

Federation Options for the European eID Interoperability Framework



Dr. Bud P. Bruegger

Comune di Grosseto (Italy)

Context



- | **Manchester Ministerial Declaration (Nov 2005)**
 - | **IOP by 2010**
 - | **Full autonomy of MS in choice of eID technology**
 - | **Strong emphasis on privacy protection**
- | **Scope: cross-border eGov Services**
 - | **Excluded from mandate: **natl. eGov** & **private sector services****
- | **Decision: Federated** in a political sense
- | **Requires an IOP Framework that interfaces to national eID solutions**
- | **Part of *Common Specifications* now IDABC – later LSP**

IDABC eIDM Interoperability Workshop



- | **May 10, Brussels**
- | **Organized by Siemens** (contractor for technical part)
- | **Three main contenders for an IOP Framework:**
 - | **Liberty Alliance (SAML 2.0, Guide)** [Sun, OASIS, Guide]
 - | **WS-*/Cardspace** [Siemens]
 - | **TLS-Federation** [Bud]
- | **Missing:**
 - | **Meta-Framework Approach**

A closer look at Solution:

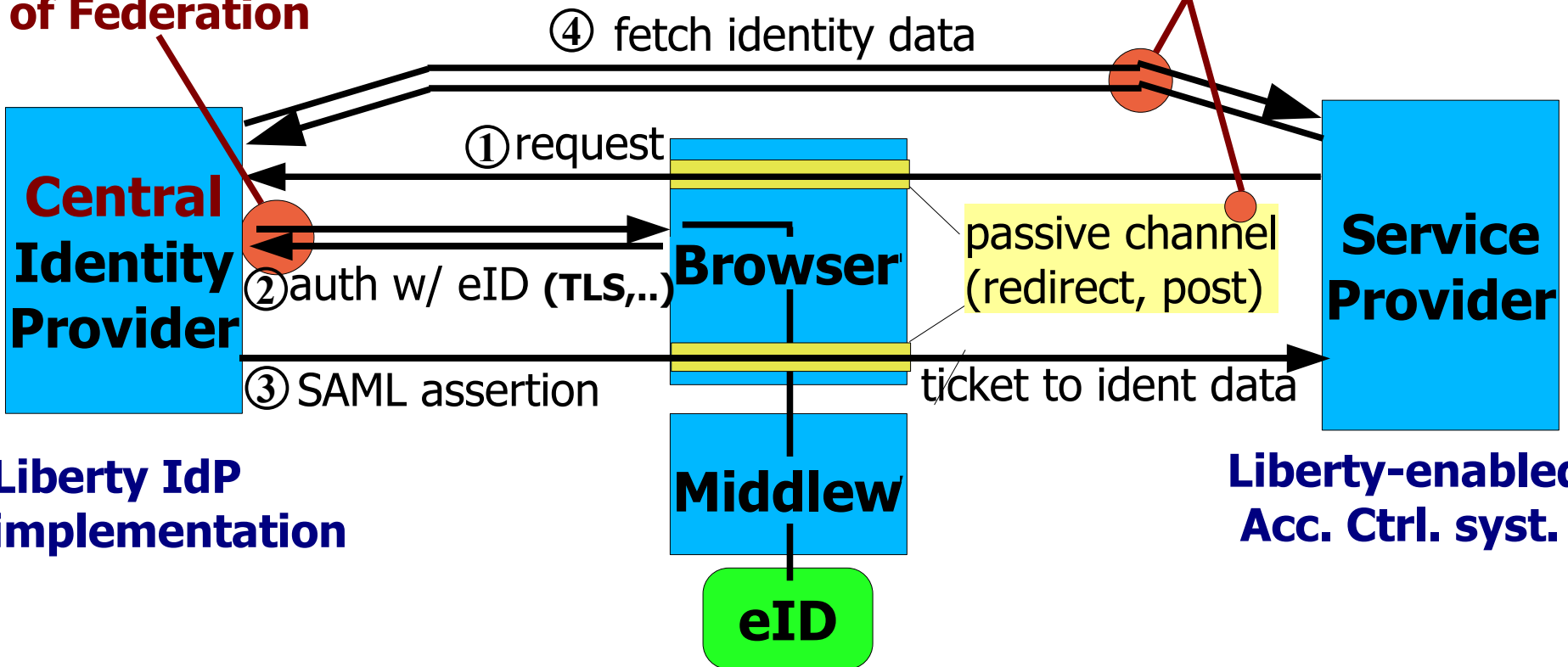


- **How do they work?**
- **How user-centric are they?**
- **Where is the “Point of Federation”**
 - **interface to national eID solution**
- **What is required?**
 - **From Service Provider**
 - **From user**
 - **From Government/Authority**

