3GPP TSG SA WG3 Security – S3#31 **S3-030722**

18th – 21st, November, 2003

Munich, Germany

Agenda Item: GAA

Source: Ericsson

Title: User authentication process decision

Document for: Discussion/Decision

1. Introduction

This document suggests a general approach to be considered by applications regarding the user authentication in order to make the application decision flexible.

2. Background

In order to face the problem of user authentication by applications, there are three Technical Specifications within the Generic Authentication Architecture WI covering

a) an Architecture for Bootstrapping,

b) a mechanism for the use of subscriber certificates and

c) the use of HTTPS to access the 3GPP applications.

TR 33.919 aims to provide a comprehensive architecture of these possible user authentication mechanisms and the relation between these different Technical Specifications.

It shall be then possible for a 3GPP application to perform user authentication with any of the mechanism defined by these three Technical Specification. According to the meeting report from SA3#30 meeting, SA3 also has the following working assumption …

> *"The SA WG3 Chairman also summarised that **for HTTP-based services**, SA WG3 have a Working Assumption that for each of the Rel-6 Services, SA WG3 will decide which mechanisms are to be used and only one way will be specified for each Service. Although it has not been decided whether GBA or GAA will be used for the Presence Service, if GBA is chosen, we would need to use either an Authentication Proxy or the Application Server (i.e. the Presence Server) with the BSF. If the Authentication Proxy is identified, should it be made mandatory for the Presence Service."*

3. Authentication decision

According to this working assumption, one may understand that a 3GPP application (e.g. Presence) will have to use one and only one of the GAA mechanisms in order to perform user authentication. However, Ericsson believes that this working assumption might be too restrictive and if not articulated in the correct terms it might be preventing 3GPP applications to work in heterogeneous authentication environments.

The actual initiation of the user authentication procedure by an application is something that should be evaluated by the own application. This evaluation is needed because there are potential reasons that make the user authentication process unnecessary.

There are scenarios where applications may not be making use of any of the mechanisms under GAA scope in order to authenticate users accessing their services. Actually, there are cases where applications will not be authenticating the users at all, for example

- There is a VPN between a Home GGSN and the network where applications reside so that only the users authenticated by the Core Network can access the applications.

- Applications rely on a third party to perform user authentication …

  a) System deploys a Proxy Authenticator, which authenticates users (e.g. making use of GBA) before they actually contact the applications. Applications are aware of this network set-up and therefore it is not required that they execute authentication themselves.

  b) System deploys an Identity Provider (IdP) according to Liberty standards [LAP], which is able to authenticate users (e.g. making use of GBA) and generate essential information regarding this authentication (SAML-based authentication assertions) for the application to authorize access to its services. Applications are aware of this network set-up and instead of authenticating the user themselves, will choose to request the IdP to perform these actions.

     Note: Refer to the Appendix at the bottom of this contribution for a more illustrative information on how this case may look like.

4. Conclusions

There are scenarios where applications should not be required to perform user authentication themselves. In some cases, the user request may be considered already authenticated, in some other cases the application will decide to trust a third party to perform such authentication.

In order to accommodate these different authentication models, 3GPP specifications about end user applications that may require authenticating the user requesting the service, should give the application the chance to decide (based on internal policies and/or network set-up) if the initiation of a user authentication process (e.g. making use of any of the GAA mechanisms) is really necessary.

It is proposed that this is agreed as an S3 working assumption while defining security solutions (i.e. user authentication solutions) at the different 3GPP applications.

For example, in S3-030525 (Draft TR 33.9bc V0.6.0 Presence Service; Security), it is stated that it shall be possible to authenticate both a principal and a watcher but it is not required that said entities are always authenticated. Moreover, it is as well stated later that a Presence Server shall authenticate the subscription requests originated from Watchers if required in the Subscription Authorization Policy, this is there is a policy to determine whether the users have to be authenticated.

This approach should be followed by the other different specifications defining 3GPP applications, this is:

- To require the possibility to authenticate users
- To require the use of a policy to decide whether the user authentication is to be perform (and just in that case which mechanism to use)

5. References

[SA#30] Draft Report of SA3#30 - version 0.0.4

[LAP] http://www.projectliberty.org/

[S3-030525] Draft TR 33.9bc V0.6.0 Presence Service; Security

6. Appendix

The following figure tries to show how a 3GPP Application (SP in the figure) will not need to make use of any of the mechanisms under GAA scope (actually may not need to authenticate the end-user itself) while delegating end-user authentication functions to a Trusted Third Party (an Identity Provider according to Liberty Alliance standard). In turn, the IdP acting as a NAF, may be making use of e.g. GBA while authenticating the user.