR** **CRNum** ⌘**rev** ⌘ Current version: **5.6.0** ⌘

*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:	⌘	Introducing the Privacy mechanism
Source:	⌘	Ericsson
Work item code:	⌘	IMS-ASEC
Date:	⌘	29/06/2003
Category:	⌘	**B**
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	*(GSM 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:	⌘	There is no privacy mechanism for IMS from Stage 2 point of view for Release 5. However this mechanism exists in Stage 3 already in Release 5. This CR aims to close the gap in Release 6
Summary of change:	⌘	Introduces relevant profiling of RFC3325 into IMS
Consequences if not approved:	⌘	The gap between Stage 2 and Stage 3 will remain for Release 6

Clauses affected:	⌘	2, 5, 6

	Y	N			
Other specs affected:	X		Other core specifications	⌘	TS24.229, TS24.228
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	This CR introduces the already agreed requirements in the Presence TR for Security and is directly copied from that TR with editorial changes.

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.

5.2 Subscriber anonymity

5.2.1 Initiator of a SIP dialog

The network shall hide the identity of the initiator of a SIP dialog in the following cases:

a. The initiator has requested from the network that her identity is hidden from the receiver of the request.

b. The initiator has agreed with the home network that the home network takes care of the identity blocking for certain messages on behalf of the initiator.

Anonymity shall be provided if the subscriber requests it. The network shall not deliver the message to the receiver if the initiator has set the anonymity request as ‘critical’, and the network is not able to provide the requested anonymity. The same anonymity rules shall apply to all messages within a SIP dialog.

Anonymity shall be provided by the last-hop P-CSCF. If the IMS originated messages are sent outside the IMS trust domain (e.g. to the open Internet), the edge proxy (e.g. I-CSCF) shall provide the anonymity.

Anonymity may be requested with multimedia sessions, or with any other services that will use IMS, such as Presence or Instant Messaging.

5.2.2 Receiver of a SIP dialog initiation request

The receiver of a SIP dialog initiation request is able to have some degree of anonymity if she registers a pseudonym as IMPU. In this case, the subscriber shall be responsible for not revealing the relationship between the pseudonym IMPU and her real identity to unauthorized parties. If she reveals her real identity, there is no anonymity

6 Security mechanisms

6.1 Authentication and key agreement

The scheme for authentication and key agreement in the IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. Figure 1. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. [3]. The HSS and the ISIM share a long-term key associated with the IMPI.

The HN shall choose the IMS AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g. keys generated by the IMS AKA scheme are transported by SIP.

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. The ISIM and the HSS keep track of counters SQN_{ISIM} and SQN_{HSS} respectively. The requirements on the handling of the counters and mechanisms for sequence number management are specified in [1]. The AMF field can be used in the same way as in [1].

Furthermore a security association is established between the UE and the P-CSCF. The subscriber may have several IMPUs associated with one IMPI. These may belong to the same or different service profiles. Only one SA shall be active between the UE and the P-CSCF. This single SA shall be updated when a new successful authentication of the subscriber has occurred, cf. section 7.4.

It is the policy of the HN that decides if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles. Regarding the definition of service profiles cf. [3].

6.1.1 Authentication of an IM-subscriber

Before a user can get access to the IM services at least one IMPU needs to be registered and the IMPI authenticated in the IMS at application level. In order to get registered the UE sends a SIP REGISTER message towards the SIP registrar server i.e. the S-CSCF, cf. Figure 1, which will perform the authentication of the user. The message flows are the same regardless of whether the user has an IMPU already registered or not.

