Tdoc S3-110127

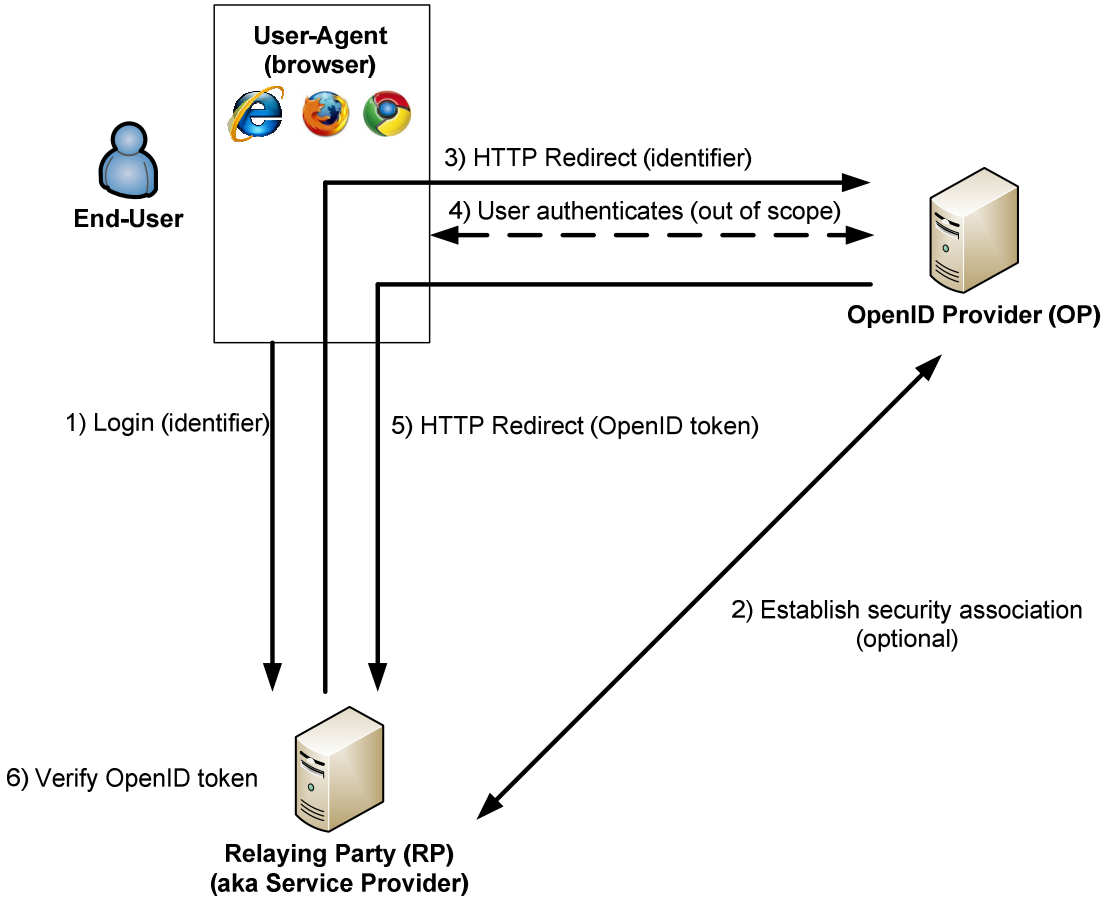
OPENID AND GBA INTERWORKING

USING A MINIMAL IMPLEMENTATION

Source: Ericsson, ST-Ericsson, Rogers Wireless
Agenda item: 8.5 Study on Security aspects of Integration of Single Sign-On (SSO) frameworks with 3GPP networks

3GPP TSG-SA3 (Security)
SA3#62, 24-28 January; Ljubljana, Slovenia

OPEN ID – QUICK RECAP



Note that the user authentication (step 4) is not specified by OpenID. In OpenID-GBA interworking, OP assumes the role of a NAF and the user authenticates using HTTP Digest with B-TID as username and Ks_NAF as password.

MOTIVATION

Standards

- GBA is standardized and ready for deployment.
- GBA provides strong authentication.
- Interworking of GBA and OpenId is described in TR 33.924.

