3GPP TSG SA WG3 Security ó SA3#35 **S3-040885**
October 5-8, 2004
St Paul's Bay, Malta

Title:	LS on GUP Security Recommendations
Response to:	LS (N4-041202) on Reply LS on Request for end to end example showing how the Liberty Alliance security framework fits the 3GPP GUP security requirements
Release:	Rel-6
Work Item:	GUP Security
Source:	SA3
To:	CN4, SA2
Cc:	

Contact Person:
Name: Bengt Sahlin
Tel. Number: +358 40 778 4580
E-mail Address: Bengt.Sahlin@ericsson.com

Attachments: None

1. Overall Description

SA3 thanks CN4 for the liaisons related to GUP Security (N4-041202).

SA3#35 discussed some still open issues on GUP security. In particular, SA3 was concerned in providing recommendations related to the following issues:

- authentication over the Rg interface in case the GUP requestor is a UE (i.e. the possible use of GBA for client authentication to avoid client certificates needs still to be analysed).
- suitable traffic protection recommendations to minimize the impact of double encryption

During these discussions SA3#35 had also the opportunity to look into CN4 concerns in N4-041202.

CN4 Specific Questions in N4-041202

SA3#35 had the opportunity to discuss around the specific questions as indicated in LS N4-041202.

- *How do peer authentication and message authentication co-exist?*

  [LAP-WSF Security Mechanisms] specification defines a set of combinations of peer authentication and message authentication mechanisms necessary to accommodate various deployment scenarios.

  Not all combinations of available security mechanisms make sense in a given setting but a concrete selection cannot be done a priori. **This is a matter of deployment, operational and security policy and the trust model the policy accords.**

  Normatively, [LAP-WSF Security Mechanisms] *recommends* that peer authentication is performed in general, combined with message authentication in the presence of active intermediaries.

- *Are both server and client certificates used?*

  Some of the peer entity authentication and message authentication combinations defined in [LAP-WSF Security Mechanisms] support mutual (sender and recipient) peer entity authentication for which both server and client certificates would be required.

However, [LAP-WSF Security Mechanisms] also supports the use of other combinations not requiring client side certificates (e.g. *urn: liberty:security:2004-04:TLS:Bearer*) or not even requiring peer entity authentication at all (e.g. *urn: liberty:security:2004-04:null:Bearer)*.

Furthermore, [LAP-WSF Conformance Reqs] specifies that Web Services Clients (GUP requestors) and Web Services Providers (GUP Servers) MUST support null and TLS peer entity authentication mechanisms and null, x509, SAML and Bearer message authentication mechanisms as described by [LAP-WSF Security Mechanisms]. This is, the support of combinations including clientTLS profile and client certificates is not mandated neither for GUP requestors nor for GUP Server.

- *What is the topology of Certification Authorities (CAs) for these certificates?*

  This would be matter of deployment and thus not under the scope of GUP specifications.

- *Are there GUP specific attributes in the X.509 v3 certificates (e.g. ESN number)?*

  This is a question where additional clarifications would be required.

  Although some later versions of the X.509 certificate specification (e.g. *X.509 Version 3)* support the notion of extensions to convey any kind of extra info appended to the certificate, our view is that it was not the intention to include GUP specific attributes in the certificate itself. GUP attributes will be, in general, retrieved as part of the body of the SOAP message.

  Although, as mentioned, it is not clear which is the specific functionality that has originated this question, we understand that there are another mechanisms for the retrieval of asserted attributes that could be used in the scope of GUP. One possible scenario would be a trusted entity (e.g. the GUP server or any other trusted authority) being able to assert the validity of a specific attribute by means of attribute assertions. I.e., the attribute would be returned in the form of a SAML or any other kind of assertion, inside the body of the SOAP request.

  It must be highlighted though that if CN4 is willing to provide this kind of functionality, then CN4 should make sure that the retrieval of this kind of data at protocol definition time it is catered for (e.g. by ensuring that the type of the "Data" XML element allows the conveyance of such kind of structures).

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

  This is a question where additional clarifications would be required.

  [LAP-WSF Security Mechanisms] supports SAML Assertion message authentication and regarding authorization, recommends the use of the Web Services Security SAML Profile. These mechanisms rely on a Trusted Authority issuing assertions including Authentication and/or Authorization statements.

  Authentication and Authorization Authorities may be co-located. When the Sender is relying on a particular Trusted Authority for both authentication (through SAML holder-of-key) and either types of authorization decision, some optimizations may be possible through that Trusted Authority issuing ìcombinedî assertions.

