3GPP TSG SA WG3 Security **S3-010629**

November 27-30, 2001

Sophia Antipolis, France

Agenda Item: TBD

Source: Ericsson

Title: P-CSCF resides in the home network

Document for: Discussion and decision

1. Scope and objectives

According to [TS33.203] the P-CSCF resides in the visited network only. However two change requests have been approved in SA2 that clarifies that the P-CSCF may be in the home network, cf. [S2-012618] and [S2-012774]. This contribution aims for updating the [TS33.203] accordingly.

2 Background

The VPLMN has very limited control over the choice of GGSN and the GGSN might be in a different network to the VPLMN. When the GGSN is in a different network to the VPLMN it is a difficult problem for the GGSN to know the addresses of all P-CSCFs in all different VPLMNs. Therefore SA2 has concluded that it is not practical to have the P-CSCF in a different network to the GGSN. This means that if the GGSN is in the HN then the P-CSCF shall also be in the home network.

5 Changes Needed to TS33.203

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. The ISIM is responsible for the handling of keys, SQN etc that are tailored to IMS. The security parameters handled by the ISIM are independent of the similar security parameters that exist in the USIM.

Although ISIM and USIM are logically independent, all the following cases are possible for implementation:

- ISIM and USIM are implemented as a single application inside one UICC
- ISIM and USIM are implemented as two distinct applications inside one UICC
- ISIM and USIM are implemented inside two distinct UICCs.

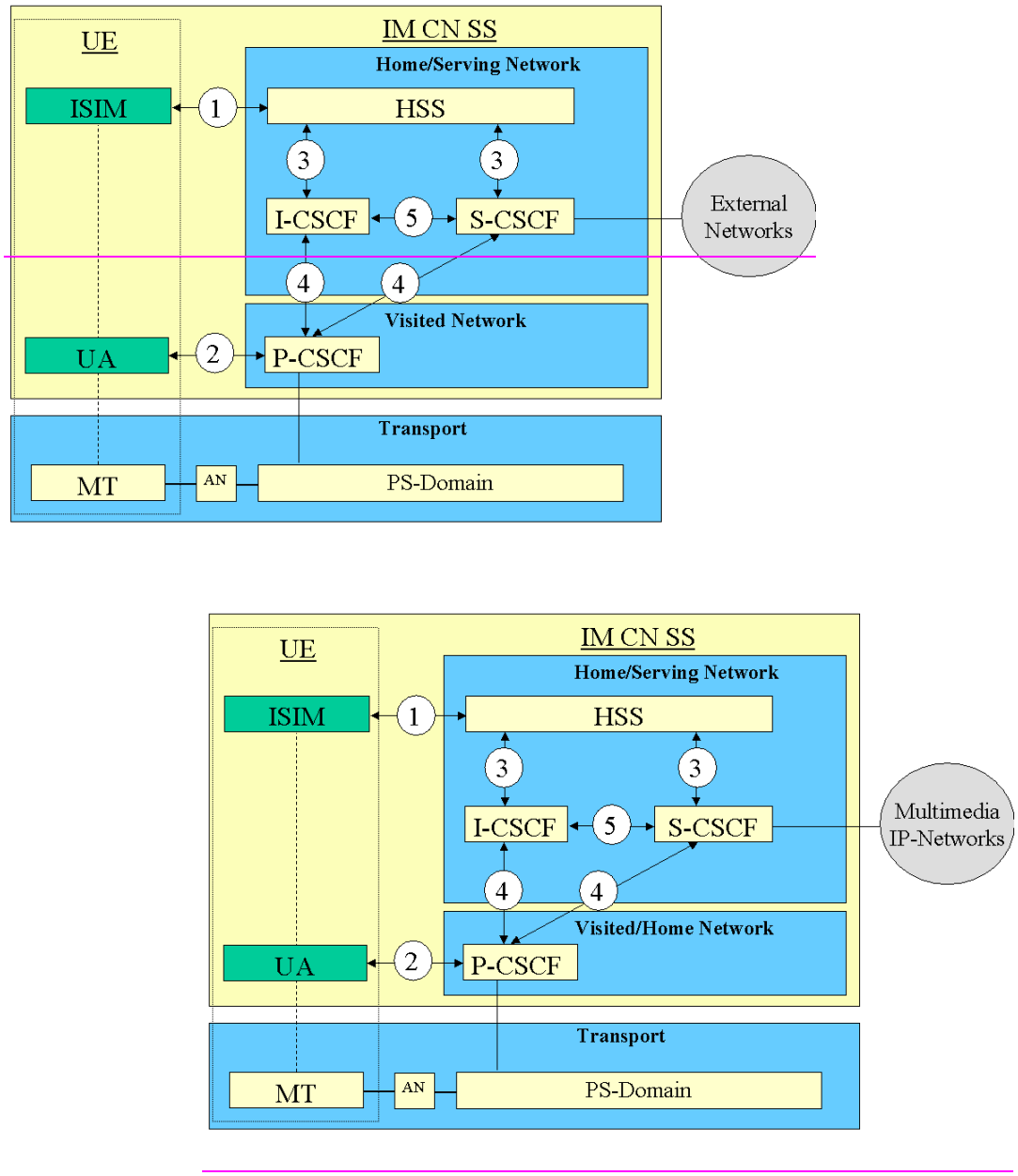

Figure 1. The IMS security architecture

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 several IMS identities i.e. the IMPI and at least one IMPU. The HN authenticates the IMPI.

2. Provides a secure link and a security association between the UE and a P-CSCF.

3. Provides security within the network domain internally for the Cx-interface. This security association is covered by TS 33.210 [5].

