GESTIÓN DE LOS ACCESOS A LA RED SARA DESDE LAS ADMINISTRACIONES PÚBLICAS DE CATALUNYA

Joan Manuel Gómez Sanz
Director Operaciones y Sistemas
Consorci Administració Oberta de Catalunya

Ignacio Alamillo Domingo
Director Asesoría e Investigación
Agència Catalana de Certificació

Palabras clave

Gestión de identidad y del acceso, contraseña, certificación electrónica, SSL, VPN, Ipsec, portal empleados públicos, SARA, MAP, Extranet Administraciones Públicas, integración de servicios.

Resumen de su Comunicación

A raíz de la puesta en marcha de la red SARA del MAP, cuyo objetivo es establecer una infraestructura de comunicaciones para facilitar la puesta en marcha de servicios de Administración Electrónica, proporcionando la conexión fiable, segura, capaz y flexible entre las diferentes Administraciones, recae sobre el ámbito autonómico facilitar el acceso a dicha red e infraestructura a todas las Administraciones Públicas que actúan en su territorio.

Esta comunicación, expone las acciones realizadas por el *Consorci Administració Oberta de Catalunya* para ofrecer una solución completa y con garantías de seguridad a todas las Administraciones Públicas de Catalunya (APC) y facilitar diferentes métodos de acceso a los servicios de la red SARA.

Antecedentes

El *Consorci Administració Oberta Electrònica de Catalunya* (Consorci AOC) es una entidad pública de carácter asociativo, y personalidad jurídica propia formado por la Generalitat de Catalunya y el consorcio local para el desarrollo de las redes de telecomunicaciones y de las nuevas tecnologías, *Localret*, en el que se encuentran integrados más de 800 ayuntamientos catalanes.

El *Consorci* AOC se constituye para la implantación y la utilización de las Nuevas Tecnologías de la Información y de las Comunicaciones (TIC) en el marco de las administraciones públicas catalanas y su prestación de servicios.

El Consejo General del *Consorci* aprobó el 21 de octubre de 2004 los objetivos estratégicos que determinan los cinco ámbitos de actuación en el mandato 2004-2007:

- Revisión del marco normativo y jurídico
- Módulos de colaboración interadministrativa
- Integración de servicios interadministrativos
- Integración de información
- Plataforma y sello AOC.

En base a la iniciativa presentada por el MAP en el Comité Sectorial de Administración Electrònic de 25 de noviembre de 2004 consecuencia del cual se crea el Grupo de Trabajo “Extranet de las Administraciones Públicas”, y a los objetivos del Consorci, se instala en sus dependencias la infraestructura necesaria (Área de Conexión) para poder acceder a la red SARA y recae sobre él la obligación de dar acceso a dicha red a las diferentes administraciones públicas catalanas.

Situación actual

El Consorci actúa como intermediario entre las Administraciones Públicas de Catalunya (APC) y la red SARA. En un extremo tenemos los servicios que son accesibles actualmente a través de esta red:

- Verificación de los datos de identidad y residencia.
- Plataforma de validación de firma electrónica.
- Notificación fehaciente electrónica.
- Pasarela de pago.
- Registro electrónico común.
- Consultas del estado de expedientes.
- Catálogos de procedimientos de las AAPP.
- Simulación de dichos procedimientos.
- Servicios de nueva creación.
- Videoconferencia.
- Voz IP.
- Entornos de trabajo colaborativo

En el otro extremo, tenemos a las APC que sus necesidades de acceso a servicios SARA son de dos tipos:

- **Usuario final:** El empleado público necesita acceder a los Servicios finalistas[1] (p.ej. Tráfico, Campaña RENTA, etc.) o acceder a un servicio del Consorci que consumen recursos de SARA.
- **Aplicaciones**: Algunos organismos tienen necesidad de que sus aplicaciones accedan a SARA para obtener algún servicio de la AGE (WS, aplicaciones host, etc.). Algunos de estos servicios pueden estar integrados en el Consorci y otros no y por lo tanto únicamente necesitan conectividad para entrar en SARA.

