Mobile Provided Identity Authentication on the Web

by

Jonas Högberg, Ericsson

for

W3C's WS on Identity in the Browser

24-5th May '11

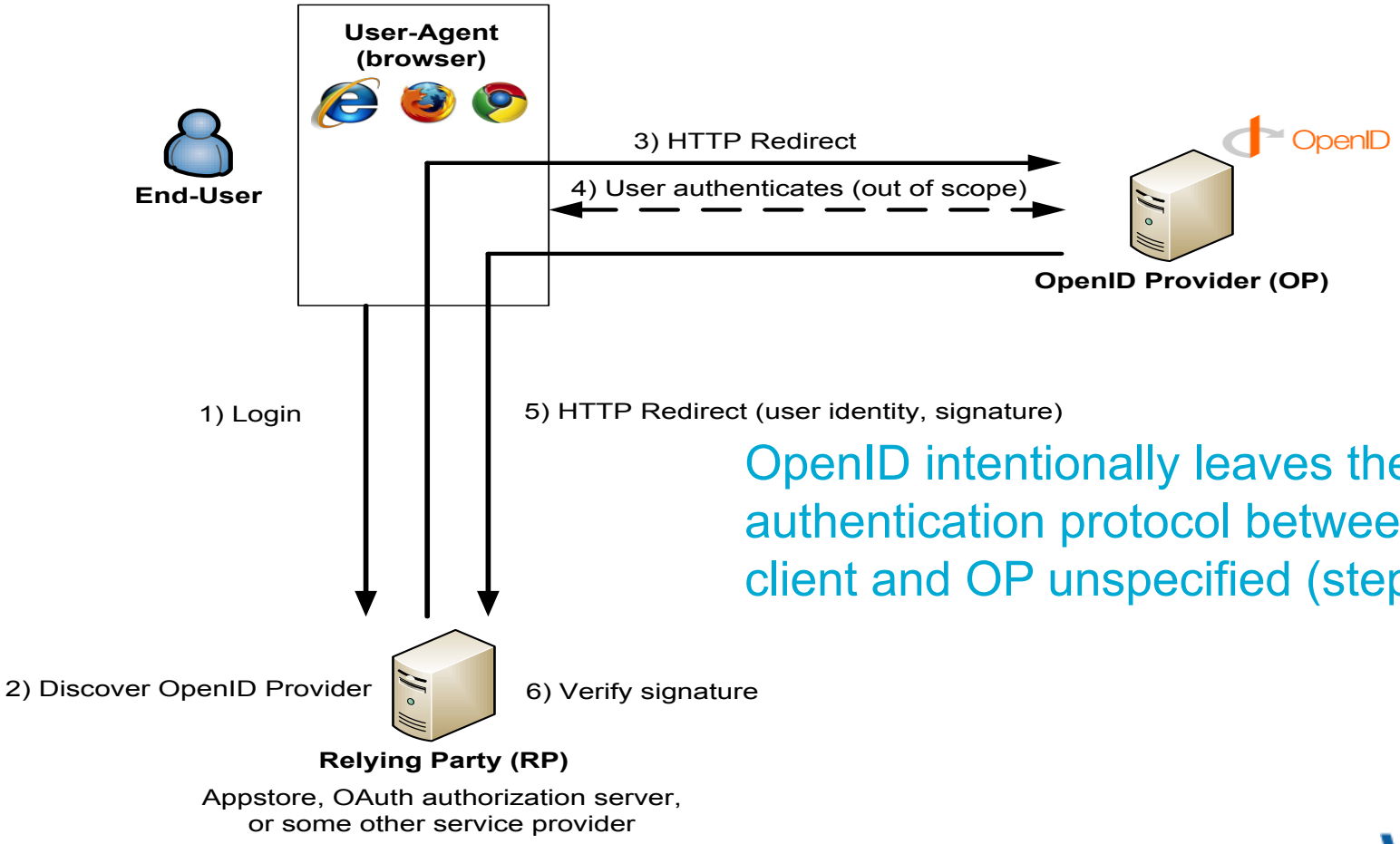
Mountain View, CA, USA

Mobile Provided Identity Authentication on the Web

- SSO with OpenID
  - OpenID is becoming the framework of choice for Identity Management in web-based services. Many well-known service providers support OpenID.
  - OpenID is therefore of interest to telecoms operators enabling them to offer Single Sign-On (SSO) to their users for a wide range of applications.
  - Operators are particularly interested in leveraging their subscriber databases and SIM credentials (i.e. GBA) for providing OpenID-based SSO to their users.

