

**Source:** Nokia  
**Title:** Liberty and GAA relationship  
**Agenda item:** 6.9.1 (GAA)  
**Document for:** Information

---

## 1 Introduction

The relationship between Liberty and GAA has been brought up during several SA3 meetings. As GAA has become mature, its relationship and possible overlap areas with Liberty can now be identified more clearly. In this contribution, we point out the details on the possible relationship between GAA and Liberty, and invite further comments on the details of the relationship and possible interaction methods.

Below is a list of previous contributions on Liberty and GAA relationship:

- Discussion document on Bootstrapping and Subscriber Certificate Use Cases that includes the Liberty use case (SA3-030407, Nokia) from SA3#29 meeting
- Introductory Presentation on Liberty Alliance (SA3-030764, Nokia) SA3#31 meeting
- Presentation on synergies between Liberty Alliance and 3GPP (SA3-030719, Nokia) SA#31 meeting
- Discussion document on the Relationship between GAA and Liberty (SA3-040813, Vodafone) SA#35 meeting

---

## 2 Discussion

Liberty Alliance Project (LAP) defines in the ID-FF specification a family of protocols. Those protocols enable reuse of an authentication done at an Identity Provider (IdP) for user authentication towards a Service Provider, that trusts this authentication confirmation of the IdP. LAP does not specify the actual means of authentication, but leaves that for agreement between the business partners. The Liberty Alliance specifications just use the provided authentication means without restricting the type of authentication mechanism, to enable easy integration with the existing infrastructure and legacy authentication mechanism (e.g. username / password). GAA, which is specific to mobile subscribers, is one of the methods that can be used to provide the authentication mechanism for Liberty. For example, the Liberty Identity Provider (IdP) can act as a NAF, as depicted in figure 1 (see also S3-030407, and S3-040719). This configuration setting would not provide any overlap in provided functionality. GAA would be used to authenticate the UE towards the IdP (via HTTP digest authentication). After the HTTP digest authentication, the LAP protocols towards Liberty SPs would be used, as outlined in the message flow diagram below. An advantage of this mobile specific configuration is that the authentication will then be more secure and user-friendly as compared to passwords.

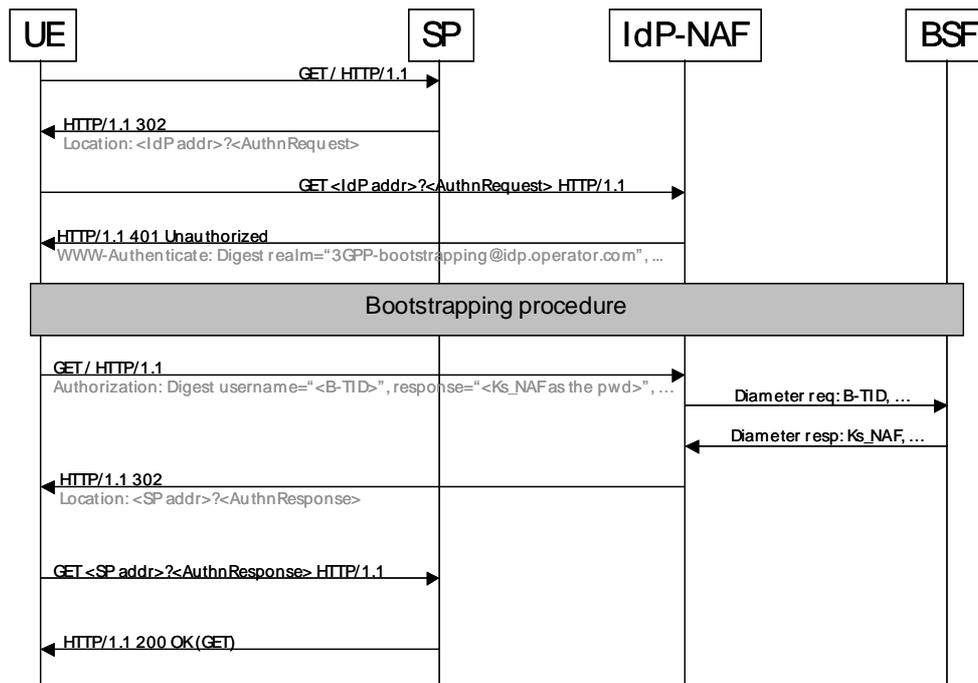


Figure 1. Example of Liberty IdP working as a NAF

### 3 Potential topics for further studies

First, Vodafone contribution (S3-040831) stated that the BSF provides a similar functionality then the Liberty IdP. Hence the IdP could also be co-located with GAA's BSF. The details of this approach are yet unknown and require further studies.

Second potential topic for further studies is the case where Liberty SP and GAA NAF are co-located, then the SP supports both Liberty protocols and GAA's NAF functionality. There is a functionality needed which authentication method it should use based on the Service Provider requirements and UE's capabilities. If the Liberty Service Provider (SP) is compared to GAA's Network Application Function (NAF), the difference is that with the Liberty protocols the SP gets authentication confirmation, but it does not get the keys of the terminal. In GAA the NAF gets the keys and the authentication confirmation. With Liberty, the SP has to verify the SAML assertion given by the IdP., In GAA, the NAF has to authenticate the UE using the GAA credentials (i.e., B-TID, and Ks\_NAF).

Third, Liberty Alliance project also does not provide guidance on the interfaces between IdP and the backend, "legacy" databases (or how the IdP is organized "internally"). Thus, if the "legacy" database is HSS, the GAA Zh interface might be a good complementing functionality. But further studies might be required there.

An open issue with GAA and Liberty interworking is that Liberty Alliance requires in their SAML tokens timestamps for the authentication. However, GAA currently only offers an expiry timestamp of the bootstrapping key to NAFs, not the timestamp of the exact timestamp when the bootstrapping was performed.

Finally, Liberty Alliance has introduced the notion of authentication context as a quality measure for the authentication, and they specified some examples for authentication contexts. 3GPP could specify a GAA specific authentication context for Liberty.

### 4 Conclusion

As briefly described in this paper, the Liberty Alliance protocols can use GAA as authentication method for mobile subscribers. The authentication will then be more secure and user-friendly as compared to passwords. Most straightforward way is to implement this is to add NAF functionality to Liberty IdP. To further support this functionality, SA3 could specify a GAA specific authentication context for Liberty.

Possible Liberty Alliance and GAA overlaps and other synergies are FFS.