Manual del integrador

Autentica

Versión 1.14.1

Fecha de versión 26/01/2024

Madrid, 26 de enero de 2024

Elaborado por la Secretaría General de Administración Digital

NIPO: Pendiente de asignación.

ÍNDICE

1. OBJETO

El presente documento servirá de guía técnica para aquellas aplicaciones que vayan a consumir los servicios que Autentica presta, detallando las indicaciones necesarias para su integración.

2. DESCRIPCIÓN

Cualquier aplicación será susceptible de integrarse con el repositorio horizontal de usuarios e identidad digital, Autentica, para tener acceso a los servicios que éste ofrece.

2.1. Servicios disponibles

Los servicios que se ofrecen desde Autentica son:

- Servicios de autenticación
- Servicios de autorización
- Servicios de provisión de atributos de usuario
- Servicios de Single Sign On (SSO)
- Servicios de aprovisionamiento y gestión de usuarios
- Servicios de interoperabilidad con diferentes escenarios de integración

2.2. ACL de Autentica

Será necesario la cumplimentación del ACL por parte de cualquier aplicación que desee integrarse con Autentica. El ACL estará disponible en el apartado de Autentica dentro del portal de Administración Electrónica (PAe), sección descargas y se hará llegar al equipo de Autentica cumplimentado a través de correo electrónico o a través de su buzón de incidencias https://ssweb.seap.minhap.es/ayuda/consulta/autentica

2.3. Nivel de seguridad de la autenticación

En Autentica existen varios niveles de autenticación configurables en función de la necesidad de la aplicación y del nivel de seguridad requerido para la misma, ya sea por la información que maneja, el tipo de usuario que accede u otras connotaciones de seguridad:

- Nivel 1
    - Obsoleto.
- Nivel 2
    - Bajo aseguramiento: existe validación que indica que las credenciales pertenecen a personas reales.
- Nivel 3
    - Aseguramiento sustancial: para la entrega de la credencial se requiere registro presencial, al menos una vez, por parte del usuario.
- Nivel 4

- Alto aseguramiento: para la entrega de la credencial se requiere registro presencial, al menos una vez, por parte del usuario. La credencial electrónica se entrega como certificado hardware criptográfico.

Esta configuración será llevada a cabo por un administrador central. De esta forma se asociará a la aplicación que finalmente realizará la integración.

Los niveles de seguridad arriba indicados se extrapolan con los sistemas de identificación existentes en Autentica:

Sistemas de identificación	
Nivel 2 (básico)	• Contraseña fuerte • Certificado electrónico • Contraseña débil únicamente en algunos casos concretos y bajo supervisión de un administrador • Acceso a internet a través de contraseña supervisado por administrador
Nivel 3 (medio/sustancial)	• Certificado electrónico con software • Certificado electrónico con hardware criptográfico
Nivel 4 (alto)	• Certificado electrónico con hardware criptográfico

2.4. Doble factor

La opción de autenticación con doble factor en Autentica, pretende dotar de un mecanismo de seguridad adicional destinado a todas aquellas aplicaciones que así lo requieran. Es un método para confirmar la identidad de un usuario utilizando algo que conocen (contraseña) y un segundo factor distinto a lo que sean o posean. Como segundo paso, el usuario debe introducir algo que le sea enviado a través de un medio alternativo.

Este mecanismo podrá ser configurable en función de la necesidad de la aplicación y del nivel de seguridad requerido para la misma. Dicho mecanismo de seguridad, será un mecanismo que se usará en paralelo con los niveles de seguridad actuales, pudiendo combinarse con todos ellos, excepto con el nivel 1, con el que no será compatible.

Para la utilización de este mecanismo debe configurarse:

- El tipo de envío del código de seguridad, ya sea a través del correo electrónico o a través de un mensaje corto SMS.
- La duración en minutos destinada a la caducidad del código.
- El número de caracteres que contendrá el código de seguridad.

2.5. Nivel de fiabilidad

Todos los usuarios cuentan con un nivel de fiabilidad del dato en base a la fuente de procedencia del mismo. Si proviene de una fuente registral (caso de RCP por ejemplo), el nivel de fiabilidad será bueno. En caso contrario el nivel de fiabilidad será sustancial o bajo.

El campo destinado a la gestión del nivel de fiabilidad en el LDAP es **dir4Assurance** y se devuelve en el XML de respuesta y en varios servicios web (ver manual de servicios web e interoperabilidad).

Los valores que actualmente contempla el atributo **dir4Assurance** son:

- 3 - Bueno
- 2 - Sustancial
- 1 - Bajo
- 0 – Nulo

2.6. Fuente de procedencia

Todos los usuarios cuentan con un atributo que determina la fuente de procedencia del usuario en base al mecanismo por el que ha llegado a formar parte del repositorio de Autentica. Dicho atributo se denomina dir4OriginSource, y refleja si se trata de un usuario provisto a través de alguna de las fuentes primarias de datos con sincronización incluida:

- Registro Central de Personal
- Registro de Entidades Locales
- Registro de Comunidades Autónomas
- Registro de Funcionarios de administración local con habilitación de carácter nacional
- Registro de Cargos Representativos
- Usuarios pertenecientes a la aplicación del Registro de Bienes y Derechos Patrimoniales de altos cargos
- Usuarios pertenecientes al LDAP de la SGAD

O a través de un alta manual:

- Alta a través de un administrador
- Alta a través de autoregistro
- Alta a través de servicios web
- Alta a través de alguna migración de datos puntual, requerida p.e. por alguna aplicación.

En función de cómo haya sido provisto el usuario en Autentica, se determinará su fuente de procedencia para la valoración final de la aplicación.

2.7. Single Sign On

Para tener acceso (independientemente del servicio de autenticación) al servicio de Single Sign On, la aplicación ha de estar federada con el repositorio. Para ello se deberá dar de alta a través del gestor de aplicaciones y por tanto deberá existir petición previa, como parte de la gestión.

Para aquellas aplicaciones que deseen usar el servicio de autenticación para el registro de sus usuarios y no el servicio de SSO, será necesario que en el proceso de alta o modificación de dicha aplicación no se marque la opción correspondiente para disponer de SSO.

