3GPP TSG SA WG3 Security — S3#37 **S3-050063**
21 - 25 February 2005
Sophia Antipolis, France

Agenda Item: 6.1.2 Early IMS

Source: Ericsson

Title: HTTPS with early IMS

Document for: Discussion/Decision

1. Introduction

Some IMS services, such as Presence/Ut interface, require the use of HTTP. Current Early IMS specification [33.978] focus on protecting SIP signalling traffic, and does not take any stand on how HTTP traffic is protected. On the other hand, the use of HTTPS as specified in [33.222] is hardly possible because of the potential lack of support of the USIM/ISIM interface in the UE side. This document further discusses the problem of HTTP traffic in early IMS context, and proposes a way forward.

2. Discussion

HTTP security is a challenging topic because there are so many standards available, e.g. IETF, 3GPP, WAP, and Liberty Alliance standards. The minimum implementation requirement in current 3GPP HTTPS specification [33.222] practically mandates TLS for server side authentication. For client side authentication, the document promotes the use of GBA with HTTP Digest, however, the use of other authentication methods, such as Liberty Alliance protocols, are also allowed. Two other GBA based TLS variants are optional, i.e. TLS with subscriber certificates, and pre-shared key TLS[1].

Assuming that USIM/ISIM interface is not available in Early IMS, the following security standards may still be available:

- OMA WAP specifications, e.g. [WAP-TLS]
- Manual passwords (with HTTP Digest MD5 and/or Liberty Alliance protocols)

Third alternative would be to re-use early IMS security mechanism also for HTTP traffic. This option is appealing because all components for this solution are already in place for early IMS, and consequently the cost of this solution would be very low.

4. Proposal

Ericsson proposes that early IMS specification should take a stand on how HTTP traffic can be protected. In minimum, the specification should give a recommendation on what mechanisms are assumed to be implemented in the UE side.

Because early IMS security mechanism could be re-used also for HTTP traffic quite easily, Ericsson proposes that such solution is also allowed in the TR.

Attached CR makes the required changes to TR 33.978.

[1] It is still open if PSK TLS will be part of R6.

5. References

[33.222] Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS), Release 6, 3GPP TS 33.222.

[33.978] Security Aspects of Early IMS, Release 6, 3GPP TR 33.978.

[WAP-TLS] OMA WAP-219-TLS, 4.11.2001: http://www.openmobilealliance.org/tech/affiliates/wap/wap-219-tls-20010411-a.pdf.

3GPP TSG-SA3 Meeting #37
Sophia Antipolis, France, 21-25 February 2005

Tdoc ⌘att_S3-050063

CR-Form-v7.1

PSEUDO-CHANGE REQUEST

⌘ **33.978** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **1.0.0** ⌘

*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:	⌘	HTTPS with early IMS
Source:	⌘	Ericsson
Work item code:	⌘	Early IMS
Date:	⌘	14/02/2005
Category:	⌘	
Release:	⌘	Release-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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Currently early IMS specifications do not take any stand on how HTTP traffic is protected. HTTP is needed for some IMS services, such as Presence/Ut interface.
Summary of change:	⌘	Adds a statement on how HTTP can be protected with early IMS.
Consequences if not approved:	⌘	Potential interoperability problems.

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

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

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

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 23.981: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Interworking aspects and migration scenarios for IPv4 based IMS Implementations".

[2] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services".

[3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage ".

[4] 3GPP TS 29.061: "3rd Generation Partnership Project; Technical Specification Group Core Network; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[5] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".

[6] IETF RFC 3261: "Session Initiation Protocol".

[7] 3GPP TS 24.229: "3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[8] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[9] 3GPP TS 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[10] 3GPP TS 29.228: "3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[11] draft-ietf-aaa-diameter-nasreq-17.txt (July 2004), "Diameter Network Access Server Application", work in progress.

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[12] 3GPP TS 29.229: "3rd Generation Partnership Project; Technical Specification Group Core Network; Cx and Dx interfaces based on the Diameter protocol; Protocol details".