[1] Llamaremos servicios finalistas a todos aquellos que son prestados directamente desde un organismo de la AGE y accesibles via interfaz gráfica (web, Citrix, etc.)

Infraestructuras proporcionadas por el Consorci AOC para dar acceso a los servicios SARA.

Los recursos proporcionados por el Consorci a las APC para acceder a los servicios de SARA son dos:

- Plataforma eaCat: Extranet Administraciones públicas de Cataluña
- PCI: Plataforma de Colaboración Interadministraiva

Plataforma eaCat:

Actualmente, el Consorci dispone de la plataforma **eaCat** *(www.eacat.net)* que actúa como extranet administrativa de las Administraciones Públicas Catalanas (APC).

eaCat es una plataforma de servicio orientada a facilitar la comunicación entre las Administraciones catalanas, es decir, un canal bidireccional de comunicación electrónico seguro tanto a nivel jurídico como técnico entre administraciones (fundamentalmente entre la administración local y la Generalitat de Catalunya).

eaCat es una herramienta que permite:

- Establecer un canal de comunicación electrónico seguro entre las Administraciones catalanas.
- Aportar validez legal a los envíos de documentación, mediante el uso de la firma electrónica reconocida
- Ejercer de oficina de registro virtual para todas las tramitaciones documentales entre ayuntamientos, consejos comarcales, otras entidades locales y la Generalitat de Catalunya
- actúa también como una plataforma de ejecución de aplicaciones.
- Tener vocación de servicio personalizado a cada usuario.

A esta plataforma, se le ha añadido una pieza más para facilitar y gestionar el acceso a los servicios finalistas y que esta conectada con el Área de Conexión. Esta pieza, es un servidor de túneles VPN sobre protocolo SSL (*Firepass de F5*) que permite garantizar la seguridad de la transmisión extremo a extremo independientemente del recurso que se acceda (web, Citrix, etc.).

A fecha de hoy diferentes departamentos de la Generalitat y más de 1.000 administraciones locales ya son usuarias de este portal, con un total de 7.800 usuarios. Por esta razón, se decidió utilizar el portal eaCat como plataforma donde integrar los servicios finalistas publicados en SARA y orientados a usuarios finales, no aplicaciones (p.ej. www.trafico.es).

Plataforma PCI:

La PCI del Consorci AOC ofrece la posibilidad de obtener diferentes transmisiones de datos y certificados telemáticos desde organismos emisores de información. El Consorci AOC, como intermediario, obtiene los datos del emisor y los muestra al organismo requirente en formato electrónico y adecuado para el posterior tratamiento posterior de los datos. Esta información se obtiene con garantías jurídicas (convenios) y con mecanismos de seguridad tecnológica basados en certificados de firma electrónica reconocida.

El Consorci AOC actúa como concentrador de las solicitudes de certificados hacia otras administraciones, aportando el siguiente valor:

- Agregador de canales: El Consorci AOC actúa como interlocutor único frente a las administraciones para proporcionar certificados telemáticos de múltiples fuentes.
- Trazabilidad / auditoria: La plataforma PCI proporciona herramientas para realizar seguimiento de las solicitudes a nivel individual o por lotes.
- Gestión de los reintentos de envío de las solicitudes.
- Mantenimiento del catálogo de certificados telemáticos disponibles.
- Relación con los organismos emisores de datos.
- Gestión de los mecanismos jurídicos para acceder a la información.

Acceso a servicios SARA desde usuarios finales

Los usuarios finales pueden decidir de acceder a dos tipos diferentes de recursos:

- **Servicios finalistas**: El empleado público accede con su navegador y vía Internet a la plataforma eaCat con usuario y contraseña o su Certificado Digital emitido por la Agencia Catalana de Certificación (CATCert). Una vez autenticado debe dirigirse al apartado de "servicios AGE".

