

S3-030719

Potential synergies between Liberty and 3GPP

Presentation in SA3#31 Munich meeting

18-21 November

Nokia

Content

- Potential synergies with GAA
 - Operator IdP uses GAA in authenticating UE
- Possible interconnections with GUP
 - GUP in General
 - GUP Security Requirements
 - GUP Architecture with a few Liberty aspects
 - A few notes on GUP Security
 - GUP Server as Redirect Server

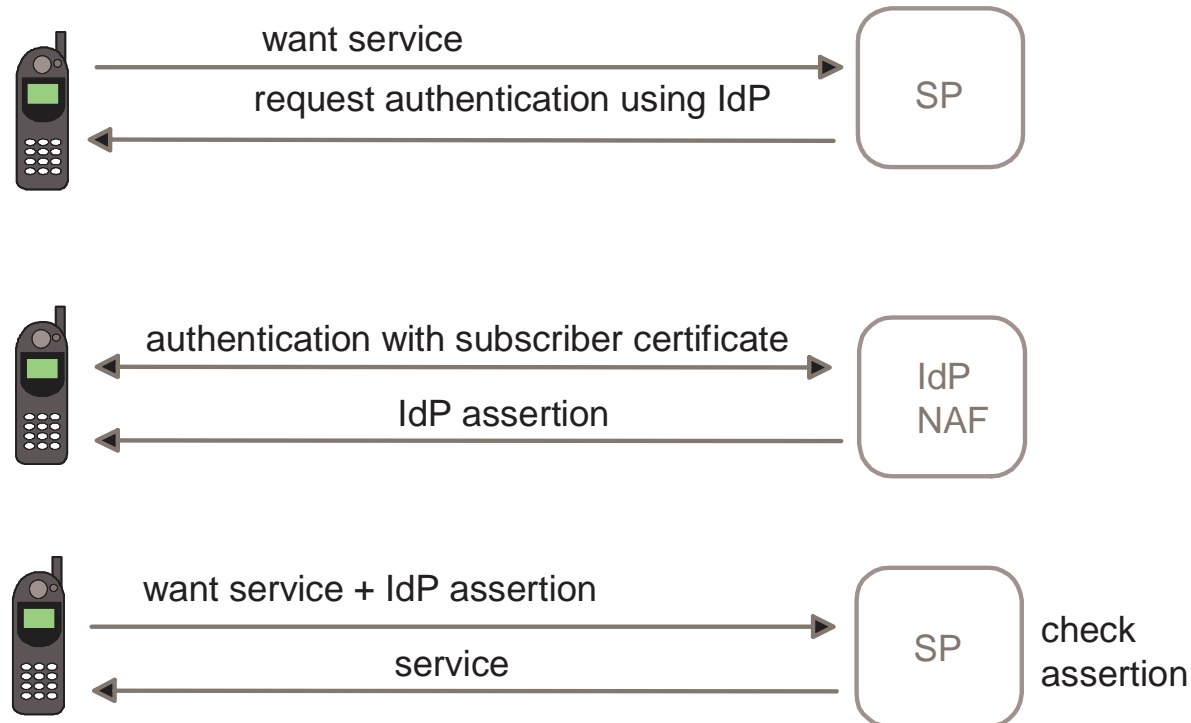
Possible synergies with GAA

- Operator IdP may use GAA in authenticating UE
 - Enables Liberty-compliant services to subscribers
 - Leverages authentication mechanisms of cellular networks for Liberty.
 - Increases the scalability of Liberty because a cellular subscriber could potentially use the IdPs of any operator with whom his home operator has a roaming agreement.

Operator IdP uses GAA in authenticating UE

(1/2)

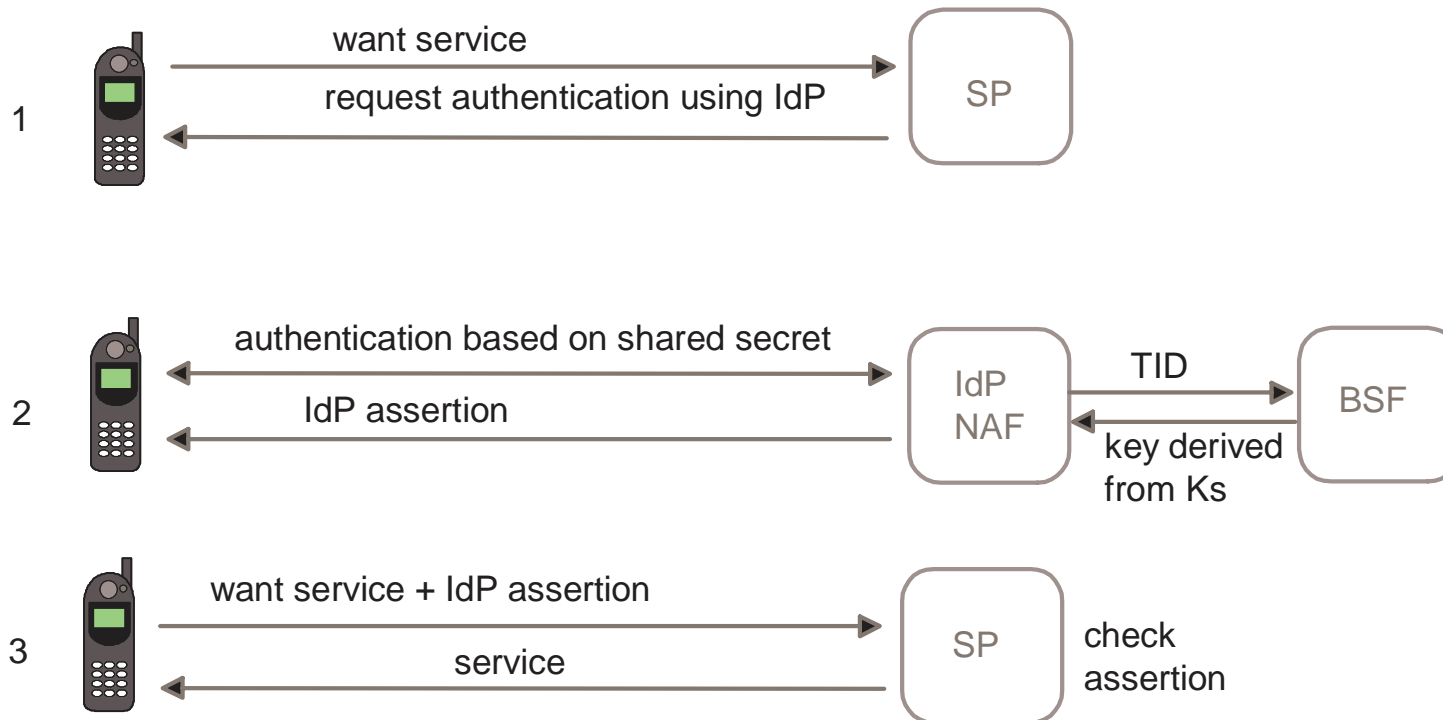
Authentication to IdP based on certificate



- The bootstrapping of shared secret from AKA and subscriber certificate enrollment has occurred before the depicted sequence

Operator IdP uses GAA in authenticating UE (2/2)

Authentication to IdP based on shared secret



- The bootstrapping of shared secret from AKA has occurred before the depicted sequence

