3GPP TSG SA WG3 Security — SA3#34 **S3-040561**

6 - 9 July 2004

Acapulco, Mexico

Source:	**Ericsson, Nokia, Intel**
Title:	**GUP Security Open Issues**
Document for:	**Discussion**
Agenda Item:	**7.17**

Introduction

This contribution is a follow-up on previous discussions held around GUP security in SA3#32 and SA3#33.

It captures the conclusions from the PowerPoint presentation around Security and Privacy at Liberty Alliance´s Web Services Framework (LAP-WSF) and tries to address open issues around GUP Security as raised in earlier discussions at SA3.

Background

SA3 has repeatedly discussed GUP security issues. In particular …

- Discussion around input paper [S3-040035] at SA3#32 meeting concluded with SA3 agreeing the working assumption to "*adopt the Liberty Alliance Project ID-WSF security solutions as the basis for the GUP security work*".
- Discussion around input paper [S3-040338] at SA3#33 meeting concluded with SA3 agreeing that *"SA3 considers that GUP security can be specified in existing 3GPP documents. Thus, an SA3 deliverable is not seen as necessary".*

This was effectively communicated to SA2 and CN4 groups in LS [S3-040199] and [S3-040385].

However, SA3 still felt that some more analysis of the following issues was required …

- *The impacts of using client certificates need to be studied in case the GUP requestor over Rg-interface is a UE. GBA (Generic Bootstrapping Architecture) based client authentication may possibly be used in this case.*
- *The impact of potential double encryption needs to be studied by SA3.*
- *Which specification would be suitable for specifying security for the Rg reference point*
- *Potential profiling of the Liberty Alliance Project ID-WSF security solution in the scope of GUP security*
- *Potential alignments of terminology in 3GPP and Liberty Alliance Project specifications*
- *Use of Liberty Alliance Project Privacy mechanisms*

This contribution tries to provide satisfactory answers to these open issues so GUP specification work can be completed including references to relevant LAP-WSF security and privacy related specifications.

Discussion

The companion presentation should have provided already a good analysis on how GUP and Liberty Alliance´s architecture relate and how LAP-WSF defined Security and Privacy mechanisms can be applied in order to fulfil GUP´s security and privacy requirements.

In particular we could find direct answers to the following SA3 Open Issues …

- *Which specification would be suitable for specifying security for the Rg reference point*

  Liberty Alliance has developed a set of normative and non-normative specifications dealing with Security and Privacy aspects …

  - [LAP-WSF Security Mechanisms]
  - [LAP-WSF Interaction Service]
  - [LAP-WSF Security&Privacy Overview]
  - [LAP-WSF Security&Privacy Best Practices]

  At least normative specifications (first two ones) shall be enough in order to address GUP Security and Privacy requirements both at Rg and Rp reference points.

  Other LAP-WSF specifications also define features relevant for security and privacy (e.g. use of "User Consent" and "User Directives" SOAP Header Blocks as defined in [LAP-WSF SOAP Bindings]) but these are already being referred by N4 anyway so there would be no need for SA3 to point to them.

- *Use of Liberty Alliance Project Privacy mechanisms*

  Liberty Alliance considers privacy and security of end-user's profile information to be extremely important. This philosophy has driven many decisions crucial in the specification development and the availability of different security functions that protects privacy as shown in the companion presentation

- *Potential profiling of Liberty Alliance ID-WSF security solution in the scope of GUP security*

  The companies signing this contribution believe that all security and privacy features as defined by LAP-WSF are applicable in order to specify security at both Rg and Rp reference points.

  - Rg reference point may expose user profile information to external applications and thus it seems reasonable to consider all security and privacy features available in LAP-WSF.
  - Operations at Rp are exactly the same as for Rg. Even when in principle, trust models for Rp and Rg might be different, GUP security and privacy requirements are stated in a generic form both for Rg and Rp reference points.

  It should be therefore convenient to consider the whole LAP-WSF security and privacy solution in scope of GUP security.

- *Potential alignments of terminology in 3GPP and Liberty Alliance Project specifications*

  To some extent, it is inevitable to face terminology issues while making references to external specifications (most probably some of the 3GPP references to IETF RFCs are in this kind of situation already). However this should not be seen as a problem or as an open issue that 3GPP should give a solution to in all cases.

  In the case of LAP-WSF and after not a very thorough reading, someone familiar with 3GPP-GUP could get a fairly good view around similarities in functionality, architecture and protocols and at the same time grab the differences in terminology.

