3GPP TSG SA WG3 (Security) meeting #33 **S3-040338**

10-14 May 2004

Beijing, China

Source: **Ericsson, Nokia**

Title: **GUP security follow-up**

Document for: **Discussion**

Agenda Item: **6.17**

Introduction

This contribution is a follow-up on previous discussions held around GUP security in SA3#32. It captures the current status of the Generic User Profile (GUP) work in 3GPP and proposed recommendation for SA2 and CN4 to be considered in their respective specifications in this area.

Background

There is a WI for GUP security in SA3 [GUPSecWID] but there is no placeholder for GUP security in any of existing specifications handled by SA3. There is not any planned SA3 deliverable for that kind of information either.

However, SA3 did have the chance to discuss 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*".

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

Discussion

Contribution [S3-040035] showed how SA2 TS [23.240] defines stage 2 system architecture for GUP. It is worth to mention that this SA2 specification is somehow already providing fairly complete stage 2 descriptions of GUP security aspects in terms of required authentication, authorization and privacy control mechanisms.

We believe that the stage 2 definition in TS [23.240] covers stage 1 security related requirements in SA1 TS [22.240] (see annexes in this contribution for further details on security related sections in SA1 and SA2 specifications).

Based on similar working assumptions at SA2 to base GUP architecture on Liberty Alliance ID-WSF architecture, TS [23.240] is already making references to relevant Liberty specifications. "Liberty ID-WSF Security Mechanisms" (normative) and "Liberty ID-WSF Security and Privacy Overview" (informative) specifications are however not refered to in TS [23.240]. These specifications e.g. show how TLS/SSL can be used and additionally provides message layer methods taking advantage of X.509 or SAML (specified by OASIS) tokens.

Annex B includes security related sections in SA2 TS [23.240] with revision marks included showing how SA2 could incorporate references to Liberty Alliance security specifications.

CN4 TS [29.240], which defines, stage 3 protocol specification for GUP, is also making extensive use of references to Liberty Alliance Project specifications. In this case, appropriate references to Liberty Alliance security related specifications are provided (see annexes in this contribution for additional details of security related sections in CN4 spec).

We believe however that section 9.3 should be completed in order to make accurate references to the security features provided by “Liberty ID-WSF Security mechanisms” specification beyond the pure SSL/TLS protection. The message layer security solutions in this specification should be definetely considered under this section.

Annex C includes security related sections in CN4 TS [29.240] with revision marks included showing how CN4 could incorporate references to Liberty Alliance security specifications.

Note that at this moment Rg reference point sections in CN4 TS [29.240] are void. This most probably is due to work priorization in CN4 but in any case it should be brought to the attention of CN4 that same security mechanisms as for Rp reference point should be available at Rg.

Liberty Alliance Project collaboration status

A collaboration framework between 3GPP and Liberty Alliance Project is in place since PCG#12 (April 14th, 2004). PCG#12 endorsed the Liberty Alliance proposal for working together. See [N4-040542] at http://www.3gpp.org/ftp/tsg_cn/WG4_protocollars/tsgN4_23_Zagreb/Tdocs/.

This framework allows for …

- Naming coordinators from each of our respective organizations. These individuals would be responsible for coordinating all cooperative work between 3GPP and Liberty Alliance. Timo Skytta, Vice President of the Liberty Alliance, and Senior Manager at Nokia, would be Liberty's coordinator.

- Hold one or more joint meetings of relevant 3GPP and Liberty Alliance Expert Groups to enable 3GPP members to directly state their requirements to Liberty.

- Encourage "overlap" members to actively participate in the Liberty Technology Expert Group to address 3GPP requirements. If desired by 3GPP, Liberty would suggest that a small number of "non-overlap" 3GPP members participate in Liberty Tech EG as invited experts (per Liberty policy). This would ensure that 3GPP requirements and issues are addressed on an ongoing basis.

- As appropriate, The Liberty Alliance project will provide early access by 3GPP members to Liberty documents that address 3GPP-specific requirements. A URL to early draft specifications, disclosed only to 3GPP, would be sent to the relevant 3GPP working group as required.