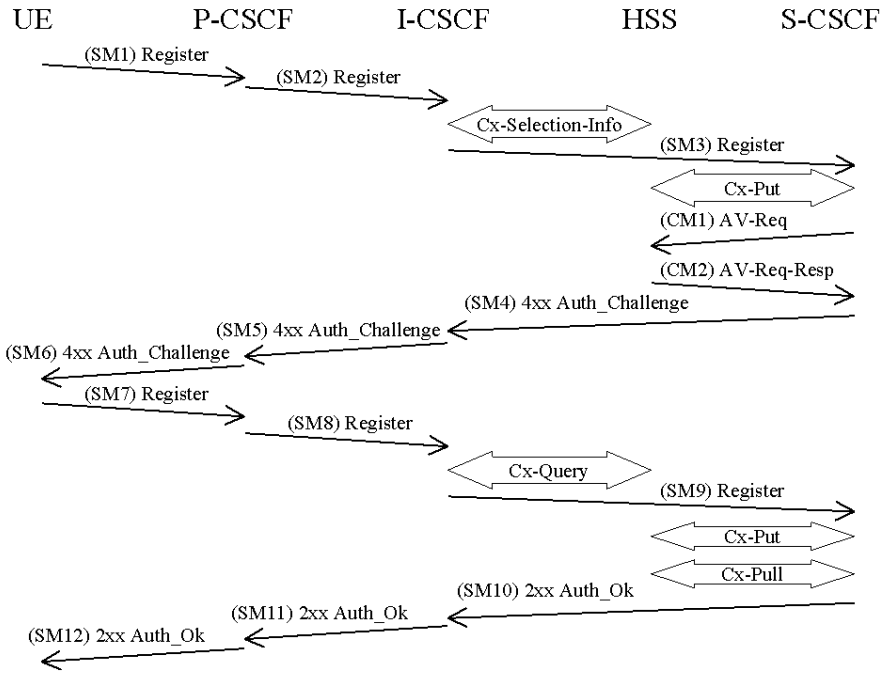


Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

The detailed requirements and complete registration flows are defined in [8] and [11].

SMn stands for SIP Message n and CMm stands for Cx message m which has a relation to the authentication process:

SM1:
REGISTER(IMPI, IMPU)

In SM2 and SM3 the P-CSCF and the I-CSCF respectively forwards the SIP REGISTER towards the S-CSCF.

After receiving SM3, if the IMPU is not currently registered at the S-CSCF, the S-CSCF needs to set the registration flag at the HSS to initial registration pending. This is done in order to handle mobile terminated calls while the initial registration is in progress and not successfully completed. The registration flag is stored in the HSS together with the S-CSCF name and user identity, and is used to indicate whether a particular IMPU of the user is unregistered or registered at a particular S-CSCF or if the initial registration at a particular S-CSCF is pending. The registration flag is set by the S-CSCF sending a Cx-Put to the HSS. If the IMPU is currently registered, the S-CSCF shall leave the registration flag set to *registered.* At this stage the HSS has performed a check that the IMPI and the IMPU belong to the same user.

Upon receiving the SIP REGISTER the S-CSCF CSCF shall use an Authentication Vector (AV) for authenticating and agreeing a key with the user. If the S-CSCF has no valid AV then the S-CSCF shall send a request for AV(s) to the HSS in CM1 together with the number m of AVs wanted where m is at least one.

CM1:
Cx-AV-Req(IMPI, m)

Upon receipt of a request from the S-CSCF, the HSS sends an ordered array of *n* authentication vectors to the S-CSCF using CM2. The authentication vectors are ordered based on sequence number. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the S-CSCF and the IMS user.

CM2:
Cx-AV-Req-Resp(IMPI, RAND1||AUTN1||XRES1||CK1||IK1,….,RANDn||AUTNn||XRESn||CKn||IKn)

When the S-CSCF needs to send an authentication challenge to the user, it selects the next authentication vector from the ordered array, i.e. authentication vectors in a particular S-CSCF are used on a first-in / first-out basis.

The S-CSCF sends a SIP 4xx Auth_Challenge i.e. an authentication challenge towards the UE including the challenge RAND, the authentication token AUTN in SM4. It also includes the integrity key IK and the cipher key CK for the P-CSCF. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of authenticate challenge.

The verification of the SQN by the USIM and ISIM will cause the UE to reject an attempt by the S-CSCF to re-use a AV. Therefore no AV shall be sent more than once.

NOTE: This does not preclude the use of the normal SIP transaction layer re-transmission procedures.

SM4:
4xx Auth_Challenge(IMPI, RAND, AUTN, IK, CK)

When the P-CSCF receives SM5 it shall store the key(s) and remove that information and forward the rest of the message to the UE i.e.

