eID standardization from a national perspective: SPID

L. Boldrin
M. De Lazzari
June 25 2015
(SPID - Italian Public Digital Identity System)
(SPID in eIDAS eID network)
(eIDAS standardization space for eID)
(some remarks)
SPID
DECRETI PRESIDENZIALI

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 ottobre 2014.

Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.


1. Richiesta di servizio
2. Inoltro verso Identity provider
3. Richiesta credenziali
4. Verifica credenziali
5. Rendirizzamento verso il service provider con asserzione di autenticazione
SPID Levels of assurance depend very much on the authentication mechanism.
• **auth. mechanism are defined in general security terms**

• **practical implementations are open (compliance must be checked against UNI norm)**
SPID in eIDAS eID network
SPID in eIDAS eID network

COUNTRY B
- Service provider
- S-PEPS

Country B
- In-bound
- Out-bound

COUNTRY C
- eIDAS eID network
- Italian C-PEPS
- SPID in-bound
- SPID out-bound

ITALY
- SPID Identity Provider

Users

InfoCert
- eID standardization - SPID perspective
- 2015

Information Copyright © InfoCert 2015
SPID in eIDAS eID network

COUNTRY B
Identity Provider

Country B
C-PEPS

COUNTRY C

eIDAS eID network

Italian S-PEPS

SPID in-bound

SPID out-bound

Users

Service provider

ITALY

InfoCert eID standardization - SPID perspective 2015

Information Copyright © InfoCert 2015
SPID in eIDAS eID network: expected deploy

COUNTRY B

Appeal to commercial SP to be tested!

Country B
PEPS

Italy PA
S-PEPS

Country C
PEPS

Italy Comm
S-PEPS 1

Italy Comm
S-PEPS 2

Country C

ITALY

Service
provider

SPID
Identity Provider

Users

Service
provider

SPID
Identity Provider

eIDAS eID network
eIDAS standardization space for eID
eIDAS standardization space for eID

**INSIDE eIDAS**
- Notification
- Cooperation
- Assurance levels
- Interoperability framework
- (Cost policy)

**OUTSIDE eIDAS**
- Member States eID schemes
- eu ID
- roles / attributes
- centralized hub, centralized db, directory service, etc.
# eIDAS standardization space for eID

**MAP to European Interoperability Framework**

<table>
<thead>
<tr>
<th>eIDAS Regulation</th>
<th>Legal</th>
<th>Organizational</th>
<th>Semantic</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>regulation</strong></td>
<td>IA</td>
<td>IA / cooperation group</td>
<td>IA / cooperation group</td>
<td>IA</td>
</tr>
<tr>
<td>Notification</td>
<td>IA</td>
<td>IA / cooperation group</td>
<td>IA / cooperation group</td>
<td>IA</td>
</tr>
<tr>
<td>Cooperation</td>
<td>IA</td>
<td>IA / cooperation group</td>
<td>IA / cooperation group</td>
<td>IA</td>
</tr>
<tr>
<td>Assurance levels</td>
<td>IA</td>
<td>IA / cooperation group</td>
<td>IA / cooperation group</td>
<td>IA</td>
</tr>
<tr>
<td>Interoperability framework</td>
<td>IA</td>
<td>IA / cooperation group</td>
<td>IA / cooperation group</td>
<td>IA</td>
</tr>
<tr>
<td>(cost policy)</td>
<td>IA</td>
<td>IA / cooperation group</td>
<td>IA / cooperation group</td>
<td>IA</td>
</tr>
</tbody>
</table>
some remarks
lessons from eSignature standardization

Standardization areas: first guess

(take form eSig rationalised framework & adapt)

1. Signature Creation & Validation
2. Signature Creation & other related Devices
3. Cryptographic Suites
4. TSPs supporting eSignature
5. Trust Application & Service Providers
6. Trust Service Status List Providers

from eSig to eID

ID Service providers
Authentication Process
Authentication Devices
Cryptographic Suites
ID Service Status List Providers

2015
lessons from eSignature standardization

Document types: first guess

...limited to the super-national quota

Guidance
Policy & Security Requirements
Technical Specifications
Conformity Assessment
Testing Compliance & Interoperability
lessons learned from eDelivery

national stand-alone initiatives (PEC, DE-Mail, IncaMail ...)

european standard proposal (ETSI-REM)

global sector-specific standard (UPU)

OUTCOMES:

1. no convergence of commercial initiatives to a single standard
2. standard only used in "inner circle" between GWs
3. GW approach for eDelivery is complex...
a commercial IdP would like to operate in different countries, with similar (if not identical) rules:

- **national quota of specifications should be low**
- **country-specific conformance might be overkill**
- **certification cost is lower if there is international CAB competition**
non-core attributes are an important part of identity

• attributes have commercial value: they may push deploy

• attribute providers should find a place in the architecture

• attribute standardization should be enforced
other cross-border eID circuits (sector-specific: telco, banking) are pushing

• they might prove less complex and good enough for the private sector

• eIDAS eID network should provide hooks for non-national circuits

• SAML is not mainstream
thank you!