  Liberty ID-WSF specifications also assumes that a service exists which aids in the discovery of identity-based web services. [LAP-WSF Discovery Service] defines protocols and schema for the description and discovery of ID-WSF identity services. GUP specification [23.240] already makes reference to this discovery functions as one of the possible options for GUP Requestors to get the contact reference information of the GUP Server if not known by other means.

  In addition to managing the registration and discovery of identity-based web services [LAP-WSF Discovery Service] also defines protocols for the DS to act as this Trusted Authority issuing authentication and/or authorization assertions (according to rules defined in [LAP WSF Security Mechanisms]), which are subsequently used in conjunction with the accessing of the discovered identity-based web service acting as centralized policy information and decision point.

DS would be also capable of informing the GUP Requestor of the preferences of the GUP Server in terms of peer entity and message authentication mechanism to be used.

However the DS is not a completely new functional entity in the GUP architecture. The support of a Discovery Service for GUP server discovery purposes is already included in stage2 specifications where it shall be also clarified that DS may be used as a Trusted Authority.

DS is defined as optional in TS 23.240. It is the understanding of SA3 that this allows operators to use other means to provide trust within the operatorís network. SA3 thinks that a trusted authority is needed, and would like to ask SA2 what component would suitable in the case there is no DS.

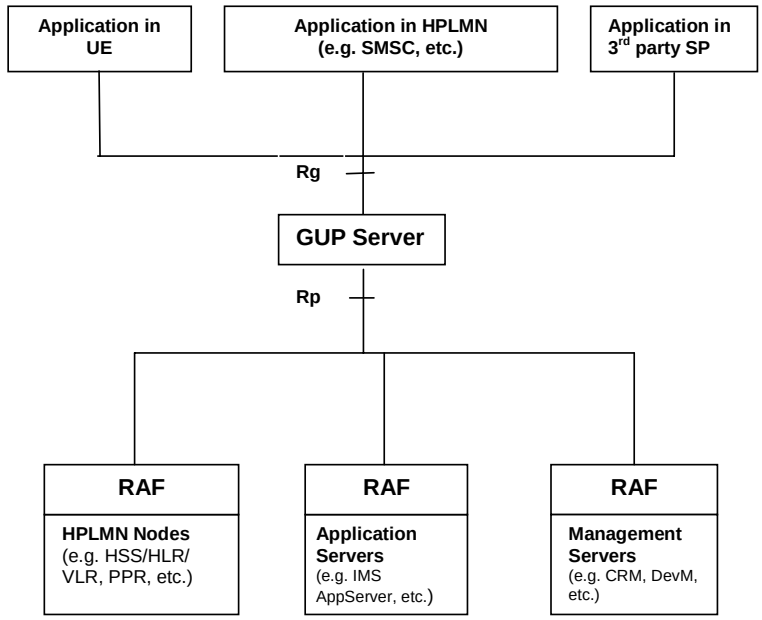
Required Actions from SA3

In LS N4-041202 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 ñ among other things ñ 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.

To this respect and based on related SA3#35 discussions, SA3 would like to highlight that the scope of applicability of GUP specifications is probably already too wide as to being able to provide simple and straightforward optimizations and recommendations of the security mechanisms to be used.

Simply take a look to the following example of mapping the GUP reference architecture to current infrastructure environment (based on [23.240]) Ö



In this example, it can be clearly seen that GUP specifications are also applicable for multiple deployment scenarios where for example GUP requestors could very well be internal applications to the operator domain, external applications to the operator domain or even UE implementations where different security, privacy and trust considerations apply.

This makes rather difficult to SA3 to provide a recommended subset of security mechanism to be used in the context of GUP. Deployers of GUP architecture should instead select the most suitable security mechanisms depending on the specific scenario, trust model and policies they would like to see applied.

UE acting as GUP Requestor over Rg-interface

There is however some recommendations that SA3 has discussed in the scenario where a UE acts as a GUP requestor over the Rg interface and that can be suggested to CN4. In particular it is recommended to CN4 to make reference to Section 3 in [LAP-WSF Client Profiles] where guidelines that would apply in this case are defined.

