Marco europeo de la administración-e

En la eEuropa actual, las administraciones públicas tienen como objetivos prioritarios los compromisos comunitarios e iniciativas incluidas en la estrategia de Lisboa. El objetivo de este plan de acción es crear un marco favorable a la inversión privada y a la creación de nuevos puestos de trabajo, impulsar la productividad, modernizar los servicios públicos y ofrecer a todos la posibilidad de participar en la sociedad de la información. eEurope 2005 pretende, en resumen, fomentar la seguridad de los servicios, aplicaciones y contenidos basados en una infraestructura de banda ancha ampliamente disponible.

Para tener éxito en la realización de este plan de acción, es de vital importancia construir un entorno de desarrollo y de uso que muestre veracidad en los procesos que se realizan y en la información que se comunica, y, por otro lado, que transmita confianza al ciudadano. Esto lo conseguiremos mediante,

- mecanismos y tecnología de autenticación robusta,
- sistemas de gestión de identidades,
- mecanismos para proteger la privacidad de los datos personales.

Por otro lado, es necesario que las adminstraciones públicas y organismos colaboren entre sí, que los procesos reguladores, los sistemas desarrollados y la información que compartan puedan ser re-usados por todos ellos, es decir, es necesario que la interoperatibilidad entre todos los sistemas involucrados sea real y efectiva, siendo necesario aspectos,

- organizativos: colaboración entre los diferentes actores de los procesos, como son las administraciones públicas, empresas, etc...
- semánticos: no solamente es necesaria la interconectividad, también es necesaria una interpretación automática, re-usando recursos.
- técnicos: interconexión de las aplicaciones mediantes componentes tecnológicamente diversos, en base a estándares y especificaciones abiertas aceptadas.

La consecución de los objetivos marcados en Lisboa parten de un punto principal y esencial: el ciudadano, la persona.

La gestión de identidades

Como se ha comentado en el apartado anterior, la identidad de una persona es la base, el punto inicial de la administración-e. Pero, ¿qué entendemos como identidad?:

- Identidad (*Identity*), se corresponde a la colección dinámica de todos los atributos de una persona (sea física o jurídica). Nos referiremos a una identidad parcial a un conjunto de atributos de una identidad.
- Gestión de identidades (*Identity Management – IDM*), se corresponde a la gestión de identidades parciales (conjuntos de atributos de una identidad).

- Sistema de gestión de identidades (*Identity Management System – IMS*), se corresponde a la infraestructura técnica y organizativa utilizada para la definición, selección y administración de los atributos de una identidad.

La habilidad para relacionar un conjunto de atributos o información a su propietario, así como la habilidad de gestionar la seguridad de determinados datos de la identidad es esencial para un sistema de gestión de identidades.

La gestión de las identidades, frecuentemente se ocupa de las siguientes tareas:

- Aprovisionamiento de cuentas de usuario y contraseñas, mediante automatismo, de acuerdo con políticas bien definidas y aplicadas.
- Implantación de sistemas de identificación de identificación única corporativa (*single sign-on*).
- Gestión centralizada de las atribuciones de los usuarios, basada en directorios de usuarios.
- Modelo de autorizaciones, que concentra en un solo punto las autorizaciones de acceso.

La necesidad de negocio que cubre la gestión de identidad es facilitar y controlar de forma eficiente los sistemas de identificación y autenticación, acceso y auditoria (AAA) que emplean las organizaciones en sus procesos basados en tecnologías de la información.
Muchas entidades, tanto públicas como privadas, se enfrentan al problema de la gran proliferación de diferentes mecanismos de identidad digital, y de la aparición de un gran número de proveedores

- Contraseñas, contraseñas dinámicas, contraseñas de un solo uso, USB tokens, smart cards, ...
- PKI emitidos por diferentes prestadores, bien a trabajadores públicos y a ciudadanos, en entornos de movilidad y de tramitación a distancia.
- Identificaciones electrónicas nacionales (DNI-e y otros).
- Aserciones de autenticación remotas/delegadas basadas en SAML,...
- Federaciones de identidades y modelos de gestión de confianza.

