3GPP TSG SA WG3 Security S3z000023

Ad-hoc meeting S3#15bis

Munich, 8 - 9 November, 2000

Source:	Siemens AG
Title:	Comments on 3G TR 33.8xx and 3G TR 33.800
Document for:	Discussion and decision
Work item:	Access security for IP-based services (Release 5), Principles for Network Domain Security (Release 4/5)
Agenda item:	tbd

Abstract

This contribution proposes changes to the draft 3G TR 33.8xx, v0.2.0 "Access security for IP-based services (Release 5)" and to the draft 3G TR 33.800 v0.2.4 "Principles for Network Domain Security (Release 4/5)".

1 Proposed changes to [TR 33.8xx], v0.2.0

General: "Release 2000" should be replaced with "Release 5".

Section 7.2 of [TR 33.8xx]:

It is proposed to replace the following text beginning with the second paragraph

„The entities that need to be authenticated mutually are the UE, the serving CSCF and the HSS. The serving CSCF will get subscriber data from the HSS that shall not be disclosed. Note that the serving CSCF for a roaming user may, depending on the policy of the home network operator, be located in the visited network.

[Editors Note: Do we need to authenticate the Proxy CSCF?]

The following features are provided:

1. *Authentication mechanism agreement i.e. the user and the serving CSCF negotiates what authentication algorithm and authentication key they shall use*
2. *User authentication i.e. the serving CSCF verifies the identity of the user*
3. *Serving CSCF authentication i.e. the user verifies that the HSS of the home network has a trust relationship with the serving CSCF"*

with

„The entities that need to be authenticated mutually are the UE and the HSS represented by the P-CSCF. The P-CSCF gets authentication information from the HSS. The communication between the P-CSCF and the HSS shall be secured with IPsec according to [3G TS 33.1de, Network Domain Security].

The following features are provided:

1. *User authentication where the P-CSCF verifies the identity of the user*
2. *Network authentication where the user authenticates the HSS and verifies that the HSS of the home network has a trust relationship with the P-CSCF"*

Justification of the proposed changes:

- As noted in section 9.1 of [TR 33.8xx] it is not clear that the S-CSCF entity will perform the IMS AKA with the user. With the reasons given in [S3z000022] we see the P-CSCF of the visited network as the network entity that shall perform the IMS AKA with the user.
- No authentication algorithm negotiation takes place before an authentication is performed, in analogy to the use of the UMTS AKA in the UMTS CS- and PS-domains.

Section 7.3 of [TR 33.8xx]:

It is proposed to replace the following text beginning with the first paragraph

„*The SIP signalling data may be confidentiality protected end-to-end between the UE and serving CSCF (this is an option). The payload may get some protection on the underlying layers e.g. by IPSec.*

The features that are provided end-to-end between the UE and the serving CSCF are cipher algorithm agreement, cipher key agreement and confidentiality of the signalling data (as an option)."

with

„*The SIP signalling data may be confidentiality protected end-to-end between the UE and P-CSCF (as an option). Confidentiality protection between IM Subsystem nodes (including P-CSCF, I-CSCF, S-CSCF and HSS) may be provided by IPsec according [TS 33.1de].The features that are provided between the UE and the P-CSCF are negotiation of confidentiality related security capabilities, cipher key establishment and confidentiality of the signalling data.*"

Justification of the proposed changes:

- End-to-end confidentiality protection should not happen between the UE and the S-CSCF, since the S-CSCF can be located in the home network, and, hence, this requirement may conflict with legal interception requirements, cf. also [S3z000022].

Section 7.4 of [TR 33.8xx]:

It is proposed to replace the following text beginning with the first paragraph

„*The SIP signalling data shall be integrity protected end-to-end between the UE and serving CSCF. The payload may get some protection on the underlying layers e.g. by IPSec.*

The features that are provided end-to-end between the UE and the serving CSCF are integrity algorithm agreement, MAC key agreement and integrity of the signalling data."

with

„*The SIP signalling data shall be integrity protected between the UE and P-CSCF. The integrity protection of the communication between IM Subsystem nodes (including P-CSCF, I-CSCF, S-CSCF and HSS) shall be provided by IPsec according [TS 33.1de].The features that are provided between the UE and the P-CSCF are negotiation of integrity related security capabilities, integrity key establishment and integrity of the signalling data.*"

Justification of the proposed changes:

-

- The S-CSCF can be located in the home network. End-to-end integrity protection between UE and S-CSCF is not a requirement, it is sufficient to provide hop-by-hop integrity protection between UE

and P-CSCF on the one hand and between IM Subsystem nodes (including P-CSCF, I-CSCF, S-CSCF and HSS) on the other hand because the involved IM Subsystem nodes have to trust each other, cf. also [S3-z000022].

- The security for IP-based communication in the UMTS core network will be defined by the SA3 work item "network domain security". The provision of integrity and confidentiality between IM Subsystem nodes is considered a special case of UMTS core network security.

2 Proposed changes to [TR 33.800]

In section 5.5.1 it is stated that the key management functionality is logically separate from that of a Security Gateway (SEG). Since there is a contradiction to some parts of section 5.2, we propose the following changes to [TR 33.800]:

Section 5.2.2.1 of [TR 33.800]:

It is proposed to remove the following part of this section from the document:

"It is proposed that the SEG should be considered an entity evolved from the Key Administration Center, KAC, previously introduced (see S3-000432) to handle the key management procedures needed for secure MAP communications. With this in mind one is able to distinguish two separate functional blocks of the SEG:

1. *The inherited KAC as being defined in (this) TR 33.800. This block is responsible for negotiation, establishment and maintenance of Security Associations, SAs, valid for the node-to-node MAP message protection mechanism.*
2. *A second IKE/IPsec compliant security mechanism (defined in IETF RFCs 2401-2412). This block is responsible for the negotiation, establishment and maintenance of different "external" SAs. There can be more than one SA set up towards any specific network. If allowed by the operator-defined policies, SAs might also be set up directly towards external hosts, servers or terminals.*"

Section 5.2.3 of [TR 33.800]:

It is proposed to change the notion "SGW" to "SEG" in the first sentence.

For the reasons given above it is proposed to remove the fourth bullet of the list given in this section.

„The point for key management as well as policy enforcement in this architecture is centralized, i.e. in the SEG(s), which makes operation and maintenance easier to handle."

Chapter 6/7 of [TR 33.800]:

As outlined in [S3-z000021] for MAP security the negotiation of security associations by using IKE together with a newly defined MAPSec DOI may not be the right approach. This should be reflected by the chapters 6 and 7 of [TR 33.800].

3 References

[S3-z000021] 3GPP TSG SA WG3 Security, S3-z000021: *SA negotiation protocol for the Z_A interface; Source Siemens;* contribution to the ad-hoc meeting S3#15bis, Munich, 8th - 9th November 2000.

[S3-z000022] 3GPP TSG SA WG3 Security, S3-z000022: *IMS authentication and integrity/ confidentiality protection; Source Siemens;* contribution to the ad-hoc meeting S3#15bis, Munich, 8th - 9th November 2000.

[TR 33.8xx] 3GPP TSG SA WG3 Security, TR 33.8xx: "Access security for IP-based services (Release 2000)"; v 0.2.0, October 2000.

[TR 33.800] 3GPP TSG SA WG3 Security, TR 33.800: “Principles for Network Domain Security (Release 4/5)”, v 0.2.4, October 2000.

[TS 33.1de] 3GPP TSG SA WG3 Security, *TS 33.1de, “Network Domain Security, v0.0.1, October 2000.*