- *The impacts of using client certificates need to be studied in case the GUP requestor over Rg-interface is a UE.*

Even when the companies signing this contribution believe that the most common case will be that where the GUP requestor over the Rg-interface is a Network-based application, the case of having a UE instead is a perfectly valid scenario implementable with normative LAP-WSF specifications.

In principle, any UE capable of implementing LAP-WSF specifications should be able to interact over the Rg interface as if it were a Network-based Application. However, LAP-WSF also provides profiles to utilize LAP-WSF specifications to enable particular scenarios where a Liberty User Agent and Device (LUAD) act as a LAP-WSF entity, while ensuring a high degree of interoperability, security and privacy. In particular section 3 in [LAP-WSF Client Profiles] contains guidelines that would apply to a UE acting as a GUP requestor over Rg-interface (LUAD acting as a Web Services Client).

SA3 has also mentioned that "*GBA (Generic Bootstrapping Architecture) based client authentication may possibly be used in this case*". In general, 3GPP-GBA shall be considered as "complementary" technology rather than "conflicting" technology so acknowledging that there might be potential areas of applicability within 3GPP-GUP, the companies signing this contribution do not believe that definition of those should fall in scope of 3GPP-GUP (at least in this stage).

- *The impact of potential double encryption needs to be studied by SA3.*

  Reasoning behind this open item probably requires additional clarification in order to get an accurate answer but in any case, the companies supporting this contribution believe that LAP-WSF specifications make a proper use of (channel and message level) encryption techniques and that there should be no impact related to the encryption performed at CN either.

Proposal

This contribution and the companion presentation should provide enough arguments to SA3 in order to be able to close remaining open items around GUP Security and in order to be able to endorse LAP-WSF specifications as the security and privacy solution to be used in GUP.

In that case, it would be necessary to inform rest of 3GPP WGs involved in GUP specification work (i.e. SA2 and CN4) to proceed to include references to relevant LAP-WSF security and privacy specifications as previously suggested in [S3-040338].

> Note: The only addition to this earlier proposal to SA2 and CN4 would be the reference to [LAP-WSF Interaction Service] specification.

Otherwise, concerned SA3 members are invited to point specific aspects of LAP-WSF specifications where GUP security and privacy requirements would not be met.

References

[S3-040035] Nokia, Ericsson, S3-040035, GUP security directions follow-up

[S3-040199] 3GPP TSG SA WG3, S3-040199, LS on GUP security directions

[S3-040338] Ericsson, Nokia, S3-040338, GUP security

[S3-040385] 3GPP TSG SA WG3, S3-040385, LS on GUP security status on SA3

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-WSF Interaction Service]
  http://www.projectliberty.org/specs/liberty-idwsf-interaction-svc-v1.0.pdf
- [LAP-WSF Security&Privacy Overview]
  http://www.projectliberty.org/specs/liberty-idwsf-security-privacy-overview-v1.0.pdf
- [LAP-WSF Security&Privacy Best Practices]
  http://www.projectliberty.org/specs/final_privacy_security_best_practices.pdf
- [LAP-WSF SOAP Bindings]
  http://www.projectliberty.org/specs/liberty-idwsf-soap-binding-v1.1.pdf
- [LAP-WSF Client Profiles]
  http://www.projectliberty.org/specs/liberty-idwsf-client-profiles-v1.0.pdf

