

eID Interoperability Scenarios

Bud P. Bruegger
Comune di Grosseto

- **Porvoo 11:**
 - **Federation Solutions on EC radar:**
 - Liberty Alliance
 - WS-*
 - TLS-Federation
 - **Missing: meta-system approach**
- **problem to solve insufficiently defined**
 - Access to services by citizens and businesses (Manchester Decl.)
 - also Back-office identity data exchange?

eID IOP: Who decides (1)

- **Gov (eIDs) have unique role:**
 - electronic identity only as secure as enrollment
 - gov's unique: population registers, background checks
 - Governments necessary to at least bootstrap any secure identity system
- **Identity Management decided by:**
 - **Computing Industry:** (user-centric=desktop -> MS)
general identity management seems disconnected from eID
- **IOP: we need all players to solve it**
- **Too little dialog betw. gov.and comput. ind.?**
 - Porvoo12: opportunity to better connect Gov and MS (desktop)

eID IOP: Who decides (2)

- **eIDs and technology are just enablers**
- **Autonomous (private sector) Service Providers decide what citizens will use**
 - **Citizens want a service, they don't care about technology**
 - Government services used infrequently
 - Private sector services (**banks**) used daily
 - Cross-border e-gov services are rare
 - A European service market place requires cross-border IOP
- **Is it possible to convince all SPs of a single solution? .. or ..**
- **Do we need a user-centric meta-system?**

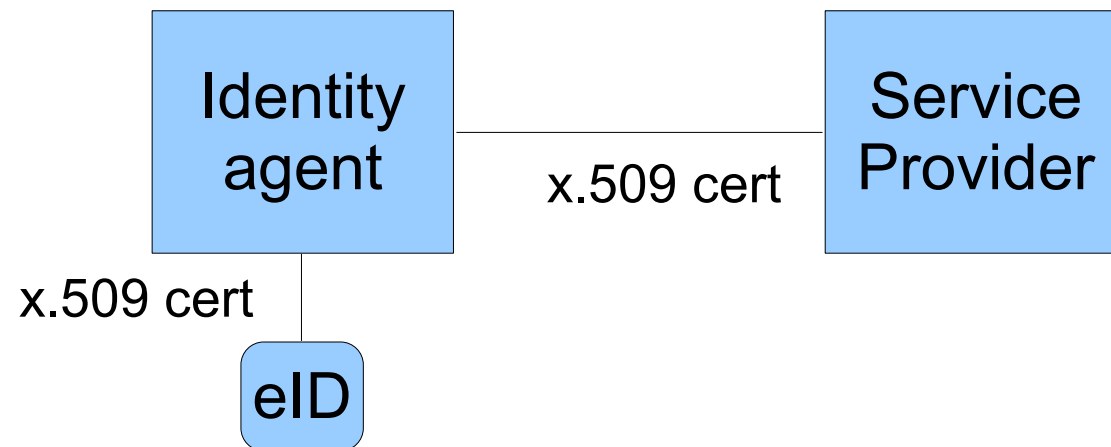
User-Centric Meta-System

- **Privacy requires User-Centric Approach**
 - User controls disclosure of personal data
- **Service Heterogeneity requires Meta-System**
 - User wants consistent experience/control, independent of:
 - The government's choice of eID technology
 - The Service Provider's choice of IDM technology
- **We need an intelligent identity agent (on the desktop)**
 - Interfaces to any eID
 - Interfaces to any SP
 - Intelligently uses IOP services (where necessary)
 - Gov. IdP, 3rd party IdP, trust management (bridge CA), ..
- **Can Cardspace/Higgins satisfy our needs?**

- **Scenarios that illustrate a user-centric meta-system approach**
- **Does not attempt to be complete**
- **Focus on TLS-Federation**

