Servicio AutenticA

El repositorio horizontal de usuarios de la Red SARA

Los nuevos servicios compartidos se encuentran con la necesidad de realizar la gestión de usuarios mediante repositorios que pueden estar dispersos o inconexos. El servicio AutenticA persigue ofrecerla de forma más eficaz, mediante un único repositorio horizontal de usuarios, así como servicios de autenticación y SSO. AutenticA está actualmente consolidado con varias aplicaciones usuarias de distintos organismos y se ofrece a través de la Red SARA, pero está prevista su próxima apertura a través de Internet. El servicio permite autenticación mediante certificado electrónico y con usuario y contraseña ofreciendo un protocolo de autenticación a las aplicaciones desarrolladas a medida y también autenticación LDAP a herramientas de terceros

FEDERICO CASTEJÓN
Jefe de Área de Tecnología Subdirección de Aplicaciones y Servicios Generales Dirección de Tecnologías de la Información y las Comunicaciones

La provisión de usuarios se realiza mediante volcados periódicos desde fuentes primarias de calidad, como el Registro Central de Personal entre otras; y también mediante altas manuales de administradores delegados o mediante solicitudes de autoregistro. También ofrece otros servicios como servicios de autorización o servicios web. Próximas mejoras incluyen la federación con Cl@ve y la integración de nuevos colectivos de empleados públicos.

El nuevo modelo de gobernanza TIC, aprobado mediante el RD 806/2014, tiene como objetivos potenciar la Administración digital y las TIC como instrumentos que posibiliten mantener el proceso de innovación y mejora de la calidad de los servicios, y racionalizar el uso de los recursos informáticos, buscando una mayor eficiencia y proporcionando un ahorro de costes. En este sentido, en octubre de 2015, la Comisión de Estrategia TIC aprobó la Declaración de servicios compartidos, de carácter obligatorio y sustitutivo de los anteriormente existentes, salvo singulares excepciones.

Estos servicios se prestan mediante un conjunto de aplicaciones y se apoyan en repositorios de usuarios para su acreditación ante los diferentes sistemas, que en algunos casos, se encuentran dispersos e inconexos. Con el fin de racionalizar y reutilizar recursos, así como realizar una gestión de usuarios más eficaz, se ha puesto en marcha el proyecto de "Repositorio horizontal de usuarios de la Red SARA – AutenticA".

Este proyecto tiene como objetivo dar respuesta a la necesidad que tienen, los diferentes servicios de administración digital de la SEAP, de disponer de un único repositorio

