

# Open Source for Interoperability in the eID Domain

<b>Bud P. Bruegger</b>	<b>Comune di Grosseto (Italy)</b>
<b>Jan van Arkel</b>	<b>CEN/ISSS WS eAuthentication (NL)</b>
<b>Stef Hoeben</b>	<b>Zetes PASS (Belgium) and OpenSC Project</b>
<b>Marc Stern</b>	<b>Computer Sciences Corporation (Belgium)</b>
<b>Martin Paljak</b>	<b>OpenSC Project (Estonia)</b>
<b>Amir Hayat</b>	<b>IAIK, TU Graz (Austria)</b>
<b>Libero Marconi</b>	<b>TrustItalia (Verisign) (Italy)</b>
<b>Antonino Iacono</b>	<b>OpenSignature Project (Italy)</b>






# Short-Medium Term Scope

- **Long Term Solution:**
  - **Standards, tight Coordination**
  - high level of **Homogeneity**
  - Time line: **7-10 years** (adoption, implementation, expiry old eIDs)
- **Reported Work: Short-Medium Term**
  - **Middleware** that can manage a..
  - high level of **Diversity**
  - **Now**
  - **Seamless transition to longer term solution**

# Origin of Reported Work

- **Internat. Collab. of Open Source Community**



platforms:     

eIDs:     extensible   ..

Card Operating Systems: **12 and extensible**

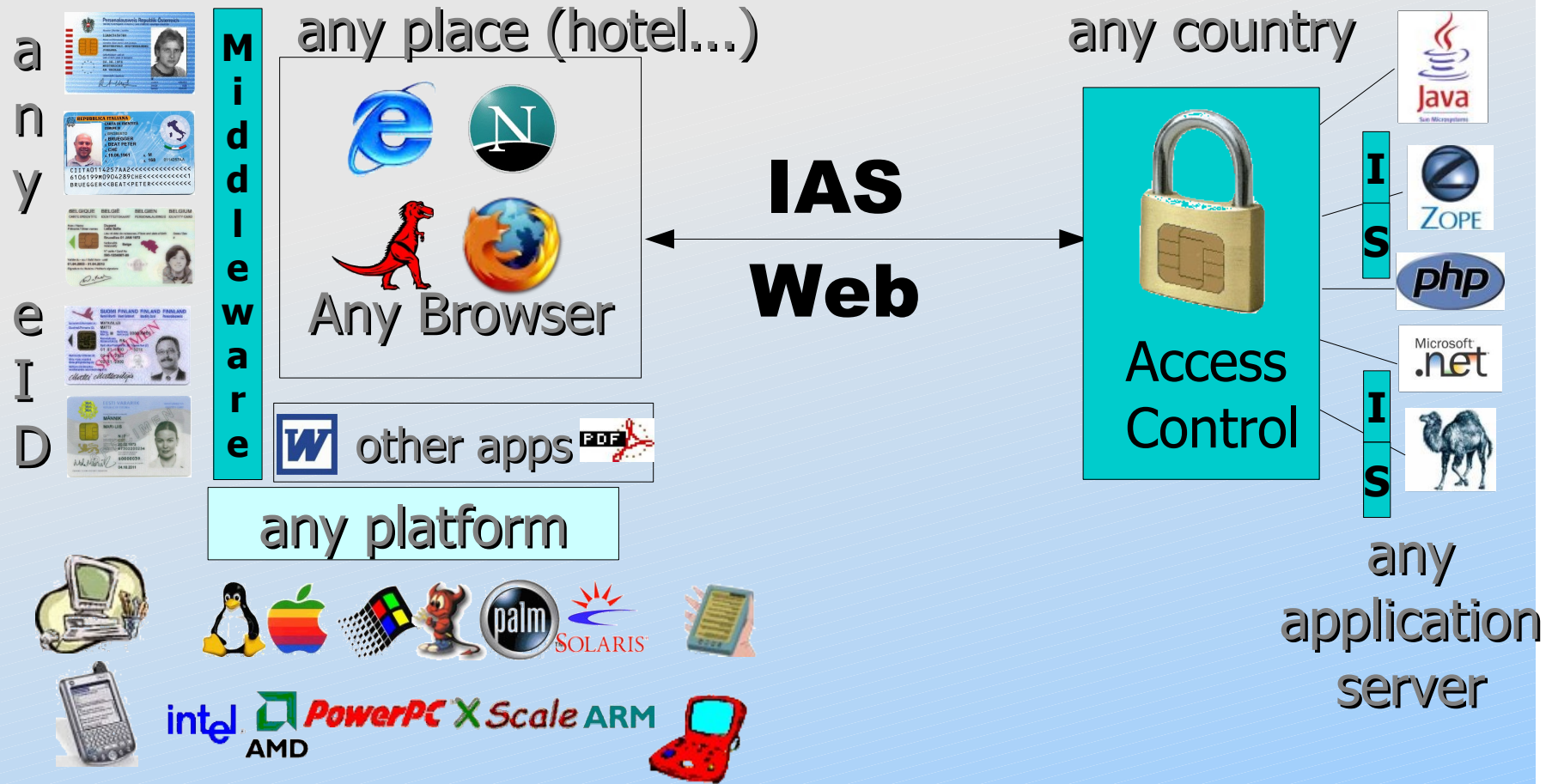
- **CSC Belgian / Fedict: Access Control Solution** 