GUP Security&Privacy Overview

3GPP TSG SA WG3 Security — SA3#34

6 – 9 July 2004

Acapulco, Mexico

Ericsson, Nokia, Intel

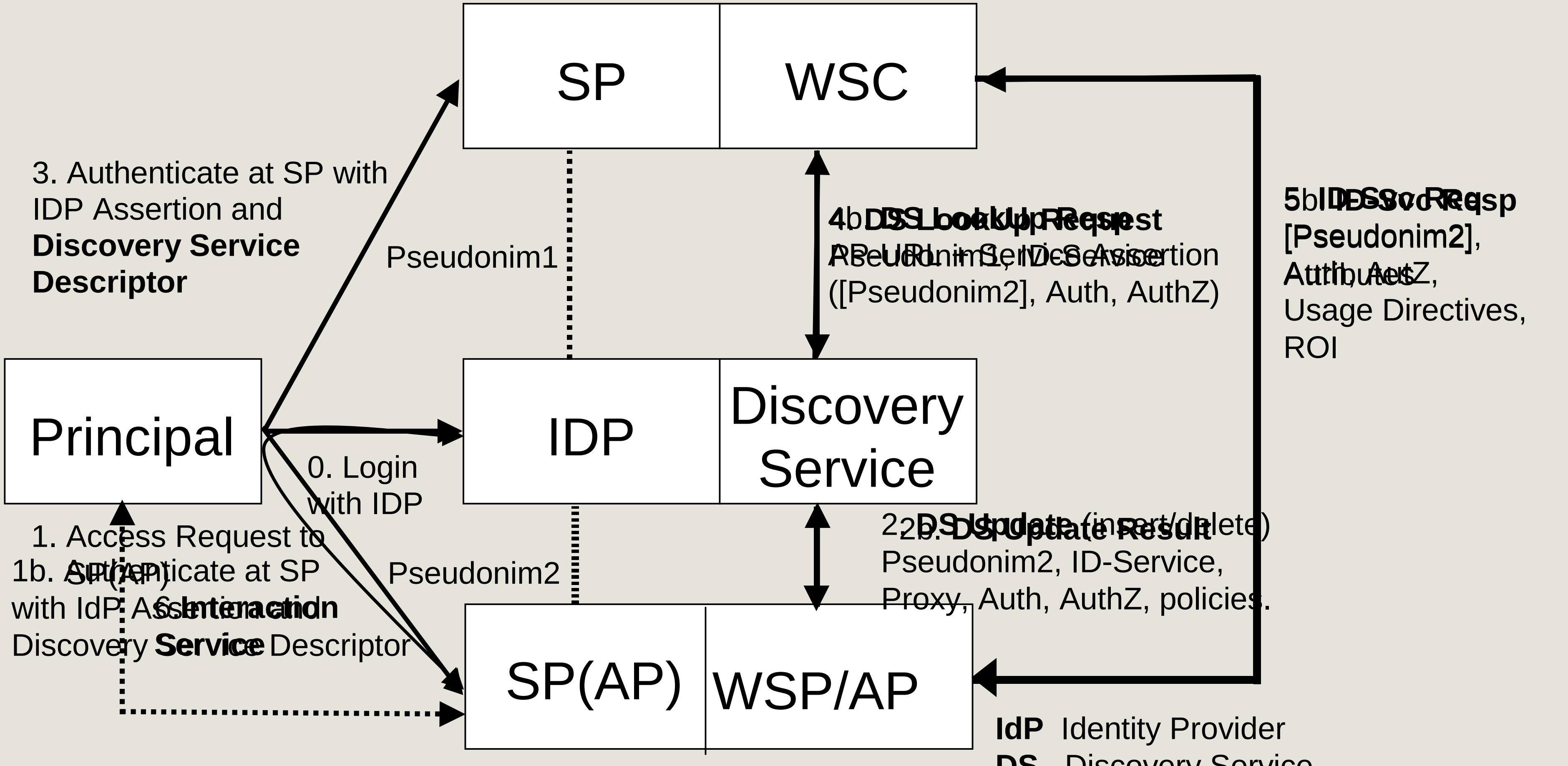
Goals&Scope

- Current working assumption at SA2 and CN4 is to base GUP architecture and protocols on Liberty Alliance Identity Web Services Framework (LAP ID-WSF) specifications.
- This is also the case at SA3 and these slides will try to provide a more in depth view on how LAP specifications can be applied in order to fulfil GUP Security and Privacy requirements.

- **Agenda**
  - Liberty ID-WSF Security&Privacy Overview.
  - GUP Security&Privacy Requirements.
  - Liberty applied to GUP Security&Privacy.

LAP ID-WSF Security&Privacy Overview

LAP Architecture Overview *(pls animate)*



3. Authenticate at SP with IDP Assertion and **Discovery Service Descriptor**

0. Login with IDP

1. Access Request to SP(AP)

1b. Authenticate at SP with IdP Assertion and Discovery Service Descriptor

6. **Interaction**

4. **DS Lookup Req**
4b. **DS Lookup Resp**
AP URI + Service Assertion
Pseudonim1, ID-Service
([Pseudonim2], Auth, AuthZ)

5. **IDSvc Req**
5b. **IDSvc Resp**
[Pseudonim2],
AuthZ,
Attributes,
Usage Directives,
ROI

2. **DS Update** (insert/delete)
2b. **DS Update Result**
Pseudonim2, ID-Service,
Proxy, Auth, AuthZ, policies.