Liberty Alliance ID FF

Central Point of Federation

not user-centric



Liberty Alliance

Requirements



- | **all cross-border Service Providers:**
 - | **Liberty-enabled Access Control System**
- | **Users:**
 - | **Standard Browser**
 - | **Natl. middleware**
- | **All Governments/Authorities:**
 - | **Liberty Alliance IdP with:**
 - | **Authentication for natl. eIDs**

WS-* / Cardspace

History

- **Microsoft Passport fails to be accepted**
- **Kim Cameron:**
 - **Laws of identity**
 - **Concepts of user-centric and meta-system**
- **open, collaborative, inclusive, neutral** (community)
- **Products: WS-* / Cardspace**
- **Comes soon on majority of desktops: XP & Vista**
- **Higgins is open source clone of Cardspace**

WS-* -- Cardspace/Higgins

Central Point of Federation

Central Identity Provider

② auth w/ eID (TLS,...)
③ WS-* claim

Browser

① request

③ WS-* claim

Identity Agent

Cardspace Higgins

Middleware

eID

Service Provider

WS-*
-enabled
Acc. Ctrl. syst.

User-centric:
selection,
consent,
control

WS-* IdP
impl.
(Secure Token
Service)

WS-*

Requirements

- | **all cross-border Service Providers:**
 - | **WS-*-enabled Access Control System**
- | **User:**
 - | **Standard Browser**
 - | **Identity Agent**
 - **Cardspace: XP, Vista**
 - **Higgins: other platforms (open source)**
 - | **Natl. middleware**
- | **All Governments/Authorities:**
 - | **WS-* IdP (Secure Token Service) with:**
 - | **Authentication for natl. eIDs**

TLS-Federation

Extension of Open Source eID IOP demonstrator

Nothing new / no new protocols

Innovative use of existing standards/techn.

Existing, mature and stable IETF Standards

Ubiquitous Technology (X.509, Apache, standard Browser functionality)

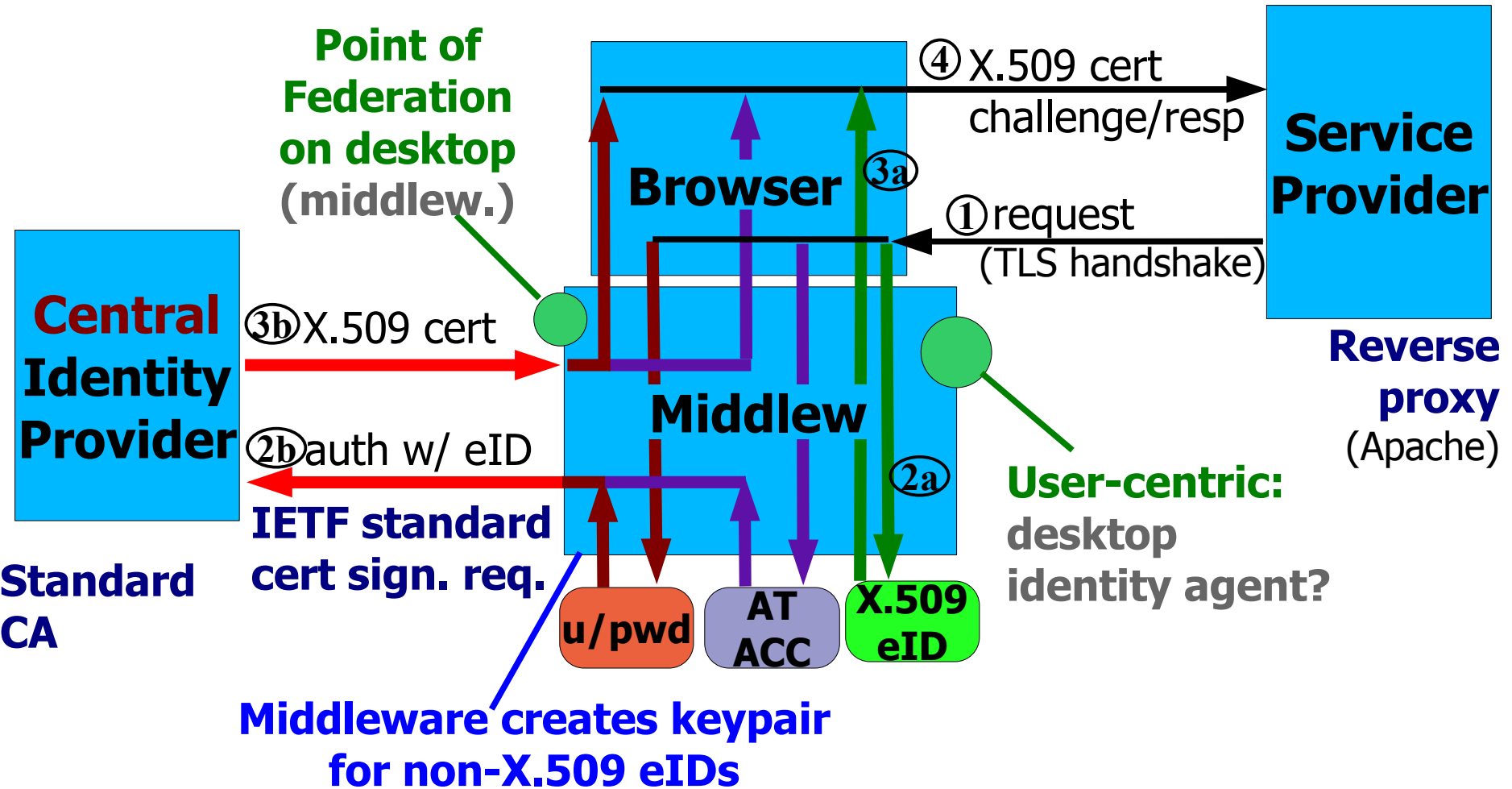
Middleware interfaces to natl. eID techn.