El servicio de Single Sign On tiene en cuenta el nivel de seguridad de cada aplicación, de modo que no es posible acceder a una aplicación habiéndose autenticado previamente en otra con un mecanismo de autenticación no permitido en la segunda.

2.8. Alta de la aplicación

Será necesario cumplimentar el ACL (disponible en el portal del PAE, sección descargas) y posteriormente enviarlo al equipo de Autentica a través de su buzón de incidencias (https://ssweb.seap.minhap.es/ayuda/consulta/autentica). De esta manera la aplicación pasará a formar parte de Autentica. Los valores principales son:

- **Nombre**: nombre la aplicación
- **URL de respuesta**: URL a la que será redireccionada la petición cuando se haya llevado a cabo la validación de forma satisfactoria.
- **IP**: se refiere a la IP (o IPs) que se resuelve por DNS de la URL de la aplicación. Cuando se reciba la petición de autenticación de un usuario, se comprobará la IP proveniente y se comparará con la almacenada en este campo. Si no coinciden, no se permitirá la comunicación.
- **Correo electrónico**: correo electrónico del administrador de la aplicación. Este dato es importante, dado que en esta cuenta de correo electrónico el administrador recibirá las instrucciones necesarias para formalizar la adscripción de la aplicación al repositorio u otro tipo de notificaciones.

- **Autorización**: determina si la aplicación consumirá servicios de autorización en Autentica.
- **Acceso desde internet**: determina si se permitirán las autenticaciones en la aplicación desde internet a través de usuario y contraseña.

2.9. Autenticación basada en SAML

Autentica soporta como medio de autenticación de usuarios la especificación SAML (Security Assertion Markup Language), el cual se recomienda su uso. Para realizar la integración de una aplicación en Autentica y que ésta use SAML para la autenticación de sus usuarios es necesario que dicha aplicación esté dada de alta en el módulo de aprovisionamiento y que en el apartado "Métodos de autenticación" esté seleccionado como método una de las dos opciones de SAML existentes, SAML Estándar y SAML Autentica. Esta acción únicamente la puede llevar a cabo un administrador central de Autentica.

La especificación SAML define tres roles:

- **Principal**, que representa al usuario que desea realizar la autenticación en una aplicación integrada con Autentica y que por tanto, solicita un servicio.
- **Proveedor de identidad**, en este caso es Autentica.
- **Proveedor de servicio**, que representa a la aplicación destino a la cual se desea acceder por parte del usuario.

En este escenario, el rol principal sería el usuario que desea autenticarse en una aplicación. Éste solicita acceso al proveedor de servicio, que será la aplicación a la cual desea acceder. El proveedor de servicio, a su vez, solicita y obtiene en caso de éxito, una confirmación de identidad desde el proveedor de identidad, que es Autentica. Teniendo como base la confirmación recibida por parte del proveedor de identidad, el proveedor de servicio suministrará la respuesta que considere oportuno al usuario, permitiendo o no el acceso a la aplicación.

En el caso de que la aplicación que vaya a utilizar el protocolo SAML Estándar así lo requiera, podrá solicitar a Autentica el fichero IdPMetadata.xml, el cual se generará a partir de la información suministrada por la propia aplicación por medio del fichero spMetadata.xml proporcionado para la configuración de la misma.

A continuación se indica un ejemplo de un fichero IdPMetadata.xml generado:

```
<?xml version="1.0" ?>
md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2024-09-20T01:20:59.933Z" cacheDuration="PT1613042423S" entityID="samlAutentica">
                    <md:IDPSSODescriptor                    WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
md:KeyDescriptor use="signing">
ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
ds:X509Data>
```

