3GPP TSG SA WG3 Security — SA3#35 **S3-040786**
October 5-8, 2004
St Paul's Bay, Malta

Source:	**Ericsson, Nokia, Intel**
Title:	**GUP Security – Recommendations for UE implementations**
Document for:	**Discussion and Decision**
Agenda Item:	**6.17 Generic user profile (GUP)**

Introduction

This contribution clarifies that [LAP-WSF Security Mechanisms] provides a variety of security profiles in order to accommodate multiple deployment scenarios.

This contribution also proposes that in the case where a UE acts as a GUP requestor over Rg interface, GUP specifications should refer to [LAP-WSF Client Profiles] as providing valuable guidance for this deployment case in particular.

Please note that this contribution is specifically focused on the Rg interface.

Background

SA3 #34 discussed GUP security based on the documents in [S3-040561]. SA3 endorsed the conclusion to use LAP-WSF specifications as the security and privacy solution for GUP. SA3 agreed that SA2 and CN4 could update their specifications according to the draft CRs in [S3-040338].

Furthermore SA3 decided that some profiling and recommendations were needed to complete work on GUP security. The profiling and recommendations are 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

Discussion

Liberty ID-WSF Security Mechanisms

[LAP-WSF Security Mechanisms] specification defines a set of authentication mechanisms, labeled by URIs, and the security properties they engender. The multiplicity of mechanisms specified is necessary to accommodate various deployment scenarios.

The following table summarizes the authentication mechanism identifiers and their security properties. Each URI is of the form urn:liberty:security:2003-08:peer mechanism:message mechanism.

URI	Peer Entity	Message
urn:liberty:security:2003-08:null:null	No	No
urn:liberty:security:2003-08:null:X509	No	Yes
urn:liberty:security:2003-08:null:SAML	No	Yes
urn:liberty:security:2004-04:null:Bearer	No	No
urn:liberty:security:2003-08:TLS:null	Recipient	No
urn:liberty:security:2003-08:TLS:X509	Recipient	Yes
urn:liberty:security:2003-08:TLS:SAML	Recipient	Yes
urn:liberty:security:2004-04:TLS:Bearer	Recipient	No
urn:liberty:security:2003-08:ClientTLS:null	Mutual	No
urn:liberty:security:2003-08:ClientTLS:X509	Mutual	Yes
urn:liberty:security:2003-08:ClientTLS:SAML	Mutual	Yes
urn:liberty:security:2004-04:ClientTLS:Bearer	Mutual	No

Each identifier represents two security properties for a given mechanism:

- Peer Entity Authentication
- Message Authentication

For either of the properties a value of "null" indicates that the particular security property is not supported by the mechanism.

The **peer entity authentication mechanisms** defined by [LAP-WSF Security Mechanisms] specification leverage the authentication features supplied by SSL 3.0 [SSL] or TLS 1.0 [RFC2246]. The mechanism identifier describes whether the recipient ("TLS") is unilaterally authenticated or whether each communicating peer ("ClientTLS") is mutually authenticated to the other peer.

The **message authentication mechanisms** indicate which attestation profile is utilized to ensure the authenticity of a message. These message authentication facilities aid the deployer in the presence of intermediaries.

- The X.509 v3 Certificate mechanism is suited for message exchanges, which generally rely upon message authentication as the principle factor in making authorization decisions.
- The SAML Assertion mechanism is suited for message exchanges, which generally rely upon message authentication as well as the conveyance and attestation of authorization information.
- The Bearer mechanism is based on the presence of a bearer token in the security header of a message. In this case, the bearer token is verified for authenticity rather than proving the authenticity of the message.

Not all peer entity authentication and message authentication combinations make sense in a given setting. Again this is a matter of deployment, operational and security policy and the trust model the policy accords.

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

From an implementation point of view, [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.

UE acting as GUP Requestor over Rg-interface

GUP specifications should be 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.

In earlier discussions around GUP security SA3 has stated that "*TLS with server and client side certificates makes a good basis for the security solution for GUP*" but as a matter of act this is not the one and only alternative available and probably not the best one for some deployment scenarios.

Deployers of GUP architecture should then select the most suitable peer entity authentication and message authentication combinations depending on the specific scenario, trust model and policies they would like to see applied.

SA3 has raised concerns on the particular case where the GUP requestor is a UE implementation in terms of the use of client certificates and double encryption.

Liberty´s ID-WSF specifications define a number of protocols that enable any party to act as a Web Service Consumer (GUP Requestor), a Web Service Provider (GUP Server)[i], or both. When user agents or devices (i.e. UE) wish to act in any of these roles, some particular issues need to be addressed.

[LAP-WSF Client Profiles] specification profiles how user agent or device implementations (UE implementations) should utilize the various Liberty Alliance specifications in order to enable particular scenarios while ensuring a high degree of interoperability, security and privacy. In particular section 3 contains guidelines that would apply to a UE acting as a GUP requestor over Rg-interface (LUAD acting as a Web Services Client).

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

> "*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].".*

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

> "*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*".

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.

Using *urn:liberty:security:2004-04:TLS:Bearer* security mechanism, the UE acting as a GUP requestor over Rg can be authenticated using bearer tokens. [LAP-WSF Security Mechanisms] does not limit the types of bearer tokens, which can be conveyed. That is customs tokens could still leverage this mechanism provided that the meaning of the token is understood by the producer and the consumer of the token.

It should be out of the scope of GUP specifications to define formats and/or retrieval mechanisms for these bearer tokens. However, in the presence of a Liberty ID-WSF Discovery Service, bearer security tokens could be optionally obtained from there and included in the message to the GUP Server. 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 a Trusted Authority issuing authentication and/or authorization statements (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.

In the case of GUP, it is assumed that the Discovery Service would be managed by the MNO. 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.

Conclusion and Proposal

This contribution clarifies that [LAP-WSF Security Mechanisms] does not simply define one single security mechanism to be used in LAP WSF deployments but a combination of multiple mechanism in order to accommodate various deployment scenarios.

The case of a UE acting as a GUP Requestor over the Rg interface is a valid GUP deployment scenario and in practice represents a Client-based Web Service Client implementation of LAP ID-WSF. For these cases, [LAP-WSF Client Profiles] does not *mandate* any mechanism in particular but *recommends* the use of at least *urn:liberty:security:2004-04:TLS:Bearer security mechanism* security mechanism, which does not imply the use of client certificates nor the risk of double encryption.

Client authentication can still be performed in this case by means of bearer security tokens optionally received from a Liberty ID-WSF Discovery Service.

It is therefore proposed that …

- GUP specifications should also refer to the recommendations provided at chapter 3 of [LAP-WSF Client Profiles] as providing valuable guidance for deployments where a UE acts as a GUP requestor over Rg-interface.
- The role of a Liberty ID-WSF Discovery Service as a Trusted Authority capable of issuing authentication and authorization statements should be also mentioned.

CN4 and SA2 should be informed of such recommendations so they can include the reference to [LAP-WSF Client Profiles] and [LAP WSF Discovery Service] within GUP specifications as appropriate. Please refer to the accompanying draft LS response to CN4 where SA2 is also involved.

References

[S3-040561] Ericsson, Nokia, Intel S3-040561, GUP security Open issues
[S3-040338] Ericsson, Nokia, S3-040338, GUP security follow-up

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-WSF Conformance Reqs] http://www.projectliberty.org/specs/draft-liberty-idwsf-1.0-scr-v1.0-08.pdf