However

- The SSO business case may not on its own be strong enough to motivate deployment of a full-fledged BSF.

Optimization

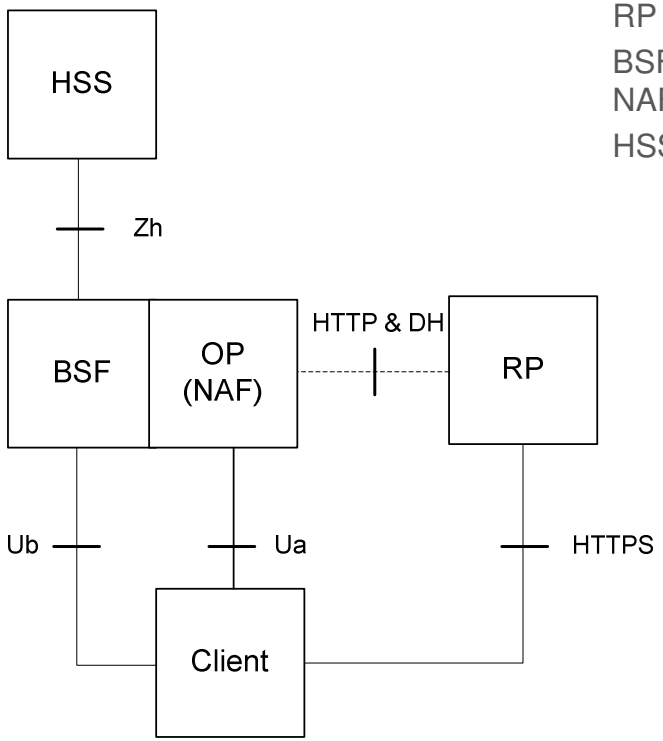
- What does a minimal BSF (BSF-lite) look like assuming it should only support GBA and OpenId interworking
- Migration from BSF-lite to a full BSF should be possible without changes to deployed clients.

DESIGN GOALS

- A simple migration path to use of full-fledged GBA.
- Aim for simplicity: Keep only the core BSF functionality, remove the rest.
- The solution should not require any BSF database
- The Client and RP (Relying Party) should follow TR 33.924

ARCHITECTURE

OP OpenId provider
RP Relying Party (service provider)
BSF Bootstrapping Server Function
NAF Network Application Function
HSS Home Subscriber Server



The signalling is exactly as in 3GPP 33.924 Section 4.4.1 except that the interface Zn (between BSF and OP) has been replaced with an internal API.

BSF IMPLEMENTATION

- Simplification 1: Make the BSF OpenID specific
  - We only need GUSS to distinguish clients supporting GBA_U and GBA_ME
  - Key derivation is simplified as we only need to derive a single Ks_NAF (for the OpenID server)
  - The BSF fetches the AV from HSS/HLR, authenticates the client using HTTP Digest AKA, and only keeps the triple (IMSI, B-TID, Ks_NAF) momentarily
- Simplification 2: Co-locate the BSF and OP
  - The interface Zn can be replaced with an internal API
  - Two DNS entries mapping to the same server IP is needed
- Simplification 3: The bootstrapping information is pushed from the BSF to the OP (=> no BSF database)
  - After authenticating the client, the BSF calls the function updateUser(IMSI, B-TID, Ks_NAF) which updates the client's password in the OP database.

WHAT CHANGES NEED TO BE MADE TO THE OP

- Already today each user has its own record or row in the OP database:

