3GPP TSG SA WG3 Security — SA3#36 **S3-040973**

November 23-26, 2004

ShenZhen, China

Agenda item: 6.1.2 Early IMS

Title: Impact on network entity considering the interworking requirement

Source: Huawei

Document for: Discussion and decision

1 Introduction

In the present TR 33.878 V0.0.3 it gives a description of the interworking scenario between UE and IMS network. As the IMS network usually comprise several network entities. In the present TR it does not give analysis of the influence on network's entities for the interworking requirement. Here we give a brief analysis of the influence on P/I-CSCF and suggest add these analysis to the TR

2 Discussion

2.1 P-CSCF

As the Early IMS authentication method was introduced later. There may be some P-CSCF that only supports Full 3GPP compliant authentication method. Then in the IMS network there may be scenario that the authentication method supported by P-CSCF was not all same. If not all P-CSCF support the same authentication method.， the unexpected implementation may appear. For example, if UE supports Early IMS authentication method only, and an assigned P-CSCF only supports Full 3GPP compliant authentication method, UE can be notified that the authentication method is different as described now in TR. UE may initiate another P-CSCF discovery process, but he maybe still get a similar P-CSCF that he does not want, although here may exist some P-CSCF support Early IMS authentication method. So if the authentication method supported by P-CSCF was not same, we need give some information to assist the P-CSCF discovery process. Now the P-CSCF discovery can be implemented in three methods, including the GPRS PDP context activation procedure, DHCP procedure or OTA procedure.

If the GPRS PDP context activation procedure is selected, it maybe easily to distinguish different P-CSCF we wanted by different APN parameter when we activate PDP context.

If the DHCP method is selected, it can not convey any user related information. It can not help UE to get the wanted P-CSCF.

The authentication supported by UE depends on the User equipment and his Subscription Data. If the OTA method is selected to assign the P-CSCF, it needs to investigate whether the DM method can satisfy the requirements. The method is FFS.

Then our suggestion is:

1) If the authentication method supported by P-CSCF is not all same, then in the P-CSCF discovery procedure, UE need give some indication to network. That indication can be used to specify the authentication method supported by UE which can help network assign the correct P-CSCF. Using different APN can be thought as a considerable method.

If P-CSCF only supports Early IMS authentication method, it may raise another problem. For example, UE support both authentication method and P-CSCF only support Early IMS method, then S-CSCF can only receive an SIP register message that indicate using the Early IMS authentication method, other SIP register message will be rejected by P-CSCF. Now P-CSCF can not give any indication in the SIP message which authentication method is supported by him. That also means that the authentication method supported by P-CSCF may not be known by S-CSCF. It may be difficult for S-CSCF to judge whether the user is binding down the authentication method or not. To avoid introduce other indication in the SIP message and also support early IMS method, two method can be used. One is that early IMS method only can be used in the home network. The other is P-CSCF in the visited network should not support early IMS only.

Then our suggestion is:

1) To avoid introduce an indication of the authentication method supported by P-CSCF in the SIP message and also support the early IMS method, two method can be used. One is only support early IMS method in the home network. The other is P-CSCF in the visit network should avoid to support Early IMS authentication method only.

2.2 I-CSCF

AS in the IMS network there have some CSCF only supported Full 3GPP compliant method before, when we introduce the Early IMS authentication method to CSCF, then different CSCF may support different authentication method. If the P-CSCF and S-CSCF are existing in the same network, such as we only provide the GPRS roaming not the IMS roaming for a roaming user, that unexpected incorrect match may be avoided. For example we can configure the authentication method supported by S-CSCF in P-CSCF. That also means P-CSCF can know which S-CSCF support the same authentication method by configure data. But it will block the operator extend the IMS network for it always need modify the data stored in P-CSCF.

In addition as the IMS network extension, P-CSCF and S-CSCF may exist in different network and owned by different operator, we can not always assume that P-CSCF will know the authentication method supported by S-CSCF in advance.

Considering the two above scenario, we think that problem can get a unified solution by using the I-CSCF. In the IMS registration procedure, the I-CSCF has an important role to select the correct S-CSCF according to the description in TS23.228 V6.7.0 section 5.1.2.1

"*3. Capabilities of individual S-CSCFs in the home network*

This is internal information within the operator's network. This information may be used in the S-CSCF selection. This information is obtained by the I-CSCF by methods not standardized in this release."

If we regard the authentication method supported by S-CSCF as one capability of individual S-CSCF ,and it was pre-obtained by I-CSCF, then, when I-CSCF receives the register message, it can select the correct S-CSCF according

to the received indication in the SIP messaging and the capability of S-CSCF. It can avoid the incorrect match between P-CSCF and S-CSCF. So we recommend that:

1) To avoid the incorrect match between P-CSCF and S-CSCF, it is recommended that the authentication method supported by S-CSCF should be regard as one capability and can be obtained by I-CSCF. Using that information can help I-CSCF to select the correct S-CSCF.

3 Conclusion

As the early IMS authentication is a new method introduced into the existing IMS network. To avoid the complexity of the interworking in the different network entities that supporting different authentication method, it need give some direction to the related network entities behavior. Here we give an initial analysis on P/I-CSCF and provide some rules to the network entities. We hope it can help to reduce the work of interworking we will encounter in the future.