…………..
Federation Relationship

IdP	Identity Provider
DS	Discovery Service
SP/WSC	Service Provider/Web Service Consumer
AP/WSP	Attribute Provider/Web Service Provider

LAP Perspective on Security&Privacy

- LAP considers security and privacy of Principal’s personal information as extremely important.
- LAP ID-WSF provides normative specifications for the secure exchange of Personal information specially at the following specifications ...
  - http://www.projectliberty.org/specs/liberty-idwsf-security-mechanisms-v1.1.pdf
  - http://www.projectliberty.org/specs/liberty-idwsf-interaction-svc-v1.0.pdf
- There are other LAP non-normative deliberables relevant to Security&Privacy...
  - http://www.projectliberty.org/specs/liberty-idwsf-security-privacy-overview-v1.0.pdf
  - http://www.projectliberty.org/specs/final_privacy_security_best_practices.pdf
  - http://www.projectliberty.org/specs/liberty-trust-models-guidelines-v1.0.pdf
- Well known standard IETF, W3C and OASIS technologies are employed:
  - Assertions & Protocol for OASIS Security Assertion Markup Language SAMLv1.1
  - Web Services Security: SOAP Message Security X509 Certificate Token Profile
    SAML Token Profile Kerberos Token Profile
  - XML-Signature Syntax and Processing
  - XML Encryption Syntax and Processing
  - TLS and SSL protocols

Security Functions Required for Privacy

http://www.projectliberty.org/specs/liberty-idwsf-security-privacy-overview-v1.0

- Authentication of the Principal and/or any other entities that could perform policy management tasks (policy definition, modification, etc.).
- Authentication of attribute requesters.
- Policy integrity in transit (at the moment of policy definition, modification or any other kind of policy management operation).
- Policy integrity in storage.
- Attribute confidentiality in transit (response from the attribute provider to the service provider).
- Attribute confidentiality in storage.
- Attribute integrity in storage and transit.
- Policy management authorization.
- Audit capability: maintenance of transaction records in secure storage.
- Avoiding collusion between identity provider and service provider.
- Data aggregation.

LAP ID-WSF Security Mechanisms

http://www.projectliberty.org/specs/liberty-idwsf-security-mechanisms-v1.1.pdf

- Liberty's Security Mechanism's specification describes profiles and requirements for securing the discovery and use of identity services.
- This specification defines mechanisms to …
  - Protect privacy,
  - Ensure authenticity (Peer Authentication + Anti-Replay protection),
  - Integrity and confidentiality protect messages between providers.
- Additionally, this specification defines how the Discovery Service, in addition to its primary role of facilitating resource discovery, can also function as a security token service, issuing security tokens that the requester will use in the request to the discovered identity service.

Other Built-In Security&Privacy Features (I)

- Liberty Specs include a number of built in Security& Privacy features ...
  - ***Pseudonymous Access*** – LAP Specs support the assignment of an arbitrary sequence of characters to identify a Principal. The opaque handle has meaning only in the context of the relationship between an IdP/DS and a SP. Thus a Principal's identity and actions are harder to track as the Principal navigates among SPs.
  - ***Anonymous Access*** – LAP Specs provide means for a Service Provider to access Identity Services without a need to know who the consumer they are providing services to really is. This allows personalization of services without disclosure of Ppal´s Identity or requiring Ppal to register at SP.
  - ***XML Digital Signature*** – All Liberty Architecture Messages have been designed to allow use of XMLDsig (***http://www.w3.org/TR/xmldsig-core***). XMLDSig allow a proper verification of the transaction parties, and if messages are signed and stored, allows for later auditing.
  - ***Consumer Consent Headers*** – All of the relevant LAP specs include the reference to the need of consumer consent for relevant transactions that explicitly claims that the Principal consented to the present interaction.

Other Built-In Security&Privacy Features (II)

- ***Access Controls*** – LAP Specs enable LAP Providers to make access control decisions on behalf of the Ppal (Ppal specifies his/her authorization policy at LAP Provider so personal information is shared only with consented sites).
  - ***Interaction Service*** – It may sometimes be necessary for an identity service to interact with the owner of the information that it is exposing, to collect attribute values, or to obtain permission to share the data with an SP.

    Interaction Service spec defines schemas and profiles that enable an Identity Service to interact with the owner of the information that is exposed by that Identity Service.