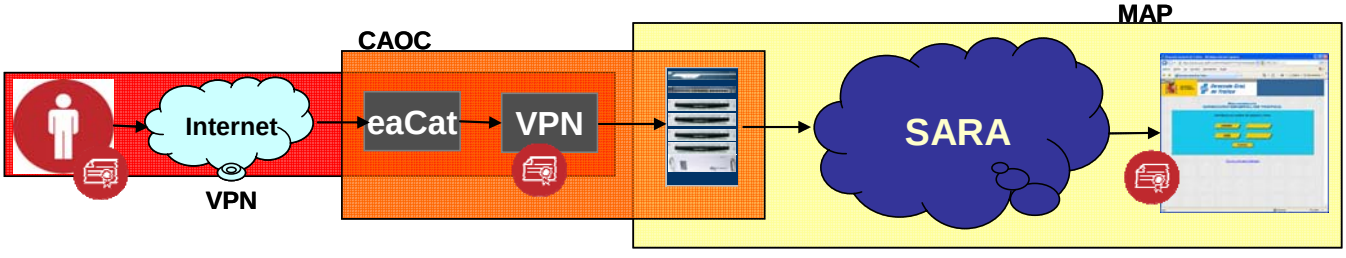
  En ese instante el portal reenvía la conexión al servidor de túneles para que realice las siguientes acciones:

  - Verificación del certificado digital del usuario, mediante el empleo de protocolo OSCP con el servicio de validación de CATcert. En este caso, resulta obligatorio el uso de un certificado digital de empleado público (en concreto, el certificado CPISR) para acceder a los servicios finalistas, de forma que si el empleado público ha accedido mediante usuario y contraseña debe volver a autenticarse.
  - Acceso al directorio del eaCat para verificar la identidad y autorizaciones del usuario identificado

  En el caso que la validación del certificado digital sea correcta y el perfil del usuario tenga permisos para acceder a uno o varios servicios finalistas, se visualizará una ventana con los accesos directos a estos servicios. Con este sistema, se garantiza la seguridad de los datos y la identidad del usuario extremo a extremo.

  La gestión del acceso de los empleados públicos a los servicios finalistas la realizan las mismas administraciones ya que cada una de ellas dispone de un usuario del portal eaCat con el perfil de gestor (designado por la autoridad competente) que esta capacitado para dar de alta, baja, modificar usuarios y configurar los permisos para acceder a diferentes servicios. Por ejemplo, es posible que un usuario deba de tener permisos para acceder al portal de la DGT (www.trafico.es), pero no para acceder a la campaña de la renta de la AEAT. La capa de gestión de usuarios del portal eaCat permite configurar individualmente el acceso a los servicios finalista, según el perfil del usuario final.

  El esquema de conexión es el siguiente:



Servicios del Consorci AOC: Es voluntad del Consorci que todos aquellos servicios disponibles en la red SARA que no disponen de una interfaz gráfica y susceptibles de ser consumidos por las APC puedan ser accesibles a través de interfaz en el eaCat con integración de la plataforma PCI, aportando el valor añadido anteriormente descrito .

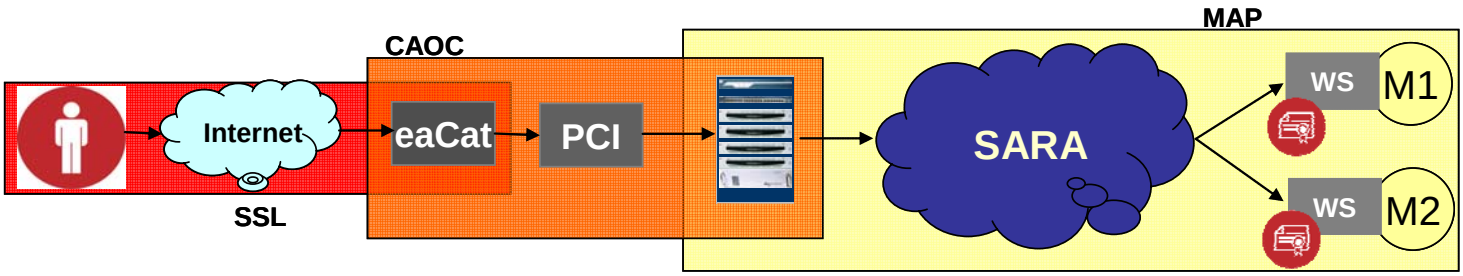
Como ya hemos mencionado, el Consorci está poniendo a disposición servicios que operan con diversos organismos autonómicos y estatales, como el servicio de Cambio de Domicilio (CATSalut, AEAT, TGSS, DNI, etc.) o el de Solicitud de Certificados (GENCAT, AEAT, TGSS, INE, Policía, etc.). Estos servicios son accesibles desde las interfaces de la plataforma eaCat, aunque la intermediación con los organismos emisores de dichos datos y certificados la realice la plataforma PCI.