- **Grosseto & Italian Local Govs interop needs**

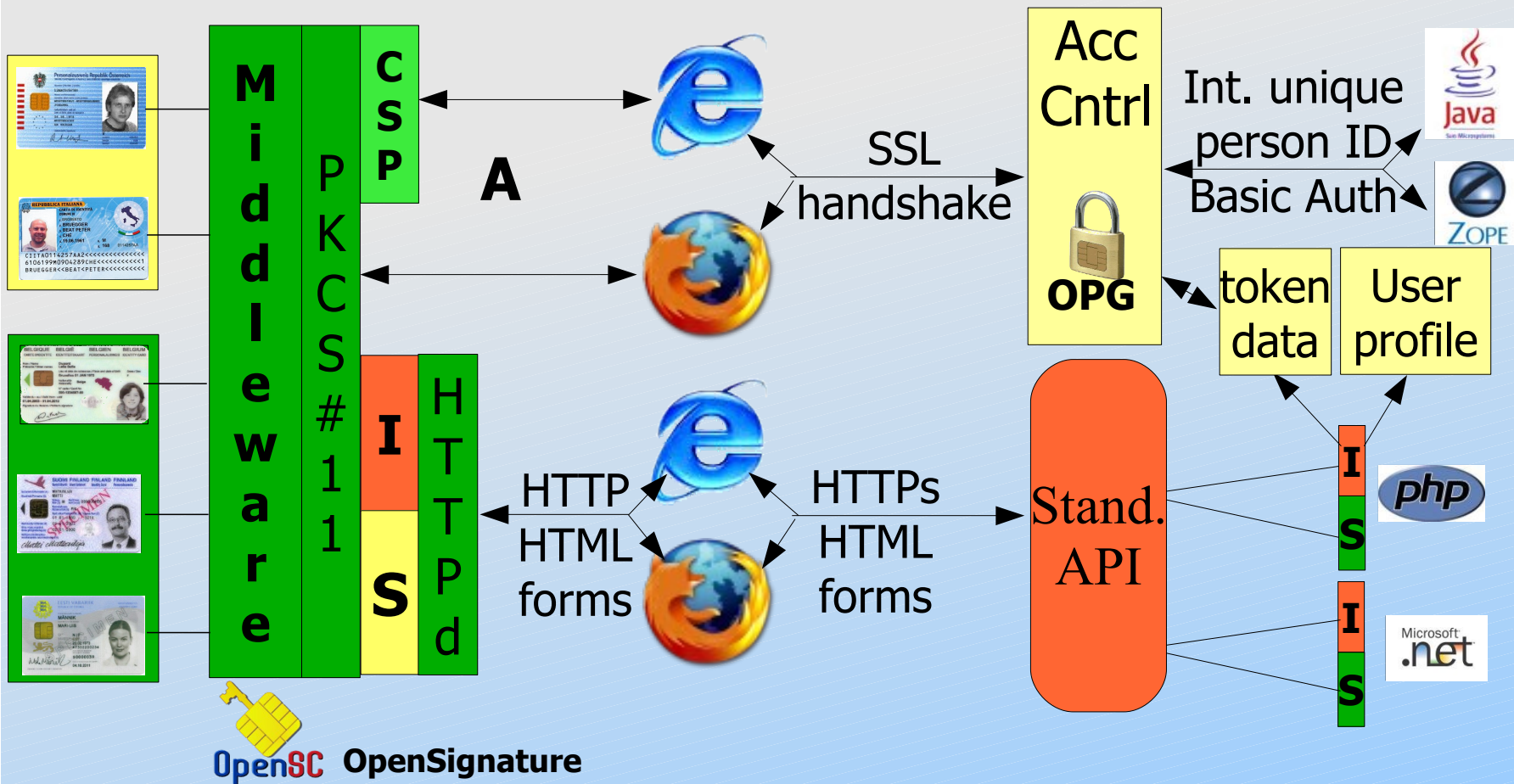
- Two national cards: **CIE, CNS**
- 28 gov. certified CAs for digital signature w/ proprietary SCs

