3GPP TSG SA WG3 Security — S3#28 **S3-030302**
6 – 9 May 2003
Berlin, Germany

Title: LS on security solutions for the Mt reference point
Work Items: Presence, IMS

Source: 3GPP SA3
To: 3GPP CN1, 3GPP SA2
Cc:

Contact Person:
Name: Günther Horn
Tel. Number: +49 89 636 41494
E-mail Address: guenther.horn@siemens.com

Attachments: S3-030223

---

1. Problem Statement:
The use of HTTP over the Mt reference point is a means for a mobile user to manage his or her data on application servers. It is obvious that the communication over the Mt reference point needs to be adequately secured. In SA3#28, several contributions (S3-030223, 224, 245, 256) proposed solutions for this issue. The key management solution proposed in S3-030223 has architectural implications for the IMS and is expected to affect stage 3 specifications for Release 6 under the control of CN1. It was felt at SA3#28 that guidance from CN1 and SA2 was needed before a decision could be taken by SA3. CN1 and SA2 are therefore kindly asked to provide such guidance on the following two issues:

Key transport over the ISC interface
S3-030223, section 5, proposes to use the Service Information XML element in the body of a 3rd party REGISTER message to transport key material from the S-CSCF to one or several application servers over the ISC interface.

Note that key transport occurs after each successful (re-)authentication. Note that the integrity and confidentiality of the derived keys distributed over the ISC interface can be ensured by means of IPsec (as specified in TS 33.210).

Transport of release information from S-CSCF to UE
In order to avoid backward compatibility problems between releases 5 and 6, the solution in S3-030223 requires that the UE be informed by the S-CSCF whether the latter is Release 5 or a later Release (for an explanation see S3-030223, section 8). S3-030223 proposes to solve this by including (for Releases 6+) the information on the release of the S-CSCF in the *nonce* parameter in the WWW-Authenticate header [cf. TS-24.228 v530, tables 6.2-9, 6.2-10, 6.2-11] of the *401 Unauthorized response* message. Please note that the *nonce* parameter, as specified in RFC 3310, may optionally contain some server specific data, which could be used to carry the required information.

2. Action on CN1 and SA2:
CN1 and SA2 are kindly asked to comment on the feasibility of the proposals. Suggestions for alternative realisations of the required functionality are also welcome.

Date of Next SA3 Meetings:

SA3#29	15 – 18 July 2003	San Francisco
SA3#30	7 – 10 October 2003	tbd

3GPP TSG SA WG3 Security — S3#28 **S3-030223**

6 – 9 May 2003

Berlin, Germany

Source: **Siemens**

Title: **Key management for the use of http at the Mt reference point in the IMS**

Document for: **Discussion and decision**

Agenda Item: **7.19 Presence, (7.1 IMS)**

Abstract

In SA3#27, several contributions (S3-030056, 60, 69, 84) discussed possible solutions for security for the use of http at the Mt reference point. Some of these solutions assumed the existence of a secret shared between the UE and the AS. This contribution proposes a solution how to establish such a shared secret, based on the IMS registration.

---

1. Introduction

A scenario currently under discussion in several 3GPP groups (e.g. SA2, SA3) is the use of HTTP communication over the Mt reference point between a UE and an IMS-based application server (AS). An example of the use of HTTP over the Mt reference point is a means for a mobile user subscribed to the IMS, to manage his or her data on the application server.

It is obvious that the communication over the Mt reference point needs to be adequately secured. In SA3#27, several contributions (S3-030056, 60, 69, 84) addressed this issue. This contribution only addresses the provision of a shared secret to the UE and the AS.

A discussion of the use of the established shared secret is outside the scope of this contribution. A companion contribution by Siemens ("Security protocols for the use of http at the Mt reference point in the IMS ") shows how this shared secret can be used in http digest (rfc2617) for UE to AS authentication. The key derivation method presented is this contribution is, however, independent of the choice of a particular security protocol on the Mt interface.

2. Outline of shared key establishment

The proposed solution for the establishment of a shared secret between the UE and an AS proceeds in several steps which are depicted in Figure 1. The steps are described in more detail in the following sections.

Step 1: IMS registration

> In the IMS registration process, the session key CK is provided to the UE and the S-CSCF. The IMS registration proceeds as described in TS 33.203v5.5.0.

Step 2: provision of information on application servers associated with a user from the HSS to the S-CSCF

Step 3: derivation of AS-specific shared keys from CK at the UE and the S-CSCF

Step 4: distribution of AS-specific shared keys from the S-CSCF to the ASs over the ISC interface.

Step 4 concludes the establishment of a shared key between the UE and the AS.

