CAT Cert

Agència Catalana de Certificació

Identity and capability management in eHealth: the CATCert approach

AOC
Administració Oberta de Catalunya

Generalitat de Catalunya

Consorci de governs locals per a la societat de la informació

The need to manage identities - 1

– Increment of digital identity complexity

  – Password, dynamic password, one-time password, based on portable secure devices (like USB tokens, mobile phones, smart cards).

  – Identity X.509 digital certificates, issued by different providers, to public employees, businesses and citizens, specially in roaming and non-physical presence scenarios.

  – National electronic identifications (DNI and others).

  – Remote/delegated authentication assertions, based in SAML, Liberty, Shibboleth, WS-S/WS-I and others, in distributed and collaborative environments.

  – Identity federation rules and trust models management.

– Merging of identity management and business processes

  – Market is going beyond the trend to integrate or synchronize identity and other attribute information in "unique directories".

  – Trend to hide organizational directories behind SOAs (less LDAP and proprietary applications, more web services).

  – Emerging middleware to integrate applications and business logics requiring identification and attribute information.

The need to manage identities - 2

- Orientation to distributed identity and attribute management
  - Perception: Distributed management may help extending the public service provision to all persons, especially in a transnational environment.
  - European initiatives like FIDIS or MODINIS consider identity and attribute management as the solution to integrate public transactions at a European-wide scale, in an interoperable form, and in concrete may leverage the national electronic identifications, and other regional identifications, like eHealth cards or citizens cards.
  - GUIDE project, built complying with European Commission's IDABC initiative, currently works in profiles and messaging based in SAML/Liberty to integrate European identities.
- Appearance of business protocols to manage identity schemas (Liberty WSF, SAML…) and access control in a highly distributed form (XACML).

CATCert strategic considerations

- Current and future situation

  - Many identities (although with more quality): public, private, national, regional, local, healthcare, finance... Trend to reduction and generalization of identities (more DNI/idCAT, less password)

  - Many networked providers regarding attributions and capacities of people: public administrations, notaries and legal registries, private entities. Trend to high specialization and on-line consumption, using web services.

- Strategy

  - Today: Validate different <u>identities</u>, generate evidence and archive it (**PSIS**).

  - Evolution: Facilitate authentication, using a common module (**PASSI**).

  - Evolution: Manage <u>persons</u>, instead of separate identities (**PASSI**).

  - Novelty: Manage <u>capabilities</u>, persons able to do things (**PASSI**).

Platform of attributes for security and signature

- Main objectives
  - Creation of a repository containing the identity data sources managed by CATCert (wide "metadirectory" concept).
  - Definition of a semantic model, and of connectors with identity providers.
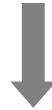 - Provision of "Attribute Authority" services, using a SOA paradigm.
- Ancillary objectives
  - Foster the adoption of different identity systems by any administration ("Web Single Sing-On common module" concept).
  - Achieve interoperable identity and attribute services between administrations.
  - Being the Catalan public identity and attribute services broker.
  - Provide to public administrations tools to manage entitlements and other forms of legal representation.
  - Allow citizens and businesses the maximum self-management level for their privacy and sensitive data.
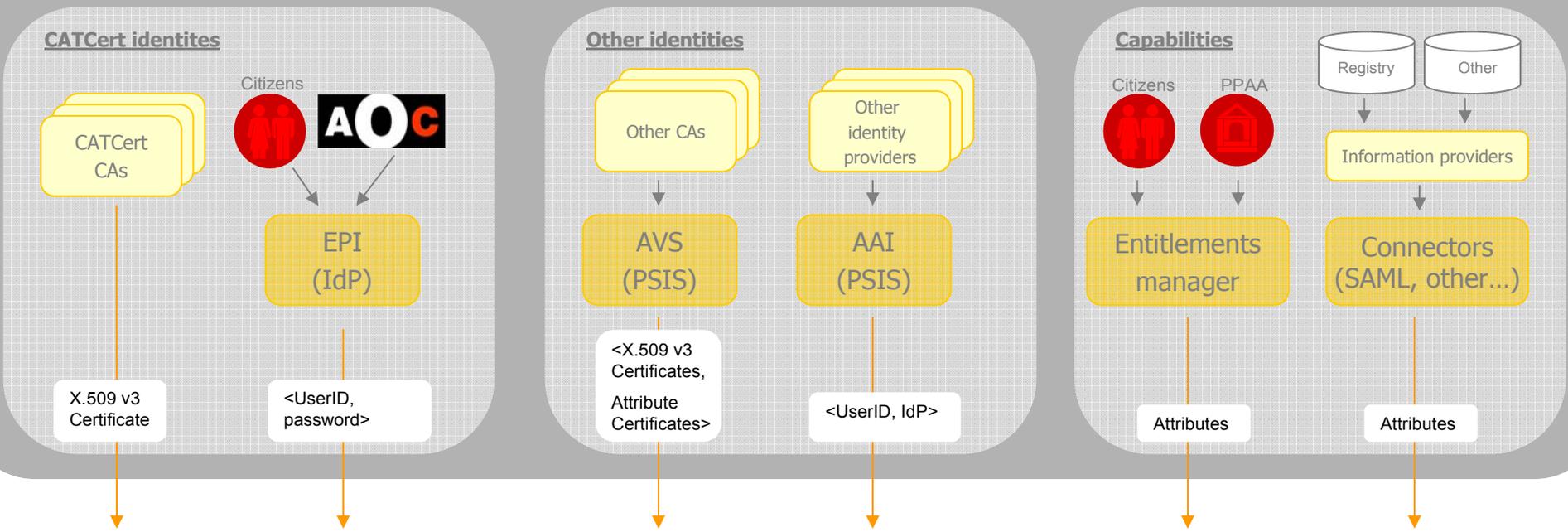
Data sources