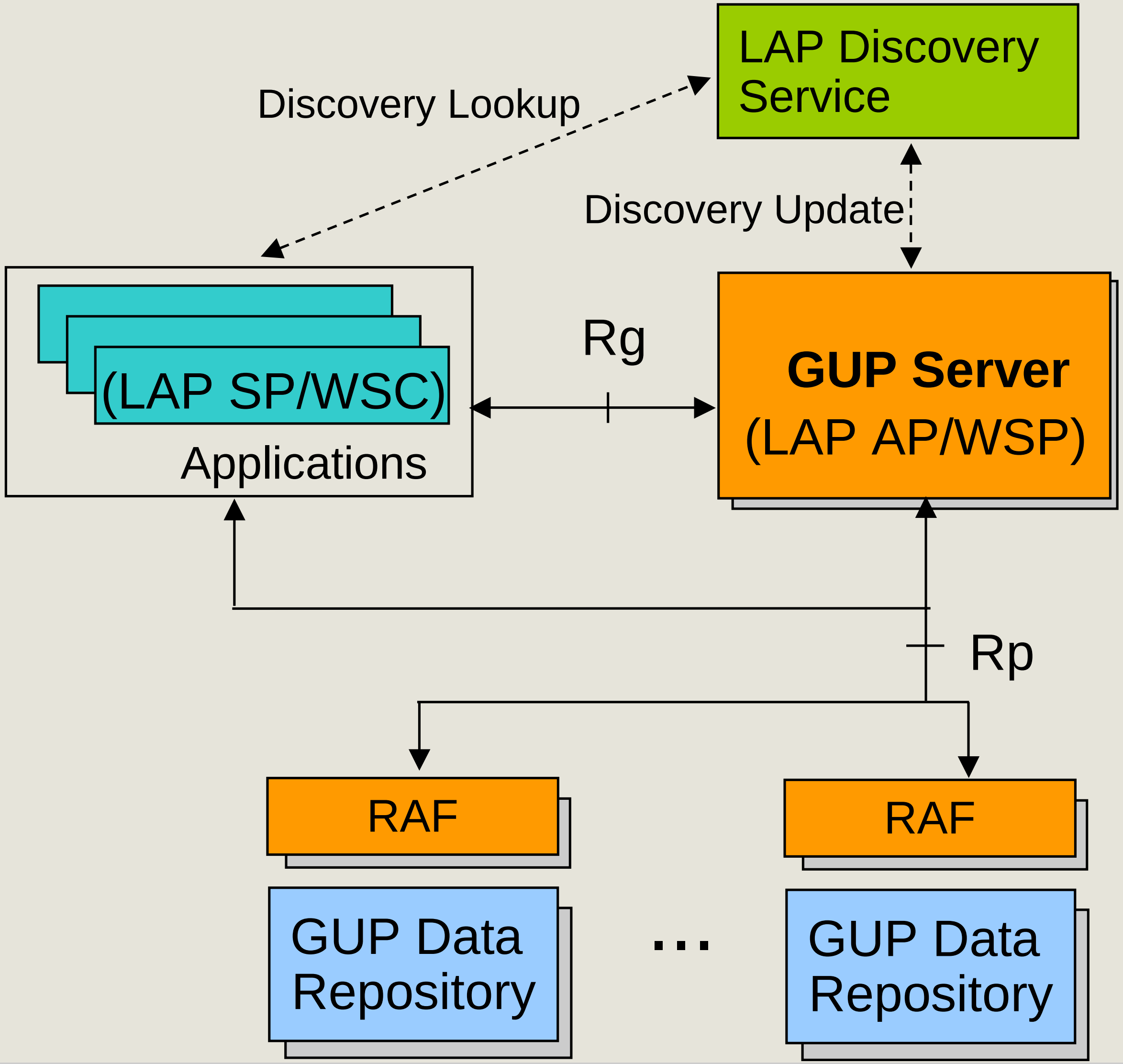
    http://www.projectliberty.org/specs/liberty-idwsf-interaction-svc-v1.0.pdf
- ***Usage Directives*** – LAP Specs describe a container that lists or points to usage directives regarding either ...
  - intended use of a requested attribute (from the requester), or
  - allowed usage of a requested attribute (from the attribute owner/holder).