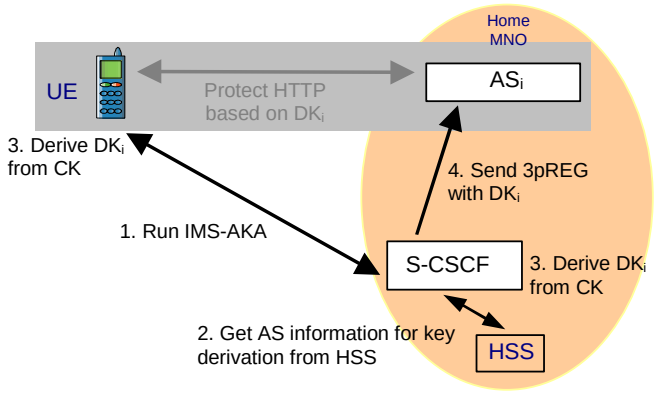

Figure 1

3. Provision of information on application servers from HSS to S-CSCF

Filter criteria are stored within the HSS for a service profile for a specific user. This information is sent by HSS to the S-CSCF via the Cx interface upon user registration with the IMS. The initial filter criteria are used by the S-CSCF to determine whether to forward a request to an application server associated with a particular user. Hence, the filter criteria are used to identify "interested" application servers. If there is a trigger set to send a REGISTER to a specific AS the S-CSCF sends a 3rd party REGISTER to this application Server. For the explanation of the a 3rd party REGISTER mechanism see section 5.

4. Key derivation

In the IMS registration process, as a result of the run of the IMS-AKA protocol, the session keys CK and IK are provided to the UE and the S-CSCF. The S-CSCF forwards CK and IK to the P-CSCF. IK is used for integrity protection between UE and P-CSCF, as specified in TS 33.203v5.5.0. In release 5, the key CK is not used as no confidentiality is provided between UE and P-CSCF. In future releases, however, confidentiality may be provided between UE and P-CSCF.

The basic idea of key derivation here is to use CK not as a confidentiality key, but as an intermediate key from which further keys are derived. Let KDF denote the key derivation function, and DKi (i=0, 1, ...) the keys derived from CK. Then DK0 is to be used for confidentiality protection between UE and P-CSCF (if required in future releases), and DKi (i=1, 2, ...) are to be used as shared secrets between the UE and application servers ASi (i=1, 2, ...). The key derivation takes place in the S-CSCF and in the UE. The S-CSCF will immediately derive the required keys as they have to be pushed to the appropriate ASs. The UE will also immediately derive the required keys and store them in non-volatile memory so that they are available also after powering off and on again, without the need for another IMS registration. It is proposed not to introduce any new functions on the USIM to support this key derivation process because then also Rel5 USIMs can be used with the key derivation feature and the number of affected components is minimised. From a security point of view, the derivation on the terminal seems acceptable as the keys are derived from CK which is also stored on the terminal.

Requirements on the key derivation function are described in the Liaison Statement from SA3 to ETSI SAGE (S3-030147). They include:

R1: It shall not be possible to gain any useful knowledge about CK from the derived keys DK1, DK2, …

R2: It shall not be possible to gain any useful knowledge about DKi from DKj.

R3: It shall be possible to derive DKi as a function of the intermediate key CK, the identity ASi-ID of the application server ASi, random input available from the run of the IMS-AKA protocol during the IMS registration (e.g RAND), and possibly the IMS identity IMPI (or IMPU) of the user, i.e. ***DKi = KDF (CK; ASi-ID, RAND, IMPI).***
(For i=0 one may want to set ASi-ID = 0.)

An initial response from ETSI SAGE to the LS S3-030147 suggests that key derivation satisfying these requirements is possible, providing an acceptable level of security, and that they were prepared to specify such a key derivation function. However, it should be noted that SAGE would like to study further whether additional input in the form of a newly generated nonce was required although SAGE indicates that they see no obvious reason for this requirement. SAGE also indicates that a suitable basis for KDF may be HMAC-SHA1.

SAGE also asks SA3 to specify an input parameter ASi-ID that is well-defined and uniquely identifies each application server.

5. Key distribution

For the distribution of derived keys DKi we propose to use a push approach, employing the "3rd party register" function of the ISC interface. This function is defined in [TS-23.218, section 6.3] (stage 2) and [TS-24.229, section 5.4.1] (stage 3). In the IMS registration the HSS informs the S-CSCF whether to send a 3rd party REGISTER message to a specific application server.

Using the body of the 3rd party REGISTER to transport key material to the application server is possible. The 3rd party registration lives as long as the IMS registration itself. This does, however, not limit the DKi lifetime to the lifetime of the IMS registration (see section 7 on key lifetime issues). In case of a re-registration (and re-authentication), a new 3rd party register can be sent to the AS, including the new keys.

The Service Information XML element which contained the initial filter criteria from the HSS can be used to transport 'service specific information' to the application server.

Issue for clarification:
TS23.218 specifies that the "service specific information" provided to the AS is transparent to HSS and S-CSCF. This means the information is administered in the HSS and then transported to the AS via S-CSCF and 3rd party register. It is the question how this requirement of "transparency" is to be interpreted in our context. Certainly, the key derivation, and adding the keys to the 3rd party register body, does not affect the SIP functionality of the S-CSCF, and therefore be considered transparent for it. Further clarification is needed here.

