3GPP TSG SA WG3 Security — S3#16 **S3-000699**

28-30 November, 2000

Sophia-Antapolis, France

Agenda Item: -

Source: Ericsson

Title: Authentication and protection mechanisms for IM CN SS

Document for: Discussion and decision

1 Scope and objectives

The scope for this document is to define mechanisms and trust relations for secure access to IM CN SS, IP Multimedia Core Network subsystem, in UMTS. It is an updated version of S3z000010. The IM CN SS in UMTS will support IP Multimedia applications such as video, audio and multimedia conferences. 3GPP has chosen SIP, Session Initiation Protocol as the signalling protocol for creating and terminating Multimedia sessions. No true end-to-end protection mechanism is provided in this document however cf. e.g. the IETF-draft draft-blom-rtp-encrypt-00.txt which describes a method for RTP Encryption for 3G Networks, see also the discussion chapter in this document.

The following are proposed in the document:

1. An authentication mechanism for IM CN SS according to the following principles
    - Re-use of UMTS AKA concept
    - Authentication performed in the HSS/AAA
2. A scheme, including Key Management, for protection of man-in-the-middle attack in IM CN SS
    - Confidentiality protection between the UE and the P-CSCF (Optional)
    - Integrity protection between the UE and the S-CSCF (Mandatory)
    - Inter operator protection by using the SEG and IPSec
3. That the IMSI is not used for User Identity instead it is proposed that the NAI as in RFC 2486 shall be used.
4. To initialise a discussion in S3 on the need for providing confidentiality protection between the UE and the P-CSCF (cf. 4.7.2)

2 Introduction

3GPP has defined three CSCFs, Call State Control Functions, the P-CSCF, the I-CSCF and the S-CSCF where P stands for Proxy and I for Interrogating and S for Serving, cf. figure 1. All of these CSCFs will act like SIP servers. The role of the S-CSCF is to provide the (roamed or non-roamed) subscriber with service control. The S-CSCF is assigned to the subscriber at registration. Depending on the policy in the HN, Home Network, the S-CSCF is in the HN or in the VN, Visited Network. It is a requirement in 3GPP that it shall be possible to hide the network topology from other operators e.g. the number of S-CSCFs. The entry point from the VN/external network to the HN is the I-CSCF. The I-CSCF is responsible for choosing the S-CSCF based on information the I-CSCF gets from the P-CSCF in the VN and the HSS, Home Subscriber Server, in the HN. The information the I-CSCF will need for the selection process is amongst other things the subscriber identity, VN capabilities, required capabilities of the S-CSCF, if the VN or the HN will be the SN, Serving Network etc. The P-CSCF shall enable the call control to be sent to the HN through the I-CSCF and also enable the SIP-messages to be sent to the UE in the VN.

The registration procedure (after that the GPRS attach and PDP context process has taken place) of the UE is divided into three flows:

1. Common initiation

2. HN-control
3. VN-control

At start of the registration the UE sends a SIP-register to the P-CSCF in the VN which then sends the SIP-registration to the HN. The I-CSCF will then make the selection of the SN and S-CSCF. The subscriber data etc is sent to the S-CSCF by the I-CSCF. It is necessary that the HN can authenticate the subscriber in a secure way using e.g. a shared secret. The authentication protocol which is used in UMTS provides mutual authentication i.e. the subscriber can authenticate the serving network and the SN can authenticate the subscriber. This mechanism is reused in the proposal presented in this document. However this requires a new mode in SIP as described in S3-000456. An analysis of different protocols for authentication is made in S3-000447 and in S3-000588.

When the UE makes a call a SIP INVITE is sent to the P-CSCF in the VN which will be forwarded to the S-CSCF which in turn forwards the INVITE based on the destination.

It is important to ensure that the subscriber gets the services he is entitled to and that he gets the services he asks for. A threat towards the UE and the HN is a man-in-the-middle attack where the attacker tries to modify the SIP-messages in whatever way his purposes might be. Therefore it is necessary to check that the SIP-messages sent from the UE have not been tampered with. This can be fulfilled by using integrity protection on the application layer using a shared secret, the Integrity Key IK, between the UE and the S-CSCF which has the subscriber data. Note that the SN i.e. the S-CSCF can be located in either VN or in HN.

The integrity protection does not protect the messages from being read by an attacker who can if no confidentiality protection is provided get information like the IP-address of the UE and what Codecs will be used in the Multimedia session etc.

Since the SIP-proxies have to be able to read certain parts of the SIP-messages hop-by-hop encryption is proposed. Either TLS or IPSec can provide hop-by-hop encryption.

Protection between the nodes within a network e.g. between the I-CSCF and the S-CSCF in the HN is open and a subject for the network owner to solve.