Al igual que en el acceso a los servicios finalistas, el empleado público debe de conectarse a la plataforma eaCat y autenticarse con sus credenciales. Una vez autorizado su acceso, accederá al área de los servicios del Consorci para rellenar los datos específicos del servicio y la plataforma eaCat realizará las gestiones pertinentes con la plataforma PCI para tramitar las solicitudes a organismos que solo son accesibles vía SARA.

En este caso, la plataforma que esta conectada en el Área de Conexión es la PCI y la seguridad de extremo a extremo se garantiza mediante Certificados Digitales de Aplicación emitidos por CATCert.

Para el empleado público el proceso es totalmente transparente y en todo momento la interfaz con la que se relaciona es la de la plataforma eaCat.

El esquema de conexión es el siguiente:



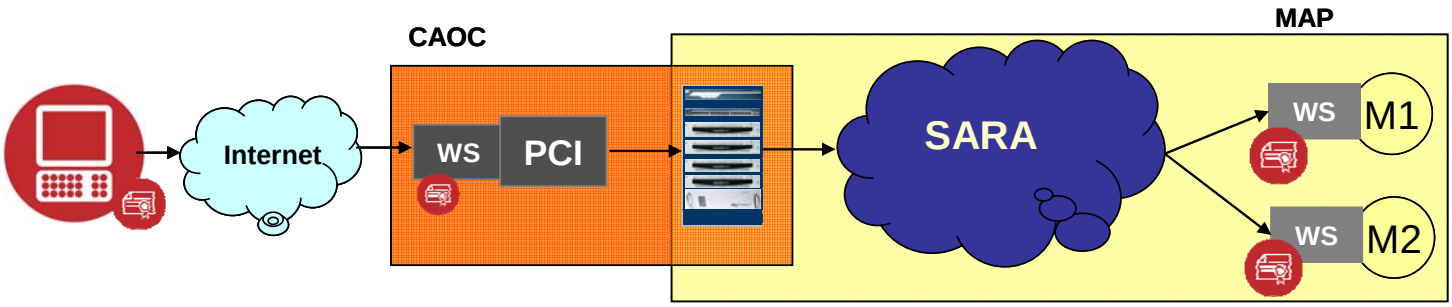
Acceso a servicios SARA desde aplicaciones

En este apartado contemplamos la posibilidad de que no sea un usuario final quien acceda a un servicio sino una aplicación instalada en una plataforma. Al igual que los usuarios finales, las aplicaciones pueden consumir servicios de SARA, a través de alguna de las plataformas del Consorci empleando servicios web (Web Service) o accediendo a servicios que son prestados directamente por algún organismo de la AGE y que están publicados en SARA donde el Consorci solo intermedia la comunicación mientras no hayan sido integrados vía PCI:

- **Servicios Consorci AOC**: Los servicios del Consorci que se encuentran disponibles vía interfaz gráfica a través de la plataforma eaCat, también resultan accesibles vía WS desde la plataforma PCI. De esta forma, aquellas administraciones que tengan capacidad de desarrollo, pueden utilizar esta vía para lograr una mayor integración de sus procesos, aprovechando las ventajas aportadas por la plataforma PCI.