↓

Platform of Attributes for Security and Signature: <u>PASSI</u>
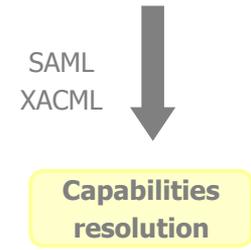
↓

Identity and attribute services

Data sources

CATCert identites

CATCert CAs

Citizens AOC

X.509 v3 Certificate

EPI (IdP)

<UserID, password>

Other identities

Other CAs

Other identity providers

AVS (PSIS)

<X.509 v3 Certificates, Attribute Certificates>

AAI (PSIS)

<UserID, IdP>

Capabilities

Citizens PPAA

Registry Other

Information providers

Entitlements manager

Connectors (SAML, other...)

Attributes

Attributes

My identities manager

Semantic model

PASSI

Usage policies manager

Taxonomy based process engine

Liberty WSF

Web SSO

Liberty WSF

Capabilities report

SAML XACML

Capabilities resolution
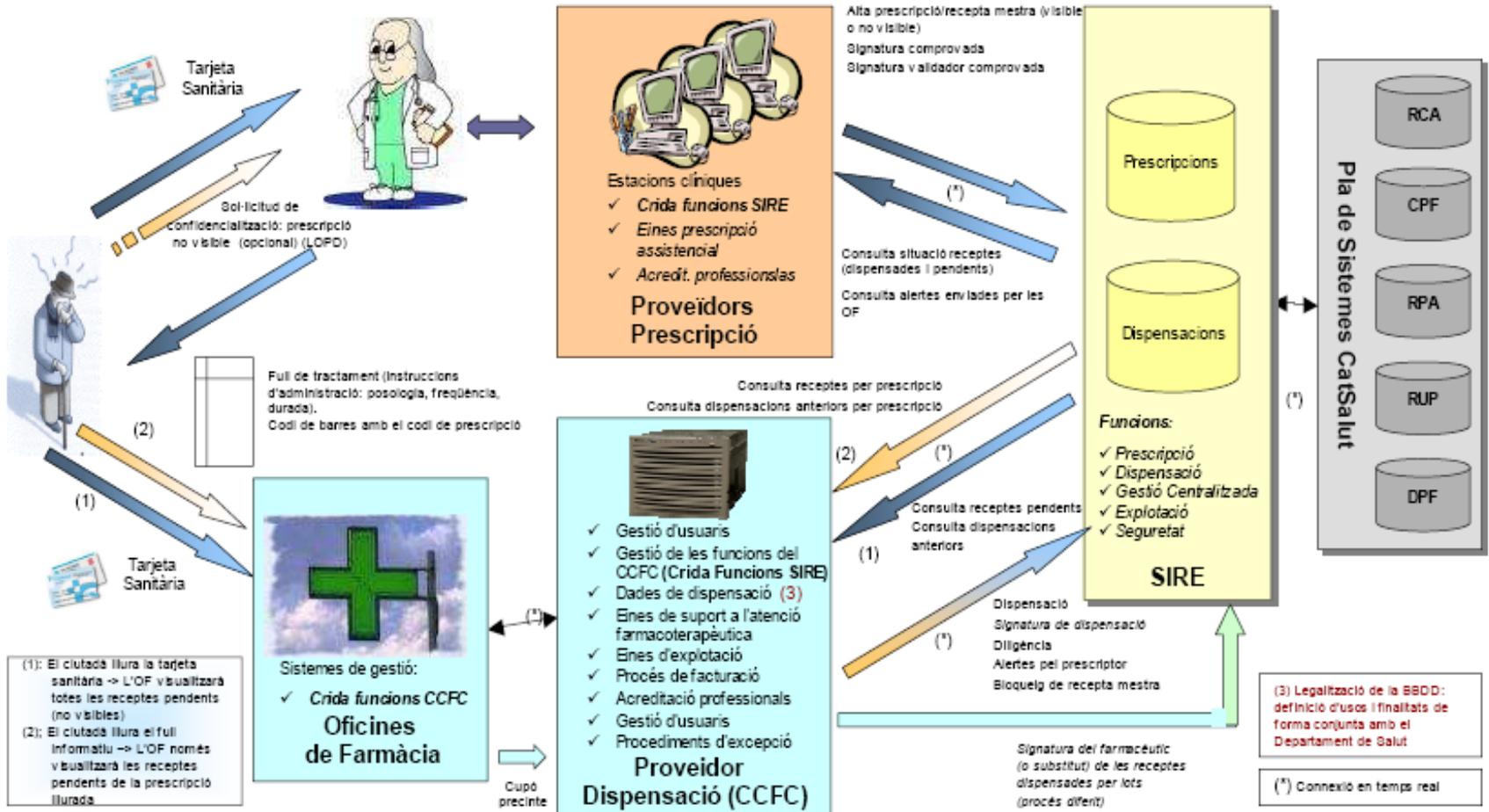
A Catalan identity scheme for eHealth - 1

– The Catalan Health Service has implemented an ePrescription project, which is up and running in a real production environment.

A Catalan identity scheme for eHealth - 2

- The project authentication mechanisms are based in an identity delegation scheme:

  - Medical doctors authenticate using UID and password or X.509v3 qualified certificate against hospitals.

  - For each new prescription, Hospitals send a web service, including a SAML assertion authenticating doctors. That secure web services are consumed by the Catalan Health Service.

  - Pharmacies authenticate using UID and password or X.509v3 qualified certificate against de Catalan Council of Pharmacies.

  - For each new dispensation, the Catalan Council of Pharmacies send a web service, including a SAML assertion, which is consumed by the Catalan Health Service, giving access to pending ePrescriptions (additional controls apply to protect personal identifiable information).

  - ePrescriptions are also signed by medical doctors, and the dispensed medicaments are reported to the Catalan Health Service with a signed message.

