tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

228

LA GESTIÓN DE IDENTIDADES Y CAPACIDADES POR LAS ADMINISTRACIONES PÚBLICAS

Ignacio Alamillo i Domingo
Director de asesoría e investigación
Agència Catalana de Certificació

Xavier Urios i Aparisi
Subdirector general de servicios consultivos y coordinación jurídica
Gabinete Jurídico de la Generalitat de Catalunya

Palabras clave

Gestión de identidad y del acceso, contraseña, firma electrónica, certificación electrónica, SAML, XACML, directorio de ciudadanos y empresas, relaciones de representación, poderes de representación, facultades de actuación, plataforma de atributos de seguridad y firma electrónica, plataforma de servicios de firma.

Resumen de su Comunicación

Cualquier relación jurídica parte de la plena identificación de las personas o entidades entre las que esta relación se establece. En este ámbito, las tecnologías de la información han supuesto un claro avance, al permitir la identificación telemática en el tráfico jurídico, ya sea público y privado.

Los modelos de identidad o certificación única se encuentran superados, encontrándonos hoy en día con el fenómeno de la multiplicación de mecanismos de identificación. Esto ha derivado en una complejidad que ha de ser superada, y que ha de llevar al establecimiento de mecanismos de gestión de la identidad que supongan una simplificación; pero, al mismo tiempo, no hemos de quedarnos en este primer paso, sino ir más allá, aprovechando las potencialidades de las tecnologías de la información, e introduciendo mecanismos de gestión de la capacidad de actuar de las personas, que permitan liberar a éstas de su acreditación ante la correspondiente Administración Pública.

El establecimiento de un sistema de gestión de identidades y capacidades por las Administraciones Públicas supone un beneficio para el administrado, una adecuada gestión y simplificación administrativa, y un avance en la protección y mejora de los derechos de los ciudadanos frentes a aquellas. Evidentemente, sin pérdida de garantías jurídicas.

Ignacio Alamillo i Domingo
Xavier Urios i Aparisi

LA GESTIÓN DE IDENTIDADES Y CAPACIDADES POR LAS ADMINISTRACIONES PÚBLICAS

1. La concepción "clásica" de la gestión de la identidad y del acceso

La gestión de la identidad y del acceso, frecuentemente conocida por su acrónimo anglosajón IAM (por "Identity and Access Management") es un área de negocio que se dedica a las siguientes tareas:

- Aprovisionamiento de cuentas de usuario y contraseñas, mediante automatismos, de acuerdo con políticas bien definidas y aplicadas.

- Implantación de sistemas de identificación y autenticación única corporativa (también denominado "single sign-on").

- Gestión centralizada de las atribuciones de los usuarios, basada en directorios de usuarios (habitualmente basados en LDAP).

- 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.

La realidad tecnológica de las infraestructuras que ofrecen soporte a los procesos de tecnologías de la información, instaladas tanto en el sector público como en el sector privado, indica que una parte muy importante de los sistemas únicamente pueden utilizar sistemas basados en contraseñas.

No parece, sin embargo, que este obstáculo sea insuperable, y de hecho la industria de las tecnologías de la información ha provisto una serie de soluciones tecnológicas al problema, de las cuales las incluida en la categoría de gestión de la identidad y del acceso son las más completas.

Muchas entidades, públicas y privadas, en efecto, se enfrentan al problema de la proliferación de cuentas de usuario y sus correspondientes contraseñas, fenómeno que deriva de la necesidad, impuesta a veces de forma artificial por muchas aplicaciones y sistemas, de tener que disponer de una cuenta de usuario y una contraseña para cada aplicación y sistema con el que se trabaja. Esta situación resulta difícil de controlar, ya que cada proveedor de la Administración dispone de su propia tecnología, decidiendo si utiliza o no autenticación certificada. Por el contrario, el factor de decisión para la compra del producto ha de ser su funcionalidad y calidad, y no tanto el sistema de autenticación empleado.

