3GPP TSG WG3 S3#17 Tdoc S3-010081
Göteborg, Sweden
27th February – 2nd March, 2001

Agenda Item: TBD

Source: Ericsson, Nokia, Lucent and Orange

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 discuss the question on where authentication of an IM-subscriber shall take place and also where integrity protection of SIP-messages shall terminate.

In this document it is proposed that

1 The authentication of the IM-subscriber takes place in the Home Network only.
2 Integrity protection of SIP-signalling shall terminate in the Home Network.
3 A different trust model for IM-services compared to the trust model for CS- and PS-services shall be adopted.

Note that it is left FFS to what extent Legal Interception and Billing requirements will impact the P-CSCF node.

2 Background

In S3 there has been some discussions about which network node shall authenticate an IM-subscriber . Two different proposals have been mainly discussed: 1) P-CSCF (or the Visited Network) and 2) the HSS (or the Home Network), cf. [S3-00689] and [S3-00699] also [S3-00679] and [S3-00710] can be consulted.

The main arguments for performing authentication in the Visited Network, case 1) above, have been

- The trust model used for CS/PS-domain shall be reused i.e. the P-CSCF will in that aspect has the role as a VLR/SGSN.

- Complexity. It is less complex to terminate the confidentiality protection and the integrity protection in the same node i.e. the P-CSCF. This would also require that authentication shall take place in the P-CSCF.

- Network domain security mechanisms shall secure communication between P-CSCF and S-CSCF.

The major difference between performing authentication in the HN and the VN is the different trust model between the Home System and the Visited System. In the first case the HN does not have to trust (in the general case) the P-CSCF that resides in a visited network, while in the second case, there is a requirement that the Serving Node (which can be a cellular operator, or a 3rd party service provider), must trust the Visited System to performs the authentication for all it's subscribers. At the last meeting in Sophia S3 #16 it was decided that a third possible implementation should also be evaluated , i.e., that the HN controls the authentication process and, at its option, could delegate the authentication to the VN, cf. [S3-16-Rep].

There have been many discussions within S2 to see if a hybrid solution for the control of the session i.e. Visited Control and Home Control shall be adopted or not. At the last S2 meeting in Los Angeles S2#16 it was decided to define Home Control only, cf. [S2-010148]. There where several reasons for this amongst other things:

- Complex to manage two architectures, instead of one

- Every problem requires more than one solution

- Combination of solutions for each issue, increases work such as session flows, registration flows

- Additional extensions to IETF protocols required (e.g. SIP extensions) to support two models

- Security architecture becomes more complex

- Multiple relationship and roaming models between various operators

- Behaviour of services need to be understood, rather than gaining from the external service creation environment per operator

All those arguments should also be reflected in S3's solution for the IM security architecture. Therefore Ericsson , Nokia, Lucent and Orange propose that authentication shall take place in the Home Network only. Additional arguments in support of this position are listed below.

As integrity protection can be seen as an important extension of (entity) authentication, it should be terminated at the same point as authentication. (this issues has to be further studied, e.g., is this acceptable from a performance point of view?)

3 Authentication of an IM-subscriber

An IM-subscriber will have its subscriber profile located in the HSS in the Home Network. The exact details of the subscriber profile are FFS but it will contain information on the subscriber that may not be revealed to an external partner, cf. [3G TR 23.228]. At registration an S-CSCF is assigned to the subscriber by the I-CSCF. The subscriber profile will be downloaded to the S-CSCF over the Cx-reference point from the HSS (Cx-Pull). When a subscriber requests an IM-service the S-CSCF will check, by matching the request with the subscriber profile, if the subscriber is allowed to continue with the request or not i.e. Home Control (Authorisation of IM-services).

All SIP-signalling will take place over the PS-domain in the user plane i.e. IM-services are essentially an overlay to the PS-domain. Hence the Visited Network will have control of all the subscribers in the PS-domain i.e. Visited Control (Authorisation of bearer resources) since the Visited Network provides with a transport service and QoS.

For IM-services a new security association is required between the mobile and the IM CN SS before access is granted to IM-services. The Home Network or a 3rd party even (which does not have to be an UMTS operator) provides the user with the IM-services.

Since the authorisation of IM-services is the responsibility of the Home Network it is proposed here that also authentication of the IM-subscriber shall be the responsibility of the Home Network. This is in line with what a 3rd party would like to have in general.

The question one might ask is if the Home Network shall have the capability to delegate the authentication of its subscriber to the Visited Network/P-CSCF or not. It is proposed here that for IM-subscribers the Home Network only perform authentication and authorisation to IM-services. The reasons are:

- The main function for the P-CSCF is routing functionality and it can not be compared with a MSC/VLR since the P-CSCF will never be able to control the call session etc. Do not make this node and the signalling flow too complicated by introducing authentication in the P-CSCF.

- Define a new trust model for the new services provided in IM CN SS. The Home Network shall control and react on authentication failures. Note also that 3GPP2 have identified the need for home control for authentication at CS and PS level and the WI "Enhanced home control of security" to support positive authentication reporting has already been approved, [SP-000421].

- Keep the number of options low. If the Home Network shall be able to delegate authentication to the Visited Network some kind of policing is necessary. The policing includes delegating but could also include (in the future) the algorithms e.g. the MAC-algorithm. This addition to complexity is unnecessary.