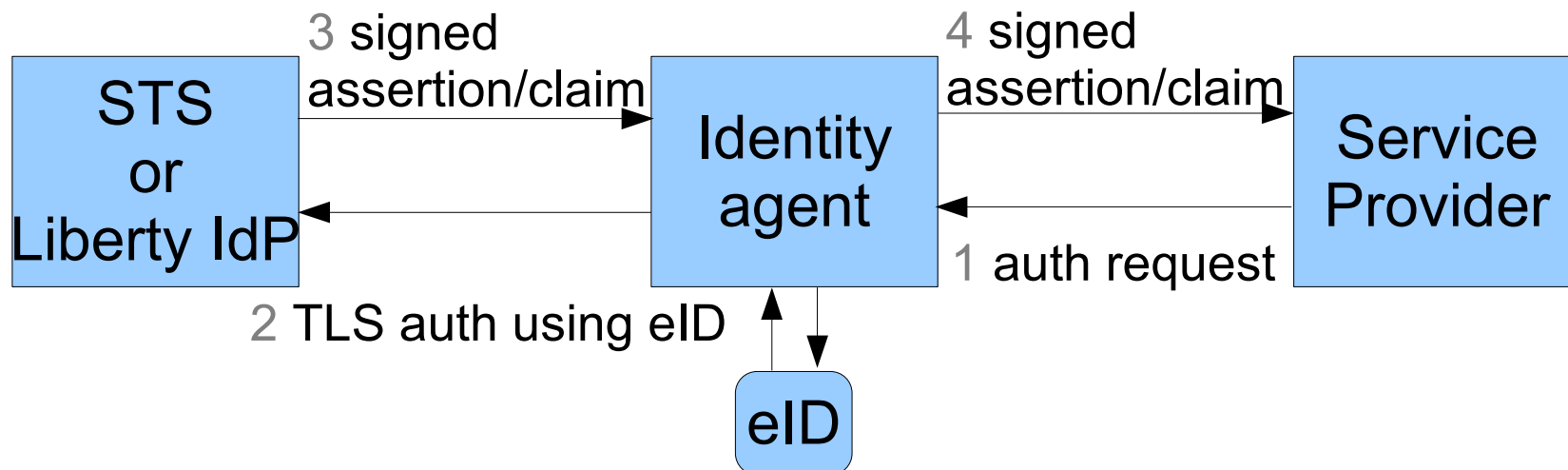
Most Common eID/SP: X.509 eID, TLS authentication

- eID has X.509 cert with unique ID
- SP uses TLS (SSL) e.g., Apache
- Identity agent creates direct link

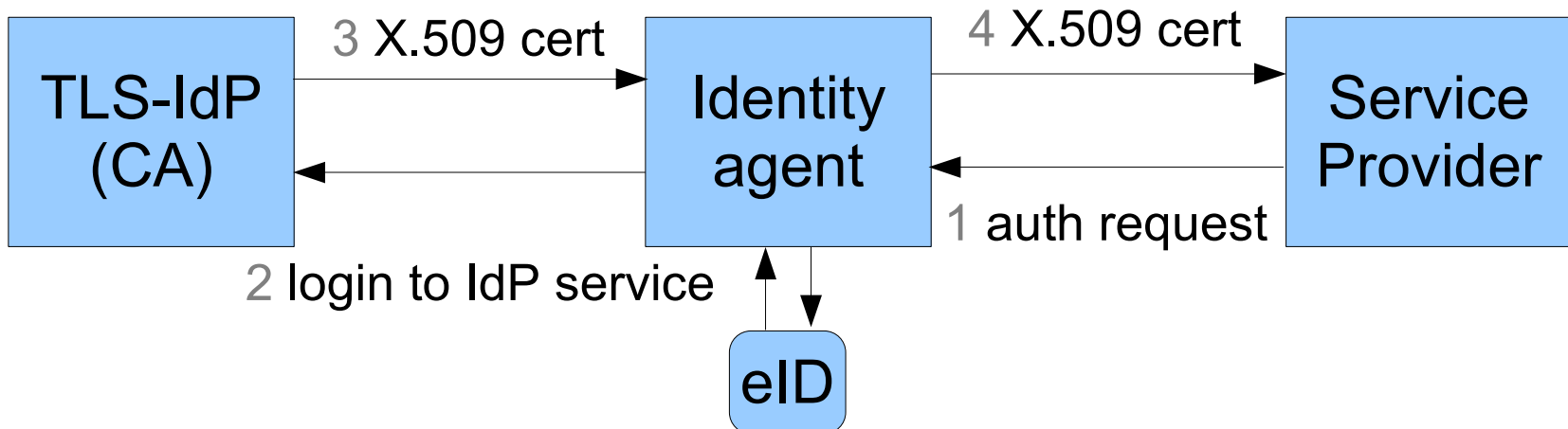


X.509 eID, WS-*/Liberty auth

- eID has X.509 cert with unique ID
- SP uses WS-* or Liberty
- **Identity agent uses IdP**