  La autenticación de las aplicaciones se realiza mediante certificados digitales de aplicación y de entidad dependiendo de la política establecida por cada organismo emisor de transmisiones de datos y certificados telemáticos.

  El esquema de la conexión es el siguiente:



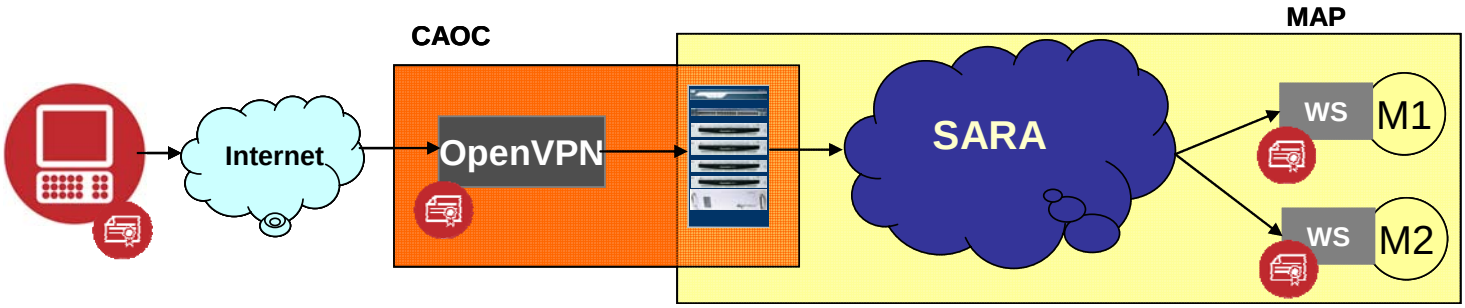
- **Otros servicios**: El Consorci facilita la conexión a aquellos servicios sin interfaz de usuario que han sido publicados en la red SARA desde algún organismo de la AGE y que todavía no están integrados en alguna de las plataformas del Consorci. Dentro de este grupo se encuentran aquellos servicios que se prestaban con líneas dedicadas X.25 y contra aplicaciones host y que después de haber sido migrados a la red SARA se sigue utilizando el mismo tipo de aplicación.

  Al tratarse de temas muy específicos y puntuales, el Consorci ha diseñado una solución técnica que facilita el acceso de las aplicaciones

remotas vía Internet al Área de Conexión, para que finalmente puedan acceder a la red SARA.

Dicha solución consiste en un servidor de OpenVPN que esta conectado en la red del Área de Conexión. Para que una aplicación remota pueda acceder a un servicio que se encuentra en SARA, se genera un cliente VPN (disponible para plataformas Windows, Linux y Solaris) el cual debe ser instalado donde se ejecuta la aplicación. Al ejecutarse el cliente VPN, abre una interfaz virtual de red, creando un túnel VPN entre la plataforma y el servidor OpenVPN, permitiendo acceder a la aplicación directamente a la red SARA.

La autenticación de los clientes al conectarse al servidor OpenVPN se realiza mediante certificados digitales. Además, para mayor seguridad, cabe la posibilidad de generar clientes que solo permitan el acceso de la aplicación remota al servicio de SARA que se precisa consumir, impidiendo el acceso de la aplicación al resto de servicios de la red.

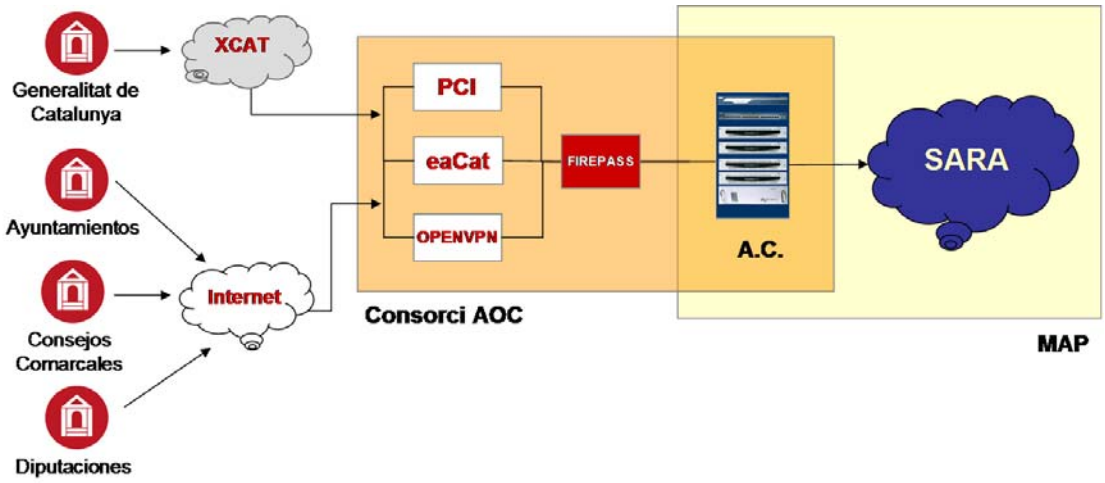


Otros sistemas de acceso a SARA

En este caso nos referimos concretamente al que esta usando la Generalitat de Cataluña ya que debido a su naturaleza y entidad, se decidió crear un enlace directo entre la intranet de la Generalitat (XCAT) y la intranet del Consorci y que esta pudiera enlazar con el Área de Conexión para poder acceder a SARA.

La necesidad de acceder a servicios de SARA de la Generalitat de Cataluña es idéntica que la del resto de Administraciones Catalanas y para acceder a los servicios finalistas o los servicios que ofrece el Consorci a nivel de usuario final o de aplicación, deberá de acceder a la plataforma eaCat o la PCI, aunque para ello no hará falta acceder vía Internet sino que podrá utilizar el enlace punto a punto.

El esquema de conectividad general seria el siguiente:



Aspectos de seguridad

Se ha hecho especial hincapié en los sistemas de seguridad en los diferentes métodos de acceso, centrando la atención en tres aspectos:

- Comunicaciones: Asegurando la confidencialidad y integridad de los datos.
- Autenticación: Usando usuario y contraseña y certificados digitales con validación CRL y/o OSCP con base en certificados de empleados públicos (CPISR), certificados de aplicación (CDA) y certificados de entidad (CESR), de acuerdo con la política de cada organismo que concede acceso a sus sistemas.
- Autorización: A nivel de grupos, recursos, servicios y listas de acceso.

Todos los datos que viajan entre el usuario y los servicios de SARA irán siempre dentro del túnel SSL para asegurar la confidencialidad e integridad, no permitiendo que estos datos puedan ser visos por alguien que no sea el propio usuario.

A diferencia de las soluciones de acceso remoto tradicionales como la red virtual basada en IPSec, la solución implementada en el acceso a los servicios finalistas, elimina la sobrecarga de trabajo asociada a la instalación,

configuración y mantenimiento de aplicaciones en la parte de cliente, siendo solo necesario un navegador que soporte SSL/TLS para poder establecer un túnel seguro.

El sistema de doble autenticación con certificado digital y contra el gestor de identidades del eaCat, hace que el acceso a los servicios finalistas sea seguro y robusto, ya que es necesario que el usuario disponga de un certificado digital valido y emitido por CATCert y que esté dado de alta en el gestor de identidades de la plataforma.

Finalmente, teniendo en cuenta los posibles problemas de seguridad que puedan surgir en los equipos de trabajo de los usuarios finales, se decidió aplicar dos filtros adicionales de control de la seguridad:

- Inspección de contenido: XSS scripting, SQL injection, Buffer Overflows, antivirus
- Validación de la política de seguridad del usuario (EndPoint Security): Determinar la identidad del dispositivo, tipo, versión del sistema operativo, navegador, determinar el estado del dispositivo, versión antivirus, cortafuegos, etc.