<ds:X509Certificate>MIIHqzCCBpOgAwIBAgIQBQAPcTH2xF1eHeQUoOpo9jANBgkqhkiG9w
0BAQsFADBHMQswCQYDVQQGEwJFUzERMA8GA1UECgwIRk5NVC1SQ00xJTAjBgNVBAsM
HEFDIENvbXBvbmVudGVzIEluZm9ybcOhdGljb3MwHhcNMjAwMTE0MTU1MzU2WhcNMjM
wMTE0MTU1MzU1WjCB1zELMAkGA1UEBhMCRVMxDzANBgNVBAcMBk1BRFJJRDEwMC4GA
1UECgwnU0VDUkVUQVJJQSBERSBFU1RBRE8gREUgRlVOQ0lPTiBQVUJMSUNBMTUwMwYD
VQQLDCxTRUNSRVRBUklBIEdFTkVSQUwgREUgQURNSU5JU1RSQUNJT04gRElHSVRBTDES
MBAGA1UEBRMJUzI4MzMwMDJFMRgwFgYDVQRhDA9WQVRFUy1TMjgzMzAwMkUxIDAeB
gNVBAMMF1NFTExPIEVOVElEQUQgU0dBRCBTU0NDMIIBIjANBgkqhkiG9w0BAQEFAAOCA
Q8AMIIBCgKCAQEArjlfI2yZW12ZY2q8I+/VIFBcXmGm5qnfs5zeiKTQzFOGukWsJarVTz5jn
qD+LItwyyvag9d5CjdCiYeHrSaXAaAjXnUNCtEioZKZFtL8TiKNWwQKzE0YKkcVHH4pPA09H
GkONXpNjWWjRclar+cVFUTy5BLVDpcLaoCqFveGAPt0Aec9xqkEBcvNof1jJCJL3lpR0KUB7r
Z3vs6x8yLq8CzdJBOqmP09TDtc0opwV7SYwiCqabVWgWQreJauiaACe4zEDYlt0r6Iypw1JE
XYQPGoe3MGXvTLopx8rJxUIUuqgRzb2Ibj59nTM7myJn6tTif36+IHpjM67CzS8qnndwIDA
QABo4IEADCCA/wwDAYDVR0TAQH/BAIwADCBgQYIKwYBBQUHAQEEdTBzMDsGCCsGAQ
UFBzABhi9odHRwOi8vb2NzcGNvbXAuY2VydC5mbm10LmVzL29jc3AvT2NzcFJlc3BvbmRlc
jA0BggrBgEFBQcwAoYoaHR0cDovL3d3dy5jZXJ0LmZubXQuZXMvY2VydHMvQUNDT01QLm
NydDCCATQGA1UdIASCASswggEnMIIBGAYKKwYBBAGsZgMJEzCCAQgwKQYIKwYBBQUH
AgEWHWh0dHA6Ly93d3cuY2VydC5mbm10LmVzL2RwY3MvMIHaBggrBgEFBQcCAjCBzQy
BykNlcnRpZmljYWRvIGN1YWxpZmljYWRvIGRlIHNlbGxvIGVsZWN0cOzbmljbyBzZWfDu
m4gcmVnbGFtZW50byBldXJvcGVvIGVJREFTLiBTdWpldG8gYSBsYXMgY29uZGljaW9uZXM
gZGUgdXNvIGV4cHVlc3RhcyBlbiBsYSBEUEMgZGUgRk5NVC1SQ00gY29uIE5JRjogUTI4MjY
wMDQtSiAoQy9Kb3JnZSBKdWFuIDEwNi0yODAwOS1NYWRyaWQtRXNwYcOxYSkwCQYHB
ACL7EABATA1BgNVHREELjAspCowKDEmMCQGCSsGAQQBrGYBCAwXU0VMTE8gRU5USUR
BRCBTR0FEIFNTQ0MwEwYDVR0lBAwwCgYIKwYBBQUHAwIwDgYDVR0PAQH/BAQDAgXg
MB0GA1UdDgQWBBTXGrsuGTf4yebIh6SSwlc1/xSrITCBsAYIKwYBBQUHAQMEgaMwgaAw
CAYGBACORgEBMAsGBgQAjkYBAwIBDzATBgYEAI5GAQYwCQYHBACORgEGAjByBgYEAI5
GAQUwaDAyFixodHRwczovL3d3dy5jZXJ0LmZubXQuZXMvcGRzL1BEU19DT01QX2VzLnBkZ
hMCZXMwMhYsaHR0cHM6Ly93d3cuY2VydC5mbm10LmVzL3Bkcy9QRFNfQ09NUF9lbi5wZ
GYTAmVuMB8GA1UdIwQYMBaAFBn4WC8U1qbMmwSYCA1M16sAp4NlMIHgBgNVHR8Egd
gwgdUwgdKggc+ggcyGgZ5sZGFwOi8vbGRhcGNvbXAuY2VydC5mbm10LmVzL0NOPUNST
DEsT1U9QUMlMjBDb21wb25lbnRlcyUyMEluZm9ybWF0aWNvcyxPPUZOTVQtUkNNLEM9RV
M/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDtiaW5hcnk/YmFzZT9vYmplY3RjbGFzcz1jU
kxEaXN0cmlidXRpb25Qb2ludIYpaHR0cDovL3d3dy5jZXJ0LmZubXQuZXMvY3Jsc2NvbXAv
Q1JMMS5jcmwwDQYJKoZIhvcNAQELBQADggEBAIywbm2i+VvROyaJjUT02tlq9XFz9umCS
y6BN2TF0AFq/c4IhVj8b7tjNJ6MemUpK/QkeWXDasobbhwYXw0HbuO3zo20kueK3X11nV
M4IxD+XwnDLM9p8VmxO6BbFbNiAhiBmvaee8b7/mby/CbCIV0sOplkcjYmWRz7NU/AKJg
dh3+v/jloVjLkVV+dC1PQu9uQ2yzZpHNagwtI457ktrtafje8o/Xamfx+6CQb1+TsmwSOqX9
+NQ1cTM7Nj5HoXNPqlePiFj62UbhfC31nEMakJs+8Q1WrNdpyCISmixHhldguf3vff0l4KwBz
M8sHVQ/j4CxwVut6oF42xOufBH4=</ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

</md:KeyDescriptor>

md:KeyDescriptor use="**encryption**">

ds:KeyInfo xmlns:ds="**http://www.w3.org/2000/09/xmldsig#**">

ds:X509Data>

<ds:X509Certificate>MIIHqzCCBpOgAwIBAgIQBQAPcTH2xF1eHeQUoOpo9jANBgkqhkiG9w
0BAQsFADBHMQswCQYDVQQGEwJFUzERMA8GA1UECgwIRk5NVC1SQ00xJTAjBgNVBAsM
HEFDIENvbXBvbmVudGVzIEluZm9ybcOhdGljb3MwHhcNMjAwMTE0MTU1MzU2WhcNMjM
wMTE0MTU1MzU1WjCB1zELMAkGA1UEBhMCRVMxDzANBgNVBAcMBk1BRFJJRDEwMC4GA
1UECgwnU0VDUkVUQVJJQSBERSBFU1RBRE8gREUgRlVOQ0lPTiBQVUJMSUNBMTUwMwYD