Possible interconnections with GUP

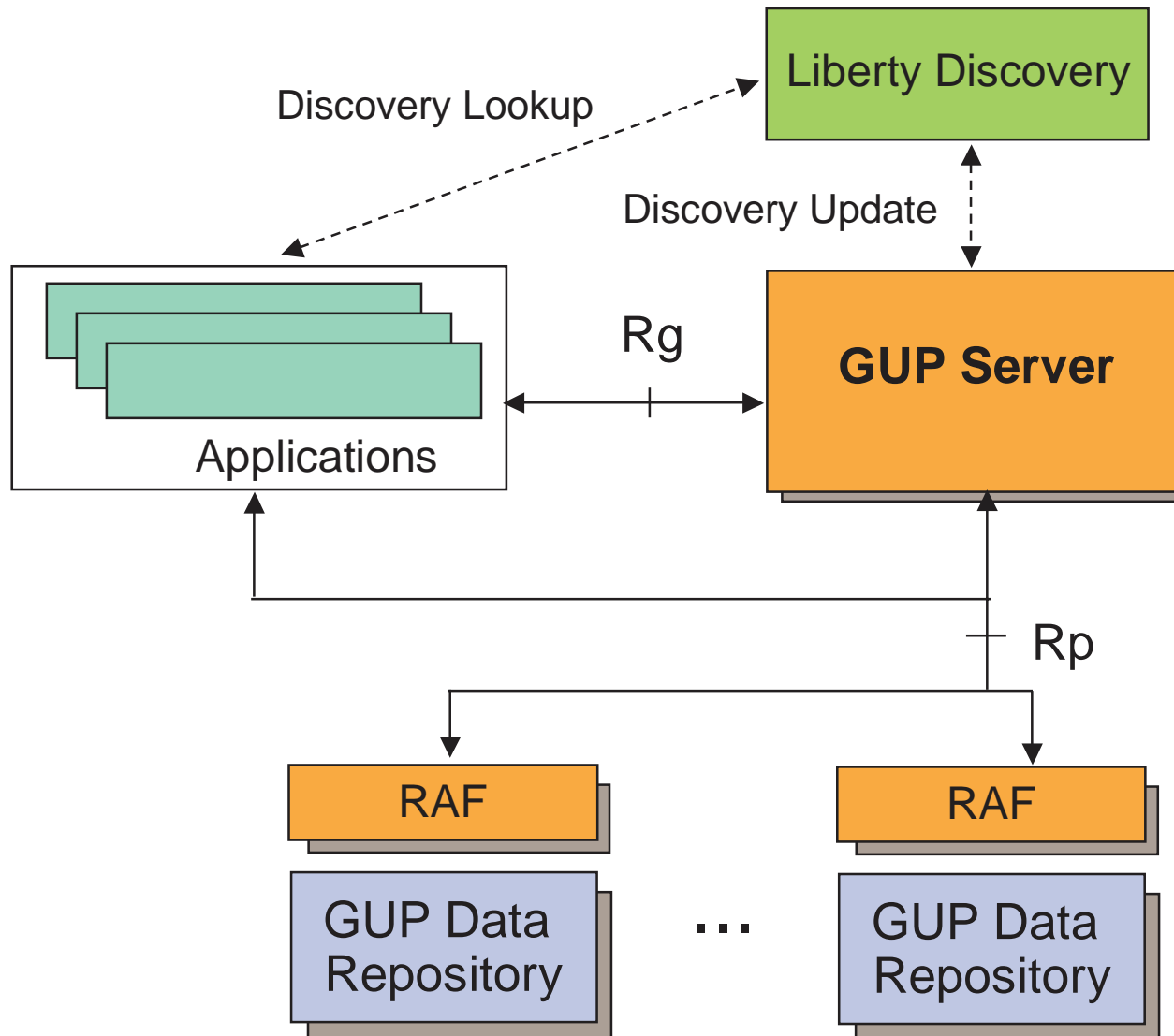
GUP in General

- Several core network domains (Circuit-Switched, Packet-Switched, IP Multimedia Subsystem), several access technologies (e.g. GERAN, UTRAN and WLAN) and increasing number of new services have introduced large amount of data associated with the user.
- The objective of specifying GUP is to provide a conceptual description to enable harmonised usage of the user-related information located in different entities.
- Technically GUP provides an architecture, data description and interfaces with mechanisms to handle the data.
- GUP can be stored in the home network and additionally storage can be extended to the UE and/or Value Added Service Provider equipment.
- GUP could be used e.g. for subscription management and data retrieval by various type of applications.
- GUP Rg interface provides a single point of access to the whole Profile and Rp a harmonised 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 Security requirements

- 3GPP TS 22.240 mentions e.g. the following requirements:
 - Authentication (recipient and sender)
 - third party may assist
 - life time limit
 - Confidentiality
 - Integrity protection
 - Access control, Authorisation and privacy
 - Non-repudiation
 - Audit log
 - Consistency checks
- Liberty ID-WSF is based on very similar requirements and fulfills most of the GUP security requirements.

GUP Architecture with a few Liberty aspects



Rg supports also third party connections like Liberty ID-WSF. It is a natural choice to adopt Liberty ID-WSF for Rg and make GUP Rg like another profile service as Liberty ID-PP (personal profile).

Similarly as in Liberty, XML is used in GUP and CN4 has chosen SOAP as the protocol. Hence Liberty Security provides a good basis for the security solutions.

RAF = Repository Access Function

A few notes on GUP Security

- Liberty ID-WSF is solving quite similar task as GUP Rg reference point => No motivation to define another overlapping but incompatible standard (also regarding security aspects)
- Liberty Discovery service may be left beyond GUP specifications but it could be still applied as specified by Liberty Alliance Project.
- Authorisation assertions and privacy policies are included also in GUP stage 2 procedure definitions (as in Liberty).
- It would be beneficial to have similar solutions for GUP Rp reference point as for Rg.
- The security aspects of redirect mode (where application request in Rg reference point is redirected so that application makes a further request in Rp) should be taken into account.
- Liberty ID-WSF security specifies TLS/SSL usage and additionally message layer security. We suggest 3GPP SA3 to further discuss if the latter is required in GUP.
- Furthermore Liberty ID-FF usage to help in authentication is proposed to be studied.
- More information in Nokia SA3#30 Porto contribution “GUP security directions”, S3-030581.