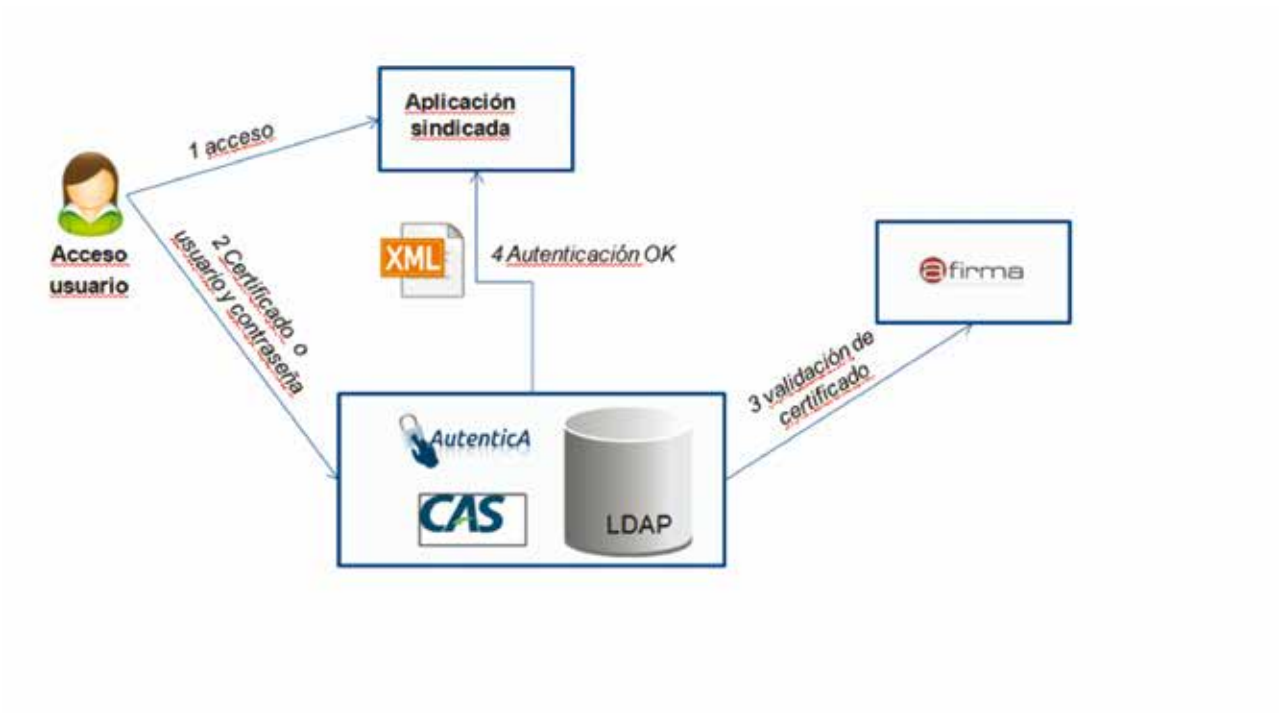

FIGURA 1. Potocolo de autenticación

horizontal de usuarios y un sistema de autenticación asociado al mismo. El servicio también proporciona un mecanismo de Single Sign-On para aquellos sistemas que se asocien al mismo. A la vez, tiene como objetivo responder a las propias necesidades de los servicios de la DTIC en esta materia y proyectarse, en el marco de sus competencias, como un servicio común más a las Administraciones Públicas que posibilita la reutilización y, por tanto, el uso adecuado de los recursos públicos y ahorro de costes. También se busca favorecer la puesta en marcha de nuevos servicios finales, de manera más ágil, al resolver el problema de la gestión de usuarios y sus entidades de forma común. Finalmente, también permite aprovechar y potenciar la utilización de infraestructuras y servicios existentes como son DIR3, RCP, Portal Funciona, Plataforma @Firma, Portal de EE.LL., PAe y Red SARA.

El servicio AutenticA fue iniciado en la Subdirección de Explotación en el ámbito de la Red SARA y a partir de septiembre de 2016 se encuentra gestionado por la Subdirección de Aplicaciones y Servicios Generales. Actualmente es un servicio consolidado, con más de un año en producción. Gestiona más de 330.000 usuarios y está dando servicio a varias aplicaciones sindicadas, de las cuales dos tienen especial relevancia por estar respaldadas por medidas CORA. Estas aplicaciones son el Inventario de Vehículos Oficiales del Parque Móvil del Estado y el Sistema Integrado del Tablón Edictal del BOE. Además de estas dos aplicaciones también se encuentra AdmElec de la IGAE y las aplicaciones Reúnete, InfoSARA, Almacén de la DTIC y SIM Plataforma de Mensajería. Próximamente se incorporarán el Portal Funciona, también de la DTIC, y la aplicación GAMO del Parque Móvil del Estado.

AutenticA facilita la realización del acceso mediante certificado y DNI electrónico. El sistema utiliza @firma para la validación, por lo que es posible autenticarse con cualquier certificado emitido en España admitido por @firma. AutenticA también permite realizar el acceso mediante usuario y contraseña. Actualmente el servicio se ofrece únicamente a través de la Red SARA, pero está prevista su próxima apertura al uso a través de Internet.

La integración o sindicación de aplicaciones con AutenticA contempla la modificación de las mismas para adaptarse al protocolo de autenticación que provee el servicio. En el caso de que sea necesario integrar herramientas de terceros, que no permitan su modificación, como por ejemplo clientes de correo, se ha contemplado permitir autenticación LDAP, en cuyo caso sólo se podrá acceder mediante contraseña.