VQQLDCxTRUNSRVRBUklBIEdFTkVSQUwgREUgQURNSU5JU1RSQUNJT04gRElHSVRBTDES
MBAGA1UEBRMJUzI4MzMwMDJFMRgwFgYDVQRhDA9WQVRFUy1TMjgzMzAwMkUxIDAeB
gNVBAMMF1NFTExPIEVOVElEQUQgU0dBRCBTU0NDMIIBIjANBgkqhkiG9w0BAQEFAAOCA
Q8AMIIBCgKCAQEArjlfI2yZW12ZY2q8I+/VIFBcXmGm5qnfs5zeiKTQzFOGukWsJarVTz5jn
qD+LItwyyvag9d5CjdCiYeHrSaXAaAjXnUNCtEioZKZFtL8TiKNWwQKzE0YKkcVHH4pPA09H
GkONXpNjWWjRclar+cVFUTy5BLVDpcLaoCqFveGAPt0Aec9xqkEBcvNof1jJCJL3lpR0KUB7r
Z3vs6x8yLq8CzdJBOqmP09TDtc0opwV7SYwiCqabVWgWQreJauiaACe4zEDYlt0r6Iypw1JE
XYQPGoe3MGXvTLopx8rJxUIUuqgRzb2Ibj59nTM7myJn6tTif36+IHpjM67CzS8qnndwIDA
QABo4IEADCCA/wwDAYDVR0TAQH/BAIwADCBgQYIKwYBBQUHAQEEdTBzMDsGCCsGAQ
UFBzABhi9odHRwOi8vb2NzcGNvbXAuY2VydC5mbm10LmVzL29jc3AvT2NzcFJlc3BvbmRlc
jA0BggrBgEFBQcwAoYoaHR0cDovL3d3dy5jZXJ0LmZubXQuZXMvY2VydHMvQUNDT01QLm
NydDCCATQGA1UdIASCASswggEnMIIBGAYKKwYBBAGsZgMJEzCCAQgwKQYIKwYBBQUH
AgEWHWh0dHA6Ly93d3cuY2VydC5mbm10LmVzL2RwY3MvMIHaBggrBgEFBQcCAjCBzQy
BykNlcnRpZmljYWRvIGN1YWxpZmljYWRvIGRlIHNlbGxvIGVsZWN0csOzbmljbyBzZWfDu
m4gcmVnbGFtZW50byBldXJvcGVvIGVJREFTLiBTdWpldG8gYSBsYXMgY29uZGljaW9uZXM
gZGUgdXNvIGV4cHVlc3RhcyBlbiBsYSBEUEMgZGUgRk5NVC1SQ00gY29uIE5JRjogUTI4MjY
wMDQtSiAoQy9Kb3JnZSBKdWFuIDEwNi0yODAwOS1NYWRyaWQtRXNwYcOxYSkwCQYHB
ACL7EABATA1BgNVHREELjAspCowKDEmMCQGCSsGAQQBrGYBCAwXU0VMTE8gRU5USUR
BRCBTR0FEIFNTQ0MwEwYDVR0lBAwwCgYIKwYBBQUHAwIwDgYDVR0PAQH/BAQDAgXg
MB0GA1UdDgQWBBTXGrsuGTf4yebIh6SSwlc1/xSrITCBsAYIKwYBBQUHAQMEgaMwgaAw
CAYGBACORgEBMAsGBgQAjkYBAwIBDzATBgYEAI5GAQYwCQYHBACORgEGAjByBgYEAI5
GAQUwaDAyFixodHRwczovL3d3dy5jZXJ0LmZubXQuZXMvcGRzL1BEU19DT01QX2VzLnBkZ
hMCZXMwMhYsaHR0cHM6Ly93d3cuY2VydC5mbm10LmVzL3Bkcy9QRFNfQ09NUF9lbi5wZ
GYTAmVuMB8GA1UdIwQYMBaAFBn4WC8U1qbMmwSYCA1M16sAp4NlMIHgBgNVHR8Egd
gwgdUwgdKggc+ggcyGgZ5sZGFwOi8vbGRhcGNvbXAuY2VydC5mbm10LmVzL0NOPUNST
DEsT1U9QUMlMjBDb21wb25lbnRlcyUyMEluZm9ybWF0aWNvcyxPPUZOTVQtUkNNLEM9RV
M/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDtiaW5hcnk/YmplY3RjbGFzcz1jU
kxEaXN0cmlidXRpb25Qb2ludIYpaHR0cDovL3d3dy5jZXJ0LmZubXQuZXMvY3Jsc2NvbXAv
Q1JMMS5jcmwwDQYJKoZIhvcNAQELBQADggEBAIywbm2i+VvROyaJjUT02tlq9XFz9umCS
y6BN2TF0AFq/c4IhVj8b7tjNJ6MemUpK/QkeWXDasobbhwYXw0HbuO3zo20kueK3X11nV
M4IxD+XwnDLM9p8VmxO6BbFbNiAhiBmvaee8b7/mby/CbCIV0sOplkcjYmWRz7NU/AKJg
dh3+v/jloVjLkVV+dC1PQu9uQ2yzZpHNagwtI457ktrtafje8o/Xamfx+6CQb1+TsmwSOqX9
+NQ1cTM7Nj5HoXNPqlePiFj62UbhfC31nEMakJs+8Q1WrNdpyCISmixHhldguf3vff0l4KwBz
M8sHVQ/j4CxwVut6oF42xOufBH4=

</ds:X509Data>

</ds:KeyInfo>

</md:KeyDescriptor>

<md:SingleLogoutService Binding="**urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect**" Location="**https://autentica.redsara.es/Autentica/servlet/AutenticaServlet?dispatcher=LOGOUT**" />

<md:NameIDFormat>**urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**</md:NameIDFormat>

<md:SingleSignOnService Binding="**urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect**" Location="**https://autentica.redsara.es/Autentica/servlet/AutenticaServlet?action=goToAutentica&appId=2945**" />

</md:IDPSSODescriptor>

</md:EntityDescriptor>

2.9.1. URL de acceso

Será necesario reemplazar el sistema nativo de autenticación de la aplicación a integrar, por el que Autentica provee. Este sistema que Autentica provee consiste básicamente en la invocación de una URL. Se invocará una URL del tipo:

https://autentica.redsara.es/Autentica/servlet/AutenticaServlet?action=goToAutentica&appId=[**IDENTIFICADOR_APLICACIÓN**]

El identificador de la aplicación será un valor numérico que se debe proveer desde Autentica. Una vez invocada la URL desde la aplicación por un usuario que desea autenticarse, Autentica tomará el control de la navegación e intentará leer el certificado electrónico del usuario si se encuentra en el repositorio del navegador (en base al nivel de seguridad establecido para la aplicación, para más detalles revisar el apartado 2.3). En caso contrario, el sistema mostrará la página para informar el usuario y contraseña.

2.9.2. SAML Autentica

En el caso de que para realizar la llamada a Autentica se esté redireccionando desde una tercera página web, se recomienda usar la instrucción JavaScript “replace()”. A continuación se muestran algunos ejemplos del uso de esta instrucción:

En el caso de que sea necesario pasar la redirección por una tercera página, se recomienda usar la función replace() de JS:

```
13   <script>
14
15   location.replace("https://pre-autentica.redsara.es/Autentica/servlet/AutenticaServlet?action=goToAutentica&appId=1481")

16   </script>
```

O en el caso de que no exista una página intermedia la llamada se puede realizar usando un “<href>” estándar:

```
1  <html lang="es">
2   <head>
3    <meta charset="ISO-8859-1">
4    <title>Pagina autenticación</title>
5    <meta name="description" content="Test autenticación Autentica">
6   </head>
7    <body>
8      <a href="https://autentica.redsara.es/Autentica/servlet/AutenticaServlet?action=goToAutentica&appId=[IDENTIFICADOR_APLICACIÓN]">
9         Acceso a login
10     </a>
11   </body>
12  </head>
13 </html>
```

2.9.2.1. XML de respuesta

Una vez desencriptada la respuesta de SAML, la variable “assertion” contiene todos los datos que interesan recoger de la “SAMLResponse”. Dentro del atributo “AUTENTICA_USER_XML” se encuentran los datos relacionados con el usuario, nombre, apellidos, cargo, puesto, destino, organismo, etc., estarán encriptados por lo que será necesario desencriptarlos nuevamente en base64 de la misma forma que la “SAMLResponse”.