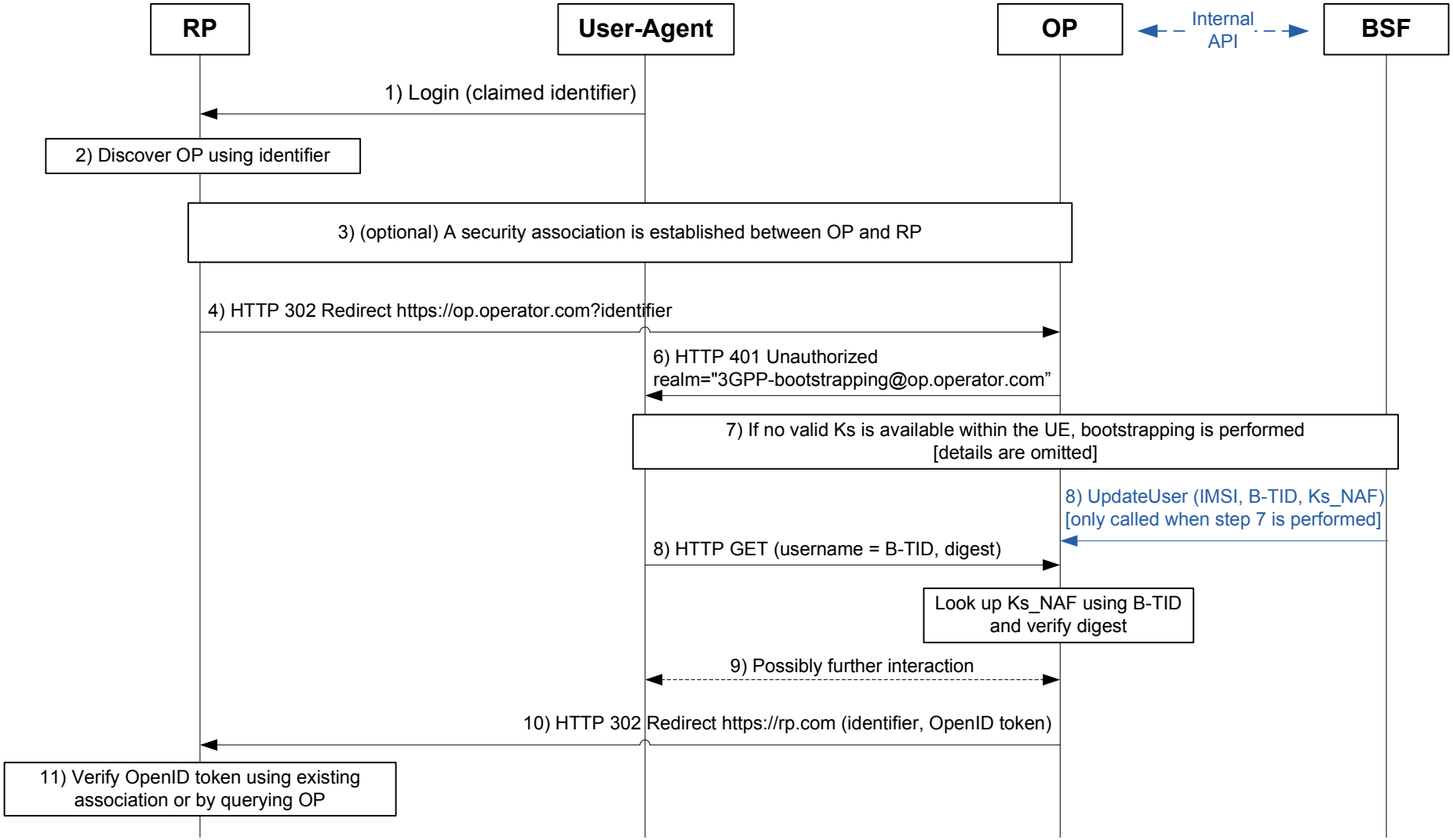
OpenId username	OpenId password	Other…

- What we need to do is basically extend the row with two extra columns:

OpenId username	OpenId password	IMSI	B-TID	Other…

- When the BSF calls updateUser(IMSI, B-TID, Ks_NAF) the following happens:
  - The row with a matching IMSI is located
  - Ks_NAF is inserted in the OpenID password column
  - B-TID is inserted in the B-TID column
- The OP authenticates the client according to 3GPP TS 24.109 Annex B *Signalling flows for HTTP Digest Authentication with bootstrapped security association* with one difference: the OP does not interact with BSF since it already has the latest (B-TID, Ks_NAF) pair.

SIGNALLING (Differences to TR 33.924 are marked blue)



CONCLUSION

- Combination OpenID and GBA offers several advantages, such as
  - High adoption of OpenId by service providers
  - High security, GBA based user authentication
  - Seamless user-experience
- Complexity of the BSF is seen a problem
- BSF-lite offers
  - Minimum of implementation work
  - No BSF database needed
  - Migration path to full version of GBA

ERICSSON