Amongst other recommendations given in this chapter, Liberty states that Ö

> ì*A LUAD-WSC that wishes to interact with a WSP SHOULD support at least the urn:liberty:security:2004-04:TLS:Bearer security mechanism as specified in [LAP-WSF Security Mechanisms].î.*

While defining the *urn:liberty:security:2004-04:TLS:Bearer security mechanism* [LAP-WSF Security Mechanisms] states that Ö

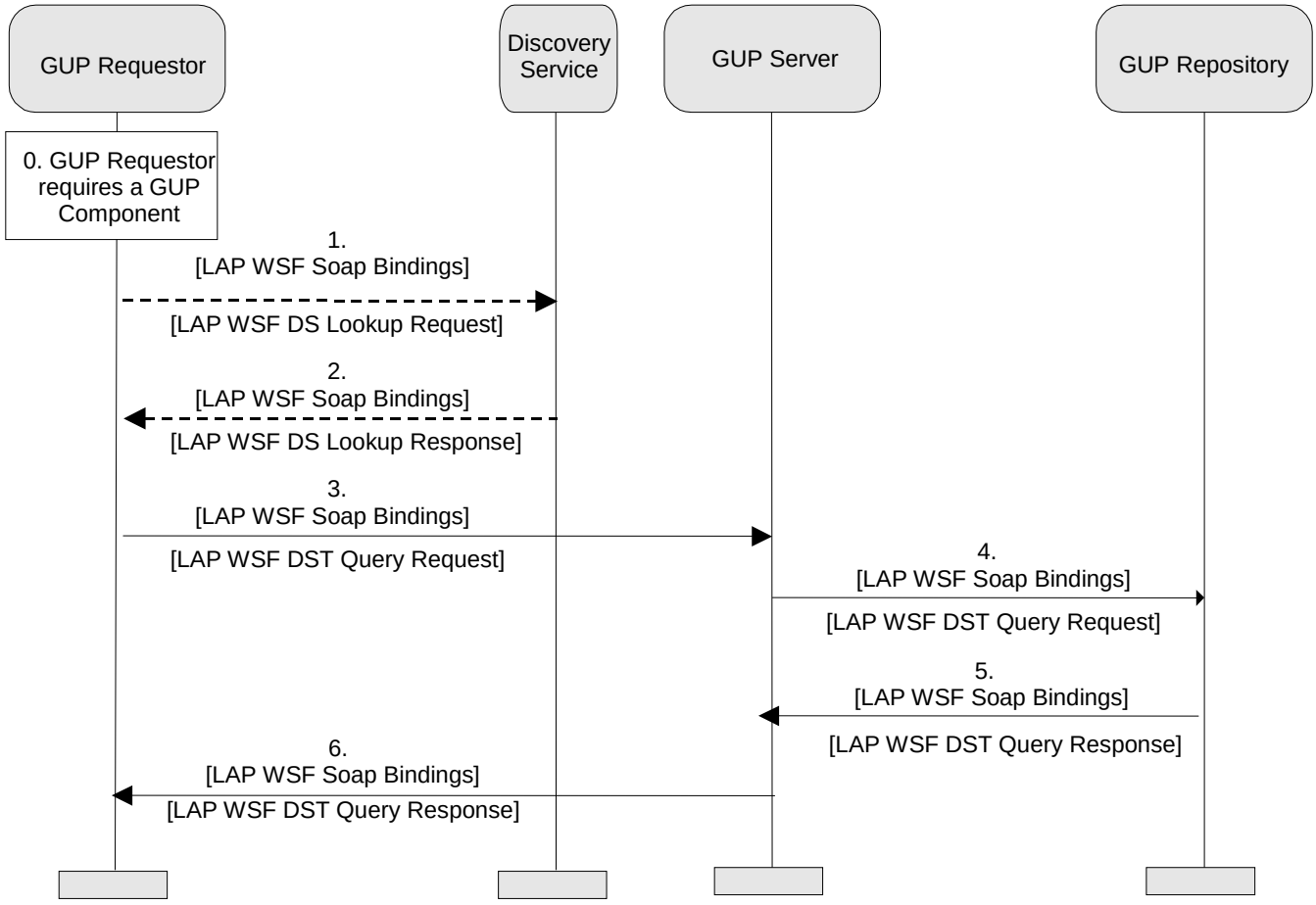
> ì*The primary function of these mechanisms is to provide for the authentication of the receiving entity and to leverage confidentiality and integrity features at the transport layer*î.

Obviously, the support of other peer entity authentication and message authentication combinations is not precluded but at least this one does not require the use of client certificates. The use of this profile seems also suitable for deployment scenarios where double encryption at transport and message level needs to be avoided.

SA3 agreed that the *urn:liberty:security:2004-04:TLS:Bearer security mechanism* shall be mandatory for use in case the UE is acting as a GUP requestor over the Rg-interface. All other authentication mechanisms are optional for use for the UE.

End-to-End Example

What follows is a purely informative example that shows protocol interactions and security considerations in a generic GUP scenario.