Ahora se tratará el AUTENTICA_USER_XML de la forma que se considere oportuno.

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<respuesta>
  <resultado>OK</resultado>
  <usuario>
        <id>1R</id>
        <userName>1R</userName>
         <isCitizen>false</isCitizen>
         <dir4DocumentID>1R</dir4DocumentID>
         <dir4DocumentType>01</dir4DocumentType>
         <cn>Nombre Ape1 Ape2</cn>
         <givenName>Nombre</givenName>
         <sn>Ape1</sn>
         <dir4LastName>Ape2</dir4LastName>
         <dir4Email>nombreape1@correo.gob.es</dir4Email>
         <dir4UserDateOfBirth>21/02/1972</dir4UserDateOfBirth>
          <dir4UserLocalityCode>1301</dir4UserLocalityCode>
          <dir4UserLocalityEntity>01</dir4UserLocalityEntity>
```

<dir4UserLocality>**Jaca**</dir4UserLocality>
<dir4UserCountryCode>**724**</dir4UserCountryCode>
<dir4UserCountry>**España**</dir4UserCountry>
<dir4UserProvinceCode>**22**</dir4UserProvinceCode>
<dir4UserProvince>**Huesca**</dir4UserProvince>
<dir4UserCCAACode>**02**</dir4UserCCAACode>
<dir4UserCCAA>**Aragón**</dir4UserCCAA>
<dir4AdministrationLevel>**1**</dir4AdministrationLevel>
<dir4OrganizationCode>**E00003801**</dir4OrganizationCode>
<dir4OrganizationDesc>**Ministerio del Interior**</dir4OrganizationDesc>
<dir4DirCenCode>**E00128701**</dir4DirCenCode>
<dir4DirCenDesc>**Subsecretaria del Interior**</dir4DirCenDesc>
<dir4JobCentreCode>**E03112104**</dir4JobCentreCode>
<dir4JobCentreDesc>**S.G. de Tecnologias de la Informacion y las Comunicaciones**</dir4JobCentreDesc>
<dir4OrganicalUnitCodeDir3>**E03112104**</dir4OrganicalUnitCodeDir3>
<st>**Madrid**</st>
<l>**Madrid**</l>
<postalCode>**28071**</postalCode>
<street>**CALLE Amador de los Ríos**</street>
<employeeType>**OTROS**</employeeType>
<telephoneNumber>**913434359**</telephoneNumber>
<title>**ANALISTA DE SISTEMAS**</title>
<uid>**1R**</uid>

<dir4UserName>**1R**</dir4UserName>
<dir4LdapBranch>**aapp**</dir4LdapBranch>
<dir4OriginSource>**Administrador**</dir4OriginSource>
<dir4SystemRegisterDate>**05/02/2014 10:24:31**</dir4SystemRegisterDate>
<dir4LastEntryDate>**13/06/2017 10:18:08**</dir4LastEntryDate>
<dir4Observations>**CERTIFICADO**</dir4Observations>
</usuario>
<Signature xmlns="**http://www.w3.org/2000/09/xmldsig#**">
<SignedInfo>
<CanonicalizationMethod Algorithm="**http://www.w3.org/TR/2001/REC-xml-c14n-20010315**" />
<SignatureMethod Algorithm="**http://www.w3.org/2000/09/xmldsig#rsa-sha1**" />
<Reference URI="">
<Transforms>
<Transform Algorithm="**http://www.w3.org/2000/09/xmldsig#enveloped-signature**" />
</Transforms>
<DigestMethod Algorithm="**http://www.w3.org/2000/09/xmldsig#sha1**" />
<DigestValue>**GIuvZt8mOoVGs+E4IxvZIHnCKTo=**</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>**KWRGET+DG7IQReqW1gGU3pqZsgBoO3gmOjIC1MnekH4wWjmemF6W7wf64+6TQJOmGHPlJ+E720vH RbZo+CgpbCHjnFnv81cRfDMGBZCbpETN7r7vp6rat1YP67K5lDWEtr9CxbgTwxBU+2Iq4pl9UQDD HovzTqlgIAeJhMlERtaW07pGDzhh+rOLLMaSpW+0Q6dsT5fkcfn4gSmgfXbhAACm84Kvn2VNHJkI I4Q5zUrWwGWPQVBrVMVsCMdop42wq+Y6r3RVkRTJOHXeckEqoOo/sUWicVSNiYy13IkpoY1MA5cW v009FE0l3RRi7tS+2TovhSRoyaTmfbBSgKhkgg==**</SignatureValue>
<KeyInfo>

<X509Data>
<X509SubjectName>**CN=AUTENTICA,OU=DTIC,O=DTIC,L=MAD,ST=MAD,C=ES**</X509SubjectName>
<X509Certificate>**MIIDXjCCAkagAwIBAgIBQDANBgkqhkiG9w0BAQsFADCBiTELMAkGA1UEBhMCRVMxDzANBgNVBAgT**
Bk1BRFJJRDEPMA0GA1UEBxMGTUFEUklEMQwwCgYDVQQKEwNNUFIxFjAUBgNVBAsTDVNBUkEgU0lT
VEVNQVMxDTALBgNVBAMTBFNBUkExIzAhBgkqhkiG9w0BCQEWFHNpc3RlbWFzLXNncGRAbXByLmVz
MB4XDTE2MDEyNjE2MzIwMFoXDTI5MDEyNjE2MzIwMFowWzELMAkGA1UEBhMCRVMxDDAKBgNVBAgT
A01BRDEMMAoGA1UEBxMDTUFEMQ0wCwYDVQQKEwREVElDMQ0wCwYDVQQLEwREVElDMRIwEAYDVQQD
EwlBVVRFTlRJQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDzIi1nGPOk0a2GM5/8
vMqVk4IuxOw9xETEVRojf5YfBcAlrGEodFp3+qfV+McD+5cEah9Gkkm+LC0rEnu7aa4leDs0pMS2
/VnQToAtSFYA2cwpLOyrXkjK7EFSIOqoYpYXL6OM71MWqqasWIdlND7dH8L4Vy4FUHndYNv815/E
DFGiECIjsI6YUrMXaUoY6sjyu1+O5mVb6Dv/F6olcNibnGCfVS3ZN2rhITLflfIewH8g8iUSD9sl
Gc4qi5l1gHFMfHmOVAEaAr0wrRA2XLEVqiY2DsRIgPMHik1go/yREKHWlxtYyqgDFqzowDeP2icP
p/Qc0dn5qFz2Zep4gliDAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAHVEE1814THH+LyVDfQIqqXG
Q5Dw6ZojVsKM9+3E+SY4OKK51sIaY7GMcRHQ1fcpgiF+Rm8g3M3N8fAVplMBbJb554QVa/u8bOgV
ooGKn5j51lsJ705Rwvs8r/1nB0LSN5XDBcGD1SbsBnjw1qZrsw/DghobMcqOV8FpRQvdht0rAiEl
COuho8Ow2BOCY8EJTof5nS87cn3G7HKYq7k1TQhffj8qeAisTjcrn8u5DQhjIXyjmfGWwbrr3hei
TPa6DS7bDYXKpvVOKMhG+qOdC6WyJqNuhT63xFcRlU6sSvpb80+GGY6IPZVzUXMFQOelo/vsVmbD
K/LeTdxrDs4zy0k=</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
</respuesta>

El XML de respuesta irá firmado con certificado electrónico, por lo que se recomienda, en base a consideraciones de seguridad, verificar la autenticidad de dicha firma en todas las llamadas que se hagan a Autentica.

Para el tratamiento de este XML se encuentra la librería aut-sdk.jar disponible en el PAe, en su sección de descargas, la cual contiene métodos y funciones para el tratamiento y posterior validación contra @firma del XML.

2.9.3. SAML Estándar

La autenticación basada en el protocolo SAML Estándar permitirá seleccionar el tipo “HTTP-Post” o “HTTP-Redirect”. La selección de uno u otro se realizará previamente con el fin de que se pueda generar el fichero idPMetadata.xml correspondiente y pueda ser enviado a la aplicación invocante.

2.9.3.1. Ejemplo de invocación

A continuación se indica un ejemplo de invocación desde un enlace, indicando el parámetro SAMLRequest.