Mobile Provided Identity Authentication on the Web

› OpenID – Quick Recap



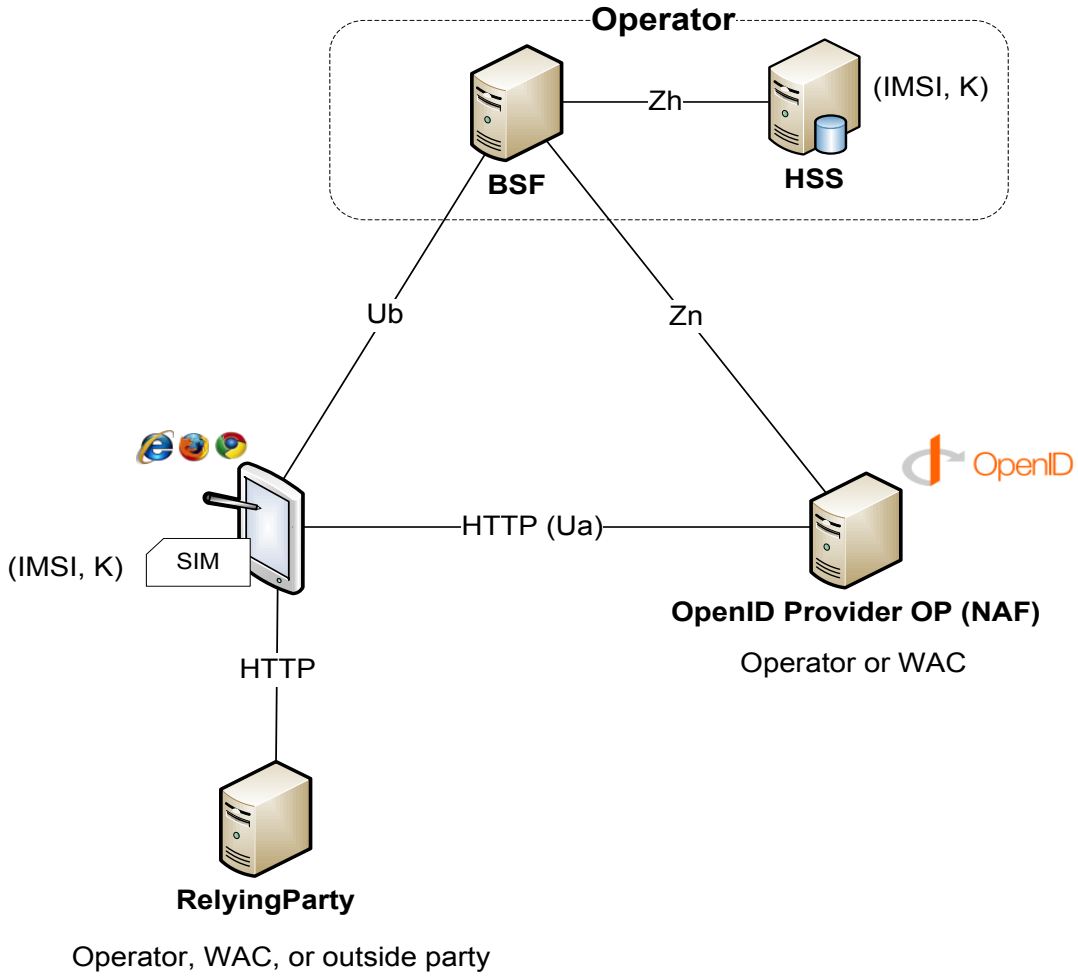
OpenID intentionally leaves the authentication protocol between client and OP unspecified (step 4).

