3GPP TSG SA WG3 Security — S3#32 **S3-040068**
09 - 13 February 2004
Edinburgh, Scotland, UK

Title **CR to TS 33.141 Presence**

Source: **Nokia**

Document for: **Approval**

Introduction

This contribution provides changes to the draft TS 33.141: Presence Service. The change is a new section where the user identity is handled by Authentication Proxy or Application Server in universal manner.

Background

There was discussion on the issue how to transfer UE's identity to application server when Authentication Proxy is used in between. S3-030540 suggests AP and AS to insert cookies, and Nokia proposed (S3-030731 and S3-030555) that the UE shall insert own identity intended to use, and the AP simply verifies the validity of the identity by utilizing the user profile retrieved from BSF. Here are conparision and contrast betweent the two approaches we found below:

1. Current HTTP implementations have own API defined already (for setting and fetching/comparing a cookie), and having a "special" cookie value would mean an extra processing step when receiving the cookie. This might also interfere with normal AS session handling using HTTP cookies. By using AP verification, this problem is dismissed.

2. It is requiring ASs to understand a particular token syntax for the cookie. Contrastly, if Authentication Proxy does the checking, then Application server does not need to understand anything about security. This would easy the interoperability between SIP vendor and IMS infrastructure vendor. The usage of Authentication Proxy is to handle the security function on behalf of application servers. If the servers have to handle specific security function, it makes the overall architecture redudant.

3. Also, an AS that doesn't care about identity could then ignore this header and do as it pleases. An out-of-the box AS could not do this if we used cookies, since it would have to know at least the "special" cookie in order to ignore it (and not think that a cookie is invalid etc.) Same problem as 2.

4. The sentence seems to suggest that only one IMPU is used: "AS can assume that the AP has authenticated the client with this identity." If so, it does not fulfil the requirement that AS would be contacted with any of the IMS IMPUs.

5. Even cookie mechanism or other type of 'X-' headers are used, the Authentication Proxy must still verify the HTTP request, to guarantee that no malicious insertion of others cookie was done by UE. So if a single point verification can fulfill the function, the insertion by AP additionally seems to be redudent.

6. A check against the requirements of using an Authentication Proxy exerpted from Presence TS:
   - Authentication proxy shall be able to authenticate the UE using the means of Generic Bootstrapping Architecture, as specified in [Ts33.220]. This is satisfied with solution proposed by Nokia.
   - 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. The valid public identity shall be transparently forwarded to application server. This is satisfied with solution proposed by Nokia.
   - Authentication proxy may not reveal the authenticated identity of the UE to the application server not belonging to the trust domain if required. The private identity is not used in HTTP message, but only the public id. This is satisfied with solution proposed by Nokia.
   - The authenticated identity management mechanism shall not prevent the application server to use an appropriate session management mechanisms with the client. Depends on whether it is the application server or Authentication Proxy connecting to the UE directly. The server can utilize the session management.
   - The UE shall be able to create multiple parallel HTTP sessions via the authentication proxy towards different application servers. This is satisfied with solution proposed by Nokia.

NOTE1: The used session management mechanism is out of the scope of 3GPP specifications.

- Implementation of check of asserted user identity in the AS is optional. This is satisfied with solution proposed by Nokia.

- Activation of transfer of asserted user identity shall be configurable in the AP on a per AS base. It is decided by AP whether the identity inserted is valid and could be transferred. This is satisfied with solution proposed by Nokia.

There is also another approach that the AP inserts a new HTTP header into every HTTP request. We see the approach is basically better ininteroperability, but still seems redudent since AP must insert the identity as well as verify the other identities used. For example, the XCAP URL always points to each public identity of a user, therefor AP not only needs to verify the headers present in the HTTP request, but also the URL. It is simplier solution to have single verification than more complicated approaches defined with cookie or X- extension header.

Conclusion:

The attached CR is proposed to add into the Presence TS.

3GPP TSG SA WG3 Security — S3#32 **Att1_S3-040068**
09 - 13 February 2004, Edinburgh, Scotland, UK

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.141 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:	⌘	The user identity management
Source:	⌘	Nokia
Work item code:	⌘	Presence security
Date:	⌘	29/1/2004
Category:	⌘	**B**
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 specification is empty on how to handle the user's identity management when accessing to each server, particular when Authentication Proxy presents.
Summary of change:	⌘	A new subclause is added to specify a generic mechanism that the terminal inserts and thus indicates its public identity intended to use, and the network server shall verify it with a common behavior specified.
Consequences if not approved:	⌘	Risk the completion of the specification in question.

Clauses affected:	⌘	6.1.3				
		Y	**N**			
Other specs affected:	⌘	**X**	**X**	Other core specifications	⌘	24.xxx
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

--------- CHANGE START---------

6.1 Authentication and key agreement

6.1.1 ~~6.1.1~~ Authentication of the user

6.1.2 Authentication of the Server

6.1.3 User identity management

The server (Authentication Proxy or Presence Server) shall obtain the UE's private identities after a successful authentication procedure, based on user profile retrieved from BSF or received from a non-GBA identity provider.

The UE shall insert its public identity to the HTTP request when accessing the intended group lists. Before accepting the request, the server shall verify the identity does belong to this subscriber, and is subscribed to the service managing the group lists.

---------END OF CHANGE---------

6.1.3 ~~6.1.3~~ Authentication Failures

6.2 Confidentiality mechanisms

6.3 Integrity mechanisms