```
<fieldset>
    <legend>Circuit Integración</legend>
    <a href="https://des-autentica.redsara.es/Autentica/servlet/AutenticaServlet?action=goToAutentica&appId=3469&SAMLRequest=hVJNT+MwEP0rkQ/c3GTT0A/TdFVarbYS7EY0cNibaw9gKbGDZ1Lov8dJtwUuRfLpzbw38954hrKuGrFo6dnewUsLSNFbXVkUfSFnrbfCSTQorKwBBSmxWdzeiHSQiMY7cspV7BPlPEMigifjLIvWq5z56TabXD6OeKKzMc+kGvFtqid8mkA2/TGaXKZ6yKIH8BgoOQsKgYfYwtoiSUsBStKUJ0OejMtkItJxeP9YVHi3Mxr8n7BAzpbGq9ZQ8AiWjJIs+uW8gt5zzsi30KkWYTezgyOwCkkYK6kf/EzUoIhjDcjlUWbgQaP0cgAYn7Tj4G9XAX0gmwPwU6pe68mV7lS7kHVzJZtmrfNhNpr2i/eJXhurjX06H+b20ITid1kWvPi7KVm0OAa8dBbbGnw33ii4v7vJWb0/U2bzWXc/0efr599a/p/qLP7Mmh2+U5f7elW4yqh9F3Yt6byVDjGaP/atAqzy+4ZABz9V5V6XHiSdLhPPDzO//tr5Ow==&RelayState=ackacolfjc%26&SigAlg=abc">
        Acceso a Circuit Integración
    </a><br/>
</fieldset>
```

A continuación se muestra el mismo ejemplo pero invocando Autentica desde un formulario:

```
<fieldset>
```

```
Acceso a Circuit Integración
<form name="frm1" id="frm1" action="https://des-autentica.redsara.es/Autentica/servlet/AutenticaServlet" method="post">
<input type="hidden" id="action" name="action" value="goToAutentica"/>
<input type="hidden" id="appId" name="appId" value="3469"/>
<input type="hidden" id="SAMLRequest" name="SAMLRequest"
value="hVJNT+MwEP0rkQ/c3GTT0A/TdFVarbYS7EY0cNibaw9gKbGDZ1Lov8dJtwUuRfLpzbw38954hrKuGrFo6dnewUsLSNFbXVkUfSFnrbfC
STQorKwBBSmxWdzeiHSQiMY7cspV7BPlPEMigifjLIvWq5z56TabXD6OeKKzMc+kGvFtqid8mkA2/TGaXKZ6yKIH8BgoOQsKgYfYwtoiSUsBSt
KUJ0OejMtkItJxeP9YVHi3Mxr8n7BAzpbGq9ZQ8AiWjJIs+uW8gt5zzsi30KkWYTezgyOwCkkYK6kf/EzUoIhjDcjlUWbgQaP0cgAYn7Tj4G9XAX0g
mwPwU6pe68mV7lS7kHVzJZtmrfNhNpr2i/eJXhurjX06H+b20ITid1kWvPi7KVm0OAa8dBbbGnw33ii4v7vJWb0/U2bzWXc/0efr599a/p/qLP7Mmh
2+U5f7elW4yqh9F3Yt6byVDjGaP/atAqzy+4ZABz9V5V6XHiSdLhPPDzO//tr5Ow==" />
<input type="submit" value="Acceso" id="entrar" />
</form>
</fieldset>
```

2.9.3.2. SAML Request

A continuación se indica una posible petición SAML:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="b316a34c-d50a-4488-9519-d8875a6357fc" Version="2.0"
IssueInstant="2022-03-07T08:17:21Z" ProviderName="CircuitAutentica" ForceAuthn="true" IsPassive="true"
Destination="https://des-autentica.redsara.es/Autentica/servlet/AutenticaServlet?action=goToAutentica&appId=3469"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="myAssertionConsumerServiceURL">
saml:Issuer>https://des-autentica.redsara.es/Circuit</saml:Issuer>
```

```
samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted" AllowCreate="true" />
</samlp:AuthnRequest>
```