Federación de identidades, ¿de qué estamos hablando?

Una federación es un esquema de confianza que permite la colaboración entre los miembros de la federación para el intercambio de usuarios y aplicaciones, aportando interoperatibilidad entre los diferentes miembros, y la re-usabilidad de las identidades emitidas por los diferentes proveedores de identidades de la federación.

- Un proveedor de identidad (idP) establece identidades y distribuyen datos sobre ellas, en un entorno local y bajo control del usuario.
- Un proveedor de servicio (sP) recibe los datos de los idP, y, en función de su valor, establecen los derechos de acceso a los servicios y personalizan las aplicaciones.

Gracias a la implantación de una federación y la definición de un círculo de confianza, se consiguen tres hechos que aportan valor a un sistema de gestión de identidades:

- Movilidad de los usuarios y la integración y personalización de las aplicaciones.
- Privacidad activa, el control de sus identidades lo ejerce el usuario.
- Simplificación de la gestión, mejorando la usabilidad de los procesos de identificación y autenticación.
- Autenticación delegada e integración de directorios.

A la implantación de las federaciones de identidades, se ha de sumar las tendencias generales de futuro que van apareciendo:

- Interación de los sistemas de gestión de identidad en los procesos de negocio:
    - Superación de la tendencia de integración o sincronización en 'directorios únicos'.
    - Tendencia a esconder los directorios de las organizaciones
    - Aparición de aplicaciones intermedias (middleware) para integrar aplicaciones y lógicas de negocio que requieren identificación.
    - La identidad y la prueba de autenticación han de seguir a los documentos electrónicos, de forma desconectada de los directorios de la organización.
- Orientación a la gestión distribuida del control de acceso, distribución de identidades y gestión de atributos:
    - Absorción de la gestión del control de acceso para las aplicaciones de gestión de identidad,
    - Aparición de protocolos de negocio orientados a gestionar de forma altamente distribuida el control de acceso.
    - Necesidad de protocolos estándares para la gestión de federaciones de identidades
    - Necesidad de protocolos para un control de acceso distribuido

En resumen, la administración-e ha de pensar no solo en gestionar las identidades de los usuarios, sinó que ha de ir más allá, y debe pensar en gestionar sus capacidades, conocer quién es, qué puede hacer y cuándo lo puede hacer.

Gestión de personas = identidades + capacidades

La gestión de personas, resuelve no solo la autenticación, acceso y auditoria en los sistemas de información, sino que también resuelve qué puede hacer, resuelve si una persona posee las capacidades necesarias para realizar un trámite, acto o procedimiento.

La solución al problema que se plantea, aporta nuevas necesidades que no se contemplaban en un sistema de gestión de identidades ni una federación de identidades:

- Políticas necesarias para la realización de los trámites, indicando las capacidades necesarias que debe reunir una persona y la lógica suficiente para definir la realización de un trámite, acto o procedimiento.
- Sistema de acreditación o alegación de facultades:
    - ímplicitamente dentro de la credencial de autenticación de la persona,
    - mediante apoderamientos, poderes, sentencias judiciales,

- mediante aserciones SAML por parte de proveedores de capacidades.
- Sistema de resolución de capacidades asociadas a un usuario:
  - mecanismos automáticos,
  - servicios inteligentes de inferencia semántica,

