Identity Management in 3GPP

Silke Holtmanns (Rapporteur of IdM related specifications/reports in 3GPP SA3 Security)

NOKIA

History of Identity Management

- Liberty Alliance seems only to take off in the enterprise area, due to the complexity (most offerings are from enterprise-software vendors)
- OpenID filled the gap for many service providers who wanted an easy and fast way for Single Sign On
- OpenID is from the “Web” i.e. does not support typical telco-protocols like Diameter
- If operators wanted to be able to offer their high quality authentication to service providers a simple and efficient way of interworking was needed
- Interworking should not require major changes to the operator network or on the service provider side

Usage - Who uses and supports OpenID?

- Some OpenID Provider & Services
  - Google, NTT DoCoMo, Flickr, Yahoo!, Microsoft, AOL, Verisign, Facebook, Wikitravel, Slashdot, Worldpress, IBM, PayPal, New York Times, SAP, Orange France, MySpace, Blogger, Bloglines, Blogspot, LiveJournal, Citi, Wave Systems,... ..
- Governmental usage of OpenID
  - US Government has a Pilot Project on OpenID
  - Japanese government
  - OpenID.ee (Estonia), openid.vrm.lt (Lithuania)
- Sources:
  - http://en.wikipedia.org/wiki/List_of_OpenID_providers
  - http://en.wikipedia.org/wiki/Category:Internet_services_supporting_OpenID
  - http://openid.net/government/
  - http://openidgermany.de/2007/09/25/erster-groser-telco-unterstutzt-openid/
  - http://spreadopenid.org/provider-comparison/

OpenID and Authentication

- OpenID authorizes requests to application servers (Relying Parties = RPs) by redirecting them to an OpenID Identity Provider (OP).

- OpenID intentionally leaves the authentication protocol between client and OP unspecified.

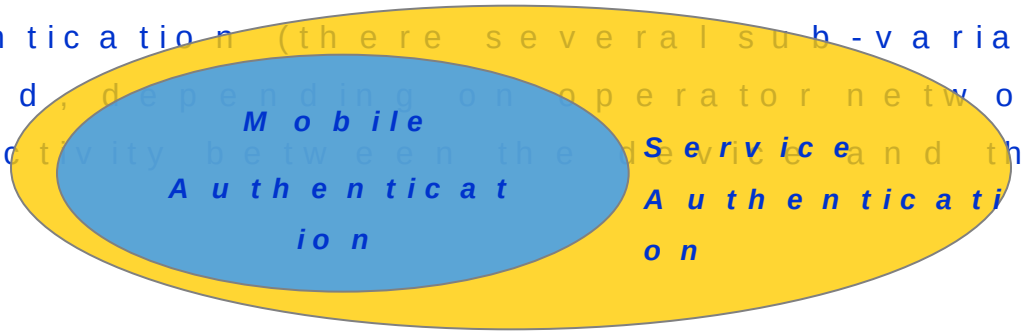
- The choice of authentication protocol depends, among other factors, on the available credentials.

- For clients on – or with access to – a 3GPP-compliant mobile phone, USIMs are a sensible choice for the SSO credentials as they allow operators to leverage their subscriber databases.

- USIMs are used in authentication with one of the variants of the AKA protocol. As client and OP communicate over HTTP, the obvious choice seems one of the two versions of HTTP Digest

3GPP TR 33.924 OpenID and Generic Bootstrapping Architecture (GBA) Interworking

- Outlines the re-usage of cellular authentication for Single Sign On (Identity Management) using OpenID for web browsing authentication
- Two variants
  - User browsing with the same device as he is authenticating with (PC with USB stick which contains UICC or phone with UICC).
  - User browsing with PC and using his phone for authentication (there several sub-variants are outlined, depending on operator network or local connectivity between the device and the PC)



Why combine OpenID with GBA?