Proposal

With this contribution, SA3 is invited to review security related sections in SA2 TS [23.240] (see appendix B in this contribution) in order to agree on the fact that there is no need for GUP security material to be included in any of existing or new SA3 specifications. Current terms in SA2 TS [23.240] with small clarifications to provide references to security related Liberty Alliance Specifications (as proposed in appendix B) should suffice in order to define stage 2 security in this area.

SA3 is also invited to review security related sections in CN4 TS [29.240] (see appendix C in this contribution) in order to decide if the proposed way of referencing the Liberty Security related specifications would be appropriate.

Additionally, it is also proposed that SA2 and CN4 are informed that SA3 has performed an early review of their GUP specifications and suggest them an accurate use of references to Liberty Security related specifications as outlined above. SA3 should of course offer review of security related chapters once SA2 and CN4 GUP specifications are in good shape.

References

[GUPSecWID]	3GPP TSG SA WG3, S3-020430, 3GPP Generic User Profile Security Work Item Description
[S3-040035]	Nokia, Ericsson, S3-040035, GUP security directions follow-up
[S3-040199]	3GPP TSG SA WG3, S3-040199, LS on GUP security directions
[N4-040542]	LAP coordinator from the 3GPP, 3GPP TSG CN WG4, N4-040542, Way forward agreed on Liberty Alliance collaboration
[22.240]	3GPP TS 29.240: “Service requirement for the 3GPP Generic User Profile (GUP); Stage 1 (Release 6)”
[23.240]	3GPP TS 23.240: "3GPP Generic User Profile - Architecture; Stage 2”
[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

Annex A: Excerpt from Service requirement for the 3GPP Generic User Profile (GUP) TS 22.240 v.6.3.0:

7 Security

Secure mechanisms shall be available for the transfer of User Profile data to, from or between authorised entities. Access to User Profile data shall only be permitted in an authorised and secure manner. The secure mechanisms to be applied shall be appropriate to the level of confidentiality of the data, the endpoints of the transfer and the routes that are available for the transfer of the data. The owner of the data, normally the body storing the master copy of the data, shall be responsible for applying the appropriate level of security to the transfer of the data.
The secure mechanisms available shall include the following:

1. Authentication of consumer
   Before any user data transfer takes place, it shall be possible for the supplier of the data to verify the identity of the consumer.

2. Authentication of supplier
   It shall be possible for the consumer of data to identify the supplier.

3. It is permissible for either the supplier or consumer of data to employ the services of a third party, known to, and trusted by, both in order to provide authentication of identity.

4. The validity of an authentication of identity shall, if required, be subject to a maximum time limit.

5. It shall be possible for the supplier of data to render the data to be unreadable by any party not authorised to receive it.

6. It shall be possible for the consumer of data to detect whether the data have been tampered with during transmission. .

7. The security mechanisms shall provide verification that the data has been sent by the supplier and received by the consumer (non-repudiation).

8. It shall be possible for the supplier and/or the consumer to create an audit log of all GUP data transfer transactions of a specified type, provided that this requirement is made known before any transfer takes place

9. User profile data in general is proprietary data. This data may not be shared with unauthorized entities. *Access control* to the data is required. This access control must also apply to data which is located at legacy systems, currently without own access control functionality.

10. Correct setting of data values in the user profile may be critical for the integrity of certain network services. Therefore, *consistency checks* are needed to minimise the risk.

11. Transaction security for the change of data should be available in order to ensure the consistent change of data at different locations.

8 Privacy and Authorisation

This clause describes the requirements for the authorisation of access to the user profile data. The Privacy can be provided by the means of authorisation mechanism.

8.1 General Requirements

It shall be possible for the user to define privacy requirements for components of the 3GPP Generic User Profile to determine access rights.
It is agreed in the subscription agreement between the home network operator and the subscriber how the access and privacy control is carried out e.g. who is able to control different parts of the user profile including the privacy settings.
The GUP shall provide means to implement access and privacy control according to the different agreements.
The GUP authorization shall be independent of who has set the privacy rules for each part of the GUP data. A generic mechanism shall be provided to ensure that only such data for which there is a valid authority can be created, read, modified or deleted.
The privacy requirements shall fulfill local privacy regulations. Lawful interception and other regulator requirements may imply that GUP data is delivered to authorities despite the privacy settings.