2.9.3.3. SAML Response

A continuación se indica una posible respuesta SAML, donde se devolverán los siguientes atributos del usuario que ha accedido de forma satisfactoria a la aplicación:

- email: contiene el correo electrónico del usuario.
- login: contiene el NIF\NIE del usuario.
- nombre: contiene el nombre del usuario.
- apellidos: contiene los apellidos del usuario.

```
- <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" ID="jnfbhneeinnfmkeapchdjapafalikbbdoekodkmm"
InResponseTo="b316a34c-d50a-4488-9519-d8875a6357fc" IssueInstant="2022-03-07T08:20:23Z" Version="2.0">
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://des-
autentica.redsara.es/samlAutentica/</saml:Issuer>
samlp:Status>
samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="nenpdnjhenjhgdmpadgflpdpbmadapmbkicgojge"
IssueInstant="2022-03-07T08:20:23Z" Version="2.0">
saml:Issuer>https://des-autentica.redsara.es/samlAutentica/</saml:Issuer>
```

```
ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
ds:SignedInfo>
ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
ds:Reference URI="#nenpdnjhenjhgdmpadgflpdpbmadapmbkicgojge">
ds:Transforms>
ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
 </ds:Transforms>
ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
ds:DigestValue>coS9Z9LOWG3XKa7SaWbDnXmtUb1hH3bALCO9OK+jVuU=</ds:DigestValue>
 </ds:Reference>
 </ds:SignedInfo>
            <ds:SignatureValue>B2MPJrDw8b+cnqjyY5WMFYlZacETdmlofyrqVHGB6XA3TavdJWjV/IzerbHeIMgyDy+OlK/IJspO
r80jsmBM9MP6daY/FWexVarx6sVRpzw2oiXT9n+/OikGuxGAYaiBCl3AlY7wlPTkhH+206mZ5udK
Mp4oIiz6Kn6RiXq0iv4LPRKjTjGcGTtghAPlt0BC5lcuQ5rSsk4bdCOXq0yDutaau4qGgv0uOgtP
4VW9Z5Tgo/BYUgNG5tr3WHrOC4hxxkOf1Ca/xpdCLi+99TQ4TRPiViMXfZwuSPLiu9fZBnqYJLzE
wOPDz1FA8HmiNIpTeS1pofdl3mzSOFz7d7hLCA==</ds:SignatureValue>
ds:KeyInfo>
ds:X509Data>
                  <ds:X509SubjectName>CN=SELLO ENTIDAD SGAD
PRUEBAS,2.5.4.97=#0c0f56415445532d533238303035363844,2.5.4.5=#13095332383030353638 44,OU=SECRETARIA
GENERAL DE ADMINISTRACION DIGITAL,O=MINISTERIO DE ASUNTOS ECONOMICOS Y TRANSFORMACION
DIGITAL,L=MADRID,C=ES</ds:X509SubjectName>
```

<ds:X509Certificate>MIIHrjCCBpagAwIBAgIQft7+0deAk5JhFQlRBPK9njANBgkqhkiG9w0BAQsFADBHMQswCQYDVQQG
EwJFUzERMA8GA1UECgwIRk5NVC1SQ00xJTAjBgNVBAsMHEFDIENvbXBvbmVudGVzIEluZm9ybcOh
dGljb3MwHhcNMjEwODEyMTE0MzEzWhcNMjQwODEyMTE0MzEyWjCB7DELMAkGA1UEBhMCRVMxDzAN
BgNVBAcMBk1BRFJJRDFCMEAGA1UECgw5TUlOSVNURVJJTyBERSBBU1VOVE9TIEVDT05PTUlDT1Mg
WSBUUkFOU0ZPUk1BQ0lPTiBESUdJVEFMMTUwMwYDVQQLDCxTRUNSRVRBUklBIEdFTkVSQUwgREUg
QURNSU5JU1RSQUNJT04gRElHSVRBTDESMBAGA1UEBRMJUzI4MDA1NjhEMRgwFgYDVQRhDA9WQVRF
Uy1TMjgwMDU2OEQxIzAhBgNVBAMMGlNFTExPIEVOVElEQUQgU0dBRCBQUlVFQkFTMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvdOB/mRKzFJSZKbDrBvZoomo+Yuc+IKr9uiYIRvTgz+y
EqucVRejRhMjsIh1MiT1GlRb+V9iST6pRj7t/aS8H6SqzizIy756TgsJz8GVRbOfX2A1XCN5QK0F
o96HmcADVj01M18ze+VQz7YG0Q/onbdx5IZwNncxOn3e0fGw2TEb85wuynhBND3ci2341+zh/zhc
HEd0rMXv6NJkTi2DiS5aVx8/ou4LjFum9HmFBrIOfbVv8r+Q5W1q494HlRqGq/rnTyGisq3YAC2i
EE/ctJJf86dza/b08lb9yFT+WBmW6Zs5Aa3CvI5+dnGrEJk/O3v+JiBMaDaMzkwFZ8NkCQIDAQAB
o4ID7jCCA+owDAYDVR0TAQH/BAIwADCBgQYIKwYBBQUHAQEEdTBzMDsGCCsGAQUFBzABhi9odHRw
Oi8vb2NzcGNvbXAuY2VydC5mbm10LmVzL29jc3AvT2NzcFJlc3BvbmRlcjA0BggrBgEFBQcwAoYo
aHR0cDovL3d3dy5jZXJ0LmZubXQuZXMvY2VydHMvQUNDT01QLmNydDCCATQGA1UdIASCASswggEn
MIIBGAYKKwYBBAGsZgMJEzCCAQgwKQYIKwYBBQUHAgEWHWh0dHA6Ly93d3cuY2VydC5mbm10LmVz
L2RwY3MvMIHaBggrBgEFBQcCAjCBzQyBykNlcnRpZmljYWRvIGN1YWxpZmljYWRvIGRlIHNlbGxv
IGVsZWN0csOzbmljbyBzZWfDum4gcmVnbGFtZW50byBldXJvcGVvIGVJREFTLiBTdWpldG8gYSBs
YXMgY29uZGljaW9uZXMgZGUgdXNvIGV4cHVlc3RhcyBlbiBsYSBEUEMgZGUgRk5NVC1SQ00gY29u
IE5JRjogUTI4MjYwMDQtSiAoQy9Kb3JnZSBKdWFuIDEwNi0yODAwOS1NYWRyaWQtRXNwYcOxYSkw
CQYHBACL7EABATA4BgNVHREEMTAvpC0wKzEpMCcGCSsGAQQBrGYBCAwaU0VMTE8gRU5USURBRCBT
R0FEIFBSVUVCQVMwDgYDVR0PAQH/BAQDAgXgMB0GA1UdDgQWBBR/WVmpRLawlHxewC4lJsqtEgQE
NzCBsAYIKwYBBQUHAQMEgaMwgaAwCAYGBACORgEBMAsGBgQAjkYBAwIBDzATBgYEAI5GAQYwCQYH
BACORgEGAjByBgYEAI5GAQUwaDAyFixodHRwczovL3d3dy5jZXJ0LmZubXQuZXMvcGRzL1BEU19D
T01QX2VzLnBkZhMCZXMwMhYsaHR0cHM6Ly93d3cuY2VydC5mbm10LmVzL3Bkcy9QRFNfQ09NUF9l
bi5wZGYTAmVuMB8GA1UdIwQYMBaAFBn4WC8U1qbMmwSYCA1M16sAp4NlMIHgBgNVHR8EgdgwgdUw
gdKggc+ggcyGgZ5sZGFwOi8vbGRhcGNvbXAuY2VydC5mbm10LmVzL0NOPUNSTDEsT1U9QUMlMjBD
b21wb25lbnRlcyUyMEluZm9ybWF0aWNvcyxPPUZOTVQtUkNNLEM9RVM/Y2VydGlmaWNhdGVSZXZv
Y2F0aW9uTGlzdDtiaW5hcnk/YmplY3RjbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludIYp
aHR0cDovL3d3dy5jZXJ0LmZubXQuZXMvY3Jsc2NvbXAvQ1JMMS5jcmwwDQYJKoZIhvcNAQELBQAD
ggEBACSyNnj3Kd05oB7fScFj+2sy5CKtHryiCIwrlLAGHWS0rik20WSrx1+hgkRJxgsKvqH5mxDz
ddWfg93+NwEP6JCHPMtPqfWMaLHGuHQfRYxKJx00akufhgH2knpAEFJhB5SGEU0gQuRSijvF5+a+