A esta situación hay que añadir la presión legal que supone la aplicación estricta de las leyes de protección de los datos de carácter personal, que ha obligado a un detallado control de acceso, incrementando aún más la aparición de cuentas de usuario y contraseñas. Curiosamente en estos casos, incluso con aplicaciones nuevas, los proveedores – y ésta parece ser también la opinión de algunas Administraciones Públicas, quizá reflejando las opiniones de los técnicos de sector privado – apuestan por el uso de sistemas basados en contraseña, y no en certificados, con el argumento de que "no se trata de aplicaciones donde haya que firmar nada". En definitiva, hemos de partir de la base de que muchos sistemas ya instalados, y muchos de los sistemas que se instalarán, precisarán en el futuro aceptar mecanismos de contraseña, tanto en el sector público como en el sector privado.

La evolución de este tipo de producto ha requerido ofrecer cada vez más funciones relacionadas con la seguridad, pasando de ofrecer soluciones estrictamente de gestión de la identificación y posterior autenticación (única) de los usuarios, a ofrecer soluciones centralizadas de las autorizaciones y permisos de dichos usuarios, así como registro centralizado de los accesos (audit, en inglés).

Hay que decir, para concluir este punto, que la mayoría de fabricantes que producen soluciones de gestión de identidad han integrado, aunque parcialmente, la gestión de la certificación digital de clave pública.

2. La gestión de la identidad en las políticas públicas

Las tendencias generales de futuro, a partir de las premisas anteriores, son las siguientes:

- Incremento de la complejidad de la identidad digital.

    - Contraseñas, contraseñas dinámicas, contraseñas de un solo uso, con base en bienes de equipo portátiles (como un token USB).

    - Certificados digitales X.509 de identidad, emitidos por diversos prestadores, bien a trabajadores públicos y a ciudadanos, en especial en entornos de movilidad y de tramitación a distancia.

    - Identificaciones electrónicas nacionales (DNI y otros).

    - Tiques de autenticación remota/delegada, basados en manifestaciones SAML, Liberty o Shibboleth, que penetran con fuerza para integrar trámites en un entorno de trabajo distribuido.

    - Federaciones de identidades y modelos de gestión de la confianza.

- Alineación de la gestión de identidad con la integración de procesos.

    - Superación de la tendencia de integración o de sincronización en “directorios únicos”.

    - Tendencia a esconder los directorios de las organizaciones (menos LDAP, más consulta vía servicios web).

    - Aparición de aplicaciones intermedias (middleware) para integrar aplicaciones y lógicas de negocio que requieren identificación.

    - La identidad y la prueba de la 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.

    - Absorción de la gestión del control de acceso para las aplicaciones de gestión de identidad, como tendencia del mercado: se aporta más valor con una solución única, con base en el directorio central de autorizaciones.

    - Aparición de protocolos de negocio orientados a gestionar de forma altamente distribuida el control de acceso: permitirá que diferentes soluciones de gestión de la identidad colaboren en procesos, con base en servicios web (XACML).

Como tendencias específicas del sector público, podemos mencionar las siguientes:

- Incremento de la adopción de la gestión de la identidad como herramienta interna de base.

  - Cada vez más entidades públicas se dotarán de un gestor de identidad y acceso como herramienta de base para su gestión interna de los usuarios.

  - El incremento de movilidad y de accesos remotos, derivados de la teletramitación de procedimientos administrativos, creará nuevas necesidades de gestión de usuarios externos.

  - El acceso de los ciudadanos a los procedimientos administrativos por Internet también incrementará, y de forma exponencial, el número de identidades a gestionar por las entidades públicas.

- Penetración de la gestión de la identidad dentro de los programas de e-gobierno.

  - Percepción de que la gestión de la identidad puede ayudar de forma importante a la prestación de servicios públicos, especialmente en el entorno comunitario.

  - Iniciativas de alcance europeo como FIDIS y MODINIS consideran la gestión de la identidad como la solución a la integración de trámites a escala europea, de forma interoperable, especialmente a tenor de las identificaciones nacionales y regionales electrónicas.

