3GPP TSG SA WG3 Security — SA3#35 **S3-040813**

October 5-8, 2004

St Paul's Bay, Malta

Agenda Item: **6.9**

Source: **Vodafone**

Title: **Relationship between GAA and Liberty**

Document for: **Discussion**

1 Introduction

In this paper we consider the relationship between GAA and Liberty. In particular, we try to identify to what extent GAA is complementary to Liberty and to what extent it overlaps with Liberty. Some conclusions and recommendations are provided.

2 Discussion

2.1 Complementary part

GAA provides two authentication methods that could be used over HTTP:

- Generic Bootstrapping Architecture – **GBA**: A symmetric method that uses 3GPP AKA to establish a session key. The session key may then be used to provide authentication e.g. using HTTP Digest.
- Support for Subscriber Certificates – **SSC:** User certificates are issued dynamically to the client environment, for subsequent (but out of scope) use in any PKI-based system. For example the certificates might provide authentication or signature functions. OMA (i.e. WAP) PKI is re-used for key-pair generation and certificate format, etc. [1]

The above is complementary to Liberty, which can accommodate various authentication methods. There is a case for positioning this part of GAA as a profile of Liberty in some way, perhaps as an authentication context. (ref: liberty-idff-guidelines-v1.2.pdf, section 5.4, liberty-authentication-context-v1.2.pdf, section 5.2.4 and 5.2.6.)

GAA doesn't describe a Directory Service (DS) or Single Sign On (SSO), so it is narrower in scope than Liberty.

2.2 Overlapping part

The GBA framework abstracts the authentication process from the process of accessing services, as in Liberty.

- The Bootstrapping Server Function – BSF – (analogous to an Identity Provider, IdP, in Liberty) mediates for authentication between the client and the Home Subscriber System – HSS (analogous to authentication provider in Liberty).

[1] The issuing of a new client certificate using SSC could be offered as a web service in itself, requiring an application server (NAF) acting as a PKI portal. This, in turn, requires authentication and a secure session, which may be achieved using GBA or by PKI using an existing client certificate.

- This results in a BSF session key being established between the client and the BSF. The client derives and uses the BSF session key and also derives a NAF-specific session key. The BSF sends a copy of the derived NAF-specific session key and user security setting data to a trusted[2] Network Application Function – NAF – (analogous to a Service Provider, SP, in Liberty), so that it and the client can engage in a secure application session.

- Liberty protocols could be used between ME, BSF and NAF by specifying GAA authentication mechanisms for SASL. (ref: liberty-idwsf-authn-svc-v1.0.pdf, section A). Alternatively, GAA authentication could be seen as “out of band” from a Liberty perspective.

- When the GUP requestor is an ME (acting in the role of a LUAD-WSC), and to avoid having to have client certificates, GBA authentication could be used where the GUP server (Liberty service provider) acts as an NAF (ref: liberty-idwsf-client-profiles-v1.0.pdf, section 3).

3 Conclusions and recommendations

1. The GAA has been developed independently of Liberty. It aims at allowing a 3GPP network operator to operate its own closely-controlled HTTP-based authentication and server/client interactions, over mobile core networks, without having to adopt Identity-based standards such as Liberty. However, it should be considered whether 3GPP should allow, as an option, the adoption of the Liberty ID-FF specs for the framework parts of GAA, like OMA have done with their OWSER.

2. The authentication part of GAA could be specified so that it appears as an authentication context that is compatible with Liberty ID-FF and Liberty ID-WSF. It should be considered whether GBA authentication, SSC authentication or both should be specified in this way.

3. The work split between 3GPP and Liberty Alliance is for further study. It may be useful to send a preliminary liaison statement to Liberty Alliance.

4 References

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

- Liberty ID-FF Guidelines v1.2, liberty-idff-guidelines-v1.2.pdf

- Liberty Authentication Context Specification, Version 1.2, liberty-authentication-context-v1.2.pdf.

- Liberty ID-WSF Authentication Service Specification, liberty-idwsf-authn-svc-v1.0.pdf.

- Liberty ID-WSF Client Profiles Specification, liberty-idwsf-client-profiles-v1.0.pdf.

[2] I.e. trusted by the home operator to handle derived keys