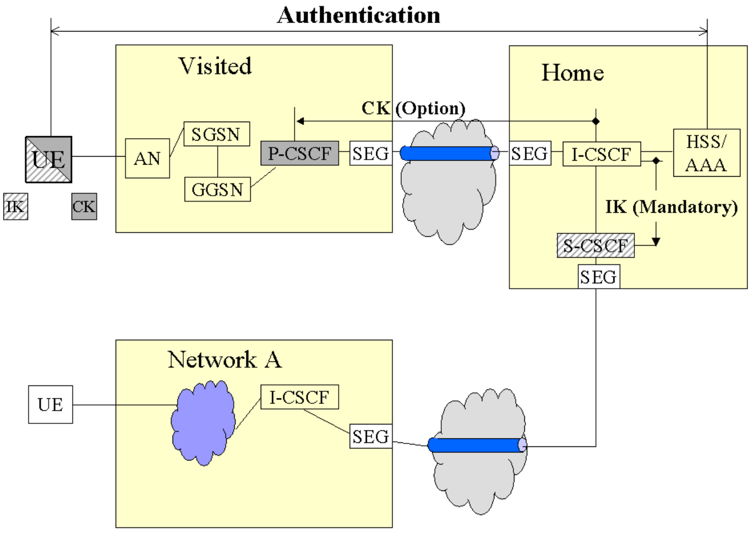

Figure 1 An overview of the architecture.

In figure 1 it is shown that the protection mechanism between the different networks is IPSec using the SEG as specified in the WI NDS. Furthermore the UE and the P-CSCF can optionally get confidentiality protection by using the shared key CK by using either IPSec or TLS. In this document WTLS is proposed. Note also that the UE and the S-CSCF share the Key IK which will be used for integrity protection between the UE and the S-CSCF. The S-CSCF is in this picture located in the HN however it is the policy of the HN that decides if the S-CSCF shall be located in either HN or VN.

3 Background

One assumption that has been made in TR 33.8xx “Access security for IP-based services” is that it is possible to reuse the AKA concept as defined in R’99 for UMTS. However this does not mean necessarily that the same algorithms are used in the multimedia domain as in UMTS.

In 23.228 v 1.1.0 it is assumed that the user is authenticated before the I-CSCF sends the Cx-Select-pull to the HSS. Therefore it is proposed in this document that the HSS authenticate the user. Another good reason for authenticating the user in the HSS is that the HN has the knowledge and control on the outcome of the authentication. Besides this allows for possible enhancements/modifications in the procedure without affecting nodes in the rest of the NW, especially those at the visited NW (P-CSCF), cf. also chapter 4.5

The I-CSCF is also responsible for assigning an S-CSCF to the user and determining based on information provided by HSS, if the home network or the visited network is chosen for session & service control. It is assumed in this document that the HSS also calculates a quintet, which has to be distributed to different nodes as described in this document.

It is a requirement in TR 33.8xx that the IM CN SS shall not rely on the security provided by the PS-domain. Furthermore the integrity protection shall take place between the UE and the S-CSCF according to TR33.8xx. As a working assumption it is assumed that SIP AKA is provided.

4 Description of the mechanisms

4.1 Access independence

The home environment shall make the authentication of the user. In this document only the aspects important for the UMTS standardisation using SIP AKA for IM CN SS have been evaluated. The core network also has to be IETF capable.

4.2 Inter operator protection

Since sensitive SIP signalling messages are sent between e.g. the visited network and the home network it has to be protected. In the WI SAWG3 NDS, Network Domain Security, it is specified that a Security Gateway, SEG, shall be at the border of a network, providing IP security for IP communication between different networks. It is therefore proposed in this document that it shall be mandatory to use the SEG for SIP signalling, cf. Figure 1.

4.3 User identity

It is proposed not to use the IMSI as the identifier of the user in the IM CN SS. There are several reasons for that. One being the requirement to be access independent and an other being the requirement to give user identity confidentiality in UMTS and hence the IMSI should not be used for IM CN SS. Instead it is proposed that the NAI, Network Access Identifier, cf. RFC 2486, shall be used which has the format *user@realm*. This is still FFS in S2.

4.4 Configurability and visibility

In UMTS R’99 the link between the UE and the RNC may be confidentiality protected and integrity protected. If the user receives a non-ciphered call then the user may reject the non-ciphered call this is worked out in R’00. This might also be an issue for aSIP since in this discussion paper it is proposed that the confidentiality protection between the UE and the P-CSCF is optional. The user should be notified whenever the confidentiality protection is turned off and also be given the opportunity to reject a non-ciphered SIP-session. This shall be FFS.

4.5 Authentication

In this proposal the authentication takes place in the HSS/AAA according to the scheme below. The proposal seems to meet the current requirements in TR 33.8xx. Note that the CK, the Cipher Key, is sent from the HSS to the P-CSCF via the I-CSCF together with a challenge using a mode called SIP AKA described in S3-000456. The UE can check that the challenge originates from the HN and respond with a RES, which is checked by the HSS/AAA. The UE can derive the CK from the challenge and the shared secret.