  - El proyecto GUIDE, construido sobre la iniciativa IDABC de la Comisión Europea, trabaja actualmente en perfiles y mensajería basados en SAML para integrar todas las identidades europeas.

Las anteriores iniciativas realmente apuntan a la gestión de identidad, en una concepción nueva, basada en modelos de delegación y federación, como la mejor posibilidad para la interconexión de los servicios de las Administraciones Públicas Europeas, al objeto de realizar la libre circulación de las personas físicas y una mayor eficiencia en el mercado interior, al tiempo que se reducen los costes burocráticos y se incrementa la lucha contra el fraude.

3. El impacto de la gestión de la identidad sobre la actividad de los prestadores de servicios de certificación

La Agència Catalana de Certificació (CATCert), al igual que otros prestadores de servicios de certificación, inició su modelo de negocio con un enfoque parcial a la solución de la problemática de la identidad, suministrando certificados electrónicos reconocidos, con o sin tarjeta, que permiten la identificación y autenticación – sin necesidad de contraseña, e incluso sin la necesidad de cuenta de usuario, en algunos casos – frente a les aplicaciones corporativas y, en especial, frente a les aplicaciones basadas en las tecnologías de Internet, como los servidores web y los servicios web de aplicación. Dicha función de identificación y autenticación ofrece un grado superior de seguridad y confianza al uso de contraseñas, permitiendo además los certificados la firma electrónica avanzada y, en su caso, reconocida.

En concreto, en el caso de los prestadores públicos de servicios de certificación, de los que CATCert resulta buen ejemplo, la estrategia hasta la fecha ha consistido en la capacitación de los órganos administrativos y de los trabajadores de las Administraciones Públicas para poder firmar documentos electrónicos y, por otra parte, la sustitución de las habitualmente inseguras contraseñas por el infalsificable certificado digital en tarjeta.

En la ejecución de esta estrategia, los prestadores de servicios de certificación y CATCert en concreto, han recibido cada vez más solicitudes para incorporar servicios relativos a la gestión de la identidad, entre los

que podemos mencionar los siguientes:

- Las Administraciones, en primer lugar, solicitan que el servicio de identificación y autenticación prestado por CATCert sea global, válido para todos los tipos de credenciales, y no sólo para certificados digitales.

- En segundo lugar, las Administraciones solicitan implantar procedimientos de autenticación única con certificados, en sus aplicaciones (single sign-on), corporativas o a través del web.

- Otras Administraciones solicitan integrar también la autenticación al sistema operativo Windows, mediante la funcionalidad denominada "smart card logon" que ofrece la tarjeta de firma electrónica, integrando todo el proceso de gestión de la identidad corporativa de su personal.

- En un estadio más avanzado, aparecen Administraciones que desean que los usuarios puedan acceder por vía telemática con mecanismos de autenticación delegada, para realizar trámites de forma integrada (por ejemplo, iniciados en un Ayuntamiento y continuados en la Generalitat), lo que requiere implantar federaciones de identidades y otros mecanismos de autenticación delegada.

- Finalmente, hay que decir que las Administraciones ya han asumido que el sistema de autenticación debería estar altamente integrado con sistemas centrales de gestión de autorizaciones y de acceso, y que parte de estos procesos podrían ser, en si mismos, delegados a terceros (por ejemplo, cuando se requiere comprobar la firma de una persona, y que consta inscrita como representante en un registro público), antes de decidir sobre su acceso al sistema o recurso correspondiente (preautorizaciones).

En definitiva, la creciente complejidad y sensibilidad de los tratamientos informatizados de la identidad, incluyendo contraseñas y certificados de todos los tipos, en el contexto europeo de libre circulación ciudadana y empresarial, ha hecho ciertamente atractiva a las Administraciones Públicas la posibilidad de concentrar la gestión de todas las identidades en su prestador público de servicios de certificación, como es el caso de CATCert.

4. Más allá de la gestión de identidad. La gestión de capacidades como técnica de simplificación administrativa

Si bien la gestión de identidad representa una oportunidad importante para las Administraciones Públicas y para los prestadores de servicios de certificación, no es menos cierto que la regulación de los trámites y procedimientos administrativos realizados mediante las tecnologías de la información y la comunicación (TIC) no ha de limitarse a una simple reproducción o adaptación del elemento presencial en la utilización de estos nuevos medios, sino que se han de aprovechar al máximo las posibilidades que los citados medios ofrecen a los efectos de, con pleno respeto al principio de seguridad jurídica, se pueda establecer un marco jurídico que no sólo asegure y fomente la utilización de las TIC, sino que también resulte eficiente y ventajoso para la Administración y el ciudadano y la empresa.

Precisamente los últimos avances de las TIC, y en especial los producidos a tenor de la "web semántica", que se relacionan directamente con el uso de las firmas digitales, ofrecen oportunidades reales para eliminar la necesidad de solicitar a los ciudadanos y empresas los documentos acreditativos de sus facultades y capacidades (en especial, derivadas de apoderamientos voluntarios y de situaciones orgánicas, como los cargos en las empresas y otras entidades), y posteriormente comprobarlos.

En definitiva, se trata de pasar de un modelo en que simplemente se gestionan las diferentes identidades de los ciudadanos y empresas, a un modelo en que se gestionan, además, sus diferentes capacidades de actuación.

Conseguir implantar estas tecnologías y métodos en los procedimientos administrativos supondrá una importante simplificación en la tramitación formal, así como una considerable reducción de los documentos que forman el expediente, sin ninguna reducción de las garantías jurídicas, lo que justifica este cambio de paradigma, que supone el paso de la gestión de la identidad a la gestión de las capacidades jurídicas personales.

Este paradigma, novedoso, precisa tanto de elementos técnicos, que se construyen sobre las tecnologías de base de la firma electrónica y la gestión de la identidad, cuanto de elementos de organización, dirigidos a la concreta disposición y organización de los medios materiales de que dispone la Administración, con el objeto de alcanzar la total eliminación de los documentos (en papel o electrónicos) que ofrecen prueba, dentro de los expedientes, de la identidad del ciudadano o empresa, y de su capacidad para actuar en el procedimiento.

Los procesos de gestión de capacidades se prestan a partir de la gestión de la identidad, por su propia naturaleza, como puede verse en el siguiente proceso, basado en las plataformas tecnológicas ofrecidas por CATCert:

- El ciudadano o empresa presenta su solicitud o escrito por cualquier canal, sea el presencial o por vía electrónica, sin aportar ningún documento acreditativo de su capacidad de obrar o facultad para actuar ante la Administración. La solicitud o el escrito han de estar firmados electrónicamente, en todo caso.

- La Administración acredita la identidad del ciudadano o empresa, mediante la comprobación de su firma electrónica basada en su certificado digital, empleando la Plataforma de Servicios de Identidad y Firma (PSIS) de CATCert.

- La Administración, a partir de esta primera comprobación, delega a la Plataforma de Atributos de Seguridad y Firma Electrónica (PASSI) de CATCert la resolución de la capacidad para el acto concreto.

- PASSI genera tantas solicitudes electrónicas de comprobaciones adicionales sobre el ciudadano/solicitud como sean necesarias par determinar su capacidad, y las remite a los órganos competentes, como podrán ser por ejemplo:

  - Notarios públicos, mediante el sistema ACAFE, incluyendo los poderes/facultades de representación generales y particulares.

  - Registros mercantiles o de la propiedad, incluyendo poderes de representación inscribibles y facultades orgánicas.

  - Registro civil, incluyendo las relaciones de representación legal.

  - Registros de otros organismos, como las asociaciones, fundaciones, cooperativas, entidades religiosas, incluyendo, según proceda, poderes de representación inscribibles y facultades orgánicas.

