



Agència Catalana
de Certificació



CATCert eIDM real cases



Administració Oberta
de Catalunya



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 federation (Liberty WSF, SAML...) and access control in a highly distributed form (XACML).
- Need to include signatures in federation schemes, as signing requires previous identity management.

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 webservice.

– Strategy

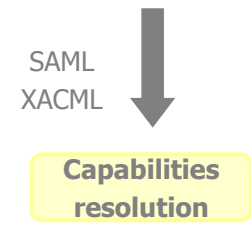
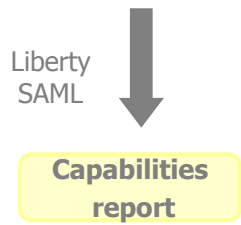
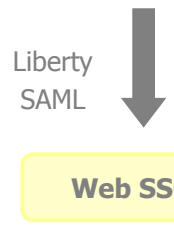
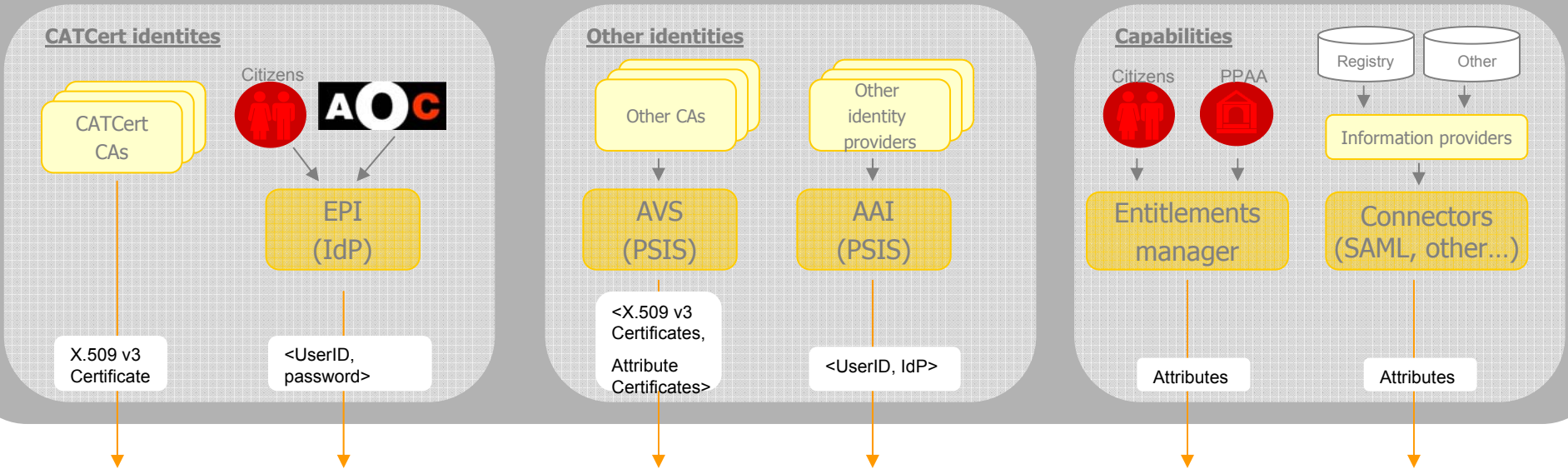
- Today: Validate different identities, generate evidence and archive it (**PSIS**).
- Evolution: Facilitate authentication, using a common module (**PASSI**).
- Evolution: Manage persons, instead of separate identities (**PASSI**).
- Novelty: Manage capabilities, persons able to do things (**PASSI**).
- Novelty: Federate signatures in identity schemas (**WSCA**).

Platform of attributes for security and signature

- Main objectives
 - Deployment of an identity and capabilities federation in the public sector.
 - 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.
- 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.

