Autentica – El repositorio horizontal de usuarios de las AAPP

Optimizando la gestión de usuarios

El servicio AutenticA es un servicio de autenticación, autorización y Single Sign On (SSO) de empleados públicos de las AA.PP., altos cargos y usuarios relacionados, en el acceso a aplicaciones internas de las AA.PP. Dispone de un repositorio horizontal de usuarios provenientes de fuentes primarias de calidad, como el Registro Central de Personal entre otras, y de altas de una estructura de administradores delegados corresponsables. Uno de los valores añadidos de AutenticA es proveer a las aplicaciones de atributos de los usuarios autenticados relacionados con la unidad y el puesto de destino, incluyendo correo electrónico y teléfono. Opcionalmente también puede proveer servicios de autorización. Este servicio se encuentra disponible en la Red SARA y a través de Internet.

Su objetivo es constituirse como el servicio común de autenticación y autorización de referencia dentro de las AA.PP. para aplicaciones internas, así como disponer de un repositorio de usuarios de las AA.PP. cada vez más

completo mediante la incorporación de nuevas fuentes primarias o sincronización con otros repositorios LDAP. Según instrucciones de la Secretaria General de Administración Digital (SGAD), todas sus aplicaciones internas deberán utilizar AutenticA.

El servicio se encuentra actualmente consolidado, con más de cuatro años de funcionamiento, y es utilizado por veinticinco aplicaciones sindicadas, estando en proceso de incorporación veintiocho más. Las aplicaciones integradas en AutenticA son en su mayoría de la SGAD, pero también hay aplicaciones de otros ministerios y organismos, como el Ministerio del Interior, el Parque Móvil del Estado, el BOE, la IGAE y la D.G. del Patrimonio. AutenticA gestiona actualmente más de 240.000 autenticaciones anuales y su repositorio permite el acceso a más de 394.000 usuarios. El servicio se ofrece a través de la Red SARA y también de Internet.

	2016	2017	2018 (enero)
Usuarios del LDAP de AUTENTICA (*)	368.649	393.127	394.616
Nº de usuarios activos en el período	1.902	2.665	5.925
Nº Total de usuarios (*)	1.946	14.298	16.071
Aplicaciones Sindicadas con AUTENTICA (*)	16	23	25
Nº de autenticaciones	45.594	240.367	72.719

Además de autenticación y SSO, AutenticA también provee servicios de autorización, de forma opcional a las aplicaciones. Mediante la realización de estas tareas, AutenticA permite a las aplicaciones la delegación completa de

la gestión de usuarios, lo que conlleva ahorros de desarrollo y de explotación.

Un valor añadido que distingue al servicio AutenticA es que proporciona información sobre el usuario a las aplicaciones en el momento de la autenticación. Esta información 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. Dicha información se encuentra almacenada en el repositorio de usuarios de AutenticA y su provisión y actualización cobra un papel fundamental en el servicio.

Medios de autenticación

AutenticA permite la autenticación de los usuarios mediante certificado y DNI electrónico. El sistema utiliza @firma para la validación, por lo que es posible autenticarse con cualquier certificado emitido en España que sea admitido por @firma. Adicionalmente, también permite realizar el acceso mediante usuario y contraseña.

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.

El servicio incorpora la funcionalidad de federación con otros repositorios de datos, a los que puede delegar la autenticación. Los usuarios pueden utilizar, bien su contraseña de AutenticA, o bien, la contraseña de su organismo, que utiliza habitualmente para su PC o su correo.