  -Registro central de asegurados del CATSalut.

- Los mencionados órganos serán los que, en el ámbito de sus competencias, decidirán si la persona se encuentra capacitada para aquel trámite en relación con el que se les pregunta, y responderán en sentido afirmativo o negativo, pero sin necesidad de entregar documentación acreditativa que forme parte del expediente de la Administración solicitante (ni de CATCert), ya que sus registros informáticos de consulta sustituyen esta parte del expediente, integrando la tramitación y simplificando la gestión del expediente por parte de la Administración que actúa.

- CATCert unifica todas las respuestas y, en función de la política indicada por la Administración, informa a la Administración sobre si la persona se encuentra capacitada o no para el acto, sin perjuicio de la decisión final, que siempre corresponde a dicha Administración.

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

La implantación del modelo de gestión de identidades y capacidades requiere el desarrollo de una plataforma específica, partiendo de las 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, también conocida como 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.

5.1. Funcionalidades principales de PASSI

PASSI ofrece soporte técnico a las siguientes funcionalidades de gestión de identidades y capacidades:

- Almacena las identidades que han sido aprovisionadas por CATCert, mediante sus diferentes servicios (incluyendo contraseñas y certificados), que serán empleadas en procedimientos de autenticación única (single sign-on) o autenticación federada (Liberty o SAML), o en procedimientos de firma electrónica.

- Almacena y relaciona las identidades aprovisionadas por terceras entidades, públicas y privadas, de forma que el usuario puede decidir qué identidades emplea para cada caso y entidad (identidad federada).

- Permite la carga de información de representantes, actuando como depósito de información del futuro Gestor de Representaciones de CATCert.

- Permite la gestión de perfiles, roles y relaciones de representación de los usuarios, y la asignación de autorizaciones de acceso a los sistemas, de acuerdo con el modelo de datos de PASSI y con las políticas de seguridad correspondientes, así como el registro de aserciones de acceso con garantía de sellado de fecha y hora.

- Permite integrarse con directorios de usuarios, mediante procedimientos de replicación, sincronización y federación, dentro de un concepto amplio de metadirectorio de ciudadanos y empresas.

- Permite que las Administraciones Públicas deleguen a CATCert partes del proceso de decisión del control de acceso a los sistemas, aplicaciones y recursos, incluyendo registros públicos, mediante el empleo del estándar XACML. En este caso, la Administración realiza a CATCert una pregunta del tipo "¿puede hacer esta identidad este acto en nombre de?".

5.2. El modelo de datos de PASSI

Para ofrecer dichos servicios, PASSI hace uso de un modelo de web semántica aplicada a la gestión de la identidad y las capacidades, basado en estándares internacionales, con los siguientes objetos:

- Persona.
- Relación.
- Entidad.
- Facultad.
- Acto.
- Procedimiento.

El objeto "Persona" describe cualquier identidad de una persona física. Puede tratarse de una identidad basada en nombre de usuario/contraseña o en certificado. Cuando la identidad se basa en nombre de usuario/contraseña, debe tratarse de una identidad suministrada por CATCert. Caso contrario, la representación se limita a una credencial SAML (los datos de identificación de la persona dentro del elemento "Subject" de la manifestación, asociado al emisor de dicha identidad, que debe figurar en el documento SAML como "Issuer" de la manifestación. Cuando la identidad se basa en un certificado, puede haber sido generada por cualquier prestador de servicios de certificación.

El objeto "Entidad" describe cualquier identidad de una entidad diferente de una persona física. Habitualmente se trata de instituciones, personas jurídicas públicas y privadas, y entidades sin personalidad jurídica propia. Las "entidades" no actúan en el tráfico, sino que lo hacen a través de personas físicas, como viene siendo tradicional en nuestro sistema jurídico.

