3GPP TSG SA WG3 Security — SA3#33 **S3-040348**
10-14 May 2004
Beijing, China

Source: **Ericsson**

Title: **AP-AS Interface Protection**

Document for: **Discussion and decision**

Agenda Item: **GAA/Presence**

1 Introduction

This contribution discusses protection for the interface between the Authentication Proxy and Application server.

2 Discussion

Draft TS 33.222 does not currently cover protection for the interface between the AP and the AS. Draft TS 33.141 contains the following editor's note:

"Editors Note: The exact requirements on the Zb interface the use of NDS/IP for Presence Security are FFS."

TS 33.210 [1] specifies how NDS/IP mechanisms can be used for confidentiality and integrity protection. For traffic between security domains, the Za interface shall be deployed. For traffic inside a domain, the Zb interface can be deployed.

3 Proposal

We think that the AP-AS interface protection should follow the same design principle that was used in IMS network domain security, which rely on NDS/P mechanisms [1]. We propose the following amendment to draft TS 33.141:

"Confidentiality and integrity protection may be provided for the interface between the AP and the AS, using the Zb interface of NDS/IP as specified in TS 33.210 [x]."

We propose the following amendment to draft TS 33.222:

"Confidentiality and integrity protection can be provided for the interface between the AP and the AS using NDS/IP mechanisms as specified in TS 33.210 [x]. For traffic between different security domains, the Za interface shall be operated. For traffic inside a security domain, it is up to the operator to decide whether to deploy the Zb interface. "

The attached pseudo-CRs implement the changes to TS 33.222 and TS 33.141.

4 References

[1] 3GPP TS 33.210 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security".

3GPP TSG-SA WG3 Meeting #33
Beijing, China, 10 - 14 May 2004

Tdoc ⌘DocNumber

CR-Form-v7

CHANGE REQUEST

⌘ **33.222** **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:	⌘	AP-AS Interface Protection
Source:	⌘	Ericsson
Work item code:	⌘	GAA
Date:	⌘	03/05/2004
Category:	⌘	**C**
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:	⌘	Introduce protection for interface between Authentication Proxy and Application Server
Summary of change:	⌘	NDS/IP can be used for protection between the AP and the AS, in line with design principles applied for IMS network domain security.
Consequences if not approved:	⌘	
Clauses affected:	⌘	Table of Contents, 2, 6.1, 6.4

		Y	N			
Other specs affected:	⌘			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 ***

Contents

*** END OF CHANGE ***

*** 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 TS 23.002: “Network architecture”.

[2] 3GPP TS 22.250: “IP Multimedia Subsystem (IMS) group management”; Stage 1”.

[3] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[4] 3GPP TR 33.919: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System description".

[5] 3GPP TS 33.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Security"

[6] IETF RFC 2246 (1999): "The TLS Protocol Version 1".

[7] IETF RFC 3268 (2002): "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)".

[8] IETF RFC 3546 (2003): "Transport Layer Security (TLS) Extensions".

[9] IETF RFC 2818 (2000): “HTTP Over TLS ”.

[10] IETF RFC 2617 (1999): "HTTP Authentication: Basic and Digest Access Authentication"

[11] IETF RFC 3310 (2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)"

[12] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

*** END OF CHANGE ***

*** BEGIN OF CHANGE ***

6 Use of Authentication Proxy

6.1 Architectural view

Figure 2 presents an architectural view of using Authentication Proxy, for example, for IMS SIP based services. The UE shall manipulate own data such as groups, through the Ua/Ut interface. The interface Ut specified in TS 23.002 [1] shall

be applicable to data manipulation of IMS based SIP services, such as Presence, Messaging and Conferencing services. The stage 1 requirements are specified in TS 22.250 [2].