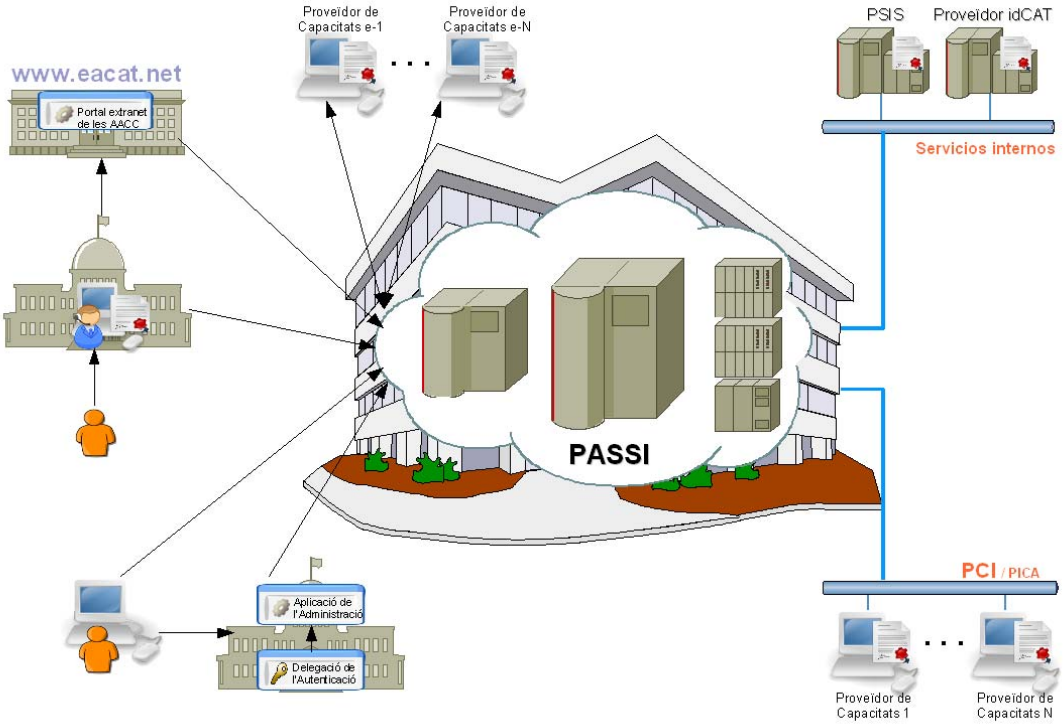

Figura 1. Visión general de la plataforma PASSI.

  - consulta a proveedores de capacidad externos.

- Sistema de control de privacidad de datos personales por parte de la persona:
  - asociación o redes de identidades,
  - políticas de autorización de consulta de identidades,
  - políticas de autorización de uso de identidades, que denominaremos políticas de representación,
  - gesión de identidades, alegaciones y atributos.
- Sistema de vinculaciones a entidades, empresas o administraciones.
  - capacidad de representación a una empresa o entidad.

Se comprueba el número de sistemas o mecanismos adicionales que se necesitan para un gestor de personas, un gestor de personas donde debe ser prioritario, esencial, el control de privacidad de datos personales por parte de las personas. A este gestor de personas le denominaremos PASSI.

La Plataforma de Atributos de Seguridad y Firma Electrónica (PASSI)

Partiendo de la tecnologías de base existentes en cuanto a firma electrónica y atribuciones, CatCert ha diseñado y se encuentra implantando la Plataforma de Atributos de Seguridad y Firma Electrónica (PASSI), con el objetivo de cubrir las anteriores necesidades, con base en los servicios de identidad y validación semántica de CatCert, ofrecidos por la Plataforma de Servicios de Identidad y Firma Electrónica (PSIS), que además obtiene y archiva las correspondientes evidencias electrónicas.
En la figura 1 se muestra una visión general de la plataforma PASSI, y cómo se relaciona con los diferentes actores que intervienen, y los diferentes sistemas con quién colabora.
En la figura 2 se muestra la arquitectura básica de la plataforma, teniendo una arquitectura habitual de una solución SOA, donde en la capa de negocio nos encontramos con 4 bloques básicos:

- Single Sign-on, donde se resuelven todos los procesos relacionados con el aprovisionamiento de identidades, autenticación y autorización de acceso a los servicios que ofrece la plataforma.
- Control de privacidad, donde se resuelven todos los procesos relacionados con la gestión de identidades por parte de la persona propietaria y las algeciones de capacidades, así como la gestión de autorizaciones y representaciones por parte de una persona. Y los procesos relacionados con la gestión de entidades y vinculaciones de personas a las entidades.
- Actos y procedimientos, donde se resuelven todos los procesos relacionados con la resolución de capacidades de las personas, consultando, si es necesario, a proveedores de capacidades externos.