- **Discussion: interopEID list**

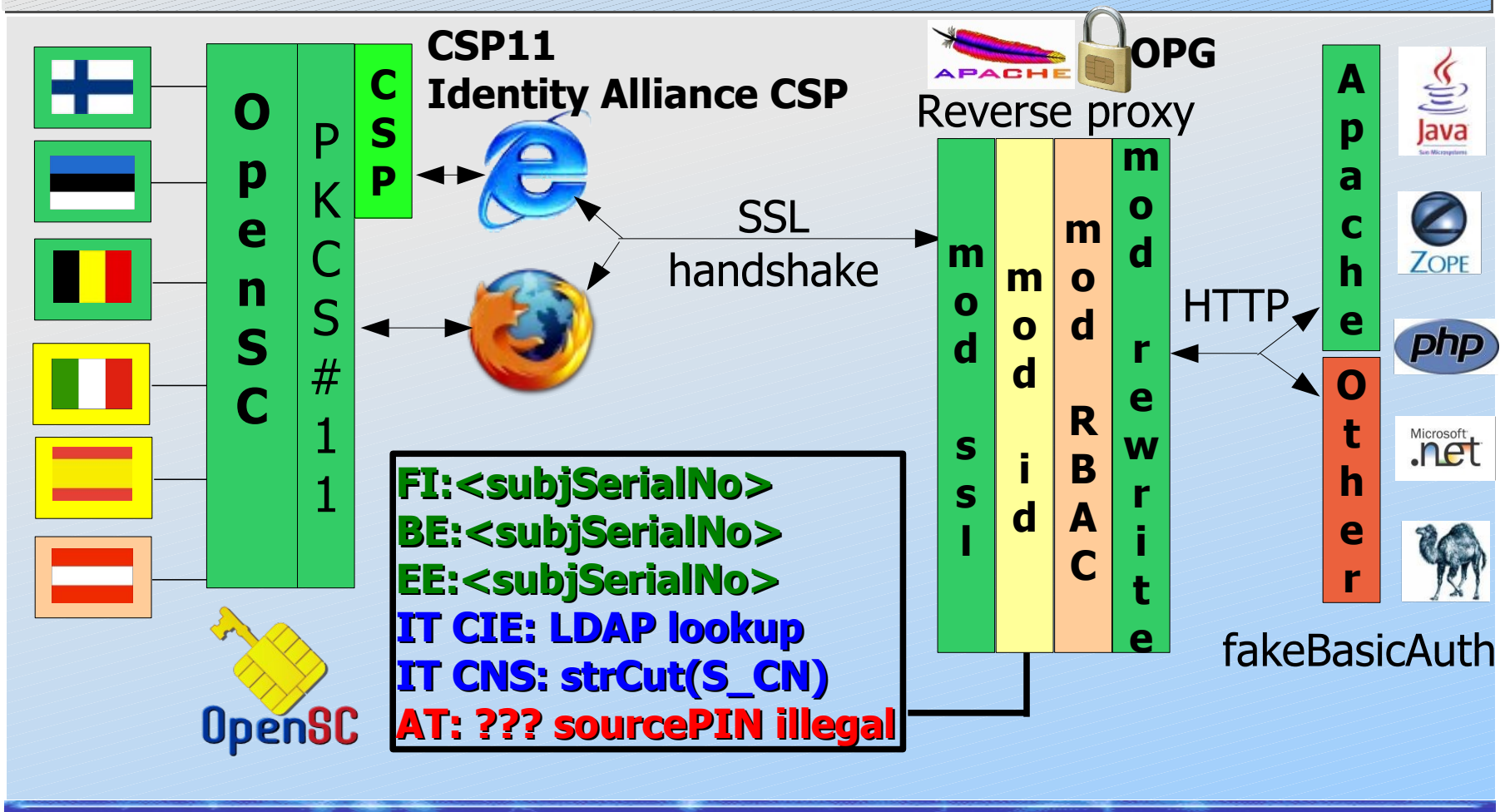
# Objectives of Interoperability



# Proposed Architecture



# Authentication



# Identification/Signature

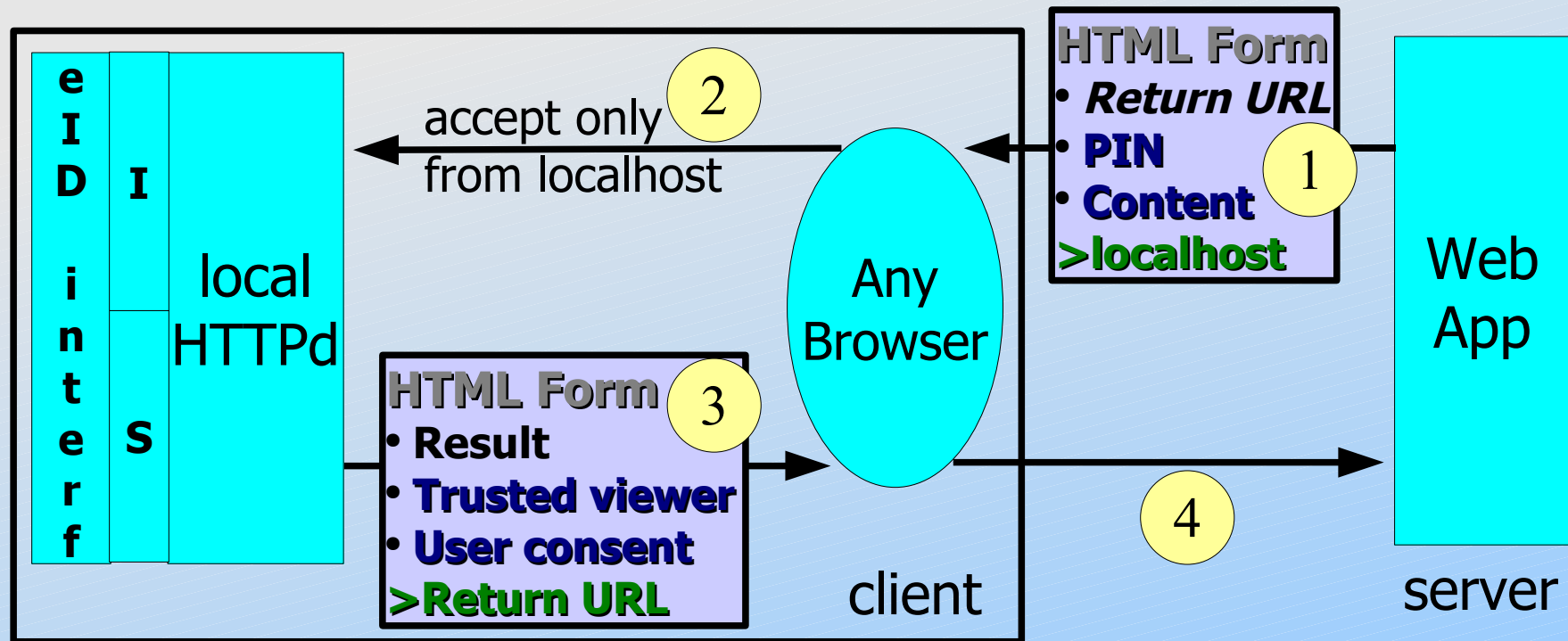
- **Lack of standard protocol (vs. SSL)**
- **Each web app its applet, plugin, activeX ctrl, client lib**
  - **Mono platform/browser**
  - **Multi-Client installations/libraries**
    - Points of control:
      - Policy enforcement
      - Security auditing
      - Look and feel

