3GPP TSG SA WG3 Security — SA3#35 **S3-040706**
October 5-8, 2004
St Paul's Bay, Malta

3GPP TSG-CN WG4 Meeting #24 **N4-041202**
Sophia, France, 16 - 20 August 2004 **Agenda Item: GUP**

Title: **LS on Request for end to end example showing how the Liberty Alliance security framework fits the 3GPP GUP security requirements**
Response to: **GUP security (S3-040673).**
Release: **Rel-6**
Work Item: **GUP**

Source: **CN4**
To: **SA3**
Cc:

Contact Person:
Name: Arnaud SAHUGUET
Tel. Number: +1 908 582 6491
E-mail Address: sahuguet@lucent.com

Attachments: none

---

1. Overall Description:

CN4 thanks SA3 for the liaisons related to GUP security (S3-040673).

The current content of the "security section" of 29.240 makes reference to Liberty Alliance security framework, but in very broad terms.

The security of the Rp reference point is based on the mechanisms described in the "Liberty ID-WSF Security Mechanisms" [15] and "Liberty ID-WSF SOAP Binding" [14] specifications, and relies on:

- SSL/TLS standard mechanisms for Transport Layer Channel Protection. (other security protocols (e.g. Kerberos, IPSEC) may be used as long as they implement equivalent security measures),
- SSL/TLS for peer-to-peer authentication and X.509 v3 certificates,
- Bearer tokens or SAML assertions for message authentication.

Regarding authorization, the mentioned specifications recommend the use of the Web Services Security SAML Profile.

The specific mechanisms are further explained in the mentioned specifications, [14] and [15], and their text has preeminence to what is described here and should be considered as normative, unless explicitly indicated.

It is up to the security policy of the operator to choose which methods to apply taking into account the security domains where the client and server reside.

Among other things, it does not answer the following questions:

- Are both server and client certificates used?
- What is the topology of Certification Authorities (CAs) for these certificates?
- Are there GUP specific attributes in the X.509 v3 certificates (e.g. ESN number)?
- How do peer authentication and message authentication co-exist?

- Does the use of Web Services Security SAML profile require to introduce a new functional entity in the GUP architecture?

Moreover, the Liberty Alliance Security Framework permits to plug in any security method. In the context of GUP, some methods may not be applicable. It would be appropriate to identify and define a subset of preferred security methods for GUP.

2. Actions To SA3:

CN4 would appreciate to receive from SA3:

- an end-to-end example of the security mechanisms involved in GUP security, based on the Liberty Alliance security framework. This example would clarify – among other things – the various entities involved, the kind of messages exchanged and security methods used,
- a recommendation in terms of preferred security methods in the context of GUP.

3. Date of Next CN4 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA