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

Comunicación

310

MODELO CATALAN. LA AGENCIA CATALANA DE CERTIFICACIÓ

Jordi Masias
Director General
CATCert

Josep Torres
Coordinador
CATCert

Emma Suevos
Directora de Calidad y Procedimientos
CATCert

Ignacio Alamillo
Director de Asesoramiento
CATCert

Jordi Masias
Josep Torres
Emma Suevos
Ignacio Alamillo

Palabras clave

Firma electrónica, certificado digital, seguridad, administración electrónica, confianza, validación, archivo seguro, integridad, confidencialidad, autenticidad, identidad digital, idCAT, Consorci AOC, interoperabilidad

Resumen de su Comunicación

El desarrollo de la administración electrónica viene muy condicionado a la confianza y a la legalidad de los trámites a través de Internet. La seguridad tanto legal como tecnológica es clave en este proceso. La aparición de la Agència Catalana de Certificació dentro del marco del Consorci AOC ha supuesto un paso adelante en el desarrollo de esta e-administración.

La provisión de identidades digitales a los ciudadanos, la emisión de certificados digitales a los empleados públicos, la utilización de los certificados digitales ya presentes en el mercado o los que van a venir (e-DNI), así como su validación están siendo elementos claves en la generación de esta confianza tan necesaria para que las administraciones públicas vayan trabajando en la prestación de servicios y trámites a través de la red.

Pero no solo es necesario garantizar la identidad, confidencialidad, integridad y autenticidad de los datos, sino que la gestión de los documentos electrónicos y su preservación empiezan a ser hoy en día la mayor preocupación de las administraciones públicas.

Jordi Masias
Josep Torres
Emma Suevos
Ignacio Alamillo

MODELO CATALAN. LA AGENCIA CATALANA DE CERTIFICACIÓ

1. Introducción

El uso de las tecnologías de la información en las relaciones entre la administración pública y los ciudadanos, así como en las relaciones interadministrativas, con el fin de facilitar la interacción y la transacción de servicios y procedimientos en línea, es un elemento clave para la mejora del funcionamiento de los servicios públicos.

Esta voluntad del uso de las tecnologías de la información en las administraciones públicas es ya palpable en la mayoría de éstas y, de hecho, últimamente se está hablando mucho del nivel de desarrollo de la Administración "on-line" y no sólo a nivel internacional, sino también aquí en España.

Las distintas administraciones han estado trabajando últimamente en la puesta en marcha de la Administración "on-line" La realidad, de todas formas, indica que el grado de desarrollo de ésta es muy diferente según las administraciones y los recursos que las mismas invierten.

Para comparar el grado de desarrollo de la administración electrónica, hemos definido tres niveles de presencia en la red de éstas, niveles que también se podrían aplicar a otras instituciones o empresas privadas.

Este criterio de niveles permite clarificar las dificultades que tienen las administraciones para pasar de un nivel al otro y evidentemente, como a la Agència Catalana de Certificació nos permite medir los esfuerzos y servicios que podemos ofrecer a las administraciones para facilitar su desarrollo.

NIVEL 1.- La administración está presente en la red, tiene una web y unas direcciones de correo electrónico desde donde el ciudadano se puede comunicar con la administración. No hay servicios personalizados y no se conoce o no se tiene garantía de la identidad del ciudadano que está accediendo a la web. Los servicios interadministrativos o internos que existen no permiten suprimir el papel en su totalidad. Hoy podemos decir que a nivel de Cataluña, prácticamente el 100% de las administraciones han adquirido este nivel.

NIVEL 2.- La administración, una vez adquirido el nivel 1, ha dado otro paso y contempla servicios y trámites personalizados y permite iniciar cierta tramitación. Aquí ya se ha conseguido garantizar la identidad del solicitante mediante algún mecanismo de autentificación (usuario y contraseña, utilización de "cookies", direcciones IP de otros servidores, de otras administraciones, etc.).

Las ventajas de conseguir este nivel son muy importantes para las administraciones, pues les permite traspasar a la red muchas comunicaciones que hasta este momento se hacían de manera presencial o a través del envío de documentación por correo. El principal problema de llegar a este nivel es la necesidad de la identificación previa de la persona que hace el trámite, ya sea un ciudadano, una empresa, otra administración o un trabajador de la administración. En estos momentos pocas administraciones catalanas, al igual que del resto de países, han conseguido alcanzar este nivel.

NIVEL 3.- La administración puede poner a disposición del ciudadano, vía telemática, cualquier trámite y servicio que ofrece de forma presencial. Este tercer nivel requiere ya no solo de identidad digital, sino de firma electrónica. Es necesario garantizar que la persona que realiza el trámite es realmente quién dice ser, pero para que esto tenga validez jurídica, es necesario garantizar el no repudio de trámite, o sea, la incorporación de la firma electrónica. También puede requerir unos mecanismos de comunicación segura interadministrativa, para facilitar al ciudadano los trámites (no se trata de pedir que aporten a la administración lo que ya tiene la administración). Muy pocas administraciones han conseguido este nivel.

Cuando la administración llega al nivel 2, pero muy especialmente al nivel 3, es muy importante tener en cuenta que, en materia de procedimientos, hace falta regular el marco jurídico general que debe permitir a las diferentes administraciones, dentro del ámbito de sus competencias, la aprobación de los procedimientos y actuaciones concretos en los cuales se pueda hacer uso de los medios electrónicos, informáticos o telemáticos, estableciendo, con carácter normativo, la validez de los documentos y de las comunicaciones telemáticas.

En el nivel 3 y para poder garantizar la identidad, la confidencialidad, la integridad, la disponibilidad, el no repudio y la conservación de los documentos, será necesario utilizar certificados digitales reconocidos o utilizar los sistemas o dispositivos que, a criterio de las administraciones, puedan garantizarlos.

Este hecho, así como la novedad de los requerimientos y de las herramientas, hacen imprescindible que las Administraciones Públicas se doten de mecanismos para garantizar el desarrollo de la Administración electrónica con todas las garantías jurídicas, técnicas y de seguridad necesarias.

2. Nuevo paradigma de la identidad digital y la firma electrónica

A diferencia de lo que habitualmente se considera, la firma electrónica es un objeto poliforme, que presenta aspectos muy diferentes en función del prisma des del que se observa. Esta cualidad, que ha generado tanto interés por ella en ámbitos diferentes, nos permite hablar de una serie de paradigmas y de evolución en el uso de la firma electrónica.

La firma electrónica nació en el primero de los ámbitos, el de la seguridad informática, a partir del uso de la criptografía de clave pública, como una posible solución a las debilidades de los sistemas de información asociados a la identificación y a la autenticación de los usuarios, especialmente basados en la confianza de los certificados a terceros.

Dentro de este paradigma nos encontramos con que el uso de la firma electrónica incluye la seguridad en el acceso a los servidores de Internet, la firma del software
a distribuir, la firma de solicitudes/respuestas de los llamados servicios web por aplicaciones informáticas que han de intercambiar información y, en menor grado, la firma producida por personas físicas, especialmente para proteger el correo electrónico y para sus trámites con las administraciones públicas.

Aún habiendo sido superado por otros, éste continua siendo el paradigma principal al cual nos referimos cuando hacemos referencia a la firma electrónica, y en este mismo paradigma hay que añadir los proyectos de identificación nacionales electrónicos emergentes en Europa (como el DNI electrónico español) que incorpora una firma electrónica. Fijémonos en el cambio dentro del paradigma que considera la firma electrónica como un aspecto de seguridad, que conduce a la obligación de disponer de la misma.

El segundo paradigma de la firma electrónica es el que la considera un elemento esencial de los documentos electrónicos y, por lo tanto, del patrimonio cultural de la sociedad. Se trata de un paradigma donde el valor de la firma electrónica no viene determinado por la seguridad que aporta, sino por la necesidad de que los documentos sean auténticos, atribuibles a las personas, "firmados" en el sentido cultural, jurídico, administrativo y histórico del término. Hablamos, por tanto, de la firma electrónica de personas físicas.

Dentro de este paradigma vemos que la firma electrónica ha penetrado, aunque tímidamente de momento, sobretodo en las administraciones públicas, a partir de la equiparación legal entre la firma electrónica y la firma escrita, de tal manera que el requisito legal del documento escrito y firmado se puede cumplir con una firma electrónica; aspecto que ha implicado la equiparación, cosa nada trivial, entre el ser humano y su agente electrónico, que es quien realmente firma por él. Que, a sensu contrario, implica por cierto que un documento, aún habiéndose producido y siendo conservado de forma muy segura, no tenga valor si no

está firmado.

El tercer paradigma de la firma electrónica está construido sobre el segundo, considerando la firma electrónica como un elemento de capacitación de las personas en el ámbito electrónico. De esta manera, se enriquece el concepto de firma electrónica para ir más allá de la identidad personal en sentido estricto y la firma electrónica incorpora de forma rápida otras condiciones o atribuciones concomitantes de la persona, como su capacidad de actuación (asociada a la edad o a la nacionalidad), su capacidad profesional (asociada a la condición de profesional acreditada por las corporaciones correspondientes) o laboral (asociada a los certificados empresariales) y, finalmente su capacidad de representar a otra persona, mediante la inclusión de poderes y facultades sobre personas físicas o jurídicas.

Este estadio supone la madurez de la firma electrónica como elemento de actuación personal en diferentes ámbitos de la vida pública y privada de una persona, y presenta la característica principal de "disponer de más de una firma electrónica", habiendo de elegir la más apropiada para cada acto a realizar. Supone la proliferación de prestadores de servicios de certificación, públicos i privados, y la inconveniencia de la reducción a la unidad; una explosión de certificados digitales que hay que aceptar i emplear en las relaciones electrónicas, públicas y privadas, que inaugura la era de las entidades de validación.

El cuarto paradigma, en el que empezamos a entrar en estos momentos, deriva de la existencia de una base suficiente de ciudadanos y ciudadanas capacitados electrónicamente para relacionarse con entidades públicas y privadas, lo que implica, de una parte, la posibilidad de dejar de solicitar cada vez la aportación documental exigida por cada organismo de su personalidad y capacidad, así como de sus facultades de representación; y, por otra parte, la posibilidad de integrar los procedimientos de negocio, tanto del sector privado como del sector público, posibilidades que genéricamente la industria califica como "gestión federada de las identidades".

En este estadio la firma electrónica se considera un enclave entre los dos mundos, real-físico y real-electrónico, de forma que el agente informático que representa el ciudadano adquiere las mismas capacidades frente a la administración o la empresa, lo que acentúa la incorporación de la firma electrónica a los documentos de legitimación, como la tarjeta sanitaria (que en algunos Estados ya incorpora el microchip con firma) o las licencias profesionales o de conducción

El quinto y último paradigma, al cual hay que considerar el más avanzado, considera la firma electrónica como un elemento absoluto de garantía de los derechos y libertades personales en una sociedad que cada vez dispone de más conexiones y accesos potenciales a la información personalmente identificable.

La firma electrónica supondrá que no haya excusa por no solicitar el debido consentimiento a los tratamientos de datos personales, reduciendo el número de casos en que resulta aceptable tramitar en base al consentimiento tácito. Igualmente, la gestión federada de la identidad permite ya hoy limitar los datos personales intercambiados, hasta el punto que se puede asegurar la identidad y la capacidad de una persona concreta en relación con un procedimiento administrativo de forma disociada del mismo, sin suministrar ningún dato personal, lo que invariablemente supondrá justificar con más rigor la necesidad de este intercambio de datos.

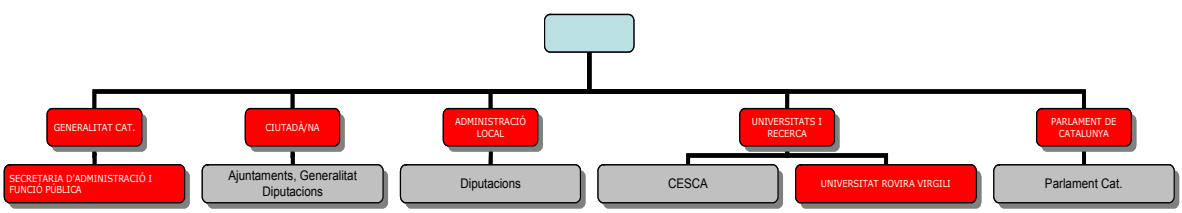
3. L'Administració Oberta de Catalunya – CATCert

El 23 de julio de 2001 se firmó por parte de todas las fuerzas políticas del Parlament de Catalunya, el Pacto Parlamentario que, conjuntamente con el esfuerzo de todas las administraciones públicas catalanas, ha hecho posible poner en funcionamiento l'Administració Oberta de Catalunya.

En este marco, el 11 de junio de 2002, se constituyó la Agència Catalana de Certificació (CATCert), que es una institución del Consorci per a l'Administració Oberta i Electrònica de Catalunya, creada en el mes de enero del mismo año.

La Agència Catalana de Certificació nace con la misión de constituirse como la entidad proveedora de servicios de seguridad, tanto jurídica como tecnológica de las administraciones y organismos públicos catalanes.

Para llevar a cabo esta misión, CATCert se ha dotado como primera herramienta, de una infraestructura de certificación digital, puesto que entendemos que el proceso de identificación y certificación del personal de las administraciones públicas se debe gestionar y prestar desde la propia administración.
En estos momentos la jerarquía es la siguiente:



Actualmente, todos los Ayuntamientos de Cataluña, los 41 Consells Comarcals, las 4 Diputaciones y los diferentes Departamentos de la Generalitat utilizan ya la firma electrónica a través de certificados digitales emitidos por CATCert.

4. CATCert: Modelo catalán de entidad de certificación.

CATCert, constituye el modelo catalán de entidad de certificación, modelo basado en cinco grandes ejes:

Servicio a las administraciones públicas: El primer objetivo de CATCert y causa principal de su creación, es la prestación de servicios de seguridad a las administraciones públicas. CATCert tiene en este sentido el objetivo de cubrir las necesidades que en materia de identidad y certificación digital se le requieran desde la administración y proveer a su vez de los servicios asociados a ésta.

Orientación a los usos: Para CATCert es más prioritario potenciar los usos de los certificados y su interacción con el ciudadano, las empresas y las administraciones, que no su emisión. Se dedican muchos más esfuerzos en ampliar las utilidades que se puedan realizar con los certificados electrónicos, que en aumentar su cantidad de emisión. De poco sirve tener emitidos gran cantidad de certificados, si éstos tienen poca utilidad.

Colaboración con las iniciativas de prestación de servicios de identidad y certificación digitales presentes en la sociedad. CATCert pone a disposición de la administración todos sus recursos para ayudar al impulso y desarrollo de las iniciativas que las mismas llevan a cabo (nuevos uso de certificados y firma, políticas de seguridad)

Adelantarse a las necesidades de las administraciones: Una de las mejores formas de prestar servicio, es prever las necesidades futuras que pueda tener la administración, investigar, desarrollar y, llegado el momento, dar una respuesta rápida y eficaz.

Prestación de servicios comunes a todas ellas: Hay una serie de servicios que forzosamente deberán utilizar todas las administraciones; firma electrónica, validación, sellado de tiempo... CATCert dispone y ofrece estos servicios, ahorrando costes económicos a la administración de forma directa y indirecta creando una uniformidad entre las distintas aplicaciones que los utilizan permitiendo así su compatibilidad (intercambio de información, federación de identidad etc...).

Para ello CATCert dispone de,:

- Conocimiento de la problemática de las administraciones públicas
- Conocimiento técnico, legal y organizativo de la seguridad
- Conocimiento de la situación de la seguridad en la sociedad
- Experiencia en el diseño y la implantación de soluciones y políticas de seguridad

5. Servicios

Para describir los servicios, resultaría reduccionista conformarse con el ámbito de actuación denominado certificación digital, cuando las vias de actuación de la Agència son diversas y complementarias entre sí. Se configuran del siguiente modo:

5.1. Emisión de certificados

a) Mediante la emisión de certificados digitales para las administraciones, se proporciona documentos infalseables de identidad y atributos, en soporte electrónico, firmados con la clave privada de la Agència Catalana de Certificació, para asegurar la autenticidad de los datos.

La firma digital se fundamenta en la tecnología denominada Infraestructura de Clave Pública (PKI), la cual se basa en la utilización de dos claves diferentes (criptografía asimétrica), así como de una función llamada resumen (hash). Hoy en día, éste es el sistema que garantiza la máxima seguridad para validar la identidad de personas al realizar trámites electrónicos, razón por la cual CATCert ha escogido la tarjeta con chip criptográfico.

CATCert suministra diversos tipos de certificados, en función de las necesidades y ámbito de actuación, a saber:

- Certificado personal de identificación y firma reconocida, que contiene información referente al titular. Se facilita a los trabajadores de las administraciones catalanas como elemento de identidad en las comunicaciones electrónicas.

- Certificado de cargo y uso, que identifica a la persona en si, pero además el cargo o la función que está desarrollando. La persona que se identifica o firma lo hace en función del cargo que ostenta y para un uso concreto (ej: compulsa)

- Certificado personal de cifrado, que dispone de dos claves, una pública y otra privada, para poder cifrar documentos, ficheros o correos. Un servicio vinculado a este tipo de certificado es el de recuperación de claves, que permite recuperar la clave privada de estos tipos de certificados y solo de éstos.

- Certificado de dispositivo de servidor seguro, que permite asegurar la identidad de un servidor de páginas web y garantizar que la transmisión de información entre el cliente y el servidor se realice de forma confidencial.

- Certificado de dispositivo programa, que permite firmar electrónicamente las aplicaciones informáticas o programas que se puedan transmitir a través de las redes de comunicaciones.

- Certificado de dispositivo aplicación, que se almacena en un servidor (preferiblemente en un dispositivo criptográfico) pudiendo ser requerido por una aplicación para firmar un documento o mensaje de forma automática bajo las reglas de la aplicación.

b) El idCAT, certificado digital para el ciudadano/a. Mediante el mismo, todos los ciudadanos/as que necesiten realizar trámites con las administraciones públicas catalanas, podrán identificarse y realizarlos de forma segura, asegurando su identidad e integridad.

Se trata de una identidad digital avanzada basada en un certificado reconocido, que se puede descargar a través de la web que cada administración habilite al efecto. Este certificado se almacena en el ordenador del ciudadano, pudiendo ser utilizado durante los cuatro años de validez.

El idCAT puede obtenerse a través de cualquiera de las administraciones públicas catalanas que hayan firmado previamente un convenio con la Agència Catalana de Certificació. Los ayuntamientos de Santa Coloma de Gramenet y Castellar del Vallés, así como las oficinas de atención al ciudadano de la Generalitat de Catalunya han sido

pioneros en esta clara apuesta en mejorar la atención al ciudadano. En estos momentos hay ya más de 60 entidades de registro en funcionamiento en distintas localidades catalanas: Manresa, Sabadell,, Lleida, Girona, Tarragona, etc.

5.2. Clasificación de entidades de certificación

Aunque CATCert se haya dotado de una infraestructura de certificación digital, teniendo en cuenta la ley de firma electrónica, no pretende solapar servicios de certificación con otras entidades de certificación reconocidas. En esta línea CATCert ha establecido acuerdos de clasificación de los sistemas de identidad digital y de firma electrónica de estos proveedores para que dichos certificados digitales puedan ser utilizados en las relaciones con las administraciones públicas catalanas.
Actualmente CATCert ha clasificado 13 entidades

5.3. Autoridad de Validación Semántica (AVS)

La plataforma de validación permite gestionar la validez de los diferentes mecanismos de identificación y certificación que se están utilizando, es decir, comprueba si el certificado está caducado, revocado, si pertenece a alguna de las entidades de certificación clasificadas por la administración, hace la homogeneización de los contenidos de los certificados, etc., y devuelve una respuesta en XML estandarizado, indicando el nivel de seguridad que tiene el certificado digital o el mecanismo de identificación (usuario y contraseña, etc...).

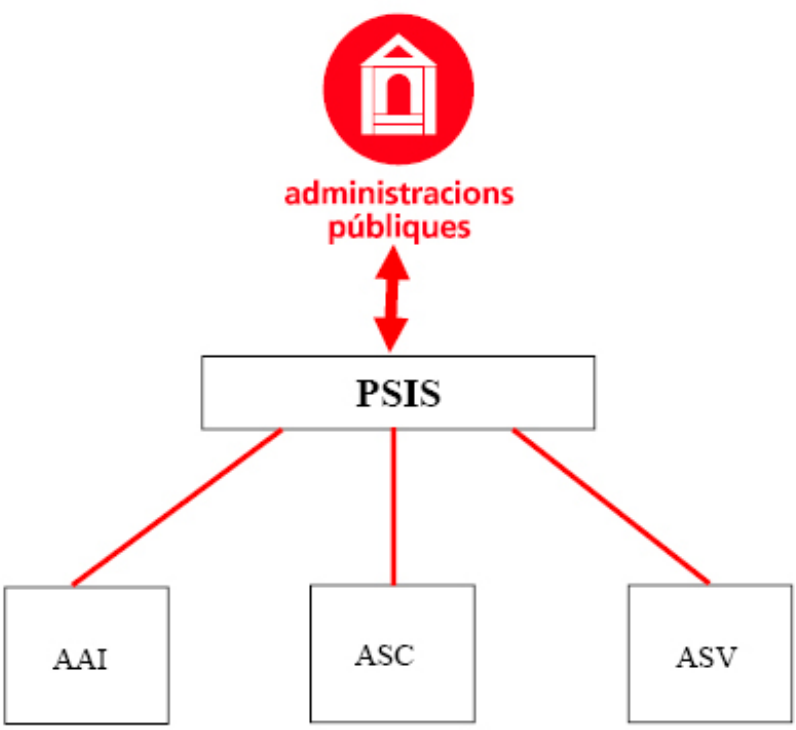
Actualmente dentro de la plataforma PSIS (Plataforma de Serveis d'Identificació i Signatura) se ha puesto en marcha el módulo de la Autoridad de Validación Semántica (AVS) de distintos tipos de elementos de confianza, como certificados digitales (X.509), firmas electrónicas en distintos formatos (PKCS#7,CMS XMLDSig), tickets firmados, etc.

La plataforma ejecuta trabajos semánticos, localizando y extrayendo la información contenida en los elementos de confianza que gestiona (los datos contenidos en el certificado) como el nombre, DNI, cargo o organización, y determinando el nivel de clasificación que corresponde al elemento que valida.

La validación de certificados se hace mediante consultas OSCP o CRL y las respuestas que devuelve el AVS a los usuarios, se firman electrónicamente con un CDA (Certificado Digital de Aplicación) para garantizar el origen y la integridad de la respuesta

Como ya se ha dicho, esta Autoridad de Validación Semántica es parte integrante de la PSIS (Plataforma de Serveis d'Identificació i Signatura) que nace con la vocación de ser la plataforma integradora y la infraestructura común para todas las administraciones públicas catalanas, prestadora de los servicios de identificación y firma digital.

En estos momentos se están validando casi 100.000 transacciones mensuales.



5.4. Autoridad de firma Centralizada (ASC)

El segundo módulo de la plataforma PSIS ofrece servicios de generación de firmas electrónicas y de cifrado de datos asistidos desde el servidor.

La firma puede ser simple para un documento, múltiple (varias firmas para varios documentos), por lotes (una sola firma para una serie de documentos) o automática (producción programada de una firma, siguiendo la política de firma, siempre que se presente un mismo tipo de documento).

A su vez la ejecución de la firma puede ser directa e inmediata a la petición del usuario, o en diferido cuando el usuario programa la generación de la firma para que se ejecute en un momento posterior.

El cifrado puede ser también genérico, para mantener datos propios de forma confidencial, o específico, para uno o diversos destinatarios concretos.

Asímismo, PSIS custodia las firmas producidas, para mantenerlas criptográficamente fiables durante el período de tiempo definido en las políticas de firma aplicada o el indicado manualmente por el usuario. La plataforma genera también un justificante de las firmas emitidas.

5.5. Autoridad de Acreditación y federación de Identidades (AAI)

El tercer módulo de la PSIS, permite establecer relaciones de confianza entre el sistema inicial, en el que se autentica el usuario, y otros sistemas finales a los que pretende acceder, de tal forma que al usuario no le es necesario volverse a autenticar, para pasar de un sistema al otro.

Facilita implantar sistemas de control de acceso, basados en autenticación única (single sing-on), en dominios de seguridad unitaria o en dominios múltiples. Federar las distintas identidades de un mismo usuario que pueden encontrarse en sistemas diferentes.

En definitiva, y a título de ejemplo, el conjunto de módulos que componen la PSIS antes descritos, serán elementos clave en el desarrollo de las siguientes funcionalidades:

REGÍSTRO TELEMÁTICO ADMINISTRATIVO: Permite la presentación de documentación original en formato electrónico firmada por el presentador. Se asigna número de entrada (asiento) y sellado de tiempo. PSIS aporta la firma y sellado de tiempo

EXPEDICIÓN AUTOMÁTICA DE CERTIFICADOS ADMINISTRATIVOS: Posibilita la solicitud y expedición telemática de certificados administrativos, entendiendo como tal a los documentos públicos que dan fe de datos o hechos que constan en los registros de la administración.

PLATAFORMA DE NOTIFICACIONES TELEMÁTICAS: Para comunicar los actos de la administración a los interesados, dejando constancia de su recepción, mediante la dirección única suministrada por la administración. El interesado recibe en su propia dirección de correo electrónico un aviso comunicándole que tiene una notificación pendiente en la dirección única.

FACTURA TELEMÁTICA: Mediante la conexión a una plataforma de factura electrónica, PSIS permite la firma electrónica de facturas utilizando el correspondiente certificado digital. El emisor de la factura puede incluso firmar por lotes todas las facturas utilizando la plataforma PSIS. A su vez PSIS puede validar las firmas que incorporan las facturas electrónicas recibidas. La propia plataforma se encarga de la custodia de dichas firmas. Todo ello permite el envío telemático de la factura sin necesidad de imprimirla en papel

VALIDACIÓN UNIVERSAL DE FIRMAS ELECTRÓNICAS: PSIS está preparada para aceptar y validar todas las firmas electrónicas que se produzcan en la Unión Europea. Facilita la interconexión entre las administraciones públicas, los ciudadanos, las empresas y los profesionales. Para la administración, es suficiente lanzar una consulta de validación hacia CATCert, con independencia del tipo de certificado a validar y de su origen. PSIS validará directamente el certificado si éste pertenece a una de las entidades clasificadas, y si no es así redireccionará la petición hacia el validador en origen y devolverá la respuesta a la administración peticionaria.

GESTIÓN DOCUMENTAL DE ORIGINALES ELECTRÓNICOS: Cumple con los requerimientos de la legislación archivística, sobre originales en soporte electrónico y copias auténticas, referentes a las garantías de preservación y acceso. Las aplicaciones conectadas a PSIS entregan a ésta la firma electrónica del documento y un resumen criptográfico del mismo (no el propio documento). PSIS valida la firma, registra la evidencia electrónica i devuelve un informe firmado y con sello de tiempo. Este informe es la única prueba que las aplicaciones deberán guardar en su gestor documental. Evita tener que validar la firma cada vez que se accede o visualiza el documento.

INTEGRACIÓN DE TRÁMITES ADMINISTRATIVOS: Facilita que los expedientes en los que interviene más de una administración puedan ser trasladados directamente de una a otra, en lugar de que sea el ciudadano el que haga los trámites. Simplifica las gestiones de los expedientes administrativos y ofrece un mejor servicio al público. Aquí la PSIS aporta distintas funcionalidades, por una parte la firma de los documentos electrónicos que circulan entre administraciones y por otro la validación de estos documentos en el momento en que estos llegan a al administración destino.

DELEGACIÓN Y AUTENTICACIÓN I FIRMA: Supone la implantación de un sistema web single sing-on administrativo (para trabajadores de la administración). Una vez identificado ante la aplicación una administración, se puede conectar a la aplicación de otra administración para continuar con los trámites sin necesidad de volverse a identificar.

6. Sellado de tiempo

Mediante el sellado de tiempo se ofrece un complemento adecuado a la seguridad ya mencionada. Dado que normalmente los trámites realizados con las administraciones están sujetos a un plazo de validez, la fecha y hora en que se han realizado, resultan una información indispensable.

El número actual de peticiones de sellado de tiempo asciende a casi 20.000 mensuales con un crecimiento mensual aproximado del 15%.

7. Asesoría y formación

L'Agència Catalana de Certificació – CATCert dispone de un equipo de profesionales con amplios conocimientos en el campo de la certificación digital que, entre otras tareas, asesoran a la Comisión Europea mediante su participación en el Grupo Directivo de Iniciativa Europea de Normalización de la Firma Electrónica (EESSI SG).

Hasta la fecha se ha participado y asesorado más de 150 proyectos distintos, tanto en el ámbito de la Generalitat como en el local.

8. Gestor de la representación

Para dar cobertura a aquellos casos en que el interesado no se persona directamente ante la administración si no que lo hace por medio de su representante, PSIS hace las pertinentes consultas ante las aplicaciones, órganos correspondientes (Notarios, Gestores) para que dicha representación quede acreditada.

9. Archivo seguro

La creciente presencia de información electrónica en el sí de las administraciones, hace necesario que éstas se planteen la necesidad de definir un sistema de archivo seguro, integral y corporativo que garantice la autenticidad e integridad de sus contenidos, así como la accesibilidad, disponibilidad, legalidad y preservación a largo plazo de los documentos electrónicos que produce y recibe.

Para hacer frente a estas necesidades, la Agència Catalana de Certificació - junto con otras instituciones catalanas- está trabajando en la definición de un marco normativo que regule la preservación digital y la estandarización de un modelo de archivo digital de documentos, un depósito seguro para toda aquella información o documentación electrónica, procedente de los diferentes sistemas de información o aplicaciones de una organización y que se deba conservar a largo plazo.

En este sentido, los esfuerzos por diseñar una política de preservación digital integral y corporativa, se centran en tres grandes puntos.

En primer lugar, la definición de los requerimientos funcionales del archivo digital y del objeto digital preservable (ODP). A grandes rasgos, el archivo seguro recibirá de las diferentes aplicaciones o sistemas de gestión los documentos en su formato originario y los transformará a objetos digitales preservables. El ODP es un conjunto de entidades físicas y lógicas estructuradas en un esquema XML que representa los documentos electrónicos de una forma estándar e independiente del modelo de objeto originario. Éste incluye el contenido del documento y sus metadatos asociados, ya sea tanto información descriptiva, contextual o tecnológica como la relacionada con la preservación.

Estos objetos se agruparían en paquetes de información: paquetes de información de ingreso, de archivo y de consulta. Una vez los ODP han ingresado en el archivo, éstos serían gestionados de acuerdo con la política de preservación, para asegurar su conservación y, si es necesario, serán migrados a nuevos formatos, de acuerdo a un registro homologado de formatos de preservación, para hacer frente a la obsolescencia tecnológica (paquetes de información de archivo). Toda esta información, será accesible a los usuarios mediante la consulta de los metadatos asociados a los documentos y éste podrá obtener copias auténticas o de consulta (paquetes de información de consulta).

En segundo lugar, la problemática del archivo de las firmas electrónicas asociadas a los documentos, está totalmente solucionado puesto que CATCert ofrece un servicio de archivo seguro dentro de la Plataforma de Servicios de Identificación y Firma (PSIS). CATCert se compromete a archivar el período de tiempo que establezca la normativa vigente todas aquellas firmas electrónicas que las diferentes administraciones le haga llegar. Esto incluye su gestión, conforme a los estándares técnicos que definen los formatos y los criterios de uso de servicios de seguridad adelantados, los cuales permiten la validación de firmas electrónicas a largo plazo, más allá de la caducidad de los correspondientes certificados digitales, y las protegen ante posibles problemas de seguridad, derivados de la obsolescencia tecnológica. De esta manera, las administraciones no se deben preocupar de su gestión y archivo.

Jordi Masias
Josep Torres
Emma Suevos
Ignacio Alamillo

Finalmente se está trabajando en la implementación de unos repositorios en disco centralizados y seguros para el archivo y recuperación de los documentos. Se trata de unas plataformas de almacenamiento de contenidos fijas que permiten normalizar la gestión de éstos en un repositorio de datos único, seguro y completo, soportado en un hardware altamente robusto, estable e íntegro. Entre sus funcionalidades podemos destacar el sistema de control de autenticidad e integridad o su accesibilidad en línea que permite a las aplicaciones de gestión, desentenderse de la ubicación física de los documentos en los dispositivos de archivo. Es el complemento perfecto, para cualquier aplicación de gestión documental o de archivo.