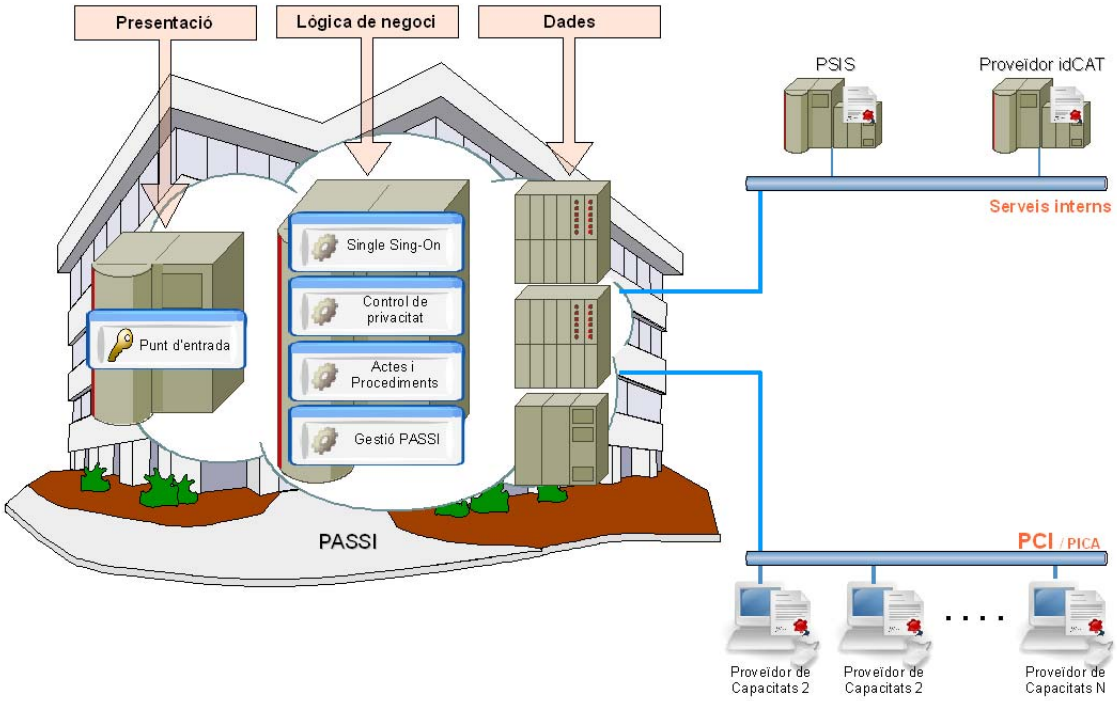

Figura 2. Arquitectura básica de la plataforma PASSI.

- Gestión de PASSI, donde se resuelven todos los procesos de gestión y configuración de PASSI, como puede ser la replicación de directorios, definición del círculo de confianza, etc...

De los cuatro bloques indicados, los módulos para el control de privacidad y actos y procedimientos son los más interesantes por su singularidad.

Identidades

Las identidades se corresponden a los actores activos y pasivos de PASSI, es decir, a todas aquellas personas fisicas o jurídicas que de alguna forma interactuan con PASSI:

- usuario, corresponde a una identidad digital de una persona física, teniendo como característica principal que puede ser utilizada para autenticarse en PASSI, y poder gestionar la privacidad de los datos.
- entidad, corresponde a una identidad digital de una persona jurídica (empresas, comunidades de propietarios, organismos y administraciones públicas, proveedores de capacidades, etc...). A diferencia que un usuario, una entidad no puede ser utilizada para autenticarse en PASSI.
- alegación, corresponde a una identidad digital de una persona física, no pudiendo ser utilizada para autenticarse en PASSI, es decir, no contiene ningún mecanismo de autenticación.
- aplicación, corresponde a una identidad digital vinculada a una persona jurídica, siendo utilizada para autenticar aplicaciones que interactuan con

PASSI, aplicaciones de administraciones que utilizan los servicios ofrecidos por PASSI.

