3GPP TSG SA WG3 Security — S3#20 **S3-010536**

16 - 19 October, 2001

Sydney, Australia

3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010118**

14 September, 2001

Sophia Antipolis, France

Source: **Hutchison 3G UK**

Title: **Confidentiality of SIP signalling between UE and P-CSCF**

Document for: **Discussion/Decision**

Agenda Item:

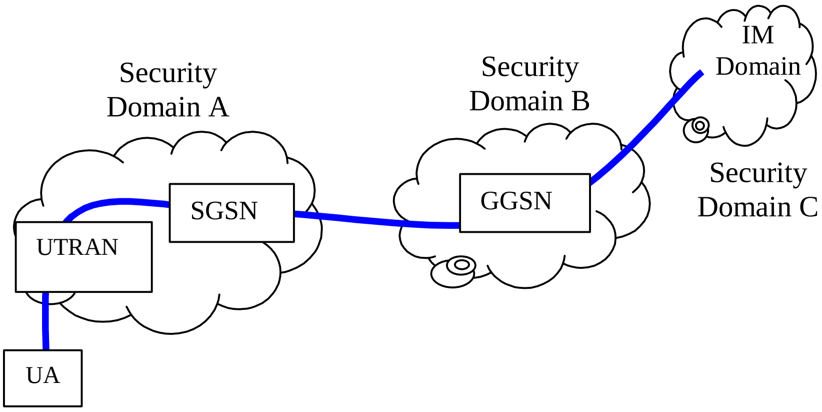
Introduction

This document proposes that aSIP security (i.e. IMS access network security) should be independent from NDS. Further, no reliance on NDS should be assumed. The document 33.203 should reflect this viewpoint.

Problems with relying on NDS for confidentiality

1) Loss of access network independence: To have the option of confidentiality, the user must be using a 3G network to access IM services. Furthermore that network must have an IM domain or at a minimum recognise the mechanism to protect SIP signalling (not all networks would be upgraded at the same time). This does not follow the basic principle that services should be transparent to the transport network. Whether confidentiality is applied should depend entirely on the IM domain and not rely on the access network. We do not want to be in the same position as with MAP that requires everyone to have updated their network before we can guarantee to provide security.

2) It may be the case that the IMS Access Network encompasses more than one security domain. In particular, the SGSN and GGSN may not be in the same UMTS network. This could happen if the visited UMTS network does not have an IM domain, or when the home network routes PS connections back to a home GGSN. This scenario is implicitly excluded by Figure 2.



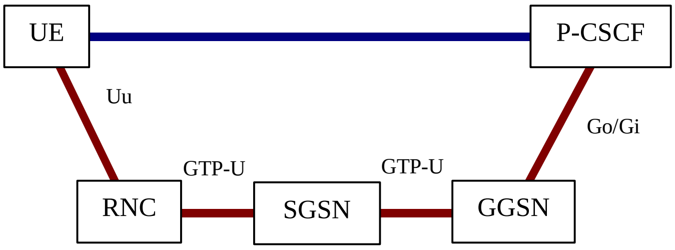
3) Amount of ciphering: Encryption/decryption between the following is needed to provide confidentiality between the UE and the P-CSCF:

Encryption between UE and RNC (probably already performed).

Encryption on GTP-U/GTP-IC between the RNC and SGSN and between the SGSN and GGSN.

Encryption on Gi/Go between GGSN and PCF/P-CSCF. NDS would have to be extended to the Gi/Go interface (this shouldn't be a major issue).

This seems to be an excessive amount of ciphering.



The solution to these concerns is to provide confidentiality between UE and P-CSCF at the SIP or upper IP layer (i.e. UE and P-CSCF terminate the encryption). This fits in better with the concept of the IM domain being independent of the PS domain. The encryption key Ckim, which is already negotiated during the IM authentication could be used. Since we are applying the integrity mechanism at the UE and P-CSCF, confidentiality could be applied at the same level without much more effort.

The only disadvantage is that this is putting more work onto the UE, i.e. it is now responsible for both integrity and ciphering (currently optional). This is a small disadvantage compared to the disadvantages given above for using NDS to provide the security.

Conclusion

In conclusion we believe the only viable place to provide confidentiality for SIP signalling is at the UE and P-CSCF, not hop by hop at the intervening network elements. No security in the UMTS CN can be assumed. We propose that this should be the SA3 position.

Actions Required

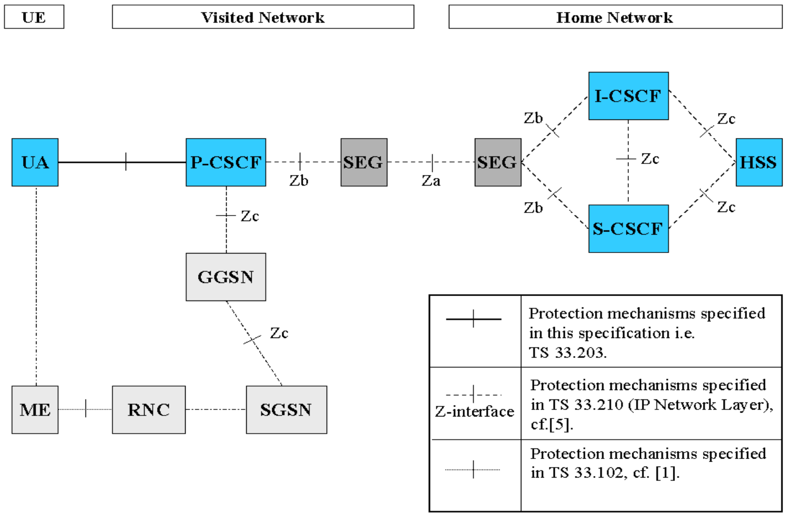
If this is agreed for SA3, the following are required:

1. The method to provide integrity should easily extend to provide confidentiality.

2. The following changes (or something similar) will be needed to TS 33.203.

Section 4 Overview of security architecture

Figure 2 (below) – Remove the UMTS network from Figure 2. We consider the inclusion of the UMTS network to be confusing and misleading. Inclusion of the Zc labels gives the impression that security mechanisms in UMTS CN NDS are used in aSIP.


UE
Visited Network
Home Network
I-CSCF
Zb
Zc
UA
P-CSCF
SEG
SEG
Zc
HSS
Zb
Za
Zb
Zc
S-CSCF
Zc
GGSN
Zc
ME
RNC
SGSN
Protection mechanisms specified in this specification i.e. TS 33.203.
Z-interface
Protection mechanisms specified in TS 33.210 (IP Network Layer), cf.[5].
Protection mechanisms specified in TS 33.102, cf. [1].

Section 5.1.2 Confidentiality protection.

Inclusion of a description of UMTS access security is out of context and misleading because it should not affect aSIP security. The phrase “protection for SIP signaling can either rely on the confidentiality mechanisms provided by UMTS and mechanisms provided by Network Domain Security” suggests that NDS is used in IMS access.

A proposed rewording of section 5.1.2 is:

> Confidentiality protection shall optionally be used between the UA and the P-CSCF. If it is provided, then it shall be as specified in section 6.2. The UA and P-CSCF shall negotiate what confidentiality algorithm shall be used for the session and shall agree on a confidentiality key CK_{IM}. IP-based services cannot rely on confidentiality being provided in the access network.
>
> Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [5].

Section 6.2 Confidentiality Mechanisms

This section should specify which cipher algorithms can be used between UA and P-CSCF. No mention should be made of UMTS access security or NDS.