- Assuming that we allow the Visited Network/P-CSCF to authenticate the IM-subscriber, then it would mean that we would have a mixture of Visited Control and Home Control for IM-Services. Visited Control, since the Visited Network controls the outcome of the authentication and Home Control, since the Home Network controls the authorisation. Therefore this will require maintaining multiple relationships, which should be avoided.
- The Home Network is the service provider and the owner of the IM-services, and which may not be an UMTS-operator. Hence being the service provider, the Home Network shall have control of the authentication of it's subscribers. Of course, the Visited environment will maintain full control at PS-level.
- The solution should not be designed such that it will be unnecessarily difficult to build a system in the future which is access independent. The P-CSCF will always be located in the Visited Network. In the Siemens proposal, [S3-000689] it has been suggested that the P-CSCF functionalities could also be put into the I-CSCF e.g. for a 3GPP2 access, which the authors believe, is a more complicated solution and it does not follow the logical model i.e. the architecture in [3G TR 23.228]. The complication is due to the fact that, in Siemens proposal, both the P-CSCF and the I-CSCF shall be able to perform IM-security and authentication.
- In a general case, the P-CSCF can not be viewed as a trusted node . The authors of this contribution propose that another trust model for IMS should be defined (compared with UMTS at CS and PS level) and the P-CSCF can not be trusted in the general case, since it may reside in an insecure environment. Under some architectural configurations, it might be quite easy to attack such a node, e.g. the fixed line case. To enhanced security, we believe that the authentication and integrity protection shall then be located behind a firewall that the Home Network controls.

In the case that the P-CSCF has to be able to read the SIP-messages, then confidentiality shall also be terminated in the P-CSCF. Confidentiality should not necessarily be provided by SIP itself , since it can be provided by lower layers. From the perspective of the Home Network, this protection may not be used in every case, therefore it is not critical to offer confidentiality protection, as long as the integrity protection is terminated in the Home Network. The fields in SIP messages that P-CSCF has to modify are excluded from the integrity protection. Whether or not this implies that extensions are required in SIP depends on the exact functionality of P-CSCF.

It is the standpoint of the authors that the SIP standard as of today needs to be extended such that the security and authentication requirements for the IM CN SS are fulfilled. Hence it is difficult to actually talk about complexity issues before the philosophy behind IM services and security is defined. When a decision has been taken in S3 and the architecture and trust model has been defined Ericsson, Nokia and Lucent can volunteer to write a problem description, an IETF draft, with general requirements, for extending the existing SIP standard.

4 Conclusions

Based on the arguments presented in this contribution, the IM-subscriber's authentication shall be the responsibility of the HN only.

A new trust model for IMS shall be adopted. The P-CSCF can not, in the general case, be trusted.

Since the P-CSCF will be a node performing routing of SIP-messages and the environment where the P-CSCF resides can not be viewed as a secure environment it shall not perform authentication of IM-subscribers.

The Home Network owns the IM-services and the ability of delivering those services shall not be dependent on the security for other accesses, such as fixed line, hence the authentication on SIP-level shall be in the Home Network. It follows then that the integrity protection shall terminate in the Home Network.

When the IM architecture and trust model has been defined Ericsson , Nokia and Lucent volunteer to write an IETF draft i.e. a problem description such that the SIP standard can be extended to fit the 3GPP requirements.

5 References

[S2-010148] 3GPP TSG SA WG2 Architecture, S2-010148 *Support of both Home and Visited Service Control?;* Source KPN, Mannesmann, Orange, SBC communications, Telia, Vodafone, Alcatel, Fujitsu, Marconi, Ericsson**,** Nokia, Siemens, January 2001.

[S3-000679] 3GPP TSG SA WG3 Security, S3-000679 *Options for Access Security for IM Domain;* Source Motorola, November 2000.

[S3-000689] 3GPP TSG SA WG3 Security, S3-000689 *IMS authentication and integrity/confidentiality protection;* Source Siemens, November 2000.

[S3-000699] 3GPP TSG SA WG3 Security, S3-000699 *Authentication and protection mechanisms for IM CN SS;* Source Ericsson, November 2000.

[S3-000710] 3GPP TSG SA WG3 Security, S3-000710 *IMS authentication in both visited and home networks;* Source Nokia, November 2000.

[S3-16-Rep] 3GPP TSG SA WG3 Security, *Draft report version 0.0.1 S3 #16*, Source Secretary 3GPP TSG-SA WG3, November 2000.

[SP-000421] 3GPP TSG SA Services, SP-000421*6 New Work Item descriptions;* Source 3GPP TSG SA3, September 2000

[S3z000010] 3GPP TSG SA WG3 Security, S3z000010: *Authentication and protection mechanisms for IM CN SS;* Source Ericsson; contribution to the ad-hoc meeting S3#15bis, Munich, 8th - 9th November 2000.

[S3z000022] 3GPP TSG SA WG3 Security, S3z000023: *IMS authentication and integrity/confidentiality protection;* Source Siemens; contribution to the ad-hoc meeting S3#15bis, Munich, 8th - 9th November 2000.

[S3z000023] 3GPP TSG SA WG3 Security, S3z000023: *Comments on 3G TR 33.8xx;* Source Siemens; contribution to the ad-hoc meeting S3#15bis, Munich, 8th - 9th November 2000.

[S3-000446] 3GPP TSG SA WG3 Security, S3-000446: *Requirements on access security for IP-based services;* Source Siemens, July 2000.

[S3-000447] 3GPP TSG SA WG3 Security: *Overview of security mechanisms for access security for IP-based services;* July 2000.

[3G TR 33.8xx] 3GPP TSG SA WG3 Security, TR 33.8xx: *Access security for IP-based services (Release 2000);* v 0.2.0, October 2000.

[3G TS 33.2xx] 3GPP TSG SA WG3 Security, TS 33.2xx: *Access security for IP-based services (Release 4)";* v 0.1.0, October 2000.

[3G TR 23.228] 3GPP TSG SA WG2, TR 23.228: IP multimedia (IM) subsystem - Stage 2; v 1.2.0, October 2000.