Relaciones entre identidades

Los cuatro tipos de identidades indicadas se relacionan entre ellas,

- asociaciones o redes de identidades, donde una persona puede asociar diferentes identidades (usuario o alegación) registradas en PASSI, permitiendo la compartición de atributos entre las identidades miembro de una misma red.
- agrupaciones, donde la administración de PASSI define perfiles de uso para las personas. Para cada agrupación se define, una política de acceso, una política de credibilidad de la información, una lista de administraciones que son miembro de una agrupación, y una lista de trámites que se pueden realizar.
- autorizaciones, donde un usuario permite el acceso a sus identidades, autoriza la consulta de su información por parte de las administraciones que decida.
- representaciones, donde un usuario permite el acceso a sus identidades, autoriza el uso de sus capacidades a otro usuario para que realice un trámite en su nombre.
- vinculaciones, donde el representante legal de una entidad vincula personas a la entidad, indicando un cargo, función o capacidad de representación hacia la entidad.

Con este conjunto de relaciones entre identidades se consigue dar respuesta a las necesidades de la plataforma PASSI para la gestión de personas. Se da ofrecen los mecanismo necesarios para un control absoluto de la privacidad de los datos personales por parte de una persona.

Resolución de capacidades

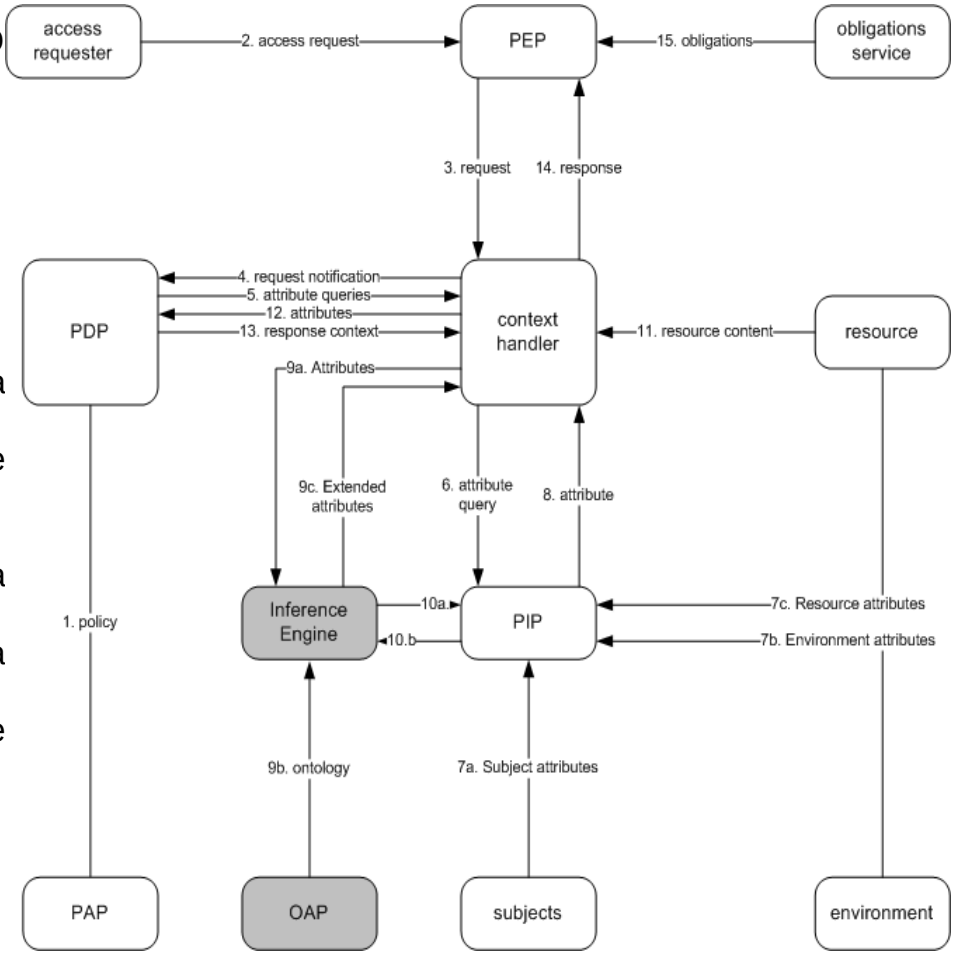

Figura 3. Esquema XACML modificado.

Para la resolución de capacidades se ha adoptado una extensión de la arquitectura XACML con técnicas de web semántica, tal y como se muestra en la figura 3. De esta forma, los trámites, actos y procedimientos serán descritos mediante el estándar de definición de políticas XACML.

El proceso seguido para la resolución de capacidades es el siguiente:

1. se resuelve la capacidad directamente de la información extraída de la identidad autenticada, es decir, la identidad que interactua con PASSI.
2. si no se consigue, se comprueba en la red de identidades donde es miembro la identidad actual, consultando tanto los atributos de los usuarios como de las alegaciones.
3. si no se consigue resolver, se intenta inferir a partir de toda la información que alberga la rede de identidades donde es miembro la identidad actual. Para realizar esta inferencia es necesario un modelo semántico, un mecanismo que nos modela a la persona física.