[13] 3GPP TS 23.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architectural requirements".

[14] 3GPP TS 33.222: " 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) ".

[15] IETF RFC 2617: " HTTP Authentication: Basic and Digest Access Authentication ".

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

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

6 Specification

6.1 Overview

The early IMS security solution works by creating a secure binding in the HSS between the public/private user identity (SIP-level identity) and the IP address currently allocated to the user at the GPRS level (bearer/network level identity). Therefore, IMS level signaling, and especially the IMS identities claimed by a user, can be connected securely to the PS domain bearer level security context.

The GGSN, terminates each user's PDP context and has assurance that the IMSI used within this PDP context is authenticated. The GGSN shall provide the user's IP address, IMSI and MSISDN to a RADIUS server in the HSS over the Gi interface when a PDP context is activated towards the IMS system. The HSS has a binding between the IMSI and/or MSISDN and the IMPI and IMPU(s), and is therefore able to store the currently assigned IP address from the GGSN against the user's IMPI and/or IMPU(s). The precise way of the handling of these identities in the HSS is outside the scope of standardization. The GGSN informs the HSS when the PDP context is deactivated/modified so that the stored IP address can be updated in the HSS. When the S-CSCF receives a SIP registration request or any subsequent requests for a given IMPU, it checks that the IP address in the SIP header (verified by the network) matches the IP address that was stored against that subscriber's IMPU in the HSS.

The mechanism assumes that the GGSN does not allow a UE to successfully transmit an IP packet with a source IP address that is different to the one assigned during PDP context activation. In other words, the GGSN must prevent "source IP spoofing". The mechanism also assumes that the P-CSCF checks that the source IP address in the SIP header is the same as the source IP address in the IP header received from the UE (the assumption here, as well as for the full security solution, is that no NAT is present between the GGSN and the P-CSCF).

The mechanism prevents an attacker from using his own IP address in the IP header but spoofing someone else's IMS identity or IP address in the SIP header, so that he pays for GPRS level charges, but not for IMS level charges. The mechanism also prevents an attacker spoofing the address in the IP header so that he does not pay for GPRS charges. It therefore counters the threat scenarios given in clause 5 above.

The mechanism assumes that only one contact IP address is associated with one IMPI. Furthermore, the mechanism supports the case that there may be several IMPUs associated with one IMPI, but one IMPU is associated with only one IMPI.

In early IMS the IMS user authentication is performed by linking the IMS registration (based on an IMPI) to a PDP context (based on an authenticated IMSI). The mechanism here assumes that there is a one-to-one relationship between the IMSI for bearer access and the IMPI for IMS access.

It should be noted that implementations needs also to supplement the early IMS security solution with a security solution for HTTP traffic in order to provide access for user for various potential self-customization services, e.g. to Presence Server. It is recommended that UE side implementations prepare to use TLS server side certificates for server authentication as specified in section 5.3.1 in [14] and HTTP Digest [15] for UE authentication. It is also possible that solutions similar to early IMS security solution are re-used to protect HTTP traffic, however, this does not require any new functionality from the UE side for interoperability.

For the purposes of this present document, an APN, which is used for IMS services, is called an IMS APN. An IMS APN may be also used for non-IMS services. The mechanism described in this present document further adds a restriction that there is only one APN for accessing IMS for a PLMN and that all active PDP contexts, for a single UE, associated with that IMS APN use the same IP address at any given time.

In the following we use the terms P-CSCF and S-CSCF in a general sense to refer to components of an early IMS system. We note however that early IMS solutions may not have the same functionality split between SIP entities as

defined in TS 23.228 [3]. Therefore, the requirements imposed on the SIP/IP core are specified in such a way that they are independent of the functionality split between SIP entities as far as possible. While the exact functionality split of the SIP/IP core may be left open, it is important that any changes to the Cx interface towards the HSS and changes to the interface towards the UE are standardised for vendor interoperability reasons.

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