Some advantages to perform the authentication in the HSS/AAA (compared to do it in the P-CSCF in the VN as proposed by Siemens in S3z000022):

- The service provider to whom the customer has to pay for the usage of IM-services should be able to detect fraud and misuse in real-time (from the email discussion from the AdHoc meeting S3#15bis)
- The HN has knowledge and control on the outcome of the authentication of the IM-subscriber
- The HN can decide whether to devolve trust e.g. for authentication (from the email discussion from the AdHoc meeting S3#15bis)
- It minimises the trust between operators (from the email discussion from the AdHoc meeting S3#15bis)
- To perform the authentication in the AAA is compliant with the requirement that says that R00 shall, as far as possible, conform to IETF “Internet standards”.

For optimisation reasons it might be necessary that the HSS/AAA send authentication information to the S-CSCF which then performs the subsequent authentication.

4.5.1 Common initiation of the registration

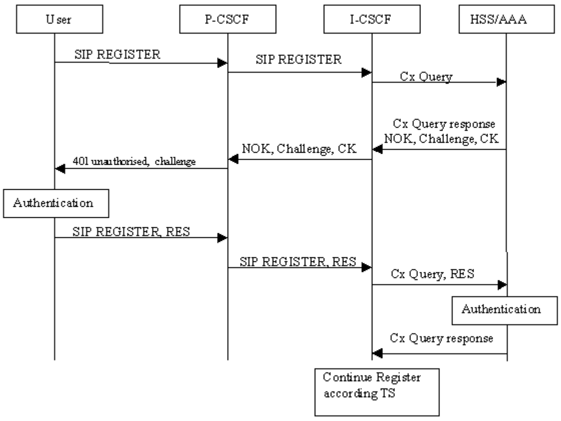

Figure 2 The user is authenticated in the HSS/AAA and the CK is sent to the P-CSCF. The HN is authenticated by the UE.

4.5.2 The S-CSCF is located in the HN

When the authentication has succeeded the I-CSCF selects an S-CSCF and in this example it is located in the HN. The HSS sends the Integrity Key, IK, to the S-CSCF. The UE has derived the IK from the challenge. All subsequent SIP messages shall be integrity protected by using appropriate algorithms and the IK.

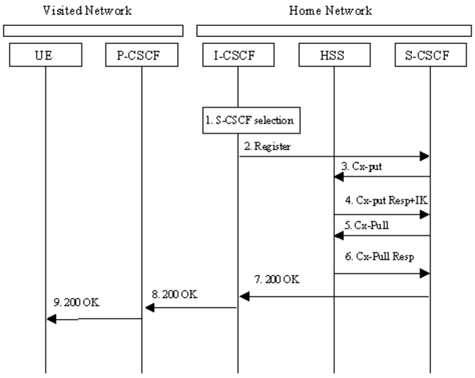

Figure 3 The registration process proceeds and the HSS sends the IK to the S-CSCF

4.5.3 The S-CSCF is located in the VN

When the authentication has succeeded the I-CSCF in the VN selects an S-CSCF. The HSS sends the Integrity Key, IK, to the S-CSCF. The UE has derived the IK from the challenge. All subsequent SIP messages shall be integrity protected by using appropriate algorithms and the IK.

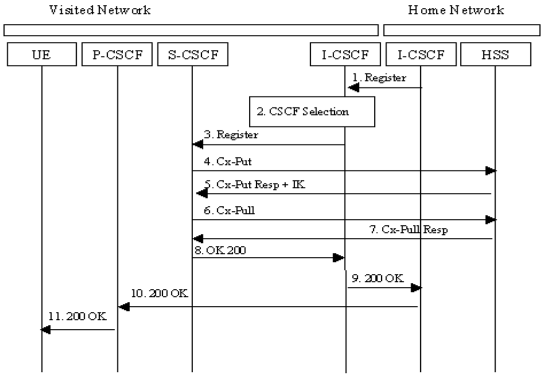

Figure 4 The registration process when the S-CSCF is located in the VN.

4.6 Integrity protection

It is proposed in this document that the SIP-messages like e.g. INVITE is integrity protected on the application layer. In draft-ietf-sip-rfc2543bis-01 it is a requirement that all SIP implementations should support PGP-based encryption and may implement other schemes. PGP may also be used for authentication. In TR 33.8xx an analysis over different protocols like PGP is outlined. However it is concluded that PGP being a PKI based system does not fulfil the 3GPP requirements. Hence another scheme, which does not necessarily have to be a 3GPP scheme, has to be defined.