Mobile Provided Identity Authentication on the Web

- OpenID and GBA Inter-working
  - OpenID intentionally leaves the authentication protocol between client and the OpenID Provider OP unspecified.
  - Possible to use GBA (Generic Bootstrapping Architecture) for client authentication
  - The inter-working of OpenID and GBA is specified in 3GPP TS 33.924
  - Basically, OP assumes the role of a NAF and the client authenticates using HTTP Digest with B-TID as username and Ks_NAF as password

Mobile Provided Identity Authentication on the Web

› Combined Architecture of OpenID and GBA



GBA

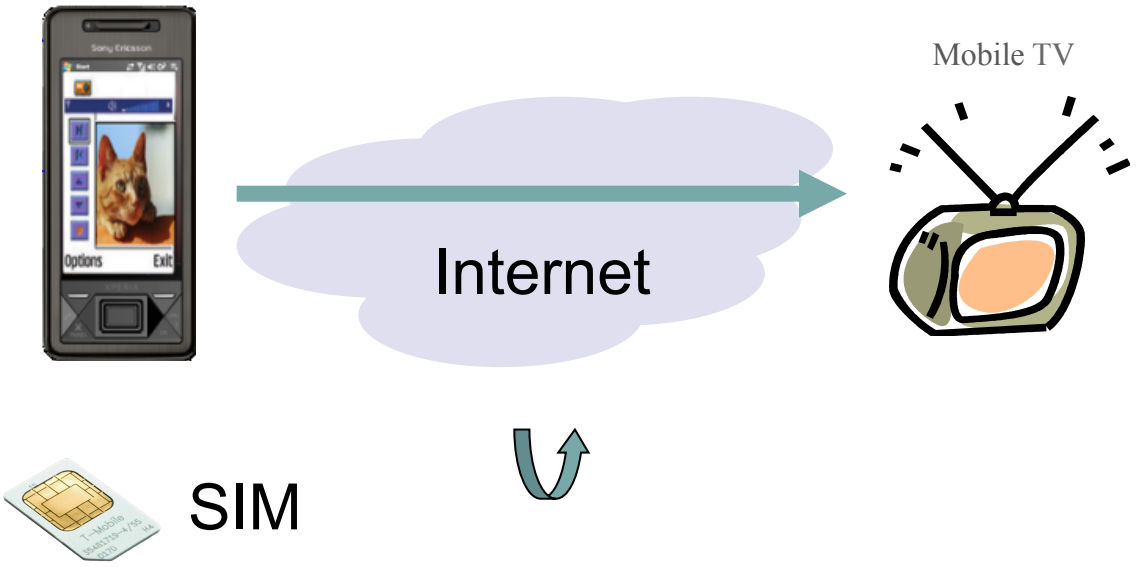
OpenID

Mobile Provided Identity Authentication on the Web

- Benefits
  - OpenID serves as a bridge between the Telco world (AKA, GBA, Diameter, etc) and the web world
  - Easy for the service provider (relying party) to integrate with the OpenID provider
  - The combination with GBA gives high security and seamless user experience
  - Based on industry standards:
    - GBA specified in 3GPP TS 33.220
    - GBA and OpenID inter-working specified in 3GPP TS 33.924
    - OpenID specified by OpenID Foundation (OIDF)
  - The service provider could be the Operator, WAC, or perhaps most interesting, an outside party

Mobile Provided Identity Authentication on the Web

› OpenID and GBA inter-working UC to logon to a service that is not provided by the operator/carrier.