- Standard for X.509 eIDs (smartcard, file sys)**

- Non-standard for non-X.509 eIDs**

- IdP to translate natl. credential to X.509 cert**

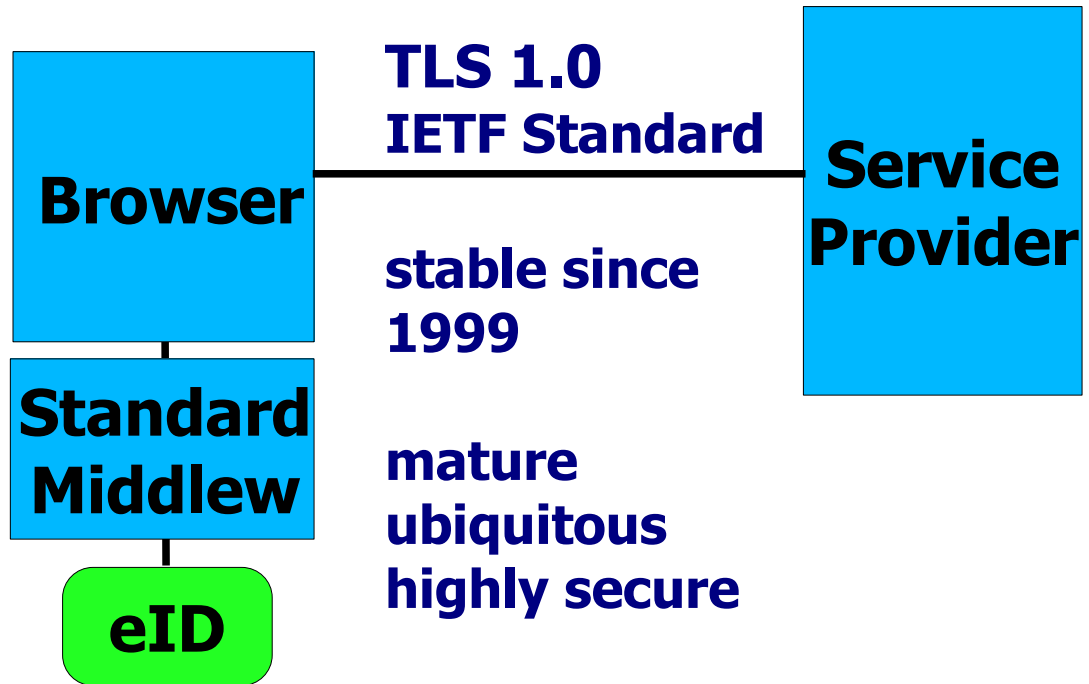
TLS-Federation



TLS-Federation