A Catalan identity scheme for eHealth - 3

– Main benefits of the proposed solution:

  – A delegated trust management system allocates roles and responsibilities to all participants.

  – The Catalan Health Service is discharged of user management.

  – Delegated authentication and authorization allows new services, both based in web services and in user interface.

– The schema is being extended to fit the needs of the Catalan Health's department Shared Clinical Records project.

  – Similar functional requirements as ePrescriptions.

  – The information is not centralized: an index is maintained at a central point, controlling access to the information at each hospital.

  – More focus on

  – Probably a higher level of security is required.

Lessons learned and future directions

– Delegated authentication and authorization is a first step into delegated trust management, and the correct policy to manage identity in very heterogeneous environments, like health services.

– SAML is Ok to transport identity information inside webservices (as it is to secure web services using WSS).

– But to give service to user interface based applications, the system must adopt the full set of Liberty specifications:

  – Further investigation on IHE interoperability profiles for cross-enterprise authentication.

  – Federation with professional associations.

  – The role of a possible health services smart card and citizen PKI. Federation with insuring companies and public institutions.

– Integration with other identity systems, such as Cardspace (identity locator service) is a need, and will have significant impact.

Many thanks!!!
Questions?

More information:

ialamillo@catcert.net

CATCert
Agència Catalana
de Certificació

AOC
Administració Oberta
de Catalunya

Generalitat
de Catalunya

Consorci de governs locals
per a la societat de la informació