eID interoperability Scenario

v0.2, 30/8/2007

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

ChangeLog:

* added another scenario case with cached derived personal data

Purpose:

The present note briefly describes the scenario of eID interability from a perspective relevant for European governments who issue eIDs and the European Commission who guides the process of reaching eID interoperability by 2010. It is hoped that the concrete scenario facilitates the discussion and comparison of potential solutions.

Background:

European Ministers in addition with some non-European countries (e.g. Iceland) have issued the so called Manchester Declaration in November 2005 which states the political objective to reach mutual recognition and interoperability of electronic identities by the year 2010. The declaration adopts the subsidiarity principle leaving full autonomy to Member States in what kind of electronic identity they issue.

This objective has been reflected in the e2010 Action Plan and consequently in a Road Map document. The Information Society branch of the European Commission is facilitating the process in which Member States chose an interoperability solution. The IDABC office of the European Commission is currently working on a first version of the Common Specifications. The de-facto standard for interoperability is expected to be created by the EC-funded Large Scale Pilot project in which Member States themselves are forming the project consortium; the STORK proposal has currently participation by 18 European Member States.

The official process is mostly oriented towards cross-border eGovernment services, leaving private-sector services out of scope.

The expected ubiquity of government certified electronic identities in the hand of every citizen has an enormous potential for enabling a sorely needed quantum leap in security of the current Internet with services across all sectors.

Governments are uniquely suited to issue generally accepted identities and cover the cost of sophisticated enrollment procedures (that typically require population registers and/or background checks, biometrics, etc.) that is required for highly secure identities.

eIDs in Europe:

The European discussion looks exclusively at government-issued (or third party issued but under government control) eIDs. The earliest national eID projects (Finland, Estonia, Belgium, Italy, Spain, ..) have well pre-dated the standardization efforts in CEN (TC224 WG15 "European Citizen Card" and there is a wide variety of technical choices. The various eIDs even fail to agree on the use of the X.509 standard--and the political decision of applying the subsidiarity concept almost makes it impossible for a single standard to take foot in Europe. Thus, IOP solutions have to work with any present and future eID credential technology.

Functionality

The scope of this scenario is the access of citizens to online services. A service typically stores data on its user that has to be accessed across sessions.

This involves two basic functionalities:

(i) authentication:
Every time users reconnect to the service, they are recognised in a way that makes it possible to find their data created in earlier sessions. This is done via some handle that can (depending on the technical choices of Member States and others) be anything from a nationally unique identifier to a single-sector random and opaque handle. Authentication includes mechanisms that guarantees that only the legitimate owners of the identity can connect to their data and that impersonating other identities is ideally impossible. Autentication is necessary at every service access.

(ii) identification:
Optionally, a service provider can require to receive a set of personal data that is certified by an accepted authority (typically a government). This data is only necessary at the first access to the service (during provisioning of the user account) and needs not be repeated. Identification is dealing with personal data and thus requests a high level of privacy protection and user control.

General Requirements:

Any solution that is acceptable to the stakeholders needs to be based on open standards, be implemented on all relevant (and emerging) plaforms, and ideally there should be at least one open source implementation. Vendor lock-in or control (e.g., via patens) makes acceptance very unlikely.

Limitations and Open Issues

The described scenario looks only at a single channel--the web. The use of eIDs from mobile devices or through other channels may require major rethinking.

An open issue is to understand how the scenario relates to the two approaches that are planned to be explored in the Large Scale Pilot project STORK, namely the portal- and the middleware-appraoch.

The actual scenario:
==========

Actor Overview:
---

* service providers

* users who are assisted by an intelligent user agent and in possession of an eID (credential)

* governments who issue the eID (credential) and possibly run an Identity Provider (IdP)

* third parties (possibly IDABC) who run IdPs that complement the government services and are necessary for interoperability of service access.

Service Providers:

SPs are autonomous players who chose the technology that protects service access based on their own capacity and agenda. We can expect the use of:
* TLS client-cert authentication (plain Apache/IIS/..)
* Liberty ID FF
* WS-*/Cardspace
* possibly others like OpenID, although in the government world the above three seem to be the most important ones.

eIDs--authentication aspects:

A representative subset of eIDs include the following types:

* smartcard- or file-system-based X.509 credential

* smartcard- or file-system-based non-X.509 credential, e.g., the Austrian Citizen Card that is complemented by a government run IdP that uses a proprietary authentication protocol and issues a standard session credential (e.g., a SAML assertion in the case of Austria)

* username/password that is complemented by a government run IdP that

uses some directory for authentication and issues a standard session credential (e.g., a SAML assertion)

eIDs--identification aspects:

A representative subset of eIDs include the following types:

* one or several smartcard- or file-system-based data files that are signed by an authority. Both data formats and signature mechanisms are typically proprietary

* a central IdP that is based on a central database (e.g. Population Register) that keeps identity data of all citizens.