El objeto "Relación" describe una relación concreta entre dos personas o una persona y una entidad. Comprende los objetos correspondientes, e información adicional sobre la relación. Cuando resulta pertinente, como en los casos de representación voluntaria, la relación indica la lista de facultades concretas para las que resulta válida la relación. En principio se consideran los siguientes tipos de relaciones, aunque el esquema ha de permitir establecer tipos adicionales:

- Relación basada en la simple vinculación entre la persona y la persona/entidad.
- Relación basada en la representación legal entre la persona y la persona/entidad.
- Relación basada en la representación orgánica entre la persona y la persona/entidad.
- Relación basada en la representación voluntaria entre la persona y la persona/entidad.
- Relación basada en la representación presunta entre la persona y la persona/entidad.

El objeto "Facultad" describe una facultad concreta de una persona, establecida por una autoridad concreta. Dicha autoridad puede ser, por ejemplo, una Administración Pública, un Notario u otra semejante. Las facultades pueden presentar límites, resultando necesario definir los tipos de límites.

El objeto "Acto" describe una acción concreta, un trámite a realizar. Se relaciona con los anteriores, de la siguiente forma:

- Acto realizado por una persona P, en su propio nombre y representación.
- Acto realizado por una persona P para otra persona P en virtud de una relación R (PRP).
- Acto realizado por una persona P para una entidad E en virtud de una relación R (PRE).

El objeto "Procedimiento", finalmente, describe series ordenadas de actos, en forma de flujos de trabajo.

Hay que remarcar que PASSI no es un depósito único de identidades y facultades, no sólo por su complejidad técnica, sino especialmente por la compleja cobertura legal que requeriría. Por el contrario, PASSI se basa en el establecimiento de unas bases jurídicas, organizativas y técnicas que permiten la interconexión de diversos registros pertenecientes a diferentes sujetos públicos, definiendo los procedimientos de consulta en línea de las facultades, con pleno respeto a la finalidad del registro público y a la protección de los datos de carácter personal.

Por otra parte, este modelo permite la evolución de los modelos de negocio de los diferentes proveedores de la información, superando la aún existente dicotomía copia simple/certificado, con efectos jurídicos diferentes (así como, en algunos casos, tasas o aranceles diferentes) que, además, únicamente ofrecen garantía en relación al momento inmediatamente posterior a la emisión de la copia o certificado (sin perjuicio de la presunción de vigencia que pueden llevar aparejada).

6. Conclusiones

La gestión de la identidad es uno de los aspectos clave en el futuro de la tramitación por medios electrónicos, sin duda alguna, especialmente en el modelo europeo e internacional.

Lejos quedarán los modelos de contraseñas o certificados únicos, arrollados por la realidad de diferentes identidades, como los DNI electrónicos nacionales, las licencias profesionales o las tarjetas de servicios municipales y de servicios de salud.

Por tanto, las Administraciones se mueves con ritmo rápido a la gestión de toda forma de identidad útil, y en concreto, a la gestión federada de dichas identidades.

Sin embargo, hay que dar un paso más, hacia la gestión de las capacidades, de forma distribuida y en corresponsabilidad con todas las Administraciones y otras entidades involucradas en dicha gestión.

La adopción de un sistema de gestión federada de las capacidades supone un avance frente al modelo actual, ineficiente y de dudosa utilidad en el mundo de las redes interconectadas. Se trata de establecer un modelo de acreditación de la identidad y capacidad de vigencia continuada en el tiempo, en que la capacidad de la persona acreditada por el registro que así lo ha comunicado a la Administración despliega todos sus efectos jurídicos mientras no se modifique o revoque aquella por cualquiera de las causas previstas legalmente.

Esto supone ser eficaz, simplificando el sistema, ahorrando consultas innecesarias, y actuando en beneficio del ciudadano, sin merma de garantías.
Finalmente, posiblemente cabe ver en estas actividades la mayor línea de expansión y de crecimiento de los prestadores públicos de servicios de certificación, que están llamados a convertirse en los expertos en la simplificación de los expedientes administrativos por supresión de los trámites de comprobación de identidades y capacidades.