4. si no se consigue, se consulta a un sistema experto que nos indica a qué proveedor de capacidades acceder para consultar o adquirir la capacidad necesaria para poder realizar el acto o procedimiento.

Este proceso de resolución de capacidades de una persona requiere la colaboración de sistemas externos, de proveedores de capacidades externos, que PASSI resuelve a través de la infraestructura de PCI.

Seguridad en PASSI

Es obvio que la seguridad en una plataforma de la naturaleza de PASSI es esencial, ya que la información que se mantiene es altamente sensible, de nivel alto según la LOPD. Este hecho crea la necesidad de aplicar e implantar una política de seguridad por niveles:

- aplicación de seguridad en todas las capas
  - firmado XML
  - túneles SSL para la transmisión de la información, realizando el proceso de autenticación de parte del servidor y del cliente.
  - certificados de autenticación, y políticas de acceso en función de la calidad del certificado utilizado,
  - encriptación de los datos de carácter personal.
- Seguridad de las aplicaciones
  - LOPD, todos los artículos que afectan
  - auditoria de código fuente,
  - auditoria mediante caja negra.
- Seguridad en la infraestructura
  - ubicación de la maquinaria necesaria,
  - control físico,
  - control lógico,
  - copias de seguridad y respaldo,
  - planes de contingencia,
- Registros de auditoria
  - transacciones firmadas,

Conclusiones

En la presente comunicación se ha presentado la plataforma PASSI para la gestión de personas. La gestión de personas es uno de los aspectos clave en el futuro de la tramitación por medios electrónicos, especialmente en el modelo europeo.

PASSI es la experiencia real de un gestor de personas definido por CatCert, y que colabora con otros sistemas e infraestructuras de la administración pública catalana, como son PSIS y PCI, con el único fin de alcanzar una administración electrónica pública eficaz, simplificando el proceso actual, ahorrando consultas innecesarias, y actuando en beneficio del ciudadano.

Finalmente, remarcar que la esencia de PASSI es salvaguardar la privacidad de los datos personales de los usuarios, que la persona tenga el control absoluto de sus datos personales, y para ello se le ofrecen sistemas de gestión como son

las asociaciones o redes de identidades, agrupaciones, autorizaciones, representaciones o vinculaciones.