8.2 Authorisation Rules

Authorisation of the requested action (create, read, modify or delete) on the user profile data depends on the following information:

- identification of the requesting application
- identification of the requesting subscriber (if delivered in the request)
- identification of the targeted user
- identification of the targeted user profile data

The disclosure of the user profile data must be considered based on the identification of the application requesting access to the data. The possible identities of the applications will not be standardised but are implementation specific. Regarding trusted applications involving other subscribers or comparable entities it shall be possible also to check the access rights of the subscriber being served by the application. This requires that the identification of the served subscriber is passed via the GUP mechanism in addition to the application identification. The access is first defined per applications and secondly per served subscriber. The access may be granted also to the public, some group or a list of subscribers.
The identity of targeted user will be based on the 3GPP network identities (Private and Public User Identities). Public User Identities would be normally applied, but especially within the operator domain the Private Identity could be used as well.
The targeted user profile data will be controlled as per the whole user profile and/or per different GUP components and/or per different GUP data elements.
Depending on the service the privacy of the requested GUP data can additionally be managed in the service level e.g. in Presence or IMS group management. The privacy rules for these services are specified in the corresponding 3GPP specifications.
The GUP shall also support the possibility that the privacy of specific GUP data is queried from other privacy control system. Existing privacy solutions should be considered and adopted if applicable (e.g. LCS).

Annex B: Excerpts from 3GPP Generic User Profile - architecture TS 23.240 v.6.3.0:

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 22.240: "Stage 1 Service Requirement for the 3GPP Generic User Profile (GUP)".

[2] Liberty Discovery Service Specification, http://www.projectliberty.org/

[3] Liberty ID-WSF SOAP Binding Specification, http://www.projectliberty.org/

[4] Liberty ID-WSF Data Services Template, http://www.projectliberty.org/

[5] Liberty ID-WSF Security and Privacy Overview, http://www.projectliberty.org/

[6] Liberty ID-WSF Security Mechanisms, http://www.projectliberty.org/

4.1.3 Authentication of profile access

A GUP functionality exists that is responsible to authenticate applications. Authentication is a vital function to be passed before any kind of access to GUP data is granted. GUP shall adopt generic mechanisms such as used for the OSA framework approach. GUP shall also be able to leverage authentication mechanisms from Liberty Alliance Project as specified in [5] and [6].

4.1.4 Authorization of profile access

A GUP functionality exists that is responsible to authorise applications to access GUP data based on User specific or common privacy rules. All attempts to access the GUP data are to be authorized according to the defined policies which shall include the requestor information, the requested data, the target subscriber and the performed operation, or some of those.

GUP leverages authorization mechanisms from Liberty Alliance Project as specified in [5] and [6].

The GUP data structures need to satisfy the requirement to provide the authorization information on the different levels: profile, component or data element. In addition to the generic authorization data, additional service specific data may be defined (e.g. for LCS). The same applies for the authorization decision logic. The execution of the authorization logic leads to a decision whether a requestor is allowed to make the request at all, and additionally to which part of data the requestor has the appropriate access rights with regard to the nature of the request.
GUP provides mechanisms for the different GUP entities for managing the authorization data.
Both HPLMN based applications and non-HPLMN based applications are expected to send requests to the GUP Server. The GUP server shall have functionality to apply different authorization criteria, policy control and load control to HPLMN and non-HPLMN applications. Policy control and load control are out of the scope of the present document.

4.1.5 Privacy control

The tight connection of authentication, authorization and subscriber specific privacy requirements results in privacy control. Privacy control implies a centralized management for access rights including the subscriber's privacy requirements.

GUP leverages privacy control mechanisms and other privacy related features from Liberty Alliance Project as specified in [5] and [6].

4.2.1.3 Authentication of profile request

The GUP Server shall make sure that the application requesting user profile data is properly authenticated. The authentication is based on the identification of the requesting application and/or the identification of the possible subscriber requesting the user profile data. The GUP Server may rely on the authentication made by other trusted entities.