El funcionamiento del protocolo de autenticación queda representado en la Ilustración siguiente. Comienza con el acceso a una aplicación sindicada con AutenticA. La aplicación redirige al usuario a AutenticA,

FIGURA 2. Autenticación para herramientas de terceros

indicando el código de la aplicación a la que está intentando acceder. El repositorio pedirá un certificado electrónico al usuario, caso de que disponga del mismo, o bien, le mostrará la pantalla de login, en la que podrá introducir su DNI o su contraseña. AutenticA valida, en su caso, el certificado del usuario en @firma, o bien la contraseña contra el repositorio LDAP. En caso de que las credenciales facilitadas sean válidas, se procederá a crear la sesión de usuario. Adicionalmente, se recopila la información del usuario almacenada en el repositorio LDAP, que se entrega a la aplicación inicial en un XML de respuesta. Como medida de seguridad, este XML se facilita firmado electrónicamente. Finalmente, el servicio devuelve el control de la navegación a la aplicación. (FIGURA 1).

Es factible integrar aplicaciones o herramientas de terceros que no puedan ser modificadas, siempre que permitan autenticación LDAP. En este caso, es necesario configurar la aplicación para uso del LDAP de AutenticA. Este procedimiento se muestra en la Ilustración 2 que se muestra seguidamente. Cuando un usuario desea autenticarse en la aplicación, ésta le mostrará una pantalla propia de login en la que introducirá su DNI o NIE, y contraseña. La aplicación validará los datos facilitados por el usuario en el LDAP y si son correctos permitirá el login en la misma. (FIGURA 2).

El valor añadido más importante que aporta AutenticA es la información adicional sobre el usuario que se provee a las aplicaciones en el momento de la autenticación. Ésta incluye datos personales básicos como el documento identificativo, DNI o NIE, y nombre y apellidos, pero sobre todo, los datos profesionales como el tipo de personal, el puesto y la unidad de destino, así como los datos de contacto, entre ellos, el correo electrónico. Esta información se encuentra almacenada en el repositorio de usuarios de AutenticA y su provisión y actualización cobra un papel fundamental en el servicio.

Para la provisión de usuarios se han tenido en cuenta varias formas. La principal es la realizada a partir de fuentes primarias que corresponden a registros oficiales o bases de datos de usuarios de calidad. Desde estas fuentes primarias se realizan volcados periódicos, por ejemplo, con carácter diario o semanal según la fuente, cuyo objetivo es mantener el repositorio actualizado.

Las fuentes primarias actualmente existentes son el Registro Central de Personal, el Registro de funcionarios locales con habilitación nacional, la aplicación de Cargos Representativos y el Portal de EE.LL. El Registro Central de Personal permite obtener información de todos los empleados públicos de la Administración General del Estado, funcionarios y laborales, que se encuentren actualmente en activo. El Registro de funcionarios locales con habilitación nacional facilita la relación de funcionarios en activo de dicho cuerpo y la aplicación de Cargos Representativos da acceso a los concejales y alcaldes de todos los municipios de España. Finalmente, el Portal de EE.LL. facilita la relación de todos los usuarios de dicho portal y de un conjunto de aplicaciones que utilizan los servicios de SSO del mismo.

Adicionalmente a la provisión desde fuentes primarias, también se permite la realización de altas de forma manual por un administrador de AutenticA. La administración del servicio considera un grupo de administración central, pero sobre todo ofrece la opción de disponer de una estructura de administradores delegados en diferentes organismos, o de administradores de aplicaciones que puedan realizar la gestión de usuarios en su ámbito.

Finalmente, los usuarios que no se encuentren ya almacenados en el

repositorio, pueden solicitar su alta en AutenticA mediante el formulario de autoregistro que recoge los datos personales y de destino del solicitante, debiendo ser firmado electrónicamente por éstos. La solicitud ha de ser aprobada por un administrador antes de que se procese el alta y se incorpore el nuevo usuario al repositorio.