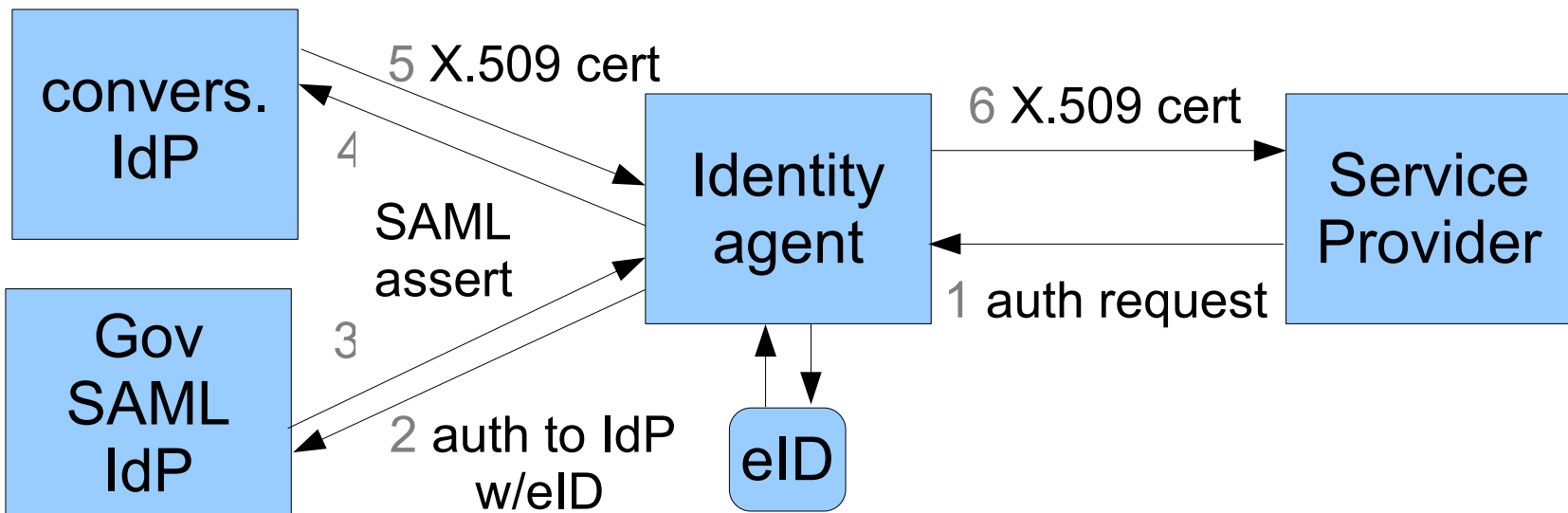


- **eID is username/password** (or any non-X.509 eID)
- **SP uses TLS**
- **Identity agent uses TLS-IdP** (= on-the-fly CA)



non-x.509 eID, TLS auth, SAML native IdP

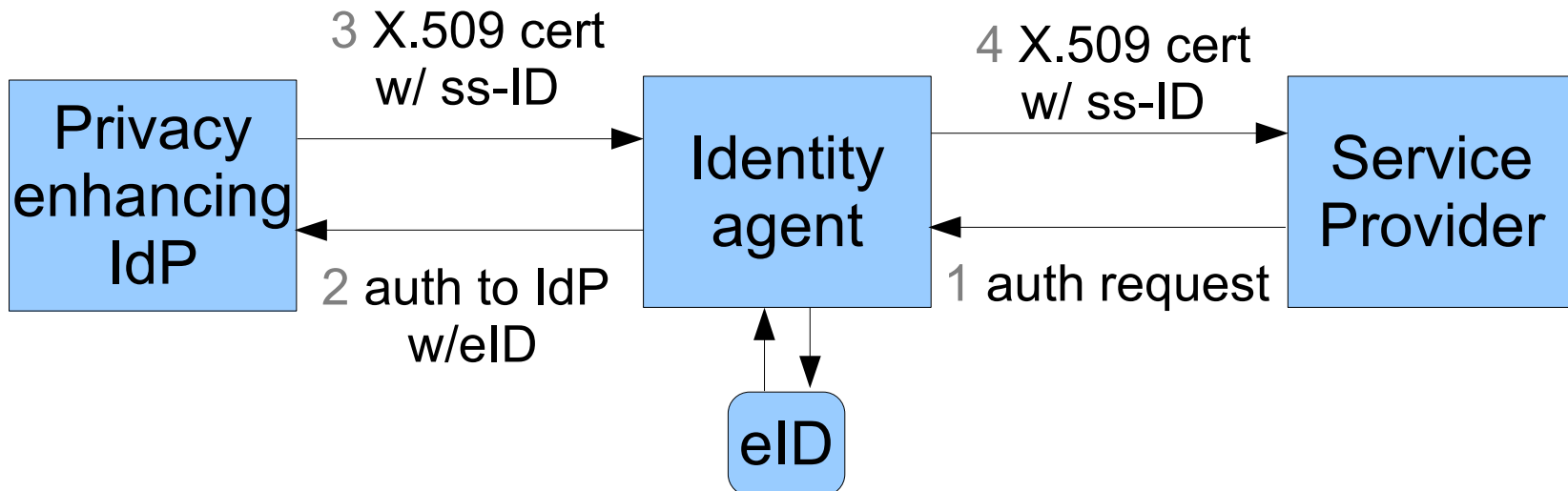
- **eID is non-x.509** (e.g., Austrian Citizen Card)
- **SP uses TLS**
- **Gov IdP uses SAML**
- **3rd Party format conversion IdP**



Privacy: Linkability

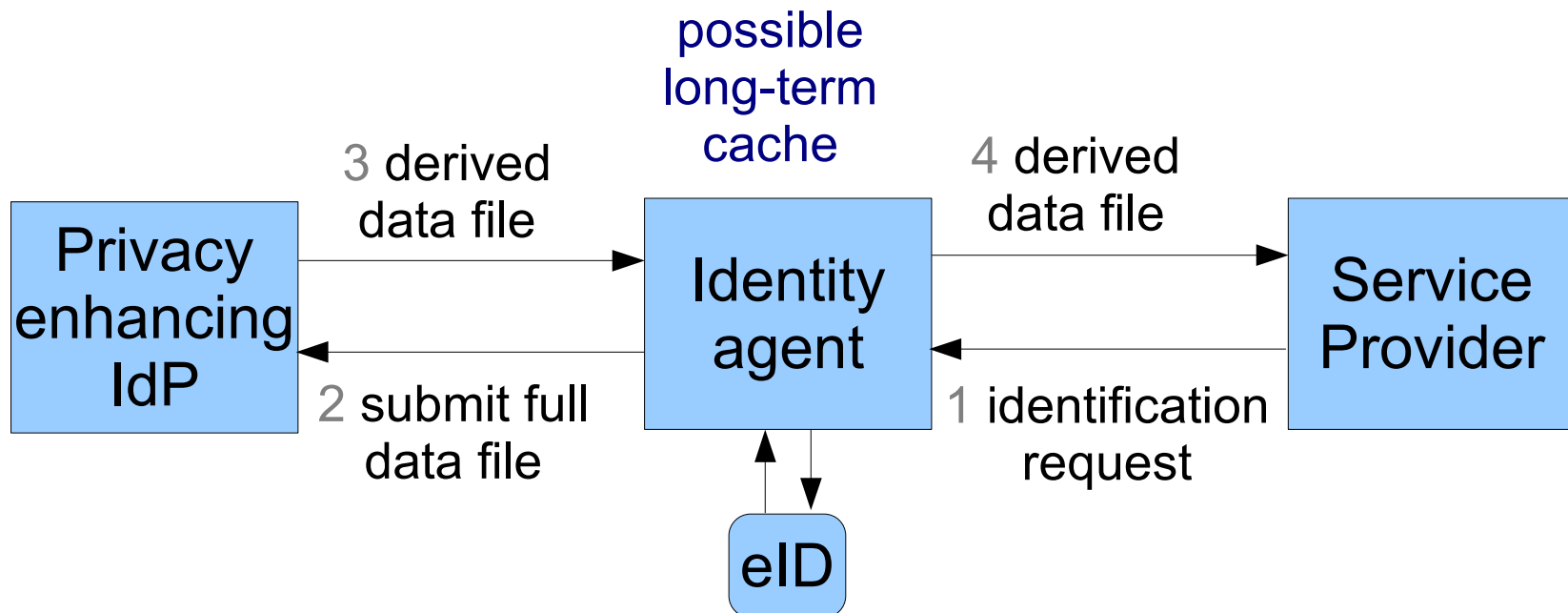
x.509 eID with unique identifier

- **When sector-specific identifiers are needed**
- **Same architecture**



Privacy: Minimal Disclosure eID with signed data file

- **Subset/derivation of pers. data under user control**
- **Same architecture**



- **We need a user-centric meta-system**
 - Impossible that all SPs agree
- **Govs (eIDs) need to work closely with desktop makers** **Porvoo12 as opportunity**
- **TLS-Federation needed to jump start IOP**
 - No need for additional gov infrastructure
- **Gradual addition of privacy-enhancement to existing eIDs is possible** (requires additional gov infra)
- **Focus of Discussion at Porvoo12:**
 - Kim Cameron, round table, ..