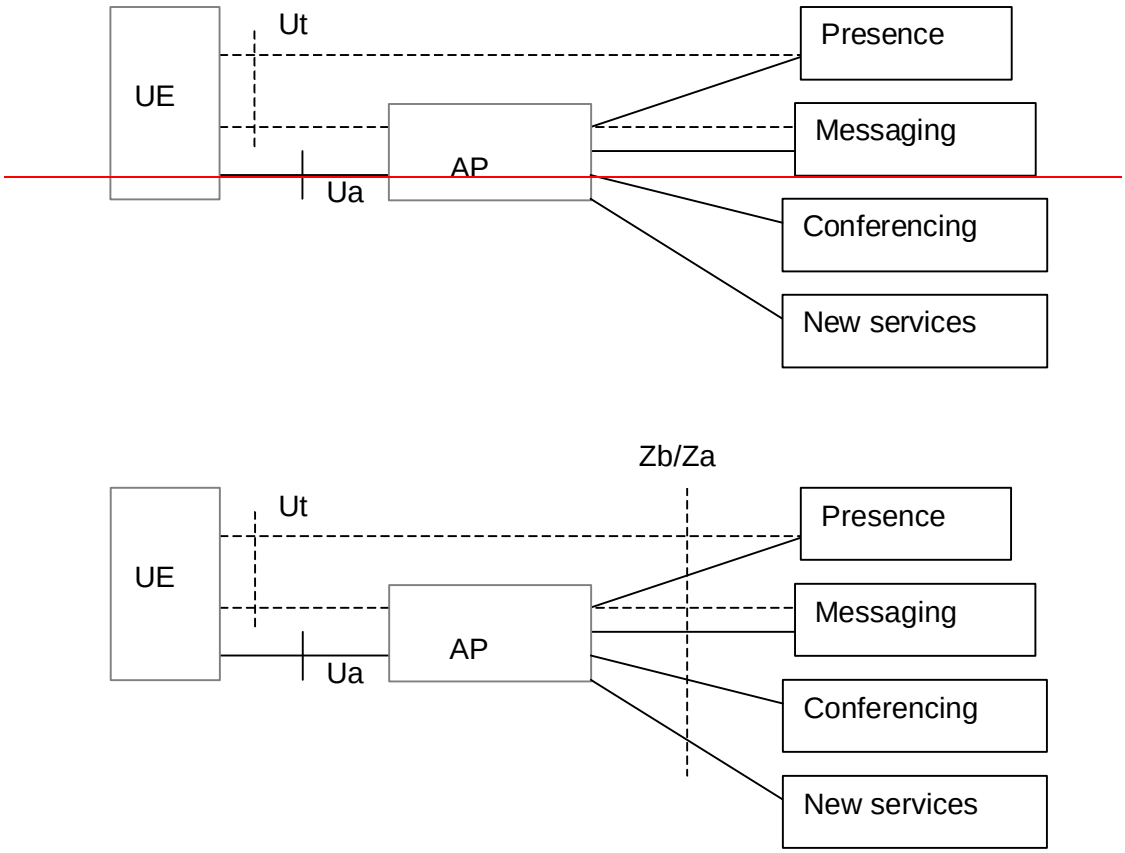

Figure 2: The architectural view using Authentication Proxy for IMS SIP based services

*** END OF CHANGE ***

*** BEGIN OF CHANGE ***

6.4 Interfaces

6.4.1 AP-AS Interface

"Confidentiality and integrity protection can be provided for the interface between the AP and the AS using NDS/IP mechanisms as specified in TS 33.210 [12]. For traffic between different security domains, the Za interface shall be operated. For traffic inside a security domain, it is up to the operator to decide whether to deploy the Zb interface. "

*** END OF CHANGE ***

3GPP TSG-SA WG3 Meeting #33
Beijing, China, 10 - 14 May 2004

Tdoc ⌘DocNumber

CR-Form-v7

CHANGE REQUEST

⌘ **33.141** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **1.1.1** ⌘

*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:	⌘	AP-AS Interface Protection
Source:	⌘	Ericsson
Work item code:	⌘	Presence
Date:	⌘	03/05/2004
Category:	⌘	**C**
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:	⌘	Introduce protection for interface between Authentication Proxy and Application Server
Summary of change:	⌘	The Zb interface may be used for protectin between the AP and the AS
Consequences if not approved:	⌘	
Clauses affected:	⌘	4, 5.1.4

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 ***

4 Overview of the security architecture

An IMS operator using the CSCFs as Watcher Presence proxies and Presentity Presence proxies may offer the Presence services on top of the IMS network, cf. 3GPP TS 22.141 [2]. The access security for IMS is specified in 3GPP TS 33.203 [4] ensuring that SIP signalling is integrity protected and that IMS subscribers are authenticated through the use of IMS AKA. The security termination point from the UE towards the network is in the P-CSCF utilising IPsec ESP.

A watcher can be sending a SIP SUBSCRIBE over IMS towards the network to subscribe or to fetch presence information, i.e. the Presence Service supports SIP-based communications for publishing presence information. The presence information is provided by the Presence Server to the Watcher Application using SIP NOTIFY along the dialogue setup by SUBSCRIBE. This traffic is protected in a hop-by-hop fashion using a combination of SEGs as specified in 3GPP TS 33.210 [10] with the access security provided in 3GPP TS 33.203 [4].

The Presence Server is responsible for managing presence information on behalf of the presence entity and it resides in the presentity's home network. Furthermore the Presence Server provides with a subscription authorization policy that is used to determine which watchers are allowed to subscribe to certain presence information. Also the Presence Server shall before subscription is accepted try to verify the identity of the watcher before the watcher subscribes to presence information. Optionally, depending on the implementation, the Presence Server may authenticate an anonymous watcher depending on the Subscription Authorization Policy.

A Presence List Server is responsible of storing grouped lists of watched presentities and enable a Watcher Application to subscribe to the presence of multiple presentities using a single SIP SUBSCRIBE transaction. The Presence List Server also stores and enables management of filters in the presence list, cf. Figure 1.