Cabe notar que en el sistema actualmente definido pueden darse diferentes políticas de acceso de los usuarios, en función de las necesidades y los requisitos de los diferentes organismos a los que se deben conectar las Administraciones catalanas. En este sentido, al objeto de maximizar la eficiencia del sistema, se considera importante establecer un estándar elevado de autenticación por parte de las Administraciones que acceden, que permita que con un único sistema de autenticación se pueda acceder a todos los contenidos.

Esto se consigue mediante el empleo de certificados de empleado público (CPISR) en tarjeta criptográfica (la tarjeta T-CAT suministrada por CATCert), y mediante el empleo de certificados de entidad (CESR), suministrados en soporte tarjeta o en soporte hardware.

Por otra parte, como mejora futura del sistema global se podría considera el establecimiento de un sistema de federación de identidad (basado en SAML o en WS-Federation), en el que cual el Consorci AOC emitiría a las Administraciones un tiquet de autenticación y autorización delegadas, que les permitiría acceder directamente a las aplicaciones. La ventaja de este sistema reside en que abstrae a las aplicaciones finalistas de la necesidad de entender diferentes tipos de certificados digitales y mecanismos de seguridad, de forma que se simplifica la gestión de la seguridad por parte de las Administraciones en ambos extremos, a la par que se crea un sistema basado en la confianza mutua.

Prueba real del sistema

Para probar el sistema, y aprovechando la campaña de la RENTA06 de la Agencia Tributaria, se realizó una prueba piloto del acceso a los servicios finalistas de SARA con la Diputación de Barcelona y 10 municipios de la provincia, sumando un total de 34 usuarios.

Durante la campaña, algunos organismos municipales ponen a disposición de la Delegación Territorial de la AEAT, sus oficinas de atención al público para que el ciudadano pueda acudir y presentar o practicar su declaración de la renta.

Aprovechando que los municipios que participaban en el piloto y que los empleados públicos dedicados a prestar este servicio eran usuario de la plataforma eaCat y disponían del certificado digital de empleado público (CPISR) de CATCert, solo hizo falta modificar el perfil de cada uno de ellos para permitir que visualizaran los servicios que la AEAT publica en SARA y que sirven para prestar el servicio de la campaña de la RENTA.

No hizo falta impartir ningún tipo de formación ya que el empleado público conocía el entorno eaCat y solo se dio la referencia de que accedieran al área “Servicios AGE” donde encontrarían los accesos necesarios a la AEAT. Dichos accesos consistían en conexiones directas a las plataformas CITRIX de la AEAT. Además en el caso que el equipo del empleado público no dispusiera de un cliente CITRIX, los filtros de seguridad detectaban esta carencia y facilitaban de forma ágil y rápida la instalación remota de un cliente CITRIX que solo se realizaba la primera vez que se conectaba, sin necesidad de intervenciones del administrador del equipo.

En total se realizaron más de 6.100 declaraciones utilizando el nuevo sistema, sin necesidad de configuraciones especiales de red, instalación de aplicaciones en los equipos de los usuarios, líneas dedicadas, modificación de las reglas de cortafuegos, etc.

Conclusiones

La intención del Consorci AOC ha sido idear una solución de acceso a la red SARA que sirva para todos los niveles de las Administraciones catalanas (ayuntamientos, consejos comarcales, diputaciones, administración de la Generalitat), y que sea suficientemente flexible para cubrir las diferentes necesidades que dispongan según su capacidad, manteniendo unos niveles altos en seguridad, tanto a nivel de autenticación como de identificación y de integridad de los datos.

Esta solución, que actúa como canal de facilitación e integración, especialmente para las Administraciones con menos recursos, puede evolucionar en el futuro hacia un sistema de confianza mutua en el intercambio interadministrativo, en la que las Administraciones emisoras de transmisiones de datos y certificados telemáticos puedan delegar a intermediarios como el Consorci AOC la gestión de las autenticaciones y autorizaciones, mediante el establecimiento de una federación de identidad administrativa, dentro del marco de la Ley 11/2007.