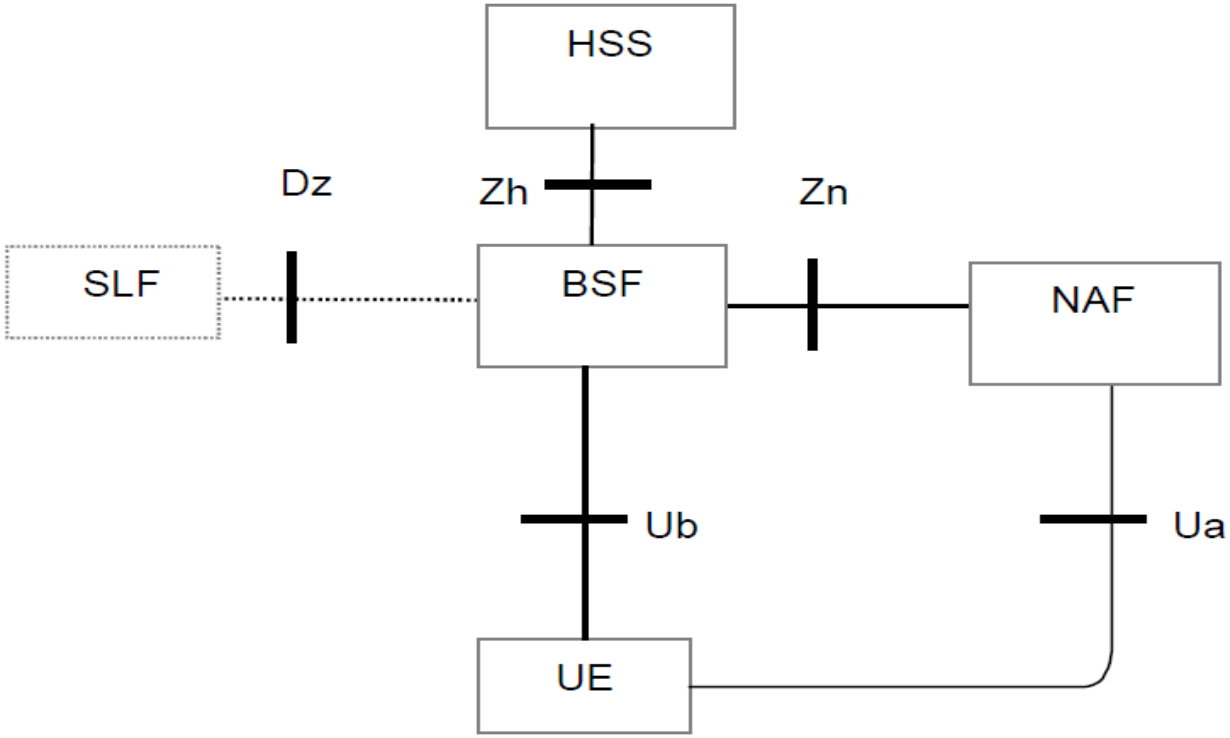
Mobile Provided Identity Authentication on the Web

- Open Issues:
  - The browser must be GBA enabled: how can we add this functionality? Plug-in? Passing of cookies?
  - How does the Relying Party (i.e. service provider) discover the OpenID Provider?
    - If the OpenID provider is hosted by the Operator:
      - Use extra HTTP header with an operator ID (MNC + MCC)
      - User selects his operator from a list
      - User enters the URL of the OpenID provider
  - Terminal support for GBA

ERICSSON

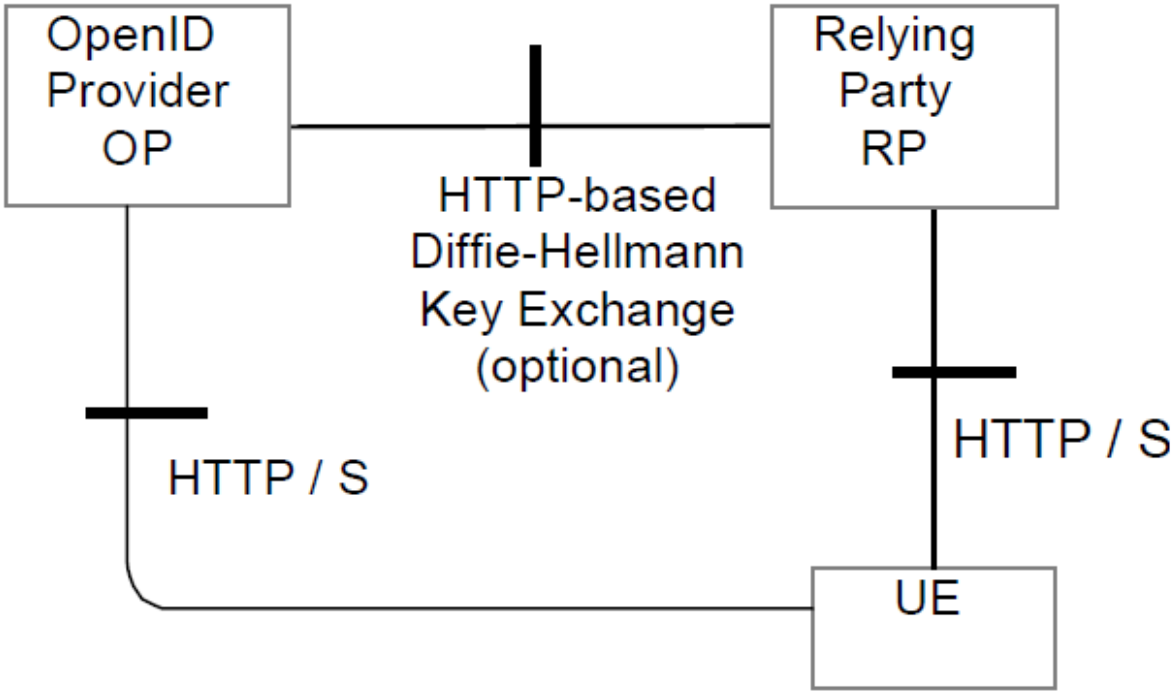
Mobile Provided Identity Authentication on the Web