Platform of attributes for security and signature

Data sources



Web signature creation application

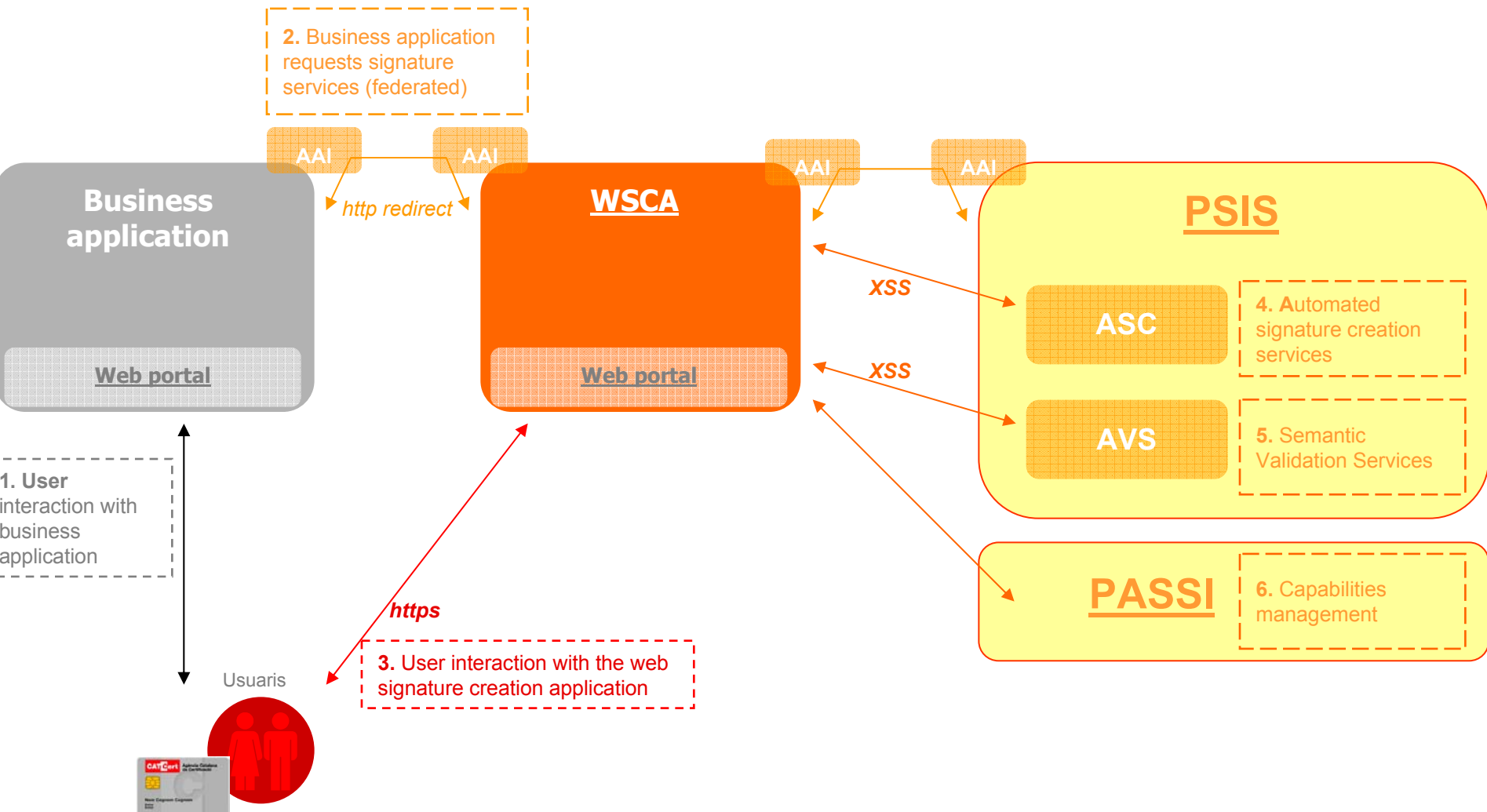
– Main objectives

- Create a general purpose web-based electronic signature server, federated with the business application.
- Reduce the cost of implement the electronic signature processes, complying with the legal and technical rules.
- Federate the electronic signature process with the identity management schema adopted by the public administration.
- Issue SAML-compliant assertions including “signature statements” (eg, The Hague apostille).