It is needless to say that the integrity and confidentiality of the derived keys distributed over the ISC interface between the S-CSCF and the AS needs to be ensured. If cryptographic protection is required then the ISC interface shall be secured by means of NDS/IP with mandatory confidentiality protection.

6. Key synchronisation

The IMS registration with subsequent key distribution via the 3rd party register mechanism provides UE and application server ASi with the required derived keys DKi. For a successful secure communication between UE and ASi it must be ensured that UE and AS apply the same derived key DKi. Situations are conceivable where this is not guaranteed. E.g. it may happen that the completion of the (re-)registration and key distribution process takes slightly longer on one side than on the other. Then, one side already uses the new derived key while the other side still uses the old derived key. Another possibility is that of key loss on the AS, e.g. due to a crash. There are at least two possible solutions for this issue:

Re-tries and re-registrations: when the security protocol (e.g. http digest) between the UE and the AS using the derived key DKi fails, the UE will retry a specified number of times. By the time of the retry, also the other side will have acquired the new key if the problem was due to a delay in the key distribution on one side. If the problem was due to a key loss then only a re-registration of the UE in the IMS will help. So, a sensible policy could be: in case of a security failure between the UE and the AS let the UE retry a specified number of times. After that, the UE has to re-register in the IMS. This method is simple, although probably not the most elegant conceivable, but seems quite likely to work in practice.

Key indications from the AS to the UE: depending on the security protocol between the UE and the AS, the AS could indicate to the UE which derived key is in use. A suitable key identifier could e.g. be the RAND used in the key derivation. This key identifier would have to be distributed over the ISC interface from the S-CSCF to the AS together with the derived key DKi. The transport of the key identifier from the AS to the UE could work as follows in the case of http digest: when the UE contacts the AS the AS replies with a *401 unauthorized* message and WWW-Authenticate header which contains a nonce. This nonce is " a server-specified data string. ... The contents of the nonce are implementation dependent." (according to rfc2617, section 3.2.1). The key identifier RAND could be made part of that nonce. If the AS has no derived key for that UE available it could send RAND=0. If the UE notices a mismatch it could immediately start a re-registration (or re-try http digest a couple of times).
(Side remark: the similar property of the nonce to be implementation-dependent has already been exploited for transporting CK, IK between S-CSCF and P-CSCF using http digest aka.)

The authors currently have a preference for the first solution, but this is ffs.

7. Key lifetimes

The derived keys DKi are available to the UE and the ASi immediately after the completion of the registration process. They are updated with every new registration or re-registration with authentication. However, the derived keys DKi are NOT deleted when a user de-registers. This allows a user to communicate with an application server even at times when the user is not registered in the IMS. The only requirement is that a user once registered in the IMS before contacting the application server.

Obviously, there is a need to limit the lifetimes of the derived keys DKi. It is proposed that both the UE and the AS set limits on the lifetime of the derived keys. When the UE notices that the lifetime of the derived key has expired it simply re-registers in the IMS. When the AS notices that the lifetime of the derived key has expired it simply deletes it. When the UE then tries to contact the AS the situation is as for the case of key loss discussed in section 6. The key lifetimes should not be set too short so as to avoid frequent failures or re-registrations. The UE should be pre-configured with a sensible lifetime value which is likely to be shorter than that in the AS.

[TS-24.228] 3GPP TS 24.228 v5.3.0 (2002-12): "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3 (Release 5)"

8. Interworking between equipment from different releases

The work on the security for the use of http over the Mt interface to which this paper contributes is part of Release 6. So, the key derivation functionality discussed here is only available when UE and S-CSCF are Release 6. (It is ffs whether also the HSS has to be Rel 6 because it has to provide the filter criteria.). But the USIM and the P-CSCF can be Release 5.

On the other hand, IMS Rel 6 may provide confidentiality between the UE and the P-CSCF. Which key is used then? This depends on the Release of the S-CSCF. It is specified for IMS Release 5 [TS-24.228, tables 6.2-9, 6.2-10] that the S-CSCF forwards CK to the P-CSCF although CK is not used in Release 5. On the other hand, when the proposal in this contribution is accepted then a Release 6 S-CSCF forwards the derived key DK0 to the P-CSCF to be used as confidentiality key, instead of CK. Consequently, when both, UE and P-CSCF are Release 6 and the S-CSCF may be Release 5 or 6, then the UE must know the Release of the S-CSCF in order to know whether to use CK or DK0 as confidentiality key.

The issue can be solved by including the information on the release of the S-CSCF in the nonce in the WWW-Authenticate header sent in http digest aka together with IK, CK (Release 5) or IK, DK0 (Release 6). While the keys are stripped off by the P-CSCF the release information would travel all the way to the UE, together with the challenge RAND and the parameter AUTN.

References

[TS-23.218] 3GPP TS 23.218 v5.3.0 (2002-12): "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model; Stage 2 (Release 5)"

[TS-24.229] 3GPP TS 24.229 v5.4.0 (2002-12): "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3 (Release 5)"