SM6:
4xx Auth_Challenge(IMPI, RAND, AUTN)

Upon receiving the challenge, SM6, the UE takes the AUTN, which includes a MAC and the SQN. The UE calculates the XMAC and checks that XMAC=MAC and that the SQN is in the correct range as in [1]. If both these checks are successful the UE calculates the response, RES, puts it into the Authorization header and sends it back to the registrar in

SM7. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of the response. It should be noted that the UE at this stage also computes the session keys CK and IK.

SM7:
REGISTER(IMPI, RES)

The P-CSCF forwards the RES in SM8 to the I-CSCF, which queries the HSS to find the address of the S-CSCF. In SM9 the I-CSCF forwards the RES to the S-CSCF.

Upon receiving SM9 containing the response, the S-CSCF retrieves the active XRES for that user and uses this to check the response sent by the UE as described in Draft-ietf-sip-digest-aka-01 [17]. If the check is successful then the user has been authenticated and the IMPU is registered in the S-CSCF. If the IMPU was not currently registered, the S-CSCF shall send a Cx-Put to update the registration-flag to *registered*. If the IMPU was currently registered the registration-flag is not altered.

It shall be possible to implicitly register IMPU(s). The implicitly registered IMPU(s) all belong to the same Service Profile. All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S-CSCF and subsequently to the P-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

When an IMPU has been registered this registration will be valid for some period of time. Both the UE and the S-CSCF will keep track on a timer for this purpose but the expiration time in the UE is smaller than the one in the S-CSCF in order to make it possible for the UE to be registered and reachable without interruptions. A successful registration of a previously registered IMPU (including implicitly registered IMPUs) means the expiry time of the registration is refreshed.

It should be noted that the UE initiated re-registration opens up a potential denial-of-service attack. That is, an attacker could try to register an already registered IMPU and respond with the wrong RES and in order to make the HN de-register the IMPU. For this reason a subscriber should not be de-registered if it fails an authentication. It shall be defined by the policy of the operator when successfully registered IMPU(s) are to be de-registered.

The lengths of the IMS AKA parameters are specified in chapter 6.3.7 in [1].

6.1.2 Authentication failures

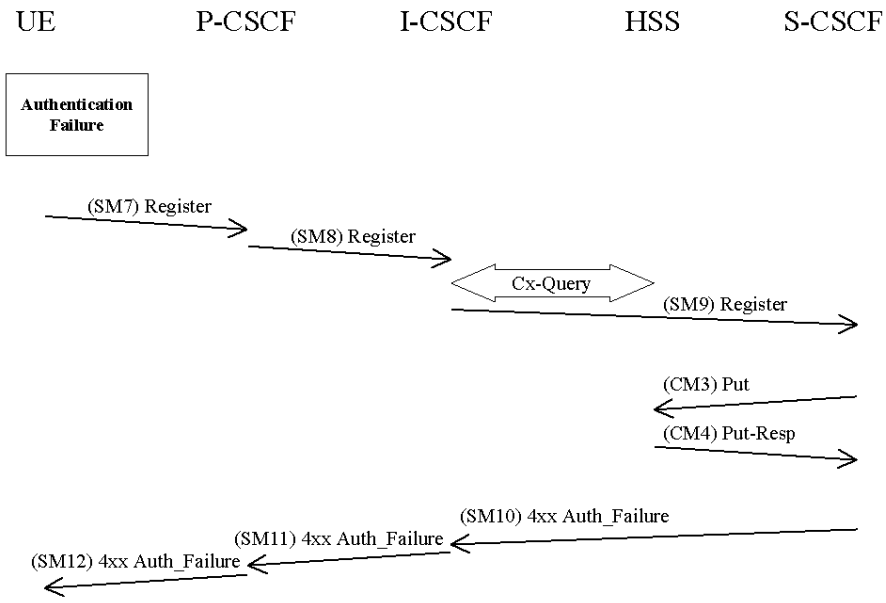
6.1.2.1 User authentication failure

In this case the authentication of the user should fail at the S-CSCF due an incorrect response (received in SM9). However, if the response is incorrect, then the IK used to protect SM7 will normally be incorrect as well, which will normally cause the integrity check at the P-CSCF to fail before the response can be verified at S-CSCF. In this case SM7 is discarded by the IPsec layer at the P-CSCF.

