3GPP TSG SA WG3 Security — SA3#35 **S3-040733**

October 5-8, 2004

St Paul's Bay, Malta

Agenda item: 6.1.2 Early IMS

Title: The choice of interim solution

Source: Huawei

Document for: Discussion and Decision

1 Introduction

It's specified in the early IMS TR "At some stage, it is expected that both fully 3GPP compliant terminals and terminals implementing the interim security solution will access the same IMS. Therefore, some indication shall be given that a terminal supports the interim solution rather than the full 3GPP solution." This contribution discusses the further network action and analyze implementation scenario with different capable terminals and SIM/ISIM/USIM.

2 Discussion

2.1 The further network action

A terminal supporting the interim solution rather than the full 3GPP solution shall give some indication to network. After the network (S-CSCF) received this indication, it should select early IMS authentication mechanism to that registering user.

With the full 3GPP solution, S-CSCF request authentication vector from HSS by Cx-MAR message. In this Cx-MAR message, an "Authentication Scheme" field exists, and the current content is only "Digest-AKAv1-MD5" available. If S-CSCF receive the register request with early IMS indication, the S-CSCF should select *"IP-based" authentication* (call this authentication of interim solution as "IP-based" authentication) other than the "Digest-AKAv1-MD5". So, the function of selecting 'IP-based" authentication scheme should be added to S-CSCF to implement the interim solution.

2.2 Implementation scenario with different capable terminals and SIM/ISIM/USIM

	Interim solution terminal(with indication to network)	Full 3GPP solution terminal (no indication to network)
SIM	(1)Implement the interim solution	(3)Implement the interim solution

ISIM/USIM	(2)Implement the interim solution	(4)Implement the full 3GPP solution

Scenario 1: Interim solution supported terminal combined with SIM. In this scenario, the terminal will indicate the network the interim solution is needed, and S-CSCF select the right authentication scheme for this combination.

Scenario 2: Interim solution supported terminal combined with ISIM/USIM. Despite it is the ISIM/USIM with full AKA authentication, the terminal is a interim solution supported terminal, the full 3GPP solution can't be implemented. As the interim solution supported terminal will indicate the network, the S-CSCF can select the right authentication scheme for this combination.

Scenario 3: Full 3GPP solution supported terminal combined with SIM. Because the SIM can't implement the AKA authentication, the interim solution has to be implemented. The full 3GPP solution supported terminal don't indicate the network the interim solution should be implemented, so the S-CSCF may select the AKA authentication scheme for this combination, and the error case will happen.

Scenario 4: Full 3GPP solution supported terminal combined with ISIM/USIM. The full 3GPP solution will be implemented.

From the above analysis, the scenario 1, 2, 4 can be implemented correctly, but the error case may occur with scenario 3. To deal with the possible error case of scenario 3, there are three alternative mechanisms:

Alternative 1: Full 3GPP solution supported terminal indication the network the interim solution is needed when the terminal detect the SIM is inserted.

Alternative 2: After the HSS receives a Cx-MAR requesting the AKA authentication scheme, if the HSS find that user is a SIM user, then HSS indicates the S-CSCF failure with cause reason "incorrect authentication scheme". The S-CSCF requests again with the right authentication scheme.

Alternative 3:" After the HSS receives a Cx-MAR requesting the AKA authentication scheme, if the HSS find that user is a SIM user, then HSS selects the interim solution and returns a Cx-MAA message with the IP address that was stored in the HSS during PDP context establishment "

Comparison of the *Alternative* 1, *Alternative* 2 and *Alternative* 3:

- The *Alternative 1* requires more functions to 3G terminal and the *Alternative 2* requires a little change to core network. The *Alternative 2* is easy to implement, with higher compatibility for the network.
- Along with development of 3G network and the update of the user, more users will use scenario 4, and scenario 3 will drop off and disappear finally. The additional function of terminal according to the *Alternative 1* will be useless in the end. This problem will not happen with *Alternative2*, oppositely, it is an advantage to the network (the additional procedure will be reduced).
- *Alternative* 3 is slightly similar with *Alternative2*, and the same point is the HSS should find whether the user is suited to the requested authentication scheme. The different point: with the *Alternative 2*, the decision is taken by S-CSCF to request again or do other action; with the method3, the decision is token by HSS, but the HSS is common entity for other entities or domains, it can't preclude the potential element may effect the HSS select right authentication scheme for user in the future, at the same time, the HSS should be kept the simple as possible. This suggests the *Alternative 2* is preferred over *Alternative3*.

According to the above comparison, the *Alternative 2* is recommended.

3 Conclusion

1 The S-CSCF shall have ability to select the right authentication scheme according to the indication of interim solution from terminal.

2 If the S-CSCF selects an AKA authentication scheme for a SIM user, the HSS shall indicate the S-CSCF the authentication scheme is incorrect.

4 Proposal

Add follow text to the TR

****

7.2.4 Identification of terminals supporting the interim solution

At some stage, it is expected that both fully 3GPP compliant terminals and terminals implementing the interim security solution will access the same IMS. Therefore, some indication shall be given that a terminal supports the interim solution rather than the full 3GPP solution. After receive this indication, the S-CSCF shall be able to select the "IP-based" authentication scheme of interim solution.

In case of a full 3GPP solution supported terminal combining with a SIM, the indication is not available with terminal, and the S-CSCF may select the "Digest-AKAv1-MD5" authentication scheme for the user. With this special case, the HSS shall be able to detect the incorrect authentication scheme for a SIM user and indicate it to the S-CSCF, and then the S-CSCF shall select the "IP-based" authentication scheme of interim solution and interact with HSS again with the correct selection.

Editor's note: The exact format, and means to carry this information, is for further study.

****