- **Solution:**

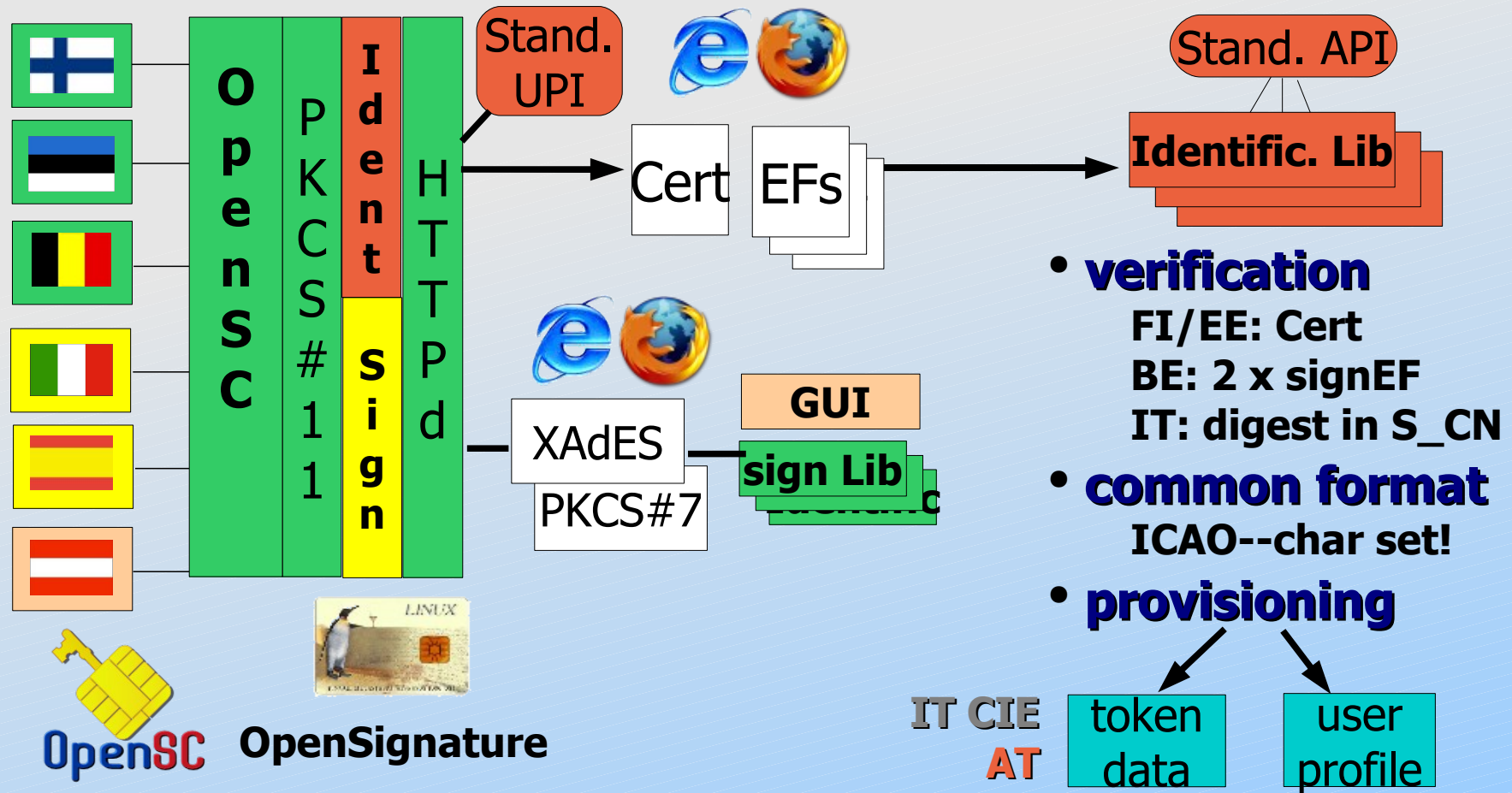
**URL Programming Interface (UPI)**

# URL Programming Interface (UPI)

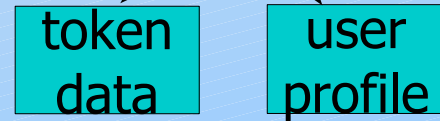
- **Single Point of Control: Consistent across web apps**
- **Smallest Common Denominator: HTTP / HTML Form**



# Identification / Signature



- **verification**  
 FI/EE: Cert  
 BE: 2 x signEF  
 IT: digest in S\_CN
- **common format**  
 ICAO--char set!
- **provisioning**



# Why Open Source Middleware

## Available Software:

- much is already completed

## Organizational model:

- autonomous national players (peers)
- single product owned by all
- everyone has full control (national distributions, auditing)
- No central authority/funding/timing required
- Long-term sustainable (no single source of funding, ...)

# Why not Closed Source?

## Why not a collection of binary PKCS#11s?

- **Combinatorial complexity**
  - Multi-OS
  - Multi-CPU
  - Multi-Version (OS, gLibC, card, PKCS#11)
- **Trust**
  - **Difficult security auditing**
    - No source
    - Test binary of every platform
  - Implicit approval of official national distributions
  - Liability issues?

# Outstanding Problems

- **Austrian Citizen Card Concept:**
  - **sector specific PINs not signed**
  - **Would work with sourcePIN but illegal**
- **eIDs with unpublished specs**
  - **Binary PKCS#11 work-around**
  - **But manageability/trust problem..**

# How to Collaborate

- **verify** approach
- help **specify** UPIs, APIs, and Formats
- **support your eID in OpenSC**
- **co-develop** outstanding components
- **test**
- **national certified distributions**

# Conclusions

- **Biggest part of work: completed**
- **Relatively small effort to complete**
- **Initial collaboration started**
- **Invitation to join**
  - **InteropEID List**
  - **InteropEID Site (Wiki, under PRC eID?)**