Step 0: GUP Requestor requires a GUP component.

Next step from GUP Requestor would depend on the particular deployment configuration in place.

- For example, GUP Requestor could have been already provisioned with all necessary data to access the GUP Server (e.g. GUP Server url, security mechanism that GUP Server is willing to use with GUP Requestor and even required security credentials to access the GUP Server). In this case, GUP Requestor would be able to directly query the GUP Server as in Step 3.
- In a more general case, the GUP Requestor might have the need to discover the exact location of the GUP Server and/or rely on a Trusted Authority in order to find out which security mechanisms and/or security credentials to use with the GUP Server. In these cases, GUP Requestor could rely on the functionality of a Discovery Service and proceed as in Step 1.

Step 1: GUP Requestor queries a Discovery Service.

GUP Requestor issues a SOAP message to the Discovery Service conforming to [LAP WSF SOAP Bindings] and [LAP WSF Discovery Service] specifications asking for the exact location of the GUP Server.

Step 2: GUP Requestor receives necessary information to access GUP Server from DS.

In its response, the Discovery Service will include the url of the GUP Server, an indication of the peer entity and message authentication mechanism to be employed and optionally, required security credentials to be able to access the GUP Server.

Step 3: GUP Requestor queries for the desired GUP component to the GUP Server.

GUP Requestor establishes the required transport security and issues a SOAP message over the Rg interface conforming to [LAP WSF SOAP Bindings] specification including the required bearer security tokens. The actual query request conforms to [LAP WSF Data Services Template] Query Request operation, which is included in the Body of the SOAP message to the GUP Server.

Step 4: GUP Server proxies the request of the desired GUP component to GUP Repository.

GUP Server issues a similar request to the GUP Repository hosting the desired GUP component, this time over the Rp interface. Typically, GUP Server and GUP Repositories would belong to the same security domain so security mechanisms employed at Rp could be less demanding than the ones used over Rg interface. However, the use of one of the available option over the others is still a deployment issue.

Upon reception of this message, GUP Repository will execute access control policies and if everything is correct will proceed to return the desired GUP component all the way up to the GUP Requestor via the GUP Server.

Step 5: GUP Repository returns the desired GUP component to the GUP Server.

Step 6: GUP Server proxies the desired GUP component to the GUP Requestor.

Relationship between GAA and Liberty

SA3 wants to inform that the relationship between GAA and Liberty was discussed at SA3 #35. SA3 agreed that further study of the relationship is needed to identify if there are overlaps between these two authentication frameworks, and to study potential synergies between them. This study is independent of the ongoing work on GUP Security, so SA2 and CN4 can progress the work on GUP security based on the current agreement to adopt the Liberty Alliance Project ID-WSF security solutions as the basis for the GUP security work.

2. Actions

To SA2 and CN4 group.

ACTION: SA3 kindly asks SA2 and CN4 to clarify the role of DS as a Trusted Authority in TS [23.240] and TS [29.240]. Especially, SA3 would like to ask SA2 what component would suitable in the case there is no DS.

CN4 is also asked to take into account the agreement in SA3 that urn:liberty:security:2004-04:TLS:Bearer security mechanism shall be mandatory for use in case the UE is acting as a GUP requestor over the Rg-interface.

3. Date of Next TSG-SA3 Meetings

SA3#36	23 - 26 November 2004	Shenzhen, China

4. References

[N4-041202] LS on Request for end to end example showing how LAP security framework fits 3GPP GUP security requirements

[23.240] 3GPP TS 23.240: "3GPP Generic User Profile - Architecture; Stage 2î
[29.240] 3GPP TS 29.240: Generic User Profile (GUP); Stage 3; Network

Liberty Alliance Specifications are publicly available at http://www.projectliberty.org/specs/index.html

- [LAP-WSF Security Mechanisms] http://www.projectliberty.org/specs/liberty-idwsf-security-mechanisms-v1.1.pdf
- [LAP ID-WSF Profiles for Liberty Enabled User Agents and Devices] http://www.projectliberty.org/specs/liberty-idwsf-client-profiles-v1.0.pdf
- [LAP ID-WSF Discovery Service] http://www.projectliberty.org/specs/liberty-idwsf-disco-svc-v1.1.pdf
- [LAP ID-WSF SOAP Bindings] http://www.projectliberty.org/specs/liberty-idwsf-soap-binding-v1.1.pdf
- [LAP-WSF Conformance Reqs] http://www.projectliberty.org/specs/draft-liberty-idwsf-1.0-scr-v1.0-08.pdf