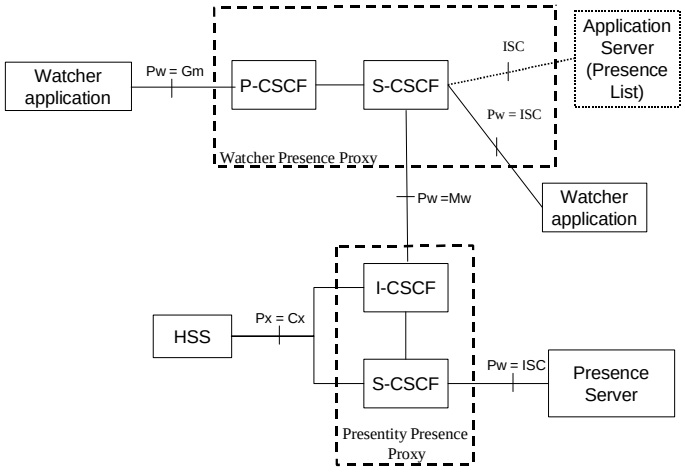

Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

A Presence User Agent shall be able to manage the data on the AS over the Ut interface, cf. 3GPP TS 23.002 [7], which is based on HTTP. This interface is not covered in 3GPP TS 33.203 [4] and it is mainly this interface for Presence use, which is covered in this specification. Before manipulation is allowed the user needs to be authenticated.

Note: In the text below the term Presence Server refers to both the Presence Server and the Presence List Server as depicted in Figure 1 above. For definitions of the Application Servers for Presence services the reader should consult 3GPP TS 23.141 [3]

The Ut interface needs the following security features:

1. it shall be possible to provide with mutual authentication between the Presence Server and the Watcher/Presentity;

2. a secure link and security association shall be established between the Presence Server and the Watcher/Presentity. Data origin authentication shall be provided as well as confidentiality protection.

Editors Note The specification need to consider [6], [8] and [9] and make appropriate profiling of these TLS protocols and the TLS version 1.1. need to be considered also.

Editors Note: The exact details of the security architecture is FFS and dependant on decisions related with the ongoing work on GBA (Generic Bootstrapping Architecture).

An overview of the security architecture for Presence Ut Interface is depicted in figure 2:

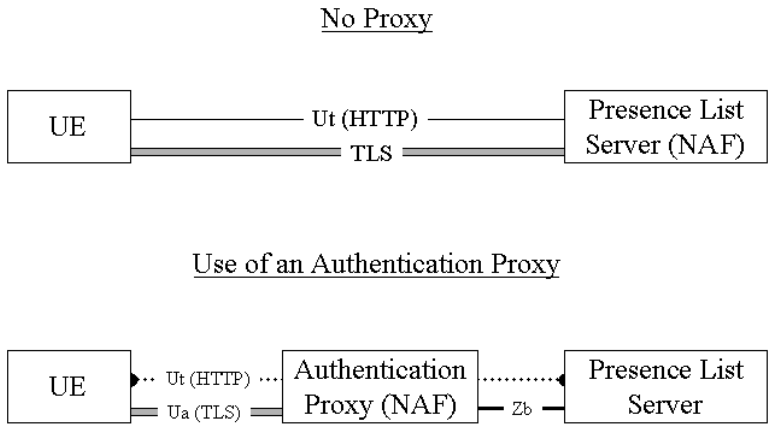

Figure 2: An overview of the Security architecture for the Ut interface including the support of an Authentication Proxy

~~Editors Note: The exact requirements on the Zb interface the use of NDS/IP for Presence Security are FFS.~~

*** END OF CHANGE ***

*** BEGIN OF CHANGE ***

5.1.4 Authentication Proxy

The Authentication Proxy may reside between the UE and the Presence Server as depicted in Figure 2. The usefulness of an Authentication Proxy may be to reduce the consumption of authentication vectors and/or to minimize SQN synchronization failures.

The following requirements apply for the use of an Authentication Proxy:

- Authentication Proxy may authenticate the UE using the means of Generic Bootstrapping Architecture.

- Authentication Proxy shall send the authenticated identity of the UE to the application server belonging to the trust domain at the beginning of new HTTP session.

- Authentication Proxy may not reveal the authenticated identity of the UE to the application server not belonging to the trust domain if required.
- The authenticated identity management mechanism shall not prevent the application server to use an appropriate session management mechanisms with the client.
- The UE shall be able to create multiple parallel HTTP sessions via the Authentication Proxy towards different application servers.
- Activation of transfer of asserted user identity shall be configurable in the Authentication Proxy on a per AS base.
- Implementation of check of asserted user identity in the AS is optional.

NOTE 1: The used session management mechanism is out of the scope of 3GPP specifications.

The use of an Authentication Proxy should be such that there is no need to manage the Authentication Proxy configuration in the UE.

NOTE 2: This requirement implies that the Authentication Proxy should be a reverse proxy in the following sense: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers - in addition to web pages on disk or generated dynamically by CGI - making these pages look like they originated at the reverse proxy

[Editors Note: The above requirement may be revisited after the following issues are fully studied:
- Feasibility of shared-key TLS
- Terminal Configurability]

"Confidentiality and integrity protection may be provided for the interface between the AP and the AS, using the Zb interface of NDS/IP as specified in TS 33.210 [10]."

*** END OF CHANGE ***