- No open third party interface to HSS / HLR
- No need for service provider to support telecommunication specific protocols
- Minimizing load on HSS by re-usage of Authentication Vectors
- Key separation for different service (no one falls, all fall)
- GBA can also be used for other services and not only for IdM, some operators have already a GBA credential server (BSF – Bootstrapping Server Function)
- Works with SIM, USIM, ISIM cards (also a 3GPP2 standard exist)
- Is already deployed by some operators

NOKIA

We want IdM light and fast!

- In the first moment GBA looks big, but the actual functions are light if used for a limited purpose e.g. an web server can be turned into a NAF by adding a library containing less then 1000 lines of code.

- The GBA software in the phone is highly sensitive, since it accesses the smart card. The access is controlled and secured. This is not something that can be just cobbled together in a couple of weeks. Remember this is SSO, if this is not secured, many user accounts are compromised. OpenID protocol runs from the browser and should not have direct UICC card access.

- GBA enabled phones are shipped and in the market (all S60 phones that are currently shipped).

- No point in inventing the wheel twice, this works, is secured and available, better to build on it, then to start from scratch. It took 8 years for GBA to take off, have you that much time to wait for an alternative?

NOKIA

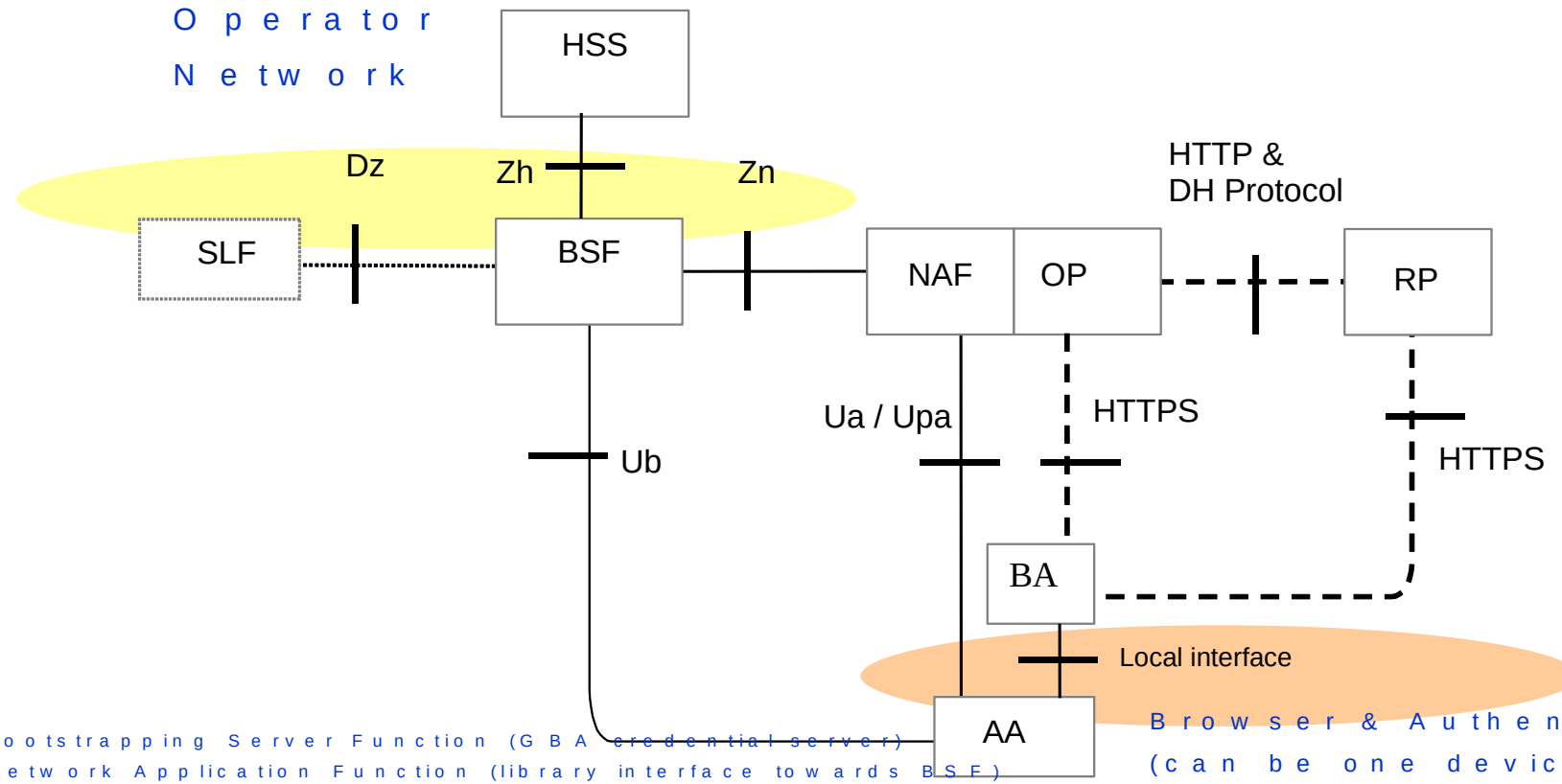
Overview of OpenID-GBA Interworking

- 3GPP Rel-9 introduced a technical report TR 33.924 for GBA - OpenID interworking, also called OpenID Identity Management Interworking
- Describes how the UICC-based keys can be used as a baseline for application security and Single-Sign On in combination with Generic Bootstrapping Architecture

- Two main variants
  - The terminal that is used for browsing is also the one that authenticates contains also the UICC
  - The terminal that is used for browsing is different then the one used for authentication (e.g. PC & phone). In this variant there are several scenarios, depending on the connection type between phone & PC