Además de personal de la Administración, se ha visto el interés de contar con el personal externo de las empresas que proveen servicios para la Administración, por lo que está permitida su incorporación al repositorio, siempre que se motive la necesidad. Su solicitud de alta debe detallar el proyecto en el que está involucrado, así como contar con la aprobación de un responsable de la Administración, como puede ser el jefe de proyecto.

AutenticA se encuentra integrado con DIR3, por lo que la codificación de unidades a las que están adscritas los usuarios, así como los códigos de países, CC.AA., provincias y localidades, utilizan la codificación de DIR3 con el objetivo de una mayor interoperabilidad.

En las entradas de los usuarios se almacena la fuente de origen de los mismos, proporcionando una medida de fiabilidad de los datos. Esto es especialmente útil para aplicaciones que tengan unos mayores requisitos de seguridad, que por ejemplo, pudieran aceptar solamente usuarios provenientes de fuentes primarias con alta fiabilidad de los datos.

El repositorio dispone de una rama restringida que permite almacenar usuarios que requieran un mayor control de seguridad en su acceso. Entre otras medidas, no aparecerán en las búsquedas que se puedan realizar desde las aplicaciones sindicadas, como por ejemplo, mediante el servicio de "Búsqueda en el Directorio de empleados" del Portal Funciona o de la aplicación Reúnete. Otra de las medidas de seguridad del repositorio es el acceso por protocolo LDAPS (LDAP + TLS).

La política de contraseñas de AutenticA considera un plazo de caducidad de las mismas, un histórico de contraseñas utilizadas para evitar su reutilización y también bloqueo de la contraseña tras un número de intentos reiterados de acceso.

A la vez, provee de servicios de autorización, siendo opcionales en cada aplicación y permitiendo almacenar un esquema de perfiles y roles asociados a los usuarios en el ámbito de la misma. Estos permisos se entregan en el XML de respuesta al momento de la autenticación del usuario y sólo en el ámbito de la aplicación a la que está accediendo el usuario. Los permisos que se contemplan son perfiles y roles que pueden ser generales o bien asociados a ámbitos de unidades de DIR3, permitiendo por ejemplo ser usuario de una aplicación en el ámbito de una secretaría de estado.

El servicio cuenta con los siguientes componentes: Servicio de autenticación, basado en Central Authentication Service de la iniciativa de Internet JA-SIG; repositorio de usuarios basado en LDAP (Lighweigth Directory Access Protocol) y módulo de aprovisionamiento de usuarios, que contiene la parte de administración y permite la gestión de los usuarios almacenados en el repositorio. También incorpora un módulo de autorización, que contempla la gestión de perfiles y roles asociados a las aplicaciones que lo utilicen y otro de interoperabilidad, que ofrece los servicios de AutenticA a través de servicios web utilizables por aplicaciones externas. Finalmente, el portal de AutenticA, contiene información sobre el servicio y permite acceso a todos los servicios disponibles.

Como próximas actuaciones en el ámbito de AutenticA, además de la apertura de sus servicios a través de Internet y la sindicación de nuevas aplicaciones, se buscará la ampliación del servicio a través de la inclusión o integración de otros repositorios de usuarios que permitan la autenticación de nuevos colectivos de empleados públicos. Esta integración se está contemplando de varias formas: bien ofreciendo el servicio de LDAP para terceros organismos que lo requieran con el fin de incluir a su personal, o bien como sincronización con fuentes externas. Estas fuentes podrán ser bases de datos de usuarios o bien repositorios LDAP.

Asimismo, se trabajará en la federación con el sistema de claves concertadas Cl@ve de la DTIC. Esta actuación permitirá que un usuario pueda autenticarse con algunos de los métodos de clave concertada que permite el servicio Cl@ve, si bien será necesario también que el usuario autenticado se encuentre en el repositorio de AutenticA. ✱