3GPP TSG SA WG3 Security **S3-040762**

5 - 8 October 2004

St Paul's Bay, Malta, October 5-8, 2004

Agenda Item:	IMS
Source:	Ericsson
Title:	Revisiting forwards compatibility towards TLS based access security
Document for:	Discussion/Decision

1. Discussion

SA3#34 adopted new naming requirements to 33.203 R6 related to potential future use of TLS in IMS access security. The requirements were adopted in order to avoid a future backwards compatibility problem if 3GPP decides to use TLS for access security some day in the future. In one TLS deployment model, it will be practically impossible for UE to figure out if the visited network should be trusted and if it belongs to the same trust domain with the home network. See more technical details in Appendix A.

SA3#34 sent LS to CN1, CN4 and SA2. In these groups, the LS caused worries on end-user experience, especially because it set naming restrictions to public user identities (IMPUs). The general feeling was that the naming restrictions should not be visible to the end-user.

The CR was also discussed in SA Plenary. Similar concerns were repeated, and the CR was rejected.

Ericsson agrees on the concerns related to IMPU naming, and would like to propose an updated version of the CR in which the naming restrictions are limited to those naming schemes which are not visible to the user, i.e. home network names and IMPIs. In fact, from security point of view, there is no need to have naming restrictions on IMPUs. The username that is authenticated in IMS access security is IMPI, and IMPUs are not directly involved.

New versions of the CR and the LS are attached to this document.

Appendix A: Technical analysis presented in TD S3-040531

2. Background

There are no current plans in SA3 to use TLS for IMS access security. However, there are some reasons why this may become interesting option in the future:

- TLS is the only mandatory access security mechanism that all SIP servers support. Consequently, it is very likely that there will be SIP terminals that support TLS but not IPsec. 3GPP may want to exploit this terminal base in the future.
- IMS UE must have TLS in Release 6 for Presence. Using the same security solution with IMS related applications would make sense from UE perspective.
- One reason why TLS was not accepted as IMS access security solution in R5 was that TLS couldn't be used with UDP. However, there have been proposals for creating a TLS variant that could do this, i.e. WTLS in former WAP forum, and recent work in IETF on DTLS (Rescorla & Modadugu 2004).

Figure 1 demonstrates the general differences between the IPsec and TLS based access security solutions. The IPsec based solution handles the security agreement and (UDP related) re-transmission at SIP layer while the TLS based solution would do these at TLS and transport layer. On the other hand, the message protection itself is located either over IP (IPsec) or transport (TLS).

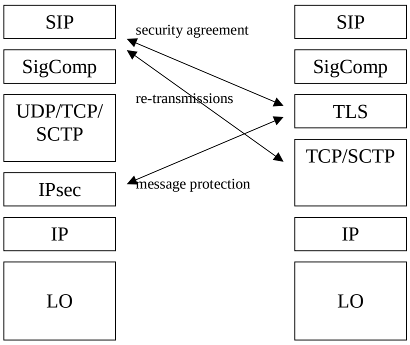

Figure 1: Change of responsibilities in protocols stack

3. Forwards compatibility requirements

Even though this document does not propose that TLS should be used in IMS for access security, it is still important to keep this option open for future. TLS could be applied in several formats for IMS in the similar way that SA3 has already discussed with HTTPS context. This section analyzes forwards compatibility requirements with three main deployment models, i.e. shared key based UE authentication with certificate-based P-CSCF authentication, certificate based mutual authentication, and shared key based mutual authentication.

3.1 Shared key based UE authentication with certificate based P-CSCF authentication

In this case, TLS would be used in the mode where the server side was authenticated using TLS server certificate, and the client using HTTP Digest AKA. TLS connection would be set up using SIP REGISTER message, and then left open for further SIP messages (cf. registration procedure in RFC 3261). Note that using a UAC initiated TLS connection to receive SIP requests to UAS is possible in this model, however, it may require some specific features from SIP/TLS implementation. Note also that TLS session cannot be resumed from P-CSCF side; only UE is able to resume TLS sessions.

There are two general recommendations specified in RFC 3261 related to server side naming of SIP registrars (see section "26.3.2.1 Registration" in Security Considerations). Firstly, UAs should not trust on the registrar (or first-hop proxy such as P-CSCF) unless the domain name in TLS server certificate match the name of the home domain of the UA (or chain back to a trusted root certificate which belongs to the UA's home domain). Secondly, the realm parameter in the HTTP Digest authentication header should also match the TLS server certificate. If these two conditions are not met, the UA is not able to verify if the registrar/first-hop proxy is authorized to act in that role (i.e. potential man-in-the-middle attack). Also in IMS, the registration procedure should be done using a TLS server certificate that somehow chain back to the home domain of the UE. That is, the site TLS certificate should identify a host within the domain of the UE. Furthermore, the realm parameter in the WWW-Authenticate header should somehow correspond with the site certificate received from P-CSCF.

All entities that support TLS must also have a mechanism for validating certificates during TLS negotiation. In practice, this means that all these entities must belong to some PKI, and possess one or more trusted root certificate/public key. TLS uses the so-called “certificate list” to communicate PKI trust models, i.e. the certificate hierarchy must be a chain. The senders certificate is always first in the list, and each following certificate must directly certify the one preceding it. The certificate lists are always static: it is not possible to offer different lists for different clients.