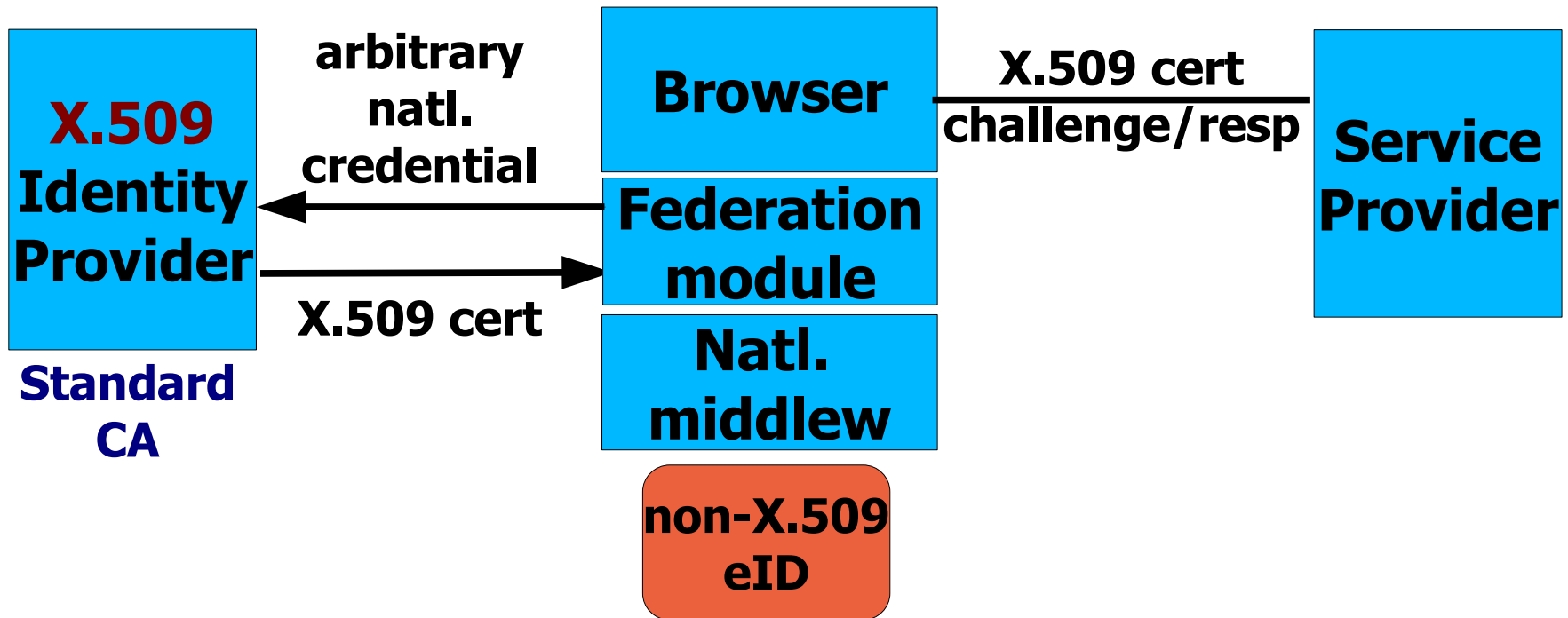
X.509 eID Country

- **No additional infrastructure**
- **80% of MSs participate at no additional cost**
- **Framework as secure as TLS, not weakest link in security chain**
- **Strong-auth-centric**