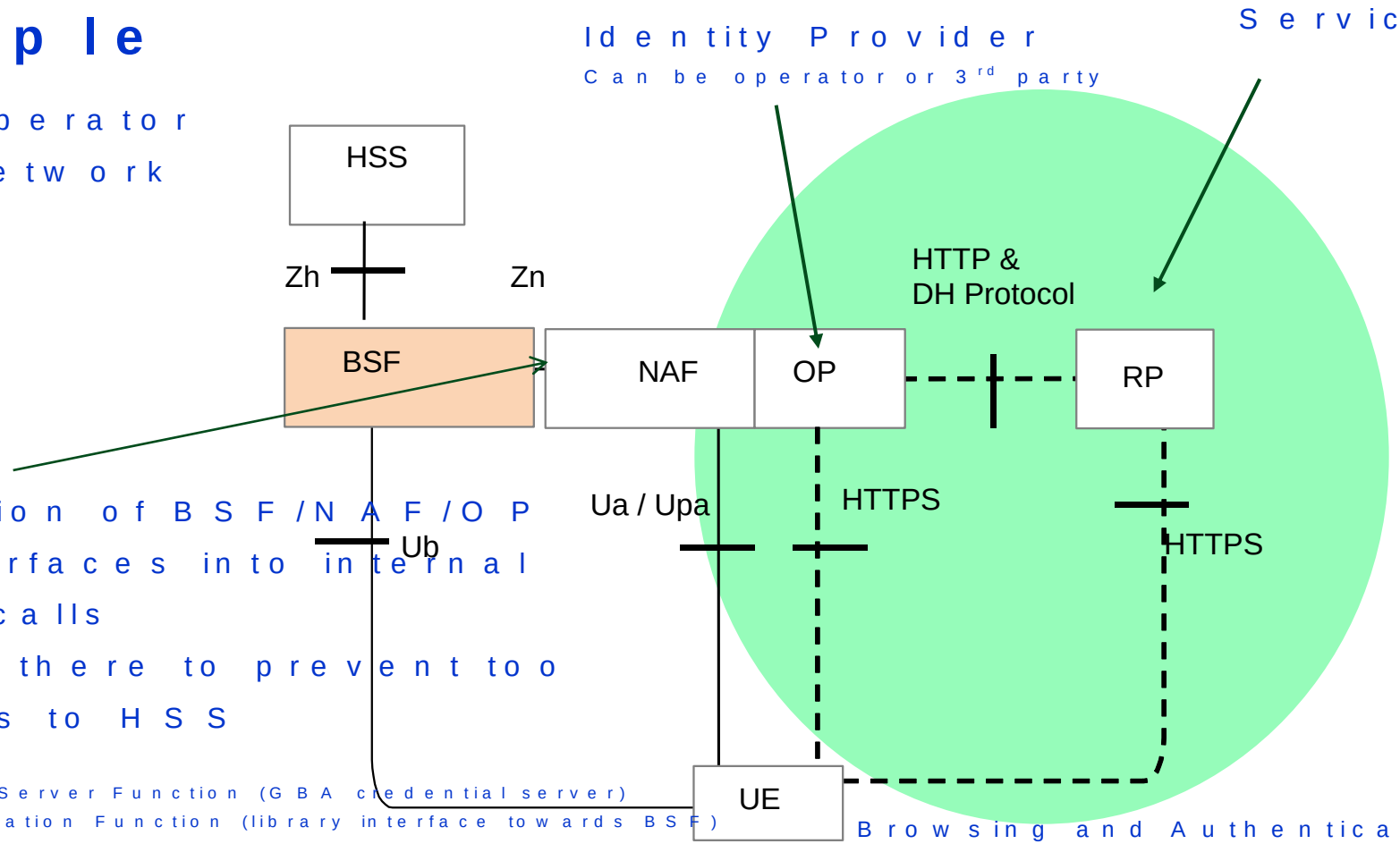
NOKIA

GBA – OpenID Interworking Architecture



BSF- Bootstrapping Server Function (GBA credential server)
NAF- Network Application Function (library interface towards BSF)
AA – Authenticating Agent (device holding UICC)
BA – Browsing Agent (browser)
RP – Relaying Party (service wanting user authentication)
OP – OpenID Provider (identity provider)
SLF – Subscriber Location Function (locates right HSS for this user)