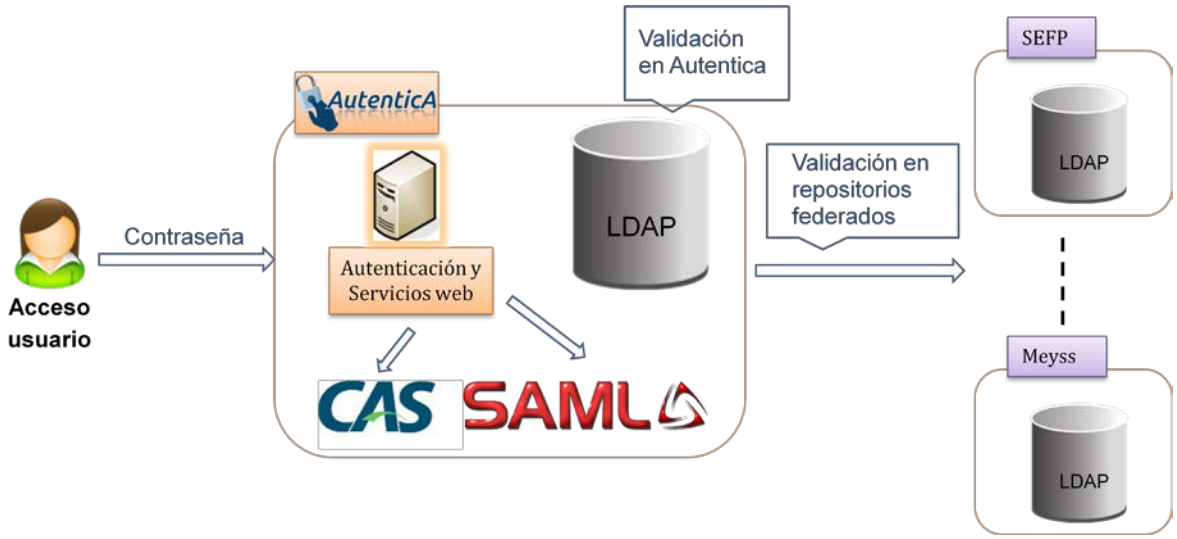


Ilustración 1. Esquema de funcionamiento

Cada aplicación puede determinar qué medios de autenticación permite para el acceso a la misma. Estos medios vendrán determinados por el nivel de autenticación de la aplicación según el Esquema Nacional de Seguridad (ENS), según se muestra en la tabla siguiente:

Nivel ENS	Nivel de Registro	Credencial	Modo de registro	Nivel LOPD
Básico	Básico	Contraseña débil	Telemático a partir de datos del LDAP	-
	Fuerte	Contraseña fuerte	Telemático con certificado electrónico	Desde Bajo
Medio	Fuerte	Contraseña fuerte con doble factor (2018)	Telemático con certificado electrónico	Desde Bajo
	Fuerte	Certificado en soporte SW	Presencial	Desde Bajo
Alto	Fuerte	DNI electrónico Certificado soporte HW	Presencial	Desde Bajo

Interoperabilidad

AutenticA soporta el protocolo de identificación y autenticación estándar *Security Assertion Markup Language* (SAML) en su versión 2.0. Adicionalmente, el servicio se encuentra integrado con DIR3, por lo que la codificación de unidades a las que están adscritos 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.

Provisión de usuarios

La forma principal de provisión de usuarios 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:

- Registro Central de Personal.
- Registro de funcionarios locales con habilitación nacional.
- Aplicación de Cargos Representativos.
- Aplicación de Altos Cargos (incorporación en desarrollo).
- Portal de EE.LL.
- LDAP de la SEFP.

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 en situación de servicio 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. 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. Por último, el LDAP de la SEFP contiene los usuarios de dicha Secretaría de Estado.

Próximamente se incorporará la información de la aplicación de Altos Cargos de la AGE.

Adicionalmente a la provisión desde fuentes primarias, también se permite la realización de altas de forma manual por un administrador de AutenticA. Para ello, se considera un grupo de administración central además de una estructura de administradores delegados en diferentes organismos, o de administradores de aplicaciones que puedan realizar la gestión de usuarios en su ámbito.

Los usuarios que no estén incluidos en el repositorio de AutenticA pueden solicitar su alta mediante el formulario de autoregistro que recoge sus datos personales y de destino, debiendo ser firmado electrónicamente por los interesados. 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 a AutenticA, 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.

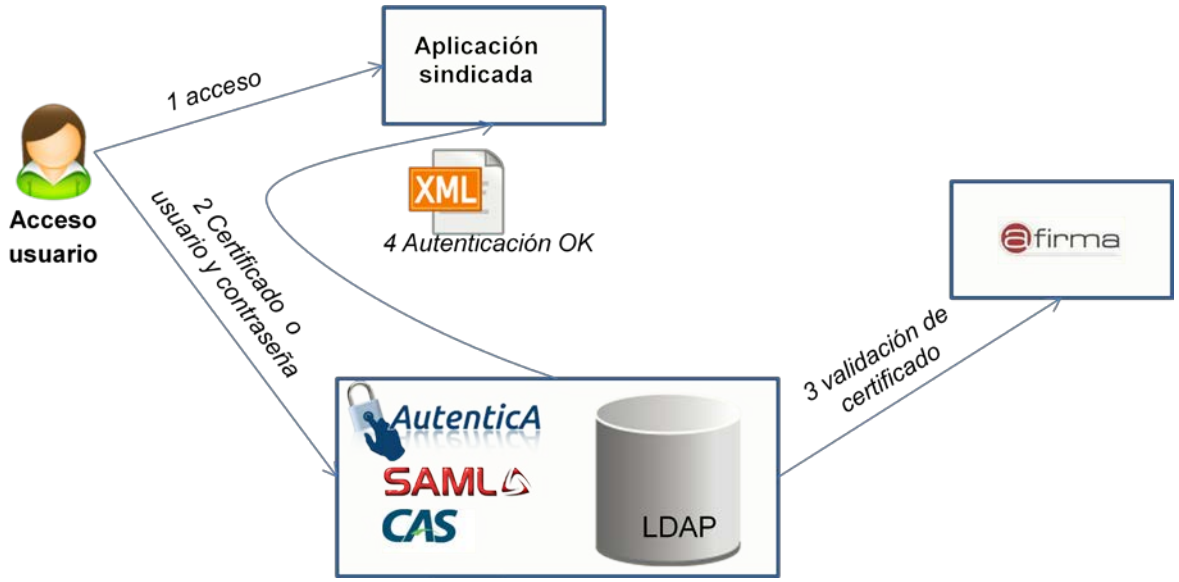
Integración de aplicaciones y librería de integración

La integración o sindicación de aplicaciones con AutenticA se puede hacer mediante el uso de protocolo SAML o mediante protocolo propio de AutenticA, basado en CAS.

Para facilitar la sindicación de aplicaciones, se ha desarrollado una librería de integración que se ofrece para tres tecnologías: Java, PHP y .NET. Esta librería proporciona un API para el acceso a la información enviada por AutenticA a la aplicación, evitando desarrollos adicionales por parte de las aplicaciones que se integran.

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, 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

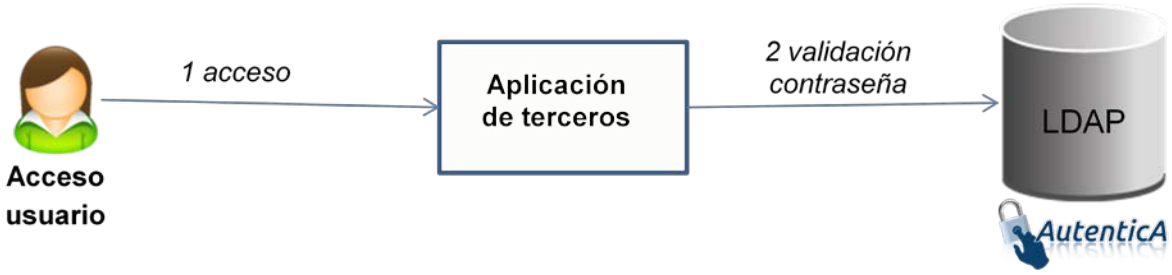
en el repositorio LDAP, que se entrega a la aplicación inicial en un XML de respuesta. En el XML se incluyen también los permisos del usuario dentro de la aplicación a la que se va a conectar. Como medida de seguridad, este XML se facilita firmado electrónicamente. Finalmente, el servicio devuelve el control de la navegación a la aplicación.



Si fuera necesario integrar herramientas de terceros que no soporten SAML (como por ejemplo con un cliente de correo electrónico), AutenticA permite la autenticación LDAP, en cuyo caso sólo se podrá acceder mediante contraseña, debiendo configurar la aplicación para uso del LDAP de AutenticA. Este procedimiento se muestra en la siguiente ilustración.

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.



Conclusiones

El servicio AutenticA es un servicio común que permite a las aplicaciones delegar la gestión completa de usuarios, con el consiguiente ahorro en desarrollo y explotación.

AutenticA ofrece servicios de autenticación, autorización y SSO a aplicaciones internas, a las que provee de información del usuario.

Dispone de un repositorio de usuarios que contiene empleados públicos, altos cargos y personal relacionado con las AA.PP. Almacena información de unidad y puesto, incluyendo correo electrónico y teléfono.

La provisión de usuarios se realiza desde fuentes primarias de calidad, como el Registro Central de Personal, entre otras. También se dispone de una estructura de administradores delegados corresponsables, para altas y visto bueno de autoregistros.

AutenciA es una solución interoperable, mediante el uso de protocolos estándar como SAML2.0 e integración con DIR3.

Como ventaja a su implantación, el servicio dispone de una librería de integración para facilitar y agilizar la sindicación de aplicaciones.

Autor: Federico Castejón Lapeyra

Secretaría General de Administración Digital

Ministerio de Hacienda y Función Pública