Note that some national legislations (e.g., Italy and Germany) explicitly prohibit the existance of central national identity databases.

Also note that static signed files are very limited from a privacy protection point of view since they drastically limit the choice of user-control over what personal data are actually disclosed. (Creating a subset or derivation of data loses the certification). For advanced privacy protection and user control, a dynamic service (IdP) is always necessary even if the authentic source of data is a file under the user's control.

[Note that a draft paper on privacy aspects raised here is available from bud@comune.grosseto.it on request]

Government run IdPs:

While all governments have the necessary infrastructure to issue national eID credentials (e.g., a CA for issuing X.509 credentials), not all run an IdP that is involved in every service access. This is a free national choice.

Of the Governments who run IdPs, we can expect the following main types:

* SAML IdPs (with Liberty or other front-ends)
* WS-*/Cardspace IdPs
* X.509 IdPs who dynamically issue certificates as session credentials (see TLS-Federation)

Third Party IdPs--authentication aspects:

Third party IdPs typically take a session credential of type A as input, verify it, and if successful issue a session credential of type B (where A,B in {SAML, STS-token, X.509 cert). Third party IdPs are typically used by intelligent user agents to convert the session credential issues by the government to a format that is acceptable to

the service provider.

Third Party IdPs--identification aspects:

Third party IdPs typically take certified identity data of type A as input, verify it, and if successful issue certified identity data of type B (where A,B in {SAML attribute assertion, STS-token, proprietary data/signature formats of current eID cards, maybe ICAO LDS). Third party IdPs are typically used by intelligent user agents to (i) convert identity data issues by the government to a format that is acceptable to the service provider and/or (ii) to limit the data content of the original data set in order to protect privacy through minimal disclosure.

The IOP Problem:

IOP is reached if an intelligent user agent manages to access any type of service provider with any kind of eID, intelligently using the government and third party provided services (IdPs) and providing as much as possible a consistent experience and user's awareness and control over data disclosure.

Sub-scenarios of particular interest:
---

* SP uses TSL client-cert-auth, X.509 eID, auth:
identity agent realizes that no IdP service is necessary and directly manages authentication.

* SP uses TLS, username/password eID, gov runs X.509 IdP (TLS-Federation):
identity agent realizes that the user needs to authenticate with username/password to the IdP and get an X.509 certificate that can be used in the TLS-handshake.

* SP uses TLS, non-X.509 smartcard eID (Austrian Citizen Card), gov runs SAML IdP (Austria), third party IdP (complex TLS-Federation):
identity agent realizes that user needs to do a proprietary authentication with her eID to the gov IdP to get a SAML "session credential", then uses the third party IdP to convert the SAML credential into an X.509 credential that can be used in the TLS handshake.

* ... similar things with Liberty and Cardspace SPs?

* SP requires "complete" identity data and can handle the format used on the available eID (a signed file): The identity agent realizes that the signed file(s) contained on the eID can be sent directly. Q: what protocols are there to do that? WS-*/Cardspace and also Liberty; but latter is not compatible with user-centric IDM???

* SP requires a minimal set of identity data in a standard format (SAML?, ICAO LDS?), eID contains a full set of data in a signed file of proprietary format, third party IdP is known to identity agent: Identity agent asks users consent for disclosure, uses the 3rd party IdP to derive and sign a minimal dataset in the required format. Protocols?

* SP requires a minimal set of identity data in a standard format (SAML?, ICAO LDS?), a corresponding signed data file is already available in the cache from an earlier interaction with an IdP: Identity agent asks users consent for disclosure, and uses the local cache copy without needing any external services.

Note: the described scenarios presently don't deal with the issues of trust management. It is assumed that all eID credentials and all IdPs are trusted. How this trust is established is outside the scope of this discussion--maybe a solution like the IDABC Bridge CA or similar is necessary here.

--
Ing. Bud P. Bruegger, Ph.D. +39-0564-488577 (voice), -21139 (fax)
Servizio Elaborazione Dati e-mail: bud@comune.grosseto.it
Comune di Grosseto jabber: bud@jabber.no
Via Ginori, 43 http://www.comune.grosseto.it/
58100 Grosseto (Tuscany, Italy)
http://www.comune.grosseto.it/interopEID/