One possible solution to the problem would be to defined IMS as one big trust domain. For example, IMS trust domain could be “ims.com”, and consequently all P-CSCFs, both in visited and home networks, should possess a certificate with this one name. Also, S-CSCF should use an operator specific identifier of IMS trust domain in the realm parameter, e.g. “operator1.ims.com” or “operator1@ims.com”. IMS specifications already include similar name space that could be re-used. The name space is specified in 23.003, section 13 for the case when USIM is used to access IMS. All home networks domain names and private/public user identities that are derived from the IMSI begins with a static string “ims.”, and end with a string “3gppnetwork.com”.

3.2 Certificate based mutual authentication

In certificate based mutual authentication, both UE and P-CSCF would have TLS certificates. Theoretically speaking, there are two ways to apply certificates for mutual authentication:

- If UE has only TLS client certificate, the deployment model is similar to what was described in section 3.1. More specifically, the TLS session should be left open after successful authentication.
- If UE has also TLS server certificate, the TLS session could be turned off after registration because also P-CSCF would be able to initiate TLS handshake (taking the TLS client role).

The use of mutual authentication between UE and P-CSCF does not remove the need for end-to-end authentication between UE and S-CSCF. Consequently, this deployment model includes all the same naming issues than what was described in section 3.1 (assuming that UE needs to avoid man-in-the-middle attacks related to registration procedure).

3.3 Shared key based mutual authentication

The use of shared-key TLS in IMS does not have the naming problems described in section 3.1. However, shared-key TLS should only be seen as an optimization, and consequently at least one certificate based TLS solution should also be supported.

4. References

Rescorla & Modadugu (2004) Datagram Transport Layer Security, IETF, work in progress, draft-rescorla-dtls-00.txt.

RFC 3261 SIP: Session Initiation Protocol, IETF, June 2002.

23.003, Numbering, addressing and identification, 3GPP, Technical Specification, V6.3.0, Release 6.

3GPP TSG SA WG3 Security — S3#35 **Att1_S3-040762**
St Paul's Bay, Malta, October 5-8, 2004

CR-Form-v7

CHANGE REQUEST

⌘	**33.203**	**CR**	**074**	⌘ **rev**	**-**	⌘	Current version:	6.4.0 ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the* ⌘ *symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Forwards compatibility to TLS based access security
Source:	⌘	Ericsson
Work item code:	⌘	IMS-ASEC
Date:	⌘	5 October 2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Current IMS specification is not forward compatible to one potential deployment mode of TLS based access security.
Summary of change:	⌘	Adds one potential solution.
Consequences if not approved:	⌘	One potential TLS deployment mode cannot be used when UE is roaming in visited network.

Clauses affected:	⌘	8.1				
		Y	**N**			
Other specs affected:	⌘	**Y**		Other core specifications	⌘	23.003
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

***** Begin of Change ****

8.1 Requirements on the ISIM application

This clause identifies requirements on the ISIM application to support IMS access security. It does not identify any data or functions that may be required on the ISIM application for non-security purposes.

The ISIM shall include:

- The IMPI;
- At least one IMPU;
- Home Network Domain Name;
- Support for sequence number checking in the context of the IMS Domain;
- The same framework for algorithms as specified for the USIM applies for the ISIM;
- An authentication Key.

Domain and realm names used in IMPI, and Home Network Domain Name shall contain IMS Trust Domain Name.

NOTE: The exact content and format of IMS Trust Domain Name is out of the scope of this specification. It could be, for example, “ims.com” or “3gppnetwork.com”.

NOTE: This requirement guarantees that TLS can be used for IMS access security between UE and P-CSCF in the future.

The ISIM shall deliver the CK to the UE although it is not required that SIP signalling is confidentiality protected.

At UE power off the existing SAs in the MT shall be deleted. The session keys and related information in the SA shall never be stored on the ISIM.

***** End of Change ****

3GPP TSG SA WG3 Security **S3-040762**

5 - 8 October 2004

St Paul's Bay, Malta, October 5-8, 2004

Title:	LS on Revisiting forwards compatibility towards TLS based access security
Release:	Rel-6
Source:	SA3
To:	CN1, CN4, SA2
Cc:	-

Contact Person:

Name:	Bengt Sahlin
Tel. Number:	+358 40 7784580
E-mail Address:	bengt.sahlin@ericsson.com

Attachments:	S3-040xxx (Updated discussion paper on the problem statement) S3-040xxy (Proposed CR)

1. Overall Description:

SA3 has continued discussions on potential future backwards compatibility problem related to the way IMPI, IMPU and Home Network Domain Name are specified in ISIM related specifications. SA3 has re-evaluated its earlier decision on introducing naming restrictions, and decided to loose the proposed requirement. It is still believed that IMS access security architecture should be based on naming scheme in which the domain and realm names are defined in that way that IMS is seen as one big trust domain. Otherwise, one deployment mode of using TLS for IMS access security is not possible in the future (see more details in the attached documents). However, it is not necessary that these naming rules are visible to the end-user, and consequently there will be no new requirements related to IMPUs. IMPI and Home Network Domain Name are still affected.

2. Actions:

To CN1 and CN4

ACTION: SA3 kindly asks CN1 and CN4 to take note of the above decision, and update related IMS specifications accordingly.

To SA2

ACTION: SA3 kindly asks SA2 to take note of the above decision.

3. Date of Next TSG-SA3 Meetings:

SA3#36	23 - 26 November 2004	Shenzhen, China