4. Provides security between different networks for SIP capable nodes. This security association is covered by TS 33.210 [5].

5. Provides security within the network internally between SIP capable nodes. This security association is covered by TS 33.210 [5].

[Editors Note: Security measures for application servers (OSA and SIP AS) and IM SSF is FFS but it seems that this is covered by NDS]

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 depending on where the GGSN resides. An overview of these two cases is given below.

1. P-CSCF in the Visited Network:

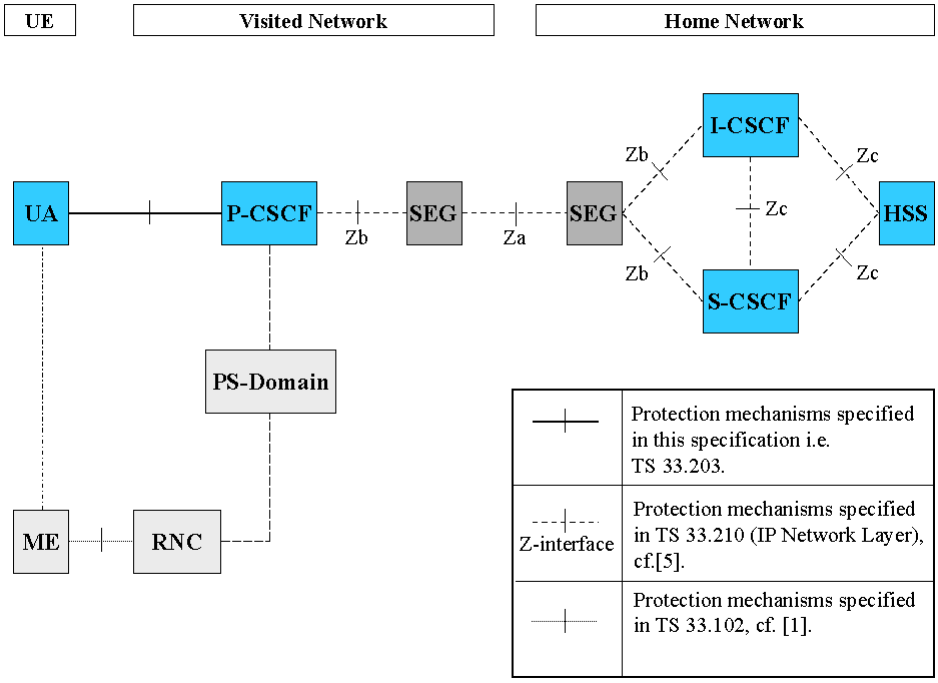

Figure 2. This figure gives an overview of the security architecture for IMS when the P-CSCF resides in the VN and the relation with Network Domain security, cf. [5].

2. P-CSCF in the Home Network:

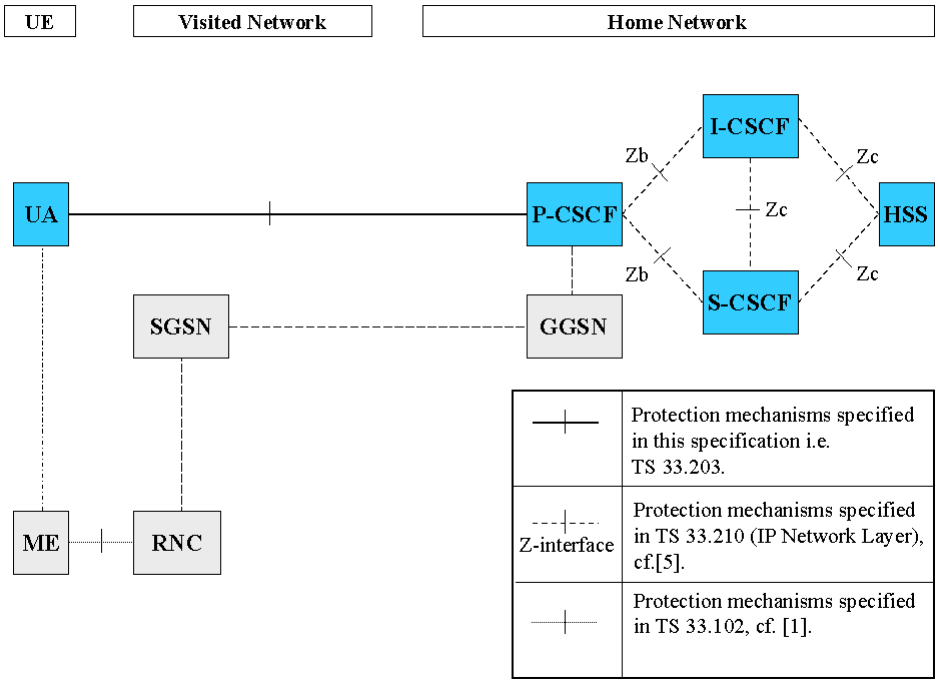

Figure 3. This figure gives an overview of the security architecture for IMS when the P-CSCF resides in the HN and the relation with Network Domain security, cf. [5].

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 specified in [5].

References

[TS33.203] 3GPP TSG SA WG3, TS 33.203, Release 5, Access security for IP-based services, Core Network Subsystem Stage 2; v0.7.0, November 2001

[S2-012618] 3GPP SA WG SA2 Architecture: TDOC S2-012618 '*P-CSCF in same network as GGSN*' Vodafone, October 2001

[S2-012774] 3GPP SA WG SA2 Architecture: TDOC S2-012774 '*GGSN & P-CSCF in the HPLMN*' Vodafone&Ericsson, October 2001