GUP Privacy&Security Requirements

GUP in General

- Several CN domains (CS, PS, IMS), several access technologies (e.g. GERAN, UTRAN and WLAN) and increasing number of new services have introduced large amount of data associated to users.
- Goal of GUP is to provide a conceptual description to enable harmonized usage of user-related information located in different entities.
- Technically GUP provides an architecture, data description and interfaces with mechanisms to handle the data.
  - GUP Rg interface provides a single point of access to the whole Profile,
  - GUP Rp provides a harmonized interface to the GUP Data Repositories (Profile Components).
  - Rg may be used by both external and internal applications and Rp mainly internally inside the Home Network.

GUP Architecture with a few Liberty aspects



LAP architecture fits into GUP´s as shown in this slide.

At Rg reference point, a GUP Application would act as a LAP SP/WSC and GUP Server would act as a LAP AP/WSP for GUP data.

It is a natural choice to adopt Liberty ID-WSF for Rg:

- Rg supports also third party connections like Liberty ID-WSF.
- Liberty Security provides a good basis for XML/SOAP security solutions.

It would be beneficial to have similar solutions for GUP Rp reference point as for Rg.

LAP DS may be left beyond GUP specs but it could be still applied as specified by LAP.

RAF = Repository Access Function

LAP Compliance with GUP Security&Privacy (I)

- 3GPP TS 22.240 defines GUP Security&Privacy Reqs.
- Liberty ID-WSF based on very similar requirements fulfilling most of GUP Security&Privacy requirements.
  - Consumer/Supplier Authentication (Section 7; Reqs 1 to 4)
    - *Chapter 6 in LAP WSF Security Mechanisms defines different peer entity auth mechanisms (incl mutual auth using ClientTLS)*
    - *This section also describes the use of X509 certificates and SAML assertions for Message authentication.*
  - Confidentiality and Integrity protection (Section 7; Reqs 5 and 6)
    - *Section 5.1 in LAP WSF Security Mechanisms defines how to use suitable SLS/TLS cipher suites (or equivalent security protocols e.g. IPsec/Kerberos) for Transport layer confidentiality and integrity channel protection.*
    - *XML-Signature & Encryption techniques are also widely used for message level confidentiality and integrity protection (sections 5.2, 5.3 and 6.3).*

LAP Compliance with GUP Security&Privacy (II)

- Non-repudiation (Section 7; Req 7)
  Audit log (Section 7; Req 8)
  - *LAP WSF Security Mechanisms makes extensive use of XML-Signature, XML-Encryption and OASIS WS-Security compliant header elements, which also provide means for Anti-reply and Non-Repudiation protection as well as enabling effective auditing.*

- Consistency checks (Section 7; Req 10)
  Consistent change of data (Section 7; Req 11)
  - *LAP WSF provides architecture and protocols for consistent query and update of user profile information while respecting its security and privacy.*
  - *LAP WSF Security and Privacy mechanisms make sure that integrity of user profile information is protected during transactions.*

LAP Compliance with GUP Security&Privacy (III)

- Access Control, Authorisation and Privacy (Section 7; Req 9 and Section 8)
  - *Chapter 8 in LAP WSF Security Mechanisms defines mechanisms to convey authorization and user profile access information (supplied by a trusted third party) which may be necessary to access a service.*
  - *Rest of relevant LAP WSF specs (Discovery Service and Data Services Template specs) also include necessary access control points allowing sharing of user profile information only with consented parties.*
  - *Use of Consent and Usage Directives Header blocks enable the transport of additional required information for effective access control decisions.*
  - *Finally, LAP WSF Interaction Service could be used to ultimately query users to allow/deny access to their user profile information.*

References

- All refered Liberty Alliance Specifications can be found at ... http://www.projectliberty.org/specs/
- Other relevant references can be found at ...
  - http://www.w3.org/TR/xmldsig-core
  - http://www.w3.org/TR/xmlenc-core/
  - http://www.w3.org/TR/xmlschema-1/
  - http://www.oasis-open.org/committees/documents.php?wg_abbrev=security
  - http://www.oasis-open.org/committees/download.php/1911/WSS-SAML-07.pdf
  - http://www.oasis-open.org/committees/download.php/2757/WSS-SOAPMessageSecurity-14-063003-merged.pdf
  - http://www.oasis-open.org/committees/download.php/2744/WSS-X509%20draft%2006-05%20merged.pdf
  - http://www.ietf.org/rfc/rfc3268.txt
  - http://www.ietf.org/rfc/rfc2246.txt
  - http://www.netscape.com/eng/ssl3/