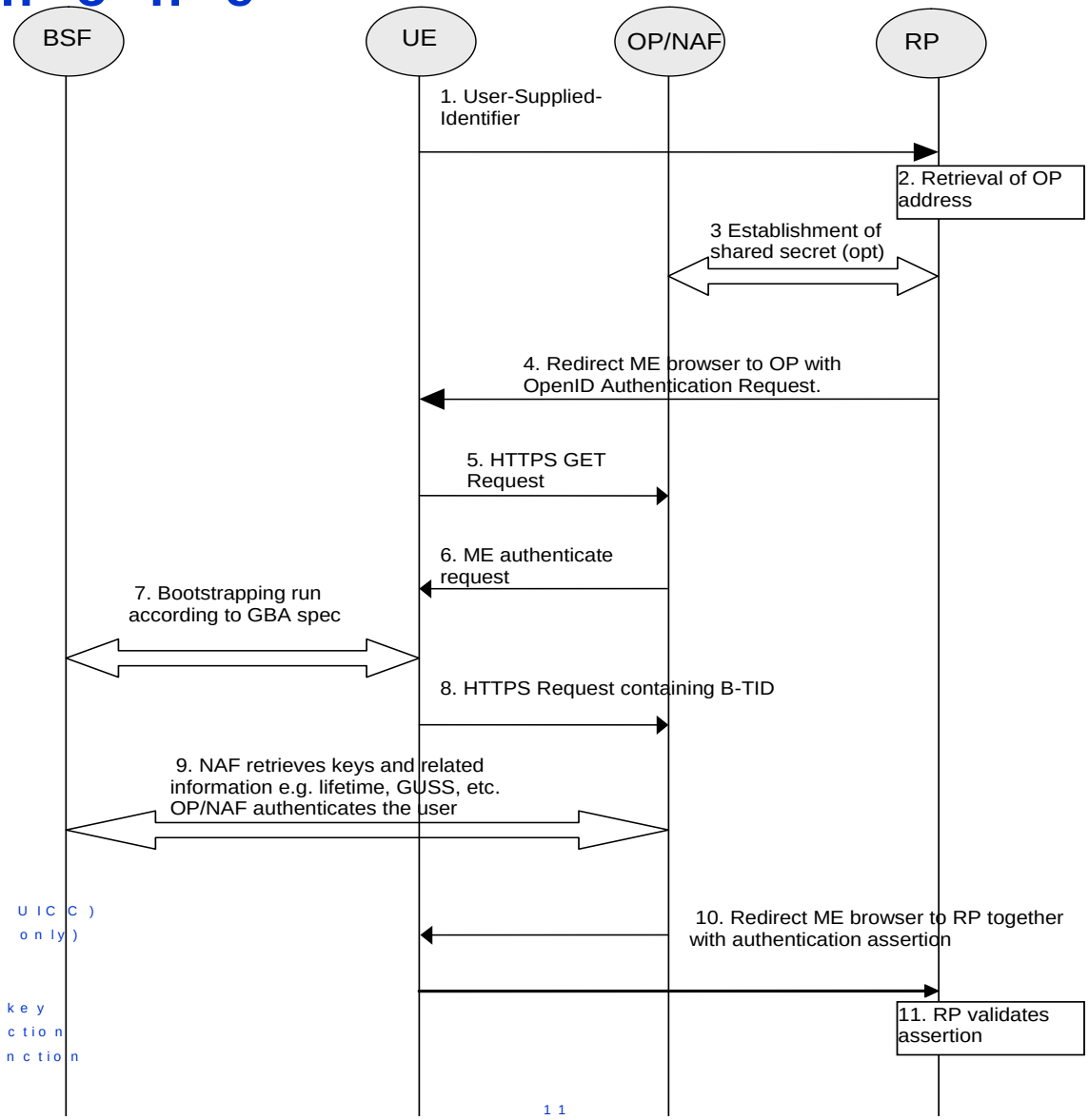
GBA – OpenID Interworking Architecture – Practical Example



- Collocation of BSF/NAF/OP Turns interfaces into internal Function calls
- BSF still there to prevent too many calls to HSS

BSF- Bootstrapping Server Function (GBA credential server)
NAF- Network Application Function (library interface towards BSF)
AA – Authenticating Agent (device holding UICC)
BA – Browsing Agent (browser)
RP – Relaying Party (service wanting user authentication)
OP – OpenID Provider (identity provider)
SLF – Subscriber Location Function (locates right HSS for this user, only needed in large networks)

Flow Diagram – Usage of SSO from phone



UE – User Equipment (phone + UICC)
ME – Mobile Equipment (phone only)
OP – OpenID Provider
RP – Relaying Party (service)
B-TID – Name for cryptograpic key
NAF – Network Application Function
BSF – Bootstrapping Server Function

NOKIA

Network Convergence

- Many operators run fixed and mobile network and would like to utilize one backend for their identity management system
- Large range of IMS endpoints do NOT have a smart card, but still would benefit from an operator provided SSO
- Security of existing IMS infrastructure should not be endangered by adding SSO for non-UICC holding devices

NOKIA

SSO Security based on SIP Digest

- 3GPP is currently working on a Technical Report TR 33.914 (50% complete, status Nov 2010)
- This reports outline how to utilize SIP Digest for Single Sign On, in particular with OpenID
- It builds upon TR 33.924 (OpenID-GBA Interwrking)
- Targets non-UICC holding devices
- Status: Introduction, Scope, Architecture, Functinal SSO description and two solutions are included
- Technical details and alignment of

NOKIA

Now Study Item on SSO

- SA3 agreed in November on a new study item, which will contain
  - GBA light version, reduced version of GBA for single sign on purpose (note that GBA is a generic enabler and when used in a very particular context, can be “boiled down”)
  - AKA re-usage without GBA, targeted for scenarios where the operator does not wish to deploy GBA and does not wish to outsource the OpenID server

NOKIA

Thanks