4.2.1.4 Authorization of profile request

The GUP Server shall take care of the authorization of the access to the user profile data. The authorization itself may be handled by a separate entity in the network, or alternatively by the RAF or GUP Data Repository. The authorization shall be based on the requestor information, the requested data, the target subscriber and the performed operation, or some of them. The authorization rules of the requested data shall be defined at least in the GUP Component level in GUP Server. (Note that the authorization may be based on also on finer granularity of the data content.) It shall be possible to manage the authorization data via the Rg and Rp reference points.

Annex C: Excerpts from 3GPP Generic User Profile - network TS 29.240 v.0.3.0:

9.3 Security, Authentication and Authorisation

~~The security of the Rp reference point is based on standard SSL 3.0 or TLS 1.0 [20] usage to provide authentication and http transport data integrity and confidentiality protection. The authentication with TLS/SSL shall be based on X.509 v3 certificates on both server and client side. 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.~~

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 basically 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 Liberty Alliance specifications recommend the use of the Web Services Security SAML Profile.

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

Editor's note: SA WG3 is expected to review this and provide further contents to this subclause.

9.4 Protocol Aspects

The SOAP protocol is applied in the Rp reference point. SOAP provides a mechanism for exchanging structured and typed information between peers using XML. It is a very generic protocol which can also be used to carry remote procedure calls. Each SOAP message has an element "Envelope" and its immediate child elements "Header" and "Body". SOAP carries the GUP procedure elements in its body part in compliance with the SOAP standard [5]. The GUP Procedure elements are placed immediately below the Body element. If there are several requests or responses, the GUP Procedure elements are carried one after another.
GUP SOAP messages are specified to run over standard http [6] as specified in [5] but implementations may also support other transport mechanims. If any SOAP level error is reported, no application data are returned.
There are a number of SOAP Header elements defined for GUP. The first part of each header is defined according to the Liberty ID-WSF SOAP Binding Specification [14] which specifies the following header blocks:

- CorrelationType Header Block
- ConsentType Header Block
- UsageDirective Header Block

Additionally the Liberty ID-WSF Security Mechanisms specification [15] defines SOAP headers for security, authentication and authorisation purposes. Those may optionally be applied in GUP requests and responses. See subclause 9.3 and 9.4.4 for more information.

9.4.1 CorrelationType Header Block

The CorrelationType Header Block is used to correlate request and response messages. The following specific attributes are defined:

- messageID
- messageIDRef
- timestamp
- id

9.4.2 ConsentType Header Block

The ConsentType Header Block may optionally be used to indicate the principal's consent for an operation. The following specific attributes are defined:

- uri
- timestamp
- id

9.4.3 UsageDirective Header Block

The UsageDirective Header Block may optionally be used for privacy protection purposes. It is able to show the privacy policy which is intended to be applied (in a request) or which should be followed (in a response). The following specific attributes are defined:

- ref
- id
- <Privacy policy instance>

9.4.4 Security header element

Liberty ID-WSF Security Mechanisms [15] specifies a Security header element. The Security header element contains XML elements:

- Assertion
- Signature

Editor's note: SA WG3 is expected to provide contents to this subclause

9.4.5 Requestor data

The GUP stage 2 3GPP TS 23.240 [1] contains a Requestor data parameter in several procedures. This subclause shows how the Requestor data parameter is carried in the SOAP headers defined by the Liberty Alliance Project. The information can be provided as follows:

- The subscriber identification matches with the concept of an invocation id in Liberty ID-WSF specifications. This id is carried inside the Security SOAP header in the Subject element.
- The application identification matches with the concept of sender id in Liberty ID-WSF specifications. This id is carried inside the Security SOAP header in the ProxySubject element.
- The authorization assertion is provided within the Security header element in the Assertion element.
- The additional info may be carried inside the Assertion (or in procedure extensions). More detailed specification is FFS.

Editor's note: Also a GUP specific new SOAP header element may need to be considered for part of the Requestor data information.