4 Proposal

Adding the above the suggestion into the present TR as below:

****

7.2.4 Interworking cases

It is expected that both fully 3GPP compliant UEs implementing the security mechanisms in TS 33.203 [2] (denoted "fully compliant" in the following) and UEs implementing the early IMS security security solution specified in the present document (denoted "early IMS" in the following) will access the same IMS. In addition, IMS networks will support only fully compliant UEs, early IMS UEs, or both. Both UEs and IMS networks must therefore be able to properly handle the different possible interworking cases.

Editor's note: The interworking solution described in this clause is agreed as a working assumption in SA3. An alternative approach based on explicit identification of early IMS support on UEs has been suggested, but a detailed proposal has not yet been developed. If compelling reasons are found to replace the working assumption with this alternative approach, then this will be done at SA3#36 (23-26 November 2004).

Since early IMS security does not require the security headers specified for fully compliant UEs, these headers shall not be used for early IMS. The Register message sent by an early IMS UE to the IMS network shall not contain the security headers specified by TS 33.203 (Authorization and Security-Client).

As a result, early IMS UEs shall not add an explicit indication for the security used to the IMS signaling. An IMS network supporting both early IMS and fully 3GPP compliant UEs shall use early IMS security for authenticating the UE during registrations that do not contain the security headers specified by TS 33.203 (Authorization and Security-Client).

Without sending an Authorization Header in the initial Register message, early IMS UEs only provide the IMS public identity, but not the IMS private identity to the network (this is only present in the Authorization header for fully compliant UEs). The IMS private identity shall therefore be derived from the subscriber's public identity in the HSS.

During the process of user registration, the Cx interface carries both the private user identity and the public user identity in Cx-MAR requests (sent by I-CSCF and S-CSCF). For early IMS, only the public user identity shall be sent to the HSS within these requests, and the private user identity shall be empty. This avoids changes to the message format to the Cx interface.

If the S-CSCF receives an indication that the UE is early IMS, then it shall be able to select the “IP-based” authentication scheme in the Cx-MAR request. The Cx interface shall support the error case that the S-CSCF selects the “Digest-AKAv1-MD5” authentication scheme based on UE indication, but the HSS detects that the subscriber has a SIM instead of a USIM or ISIM. In this case the HSS shall respond with an appropriate error command. The S-CSCF will then respond to the UE with a 403 Forbidden message. If the UE is capable of early IMS then, according to step 5, the UE will take this as an indication to attempt registration using early IMS.

For interworking between early IMS and fully compliant implementations during IMS registration, the following cases shall be supported:

1. Both UE and IMS network support early IMS only

   IMS registration shall take place as described by the present document.

2. UE supports early IMS only, IMS network supports both early IMS and fully compliant access security

   The IMS network shall use early IMS security according to the present document for authenticating the UE for all registrations from UEs that do not provide the fully compliant security headers.

3. UE supports both, IMS network supports early IMS only

   If the UE already has knowledge about the IMS network capabilities (which could for example be preconfigured in the UE), the appropriate authentication method shall be chosen. Fully compliant security shall be used, if the network supports this, otherwise early IMS security shall be used.

   If the UE does not have such knowledge it shall start with the fully compliant Registration procedure. The early IMS P-CSCF shall answer with a 420 “Bad Extension” failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial Register message (this header cannot be ignored by the P-CSCF).

   The UE shall, after receiving the error message, send an early IMS registration, i.e., shall send a new Register message without the fully compliant security headers. The network shall respond with a 200 OK message according to the registration message flow as specified in clause 7.2.5.1.

4. UE and IMS network support both

   The UE shall start with the fully compliant IMS registration procedure. The network, with receiving the initial Register message, receives indication that the UE is fully compliant and shall continue as specified by TS 33.203.

5. UE supports early IMS only, IMS network supports fully compliant access security only

   The UE sends a Register message to the IMS network that does not contain the necessary security headers required by fully compliant IMS. In this case the IMS network will answer with an error message (403 Forbidden with “Authentication Failed” reason phrase) indicating to the early IMS UE that the authentication method is incorrect. After receiving the error message, the early IMS UE shall stop the attempt to register with this network, since early IMS is not supported.

6. UE supports fully compliant access security only, IMS network supports early IMS only

   The UE shall start with the fully compliant IMS registration procedure. The early IMS P-CSCF shall answer with a 420 “Bad Extension” failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial Register message (this header cannot be ignored by the P-CSCF). After receiving the error message, the UE shall stop the attempt to register with this network, since the fully 3GPP compliant security according to TS 33.203 is not supported.

7.2.4.1 Impact on network entity

To avoid the interworking complexity in the future, it need give some rules on the network entity:

1) If the authentication method supported by P-CSCF is not all same, then in the P-CSCF discovery procedure, UE should give some indication to the network. That indication can be used to specify the authentication method supported by UE which can help network assign the correct P-CSCF.

NOTE: Using different APN can be thought as one considerable method.

2) To avoid introduce an indication of the authentication method supported by P-CSCF in the SIP message and also support the early IMS method, two method can be used. One is only support early IMS method in the home network. The other is P-CSCF in the visit network should avoid to support Early IMS authentication method only.

3) To avoid the incorrect match between P-CSCF and S-CSCF, it is recommended that the authentication method supported by S-CSCF should be regarded as one capability, and can be obtained by I-CSCF, that can help I-CSCF to select the correct S-CSCF.

****