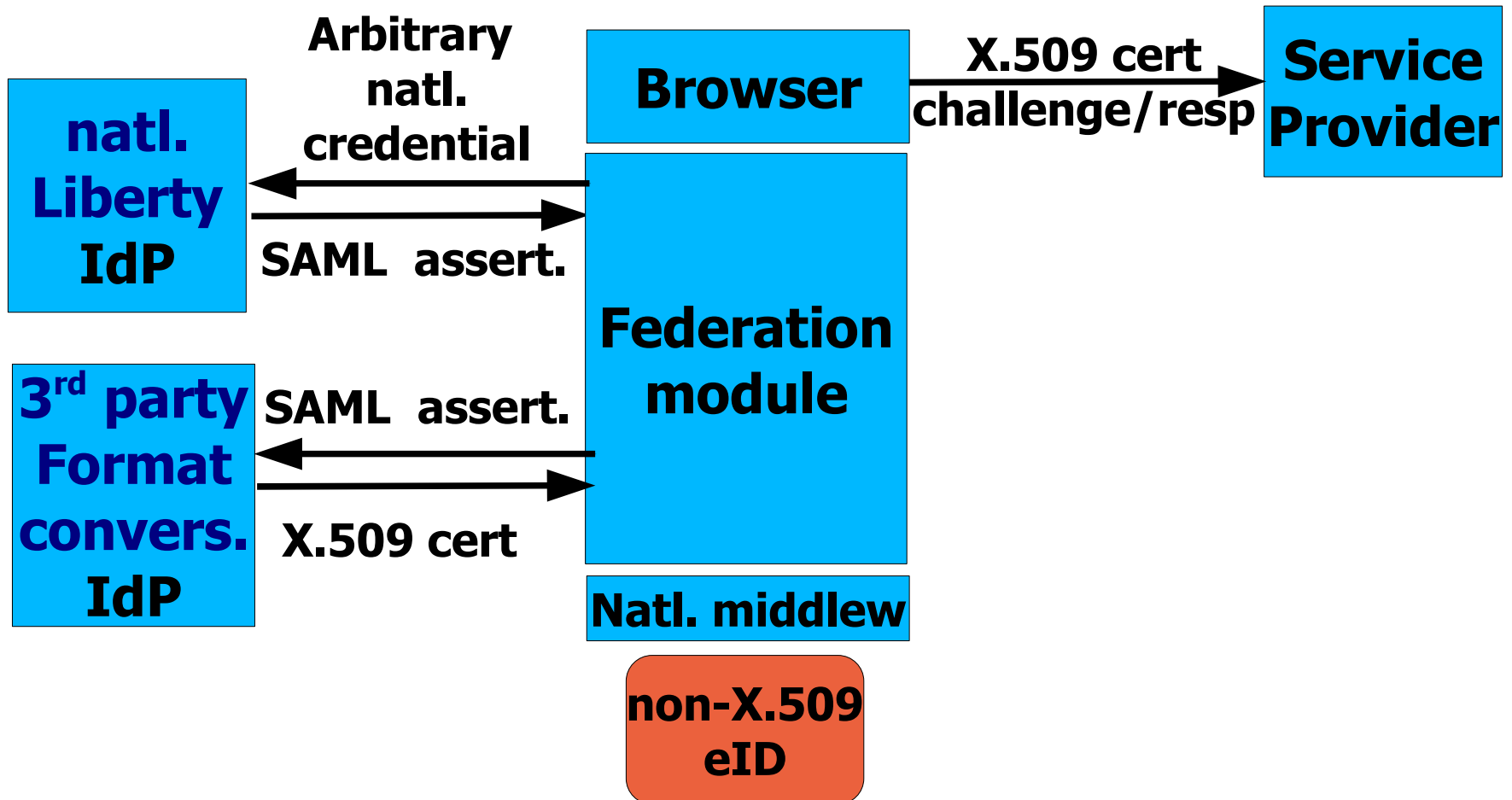
TLS-Federation

non-X.509 eID / X.509-IdP



TLS-Federation

non-X.509 eID / no X.509-IdP



TLS-Federation Requirements

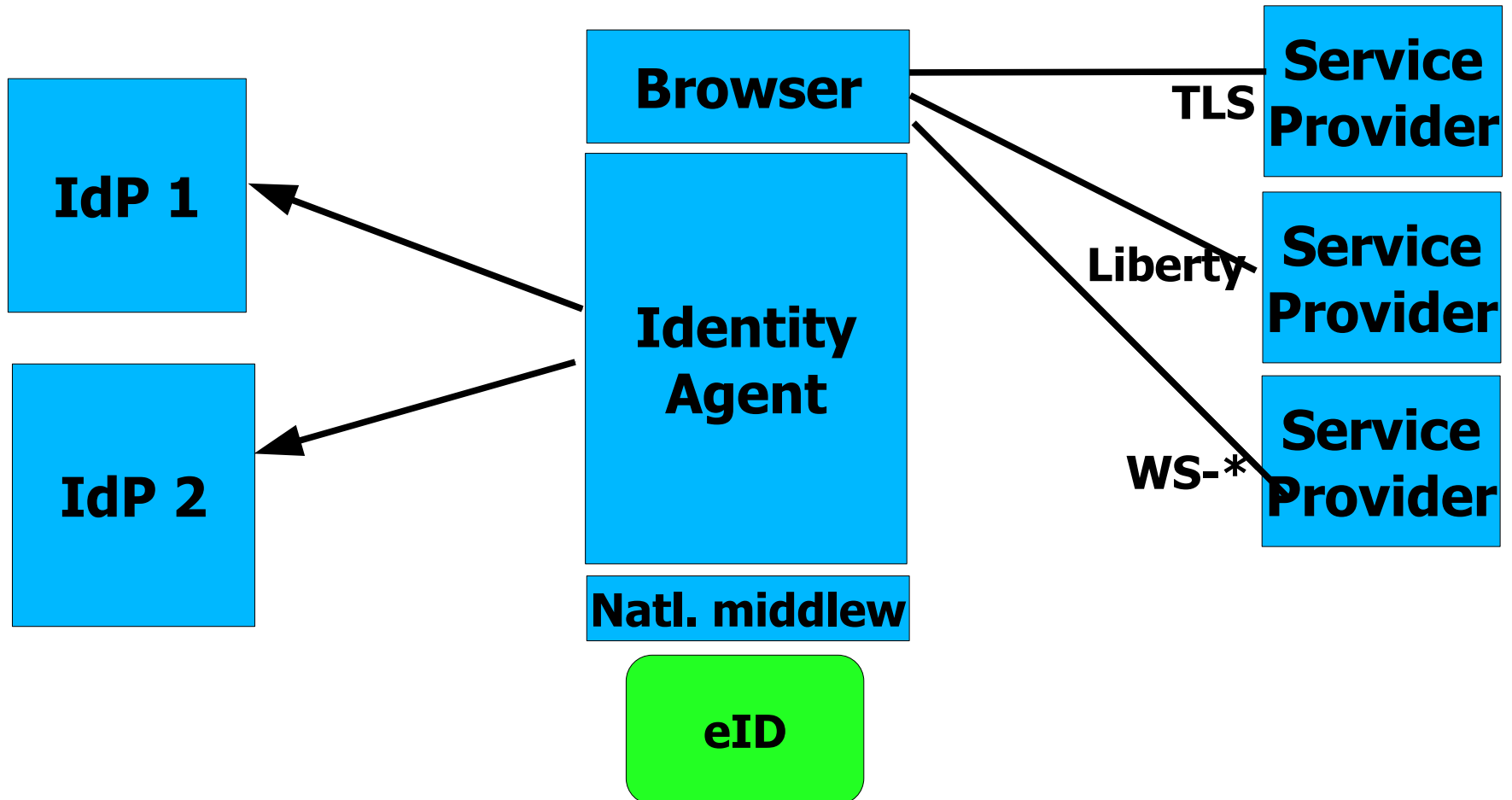
- | **all cross-border Service Providers:**
 - | **HTTP Server (w/ SSL) or Reverse Proxy**
 - Belgian Reverse Proxy (Apache)
 - Open Source IOP Demonstrator (Apache)
- | **User:**
 - | **Standard Browser**
 - | **Natl. middleware**
- | **All Governments/Authorities:**
 - | **X.509 MS: nothing (>80% ?)**
 - | **Others: natl. X.509 IdP (reuse sign. infra)**
or **3rd party Format Converting IdP**

Meta-Framework



- | **Many IDM protocols are supported:**
 - | **Liberty-Alliance**
 - | **WS-***
 - | **TLS**
 - | **OpenID**
- | **Service Provider chooses freely**
- | **User-Centric:**
 - | **Identity Agent interfaces with IdPs and SPs**

Meta-Framework



Meta-Framework Initiatives



- | **Open Source Identity Selector (OSIS) / Higgins**
 - | **Grosseto adding European eID requirements**
- | **Microsoft announced OpenID support in Cardspace**
- | **Microsoft Italy: TLS-Federation support in Cardspace**
 - | **Demonstrator for Porvoo 12?**
 - | **Italian Government Security Program?**
- | **SMILE FP7 proposal (funding)**

Conclusions



- | **Not only Liberty Alliance and WS-***
- | **TLS-Federation**
 - | **Unconventional use of existing stable IETF standards/techn.**
 - | **High security (workhorse of strong auth)**
 - | **Simple, in line with status quo, easy to replicate**
- | **Meta-Framework**
 - | **Free choice of Service Provider:**
 - Liberty Alliance, WS-*, TLS-Federation, OpenID, ...
 - | **Only politically feasible solution?**
 - | **A possible focus for Porvoo 12**

Thank You



Contact:

Bud P. Bruegger

<bud@comune.grosseto.it>