› Simple Network Architecture for GBA



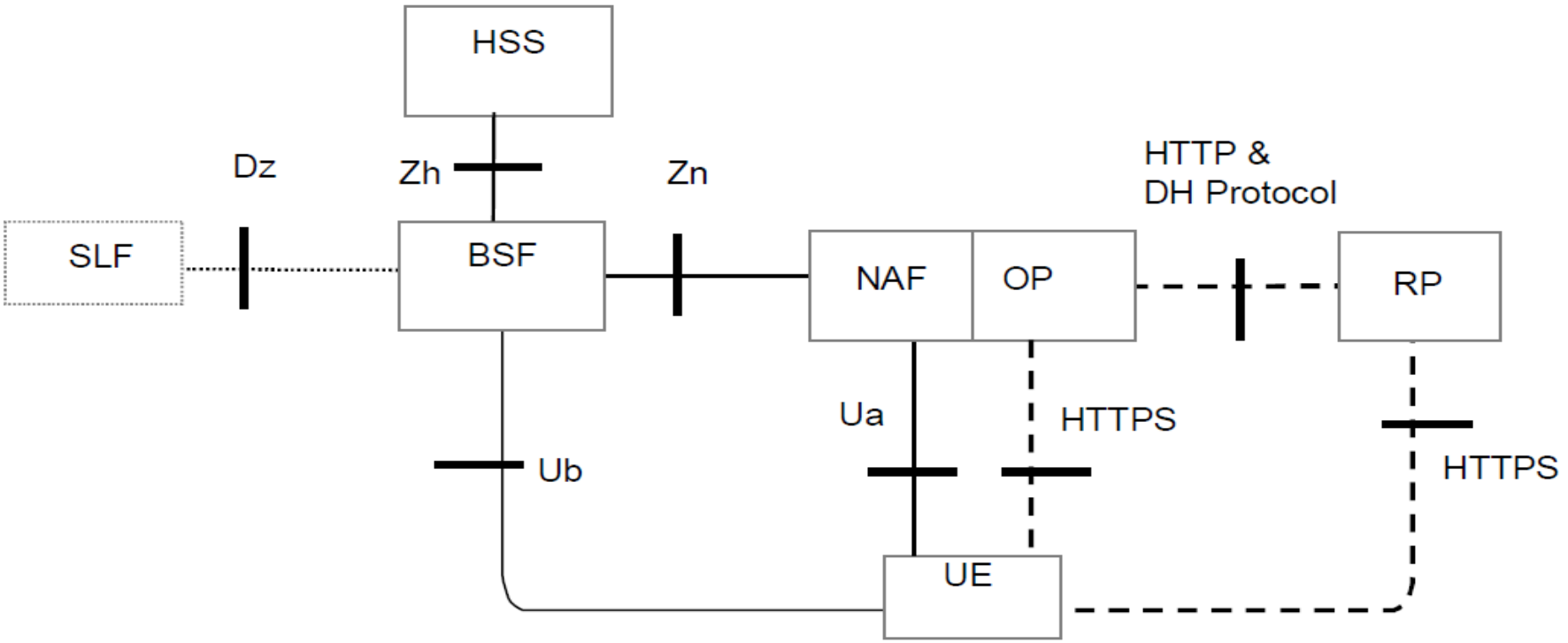
Mobile Provided Identity Authentication on the Web

› Simple OpenID Network Architecture



Mobile Provided Identity Authentication on the Web

› Combined OpenID and GBA Network Architecture



Mobile Provided Identity Authentication on the Web

› Signaling: