

# **The Road to European eID Interoperability**



## **Alternative Point of View on *Road Map* and *Common Specifications***

**Bud P. Bruegger**  
**Comune di Grosseto**  
**Italy**

# Outline

- | **Already agreed on choices?**
  - | **Federated**
  - | **Multi-level IDM**
  - | **Authentic sources**
- | **The Key Architectural Choices**
  - | **Federated centralization vs. decentralized**
- | **Requirements** compare alternatives
- | **Proposed Alternative “Federated” Arch.**
  - | **Strong authentication – centric**
  - | **Gateways to integrate other approaches**

# Agreed on choices ?

“Common choices already agreed between the MS for any eIDM system are that it must be:

- | (a) Federated
- | (b) Multilevel eIDM
- | (c) Relying on authentic sources
- | ...”

| **What exactly does this mean?**

| **Is this in line what we have been doing?**

# What is *Federated* ?

- ! **Every MS has full autonomy for its eIDM system**
  - ! **Political fact, Exception: *Common Specifications***
- ! **IOP framework needs to support all national choices**
  - **X.509 smartcard- or file-based eIDs** (FI, BE, EST, IT, Malta..)
  - **Non-X.509 eIDs with dynamic IDs by TTPs** (AT)
  - **username/password**
  - ! **Is preferential treatment of one legitimate:**
    - **Strong-authentication-centric framework?**
- ! **A technology: *SAML 2.0, Liberty Alliance ID-FF 1.2***
  - ! **Does anyone have SAML infrastructure?** (AT, ??)
  - ! **Technical choice *before* agreeing on requirements?**
  - ! **Technical doubts!** (next slides)

# **SAML/Liberty Alliance: usern./pwd technology**

- | **Standardization of Corporate Single Sign On**

- | ***Strong Authentication Expert Group*** Liberty Alliance

- | **Only since fall 2005**

- | **“A lot of work is being done in this space quickly, so check here often for updates on this very important strategic initiative”**

- | **Results?**

- | **Architecture is for username/password**

# **SAML/Liberty Alliance:**

## **security concerns**

### **Source:**

***Security and Privacy Considerations  
for the OASIS SAML V2.0***

### **Countermeasures:**

- **Max clock difference**
- **Set tightly and verify *notBefore, notOnOrAfter***
- **Set *OneTimeUse***
- **Use and verify *subjectLocality***
- **Verify that directly redirected**

**Complexity vs. Security?**

**Compare to TLS** (client-cert-auth, Reverse Proxy)

# **SAML/Liberty Alliance:** **really stable enough?**

- | **If successful, the EU IOP framework will connect:**
  - | **A VERY LARGE number of service providers**
  - | **From gov at all levels, private sector**
- | **Every modification requires upgrade of all service providers!**
- | **How stable is SAML/Liberty Alliance?**
  - | **SAML**
    - **1.0: Nov 2002**
    - **1.1: Sept 2003**
    - **2.0: March 2005**

## **Compare:**

- | **Stability of HTTP 1.1 and TLS 1.0**
- | **Transition from HTTP 1.0 to HTTP 1.1**

# Federated IDM technology: which ?

- | **At least three main standards**
  - | **Liberty Alliance** (SAML-based; Sun, IBM, HP, ...)
  - | **Shibboleth** (SAML-based; Internet 2, Universities)
  - | **WS-\*** (not SAML-based; Microsoft, ...)
- | **Is there a consensus?**

# Multilevel eIDM

## all equal ?

- **Multiple levels of security**
  - **Credential technology (password, .. ,smartcards)**
  - **Registration procedures**
- **Security Level determines Architectural Choices !!!**
  - **Lowest common denominator solution unsatisfactory**
  - **Architecture needs to be centered on strongest level**
  - **Unavoidable: preferential Treatment of some levels and thus credential types**

# ***Authentic Sources of identity data***

## **central DBs vs. citizen-controlled eID**

### **Definition eID:**

- The gov. provides its citizens with a means to remotely authenticate and identify themselves**

### **"authentic" Source: always Citizen (business)**

### **Additional central DBs ?**

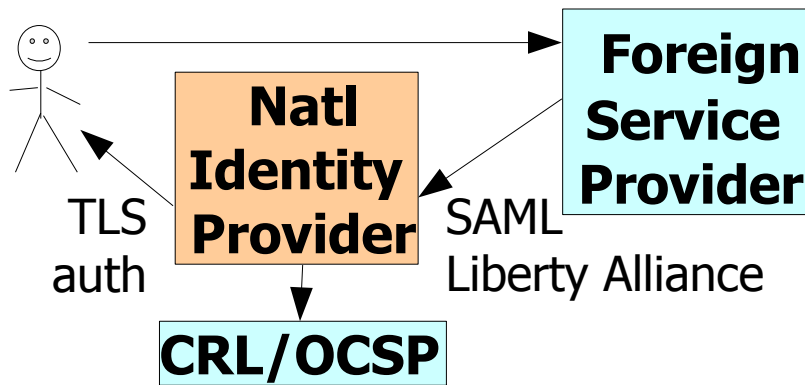
- Privacy: citizen authorizes data access**

- Feasibility: trust management between SPs and IPs impossible if private sector involved**

## ***Authentic sources compatible with our eIDs?***

# The key architectural choice

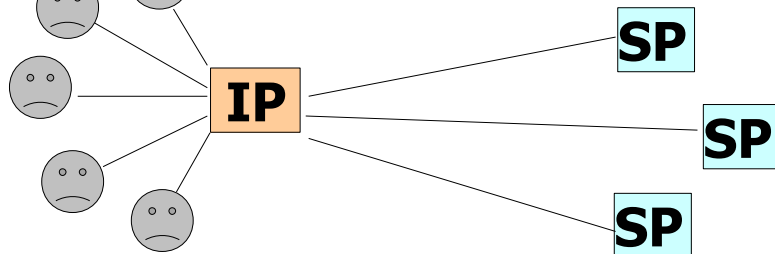
## Federated Centralization



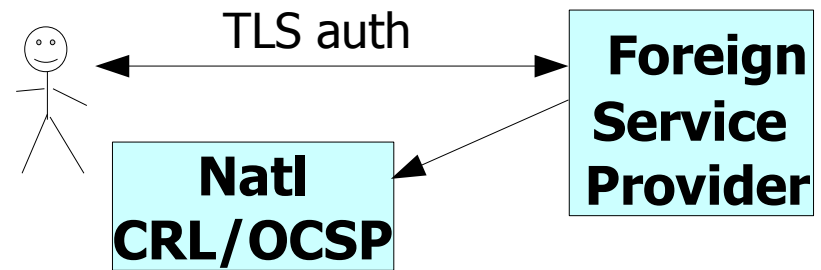
Citizen always needs natl. IP

Additional infrastructure

high-volume / h-availability

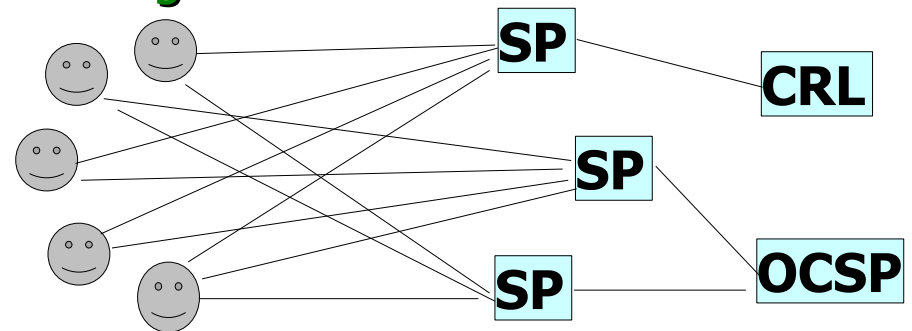


## Decentralized TLS



eID makes citizen (almost) autonomous

Existing natl infrastructure



# Requirements

## [1] Sustainability

- **EC funds large scale pilots (2008); objectives:**
  - **Critical mass of MS**
  - **Self-replicating and self-sustainable**
- **Requirements:**
  - **As simple as possible**
  - **Avoid unnecessary components/costs**
  - **Only existing national infrastructure if ever possible**
- **Conclusions:**
  - **TLS approach can do with existing infrastr. (90% of MS)**  
**X.509 and TLS are already ubiquitous technologies**
  - **Federated approach needs additional infrastr.**

# Requirements

## [2] Security

### Information Society:

- needs a leap from username/pwd to strong auth
- X.509/TLS has already been ubiquitous technology
- BUT Major impediment: cost of issuing credentials**
- eID roll-outs are removing this last impediment**

### Requirements:

- Security must be a high priority**
- Strong authentication must be a priority**

### Conclusions

- TLS more secure, strong-auth-oriented**
- Liberty less secure, username/password-oriented**

# Requirements

## [3] Privacy

- | **Privacy is a stated Priority**

- | **Privacy Risks:**

- | **Federated Architecture:**

- | **Central National Identity Provider:**

- | **Knows every access of every citizen to each service**

- | **TLS Architecture:**

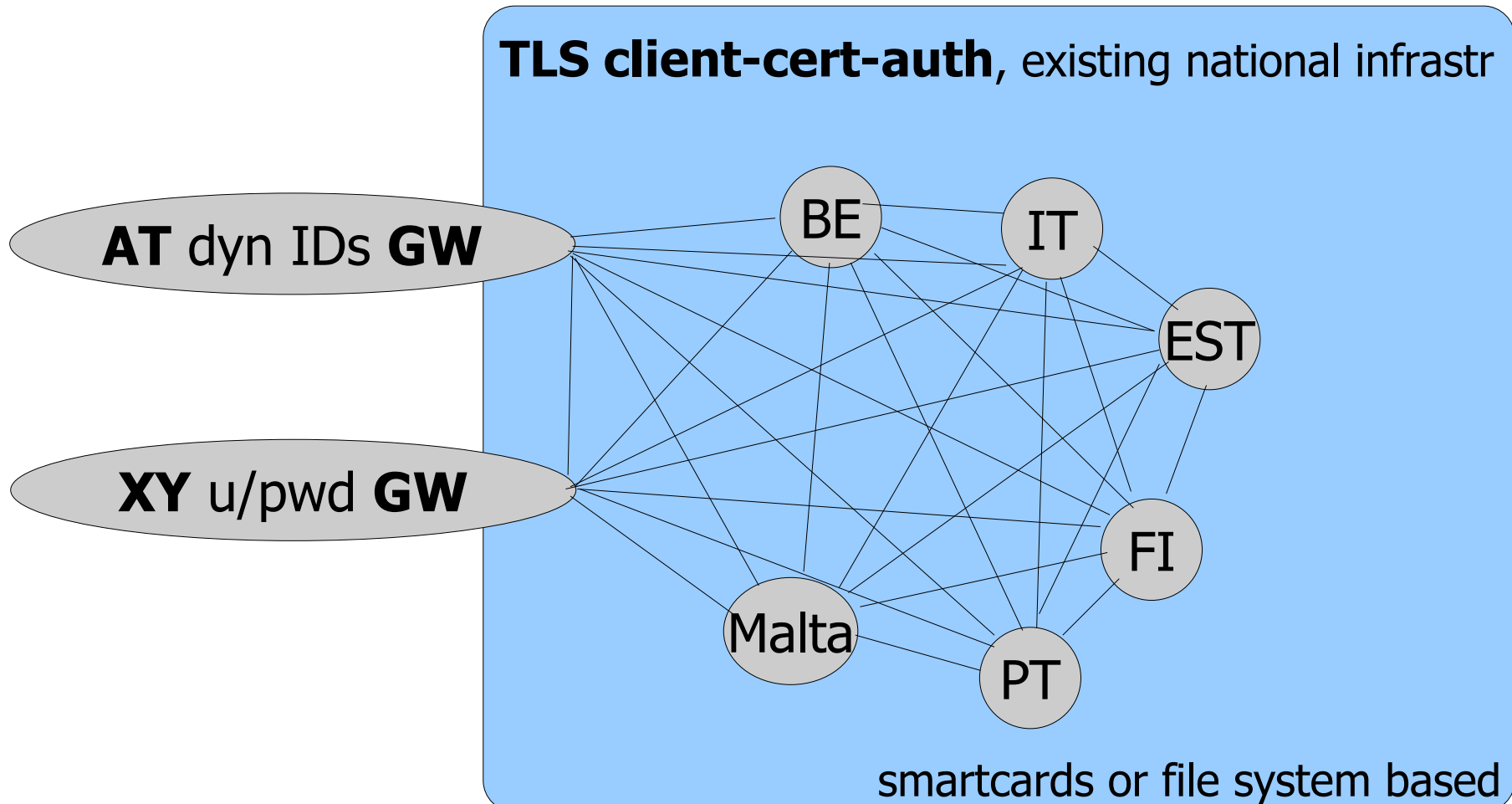
- | **OCSP: Similar, but maybe easier to control**

- | **CRLs: No central tacking possible**

- | **Conclusions:**

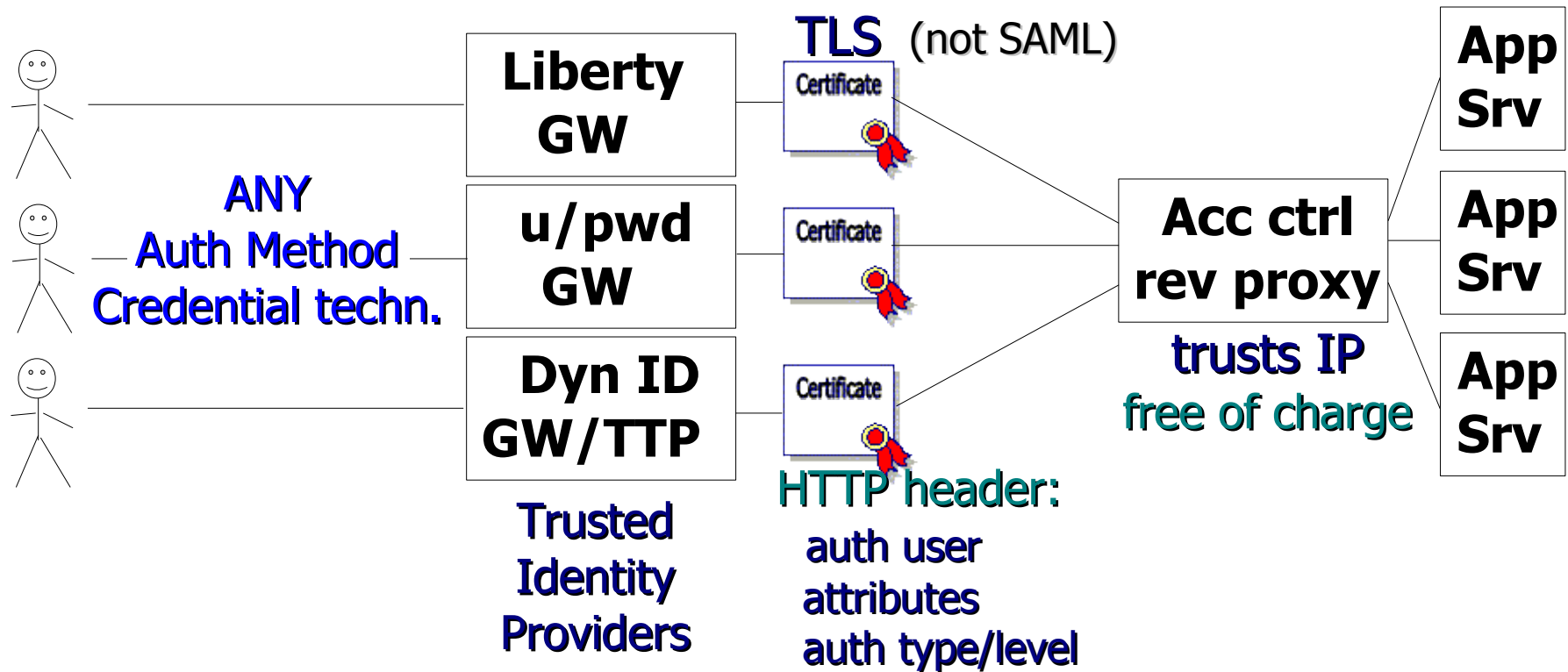
- | **TLS more privacy friendly in cross boarder setting?**

# Proposed IOP Framework



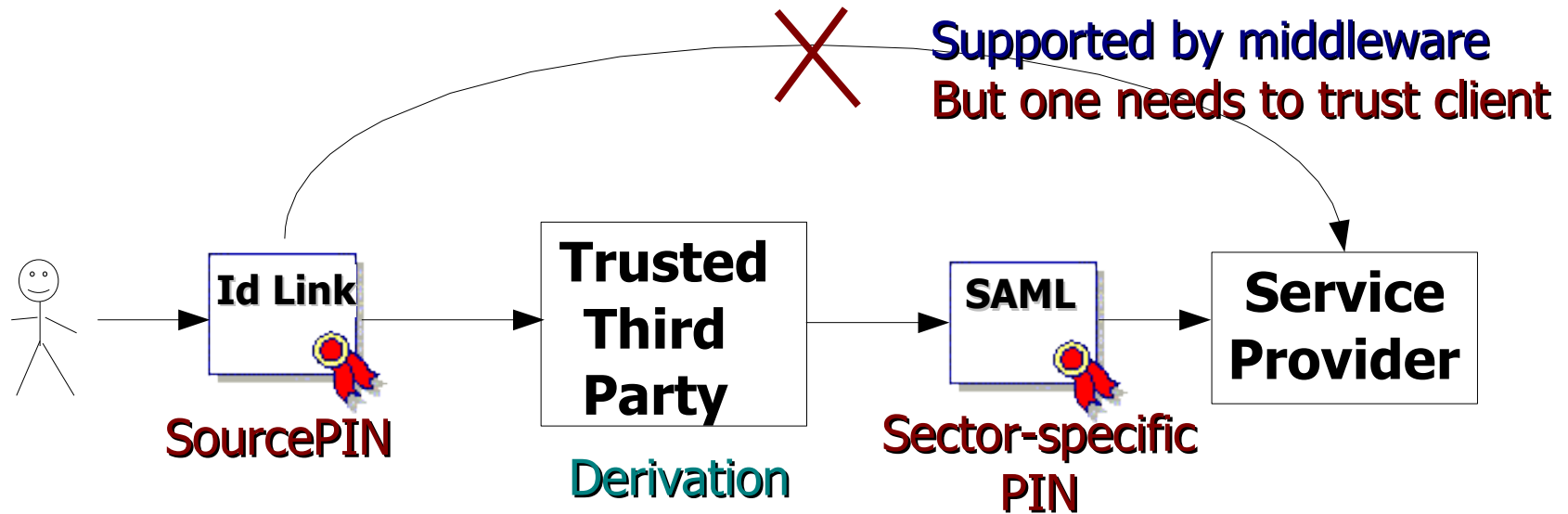
# TLS: light-weight “federation” with ANY Credential techn.

- How to integrate non-X.509 credentials? -> GWs



# Austrian Derived IDs

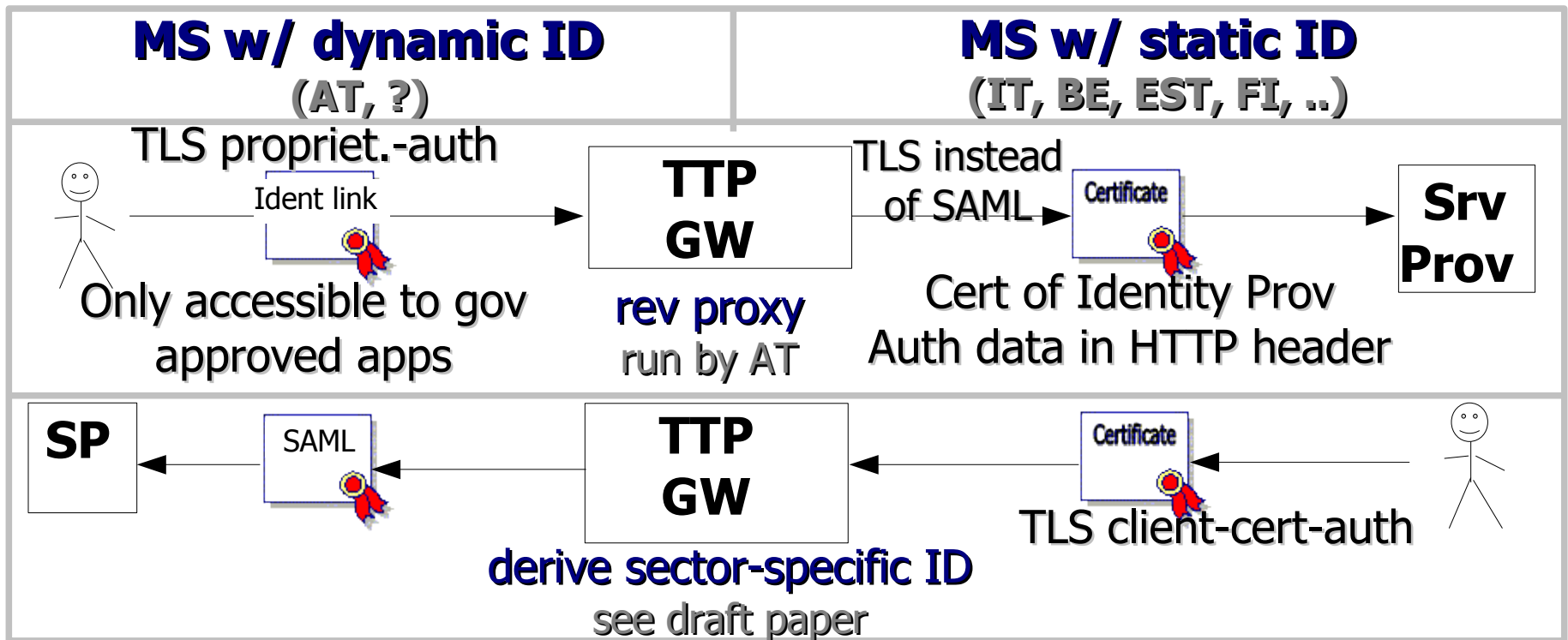
## Austrian approach requires a TTP



by law, only gov-  
approved apps have  
access to sourcePIN

# Static-Dynamic ID GW

- Dynamic ID approach requires TTP
- Combine with Gateway



# ***Common Specification***

## **What is needed for access to services?**

- | **Authentication Protocol**
  - | **Liberty Alliance ID-FF**
  - | **TLS client-cert-auth**
- | **Common Format for Identity Data**
  - | **SAML 2.0**
  - | **ICAO ++ ?**
- | **Protocols for Identity Data Access**
  - | **from central authentic source**
  - | **from citizen's eID**
    - **UPI as standard protocol**
  - | **via Citizen to central DB (UPI ++?)**

# Conclusions

**Premature to state technical choices in documents**

**~~SAML / Liberty Alliance ID-FF~~**

**Necessary Consensus Process**

**Clear problem statement / use case**

**Agree on requirements**

**Find technical options**

**Only then make technical choice**

**We need strong MS participation!** (Dec 4)

**Smartcard-based eIDs need to be more strongly represented**

# Contacts



Bud P. Bruegger <bud@comune.grosseto.it>

Jan van Arkel <arkel@cardlife.nl>

Marc Stern <mstern@csc.com>

Amir Hayat <hayats@sbox.tugraz.at>

Martin Meints <meints@datenschutzzentrum.de>

**InteropEID list:**

<http://www.comune.grosseto.it/interopEID/>