The integrity key IK is derived by the 3GPP AKA scheme and sent from the HSS to the S-SCSF. The UE in turn can calculate the IK (and CK) from the challenge sent from the HSS.

If the S-CSCF is in visited network then the IK has to be sent through the I-CSCF in home to the I-CSCF in the visited domain and finally to the S-CSCF in the visited network.

For example, if the SIP request is to be:

INVITE sip:watson@boston.bell-telephone.com ***SIP/2.0***
Via: SIP/2.0/UDP 169.130.12.5
Authorization: PGP version=5.0, signature=...
From: A. Bell <sip:a.g.bell@bell-telephone.com>
To: T. A. Watson <sip:watson@bell-telephone.com>
Call-ID: 187602141351@worcester.bell-telephone.com
Subject: Mr. Watson, come here.
Content-Type: application/sdp
Content-Length: ...
v=0
o=bell 53655765 2353687637 IN IP4 128.3.4.5
s=Mr. Watson, come here.
t=0 0
c=IN IP4 135.180.144.94
m=audio 3456 RTP/AVP 0 3 4 5

Then the text in italic and in bold is integrity protected (using a canonical form) and the underlined text is not protected since some parts of it will be changed by proxies (of course the Authorization part has to be unchanged). The requirement then is that all parts of the SIP message that are not changed by a SIP-proxy shall be integrity protected and the protections shall terminate in the S-CSCF.

It is proposed that 3GPP define one integrity protection algorithm that should be standardized into the SIP-standard.

A description on the registration flow is given in Figure 2-4 and it is proposed that the integrity protection shall take place immediately after that the registration has ended i.e. when the 200 OK has been sent to the UE. The first SIP message that is sent either by the UE or the S-CSCF should then be integrity protected.

4.7 Confidentiality protection

4.7.1 WTLS

As an option it is proposed that confidentiality and integrity protection take place between the UE and the P-CSCF. Using appropriate mechanisms defined in WTLS may protect the SIP messages between the UE and the P-CSCF. WTLS may then use the CK as a pre-master secret, which in turn is used for calculation of a key block containing material for encryption key, MAC-secret and IV. Using this option then the UE and the P-CSCF will have a security association. Furthermore it fulfils the requirement in 33.8xx that the protection in IM CN SS shall not rely on the protection mechanisms in the PS-domain. There is a requirement in the TR 33.8xx stating that it shall be an option that confidentiality takes place between the UE and the S-CSCF but since several fields in the SIP messages can not be encrypted we have to rely on hop-by-hop protection using either TLS or IPSec. It is proposed that WTLS be used since it is optimised for low-bandwidth bearer networks with relatively long latency, which is not the case for IPSec. The exact mechanisms and the use of WTLS is FFS.

The message flow for the shared secret handshake is described below (all in all about 100 bytes):

```
Client                                         Server


ClientHello                --------->
                                               ServerHello
                                               [ChangeCipherSpec]
                           <---------          Finished
[ChangeCipherSpec]
Finished
Application Data           --------->

Application Data           <-------->          Application Data
```

A description on the registration flow is given in Figure 2-4 and it is proposed here that the shared-secret handshake shall take place after that the registration has ended i.e. when the 200 OK is sent to the UE the UE then sends the Client Hello to the P-CSCF.

WTLS offers several strong algorithms like e.g. IDEA CBC and SHA1. It should be 3GPP SA3 that decides what algorithms offer enough protection and if new ones should be introduced in WTLS.

4.7.2 What confidentiality protection is needed for IM CN SS?

Since it is mandatory to implement IPv6 for the terminals and also for all the IM CN nodes IPSec will also be implemented. Furthermore there is already protection defined for the Uu interface between the UE and the RNC. Therefore other security mechanisms like IPSec can be used over e.g. the Gn and Gi interfaces.

It is therefore proposed to initialise a discussion within S3 on the need for providing confidentiality protection of the SIP-signalling hop between the UE and the P-CSCF using either WTLS or protection mechanisms defined on the SIP-level.

5 Discussion

There are some issues that have not been discussed in this document but they are worthwhile to mention here.

No end-to-end solution is provided in this proposal i.e. UE-UE. However using security mechanisms like e.g. an RTP-cipher for the multimedia application itself can possibly solve this. Ericsson has sent a draft to the IETF on “RTP Encryption for 3G Networks” cf. draft-blom-rtp-encrypt-00.txt. This document describes a method for confidentiality protection (encryption) of the payload in conversational multimedia applications running over the Real-time Transport Protocol [RTP]. The proposal is based on the 3GPP (3rd Generation Partnership Proposal) confidentiality algorithm "f8", and the new Advanced Encryption Standard (AES). Then a key management scheme has to be defined for end-to-end security.

It is assumed in this document that the principles according to S3-000456 are available i.e. that an AKA mode exists for SIP. This mode does not exist today.