If the integrity check passes but the response is incorrect, the message flows are identical up to and including SM9 as a successful authentication. Once the S-CSCF detects the user authentication failure it should proceed in the same way as having received SM9 in a network authentication failure (see clause 6.1.2.2).

6.1.2.2 Network authentication failure

In this section the case when the authentication of the network is not successful is specified. When the check of the MAC in the UE fails the network can not be authenticated and hence registration fails. The flow is identical as for the successful registration in 6.1.1 up to SM6.



The UE shall send a Register message towards the HN including an indication of the cause of failure in SM7. The P-CSCF and the I-CSCF forward this message to the S-CSCF.

SM7:
REGISTER(Failure = *AuthenticationFailure*, IMPI)

Upon receiving SM9, which includes the cause of authentication failure, the S-CSCF shall set the registration-flag in the HSS to *unregistered*, if the IMPU is not currently registered. To set the flag the S-CSCF sends in CM3 a Cx-Put to the HSS. If the IMPU is currently registered, the S-CSCF does not update the registration flag.

CM3:
Cx-AV-Put(IMPI, Clear S-CSCF name)

The HSS responds to CM3 with a Cx-Put-Resp in CM4.

In SM10 the S-CSCF sends a 4xx Auth_Failure towards the UE indicating that authentication has failed, no security parameters shall be included in this message.

SM10:
SIP/2.0 4xx Auth_Failure

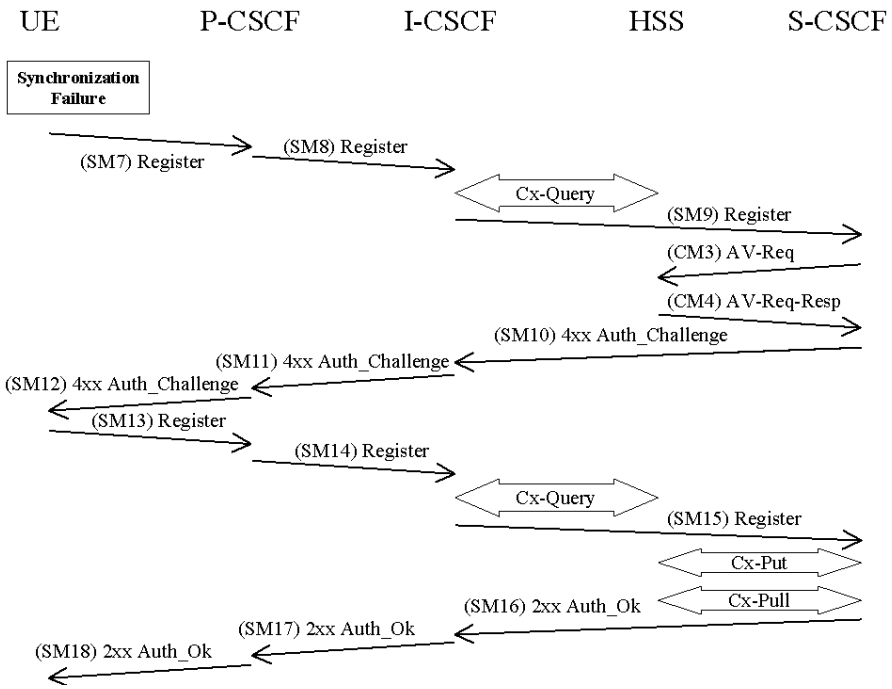
Upon receiving SM10 the I-CSCF shall clear any registration information related to the IMPI.

6.1.2.3 Incomplete authentication

If the S-CSCF does not receive a response to an authentication within an acceptable time, it considers the authentication to have failed. If the IMPU was not already registered, the S-CSCF shall send a Cx-Put to the HSS to set the registration-flag for that IMPU to unregistered (see message CM3 in clause 6.1.2.2). If the IMPU was already registered, the S-CSCF does not change the registration-flag.

6.1.3 Synchronization failure

In this section the case of an authenticated registration with synchronization failure is described. After re-synchronization, authentication may be successfully completed, but it may also happen that in subsequent attempts other failure conditions (i.e. user authentication failure, network authentication failure) occur. In below only the case of synchronization failure with subsequent successful authentication is shown. The other cases can be derived by combination with the flows for the other failure conditions.



The flow equals the flow in 6.1.1 up to SM6. When the UE receives SM6 it detects that the SQN is out of range and sends a synchronization failure back to the S-CSCF in SM7. Draft-ietf-sip-digest-aka-01 [17] describes the fields to populate corresponding parameters of synchronization failure.

SM7:
REGISTER(Failure = *Synchronization Failure,* AUTS, IMPI*)*

Upon receiving the *Synchronization Failure* and the AUTS the S-CSCF sends an Av-Req to the HSS in CM3 including the required number of Avs, m.

CM3:
Cx-AV-Req(IMPI, RAND,AUTS, m)

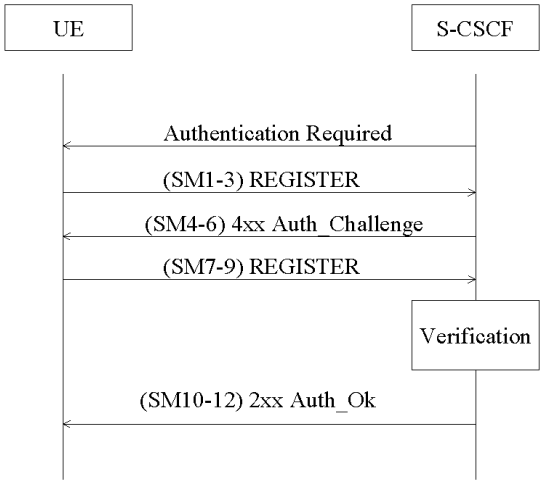
The HSS checks the AUTS as in section 6.3.5 in [1]. After potentially updating the SQN, the HSS sends new AVs to the S-CSCF in CM4.

CM4:
Cx-AV-Req-Resp(IMPI, n,$RAND_1$||$AUTN_1$||$XRES_1$||CK_1||IK_1,….,$RAND_n$||$AUTN_n$||$XRES_n$||CK_n||IK_n)

The rest of the messages i.e. SM10-SM18 including the Cx messages are exactly the same as SM4-SM12 and the corresponding Cx messages in 6.1.1.

6.1.4 Network Initiated authentications

In order to authenticate an already registered user, the S-CSCF shall send a request to the UE to initiate a re-registration procedure. When received at the S-CSCF, the re-registration shall trigger a new IMS AKA procedure that will allow the S-CSCF to re-authenticate the user.



Both the UE and the P-CSCF shall shorten the lifetime of the old SA pair generated from the last successful authentication, so as to guarantee that the new SA pair shall be used.

The UE shall initiate the re-registration on the reception of the Authentication Required indication. In the event that the UE does not initiate the re-registration procedure after the request from the S-CSCF, the S-CSCF may decide to de-register the subscriber or re-issue an Authentication-Required.

6.1.5 Integrity protection indicator

In order to decide whether a REGISTER request from the UE needs to be authenticated, the S-CSCF needs to know about the integrity protection applied to the message. The P-CSCF attaches an indication to the REGISTER request to inform the S-CSCF that the message was integrity protected if:

- the P-CSCF receives a REGISTER containing an authentication response and the message is protected with the SA created during this authentication procedure; or

- the P-CSCF receives a REGISTER not containing an authentication response and the message is protected with the SA created by latest successful authentication (from the P-CSCF perspective).

For all other REGISTER requests the P-CSCF attaches an indication that the REGISTER request was not integrity protected or ensures that there is no indication about integrity protection in the message.

6.2 Confidentiality mechanisms

No confidentiality mechanism is provided in this specification, cf. clause 5.1.3.

6.3 Integrity mechanisms

IPsec ESP as specified in reference [13] shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. IPSec ESP general concepts on Security Policy management, Security Associations and IP traffic processing as described in reference [14] shall also be considered. ESP integrity shall be applied in transport mode between UE and P-CSCF.

The method to set up ESP security associations (SAs) during the SIP registration procedure is specified in clause 7. As a result of the registration procedure, a pair of unidirectional SAs between the UE and the P-CSCF, shared by TCP and UDP, shall be established in the P-CSCF and later in the UE. One SA is for traffic from the UE to the P-CSCF (inbound SA at the P-CSCF) and the other SA is for traffic from the P-CSCF to the UE (outbound SA at the P-CSCF).

The integrity key IK_{ESP} is the same for the two simultaneously established SAs. The integrity key IK_{ESP} is obtained from the key IK_{IM} established as a result of the AKA procedure, specified in clause 6.1, using a suitable key expansion function. This key expansion function depends on the ESP integrity algorithm and is specified in Annex I of this specification.

The integrity key expansion on the user side is done in the UE. The integrity key expansion on the network side is done in the P-CSCF.

The anti-replay service shall be enabled in the UE and the P-CSCF on all established SAs.

6.4 Hiding mechanisms

The Hiding Mechanism is optional for implementation. All I-CSCFs in the HN shall share the same encryption and decryption key Kv. If the mechanism is used and the operator policy states that the topology shall be hidden the I-CSCF shall encrypt the hiding information elements when the I-CSCF forwards SIP Request or Response messages outside the hiding network's domain. The hiding information elements are entries in SIP headers, such as Via, Record-Route, Route and Path, which contain addresses of SIP proxies in hiding network. When I-CSCF receives a SIP Request or Response message from outside the hiding network's domain, the I-CSCF shall decrypt those information elements that were encrypted by I-CSCF in this hiding network domain.

The purpose of encryption in network hiding is to protect the identities of the SIP proxies and the topology of the hiding network. Therefore, an encryption algorithm in confidentiality mode shall be used. The network hiding mechanism will not address the issues of authentication and integrity protection of SIP headers. The AES in CBC mode with 128-bit block and 128-bit key shall be used as the encryption algorithm for network hiding. In the CBC mode under a given key, if a fixed IV is used to encrypt two same plaintexts, then the ciphertext blocks will also be equal. This is undesirable for network hiding. Therefore, random IV shall be used for each encryption. The same IV is required to decrypt the information. The IV shall be included in the same SIP header that includes the encrypted information.

6.5 Subscriber anonymity mechanisms

6.5.1 Anonymity of SIP dialog initiator

The anonymity mechanism is optional for implementation in UA. The UA may provide anonymity for the subscriber following the privacy mechanisms described in [22] and [23]. This includes populating the SIP headers with values that reflect the privacy requirements of the subscriber, as well as requesting further privacy from the network.

The UA may use the following priv-value types of the Privacy header in [22] and [23]:

c. 'none'

d. 'id'

e. 'critical'

f. 'user'

[Editors note:priv-value types 'header' and 'session' are FFS.]

The home network (e.g. S-CSCF or an Application Server) may provide the anonymity on behalf of the UA using the following priv-value type [22]:

g. ‘user’

P-CSCF and the edge proxy (e.g. I-CSCF) must implement the following priv-value types of the Privacy header in [22] and [23]:

h. ‘none’

i. ‘id’

j. ‘critical’

k. ‘user’

[Editors note:priv-value types ‘header’ and ‘session’ are FFS.]

P-CSCF and the edge proxy shall monitor the privacy requests in all terminating SIP requests, and provide the requested privacy (e.g. hide the identity of the subscriber). P-CSCF and the edge proxy shall not provide privacy for originating SIP requests.

6.5.2 Pseudonym IMPU

Subscriber may use pseudonym IMPU to obtain some degree of anonymity towards other end users. From system point of view, the pseudonym IMPU is like any other IMPU. All existing rules related IMPUs shall apply.

Note: Unprotected SIP REGISTER messages include identity information that may be intercepted by unauthorized parties when sent over the air-interface. These messages may be used to combine the IMPU and IMPI information, and consequently this information may reveal the parallel IMPUs related to the pseudonym IMPU.

[Editors note: There may be a need for additional rules related to the registration of pseudonym IMPUs.]

[Editors Note: It FFS if the term anonymity is the best in this context since it has a different meaning in IETF where anonymity means that the user is hiding everything from the rest world.]