– Ancillary objectives

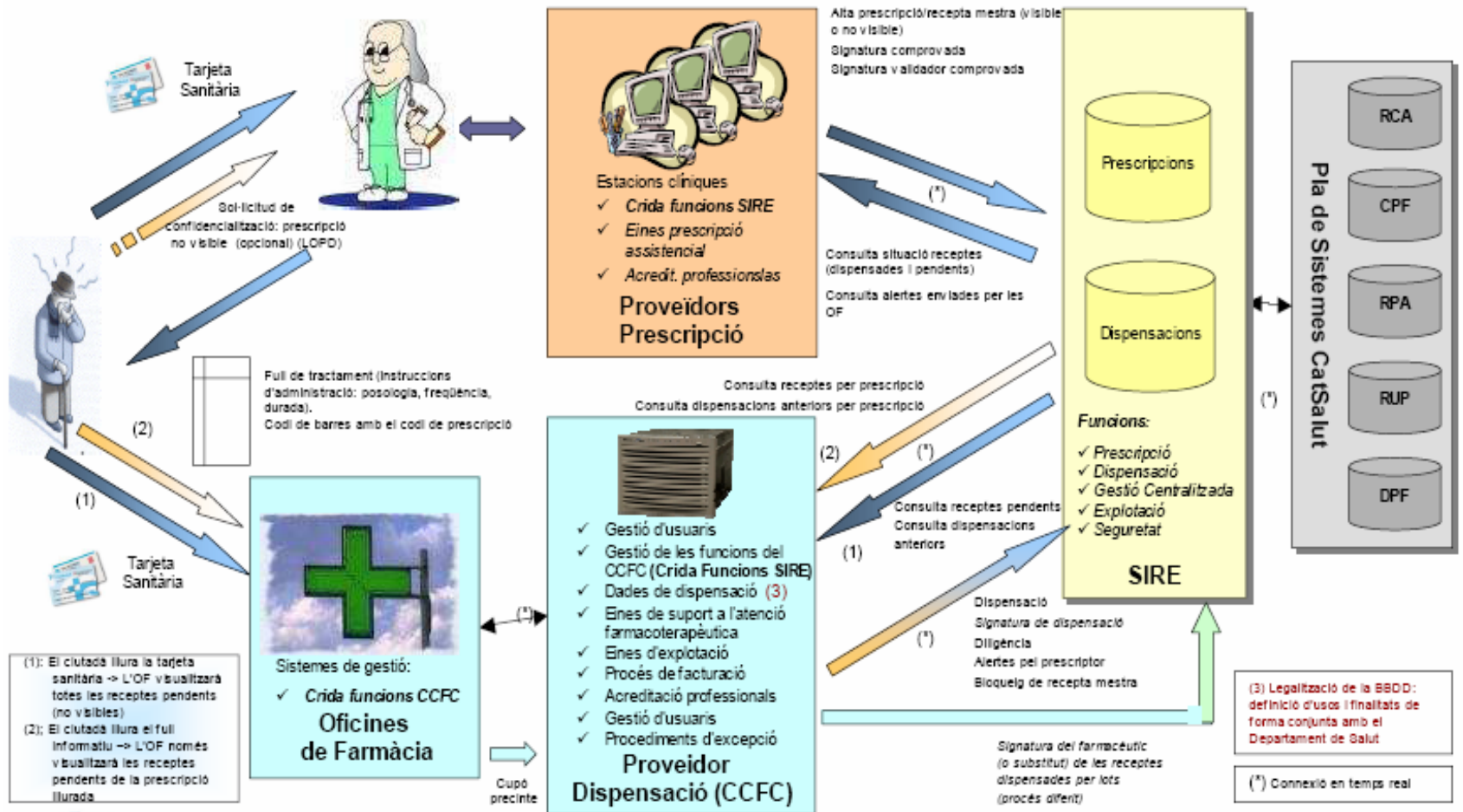
- Implement all signature formats (CMS, XMDSig, CAdES, XAdES, etc)
- Implement automatic signature creation and validation, controlled under signature policies and SAML authentication and authorization statements.
- Integrate the solution in PDAs and DVB3, using federated authentication implemented in the devices.

Web signature creation application



Practical experience: e-Prescription in Catalonia - 1

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



Practical experience: e-Prescription in Catalonia - 2

- The project authentication mechanisms are based in an identity federation:
 - Medical doctors authenticate using UID and password / X.509v3 qualified certificate.
 - Hospitals issue SAML assertions that are consumed by the Catalan Health Service, giving access to the ePrescription application.
 - Pharmacies authenticate using UID and password / X.509v3 qualified certificate.
 - The Catalan Council of Pharmacies issue SAML assertions that are 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.



**Agència Catalana
de Certificació**

More information:

ialamillo@catcert.net



**Administració Oberta
de Catalunya**



Consorti de governs locals
per a la societat de la informació