VhX9evLt3RwnGYIwcPo34MTlr+PHR7PTgzjGxYn/8g8etrOeGe3eZAIp0YNTDSUA1BLSdhDjM6zP
7DdTOFJGcfu3pJAx3EpuEBaSQlyxc2FWDqWrP6xPKgz5VdqsJ4Zlekka0SRI+ub/dNQ4I44Pj+qs
15FWSUF3Mt+VBNizg2omHpdcccB2xpgBsBN5k0GzT50=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
saml:Subject>
<saml:NameID Format="**urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName**">**33333460C**</saml:NameID>
saml:SubjectConfirmation Method="**urn:oasis:names:tc:SAML:2.0:cm:bearer**">
<saml:SubjectConfirmationData InResponseTo="**b316a34c-d50a-4488-9519-d8875a6357fc**" NotOnOrAfter="**2022-03-07T08:30:23Z**" Recipient="**https://circuitsandbox.net/ssologin/callback?provider=sso_cora_test**" />
</saml:SubjectConfirmation>
</saml:Subject>
saml:Conditions NotBefore="**2022-03-07T08:15:23Z**" NotOnOrAfter="**2022-03-07T08:30:23Z**">
saml:AudienceRestriction>
saml:Audience>**http://des-autentica.redsara.es/samlAutentica/acs.jsp**</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
saml:AttributeStatement>
saml:Attribute Name="**email**" NameFormat="**urn:oasis:names:tc:SAML:2.0:attrname-format:basic**">
saml:AttributeValue>**Correo.33333460C@externos.correo.gob.es**</saml:AttributeValue>
</saml:Attribute>

```
saml:Attribute Name="login" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
saml:AttributeValue>33333460C</saml:AttributeValue>
 </saml:Attribute>
saml:Attribute Name="nombre" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
saml:AttributeValue>NOMBRE_33333460C</saml:AttributeValue>
 </saml:Attribute>
saml:Attribute Name="apellidos" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
saml:AttributeValue>APE1 APE2</saml:AttributeValue>
 </saml:Attribute>
 </saml:AttributeStatement>
saml:AuthnStatement AuthnInstant="2022-03-07T08:20:23Z">
saml:AuthnContext>
saml:AuthnContextClassRef>urn:federation:authentication:windows</saml:AuthnContextClassRef>
 </saml:AuthnContext>
 </saml:AuthnStatement>
 </saml:Assertion>
 </samlp:Response>
```

A continuación se indica un ejemplo de la recogida de la respuesta SAML por parte de la aplicación, se ha de recuperar el valor "SAMLResponse" de la siguiente forma:

```
String samlResponse = req.getParameter("SAML_RESPONSE");
if (samlResponse == null){
      //samlResponse es nulo, buscamos en atributo
      samlResponse = (String)req.getAttribute("SAML_RESPONSE");
}
```

Una vez recuperada la variable "SAMLResponse" hay que desencriptarla en base64:

```
byte[] samlResponseDecoded =
Base64.getDecoder().decode(samlResponse);
String samlResponseDecodedString = new String(samlResponseDecoded);
```

2.10. Autenticación basada en CAS

Autentica soporta dos estándares de autenticación: CAS y SAML (para este último ver sección 2.8). En el caso de la autenticación basada en CAS (Central Authentication Service), no se usan las instrucciones que el estándar indica, sino que se ha creado una capa de software alrededor de estas con el objetivo de que la autenticación, por parte del integrador de la aplicación a integrar, sea más fácil e intuitiva. Dicho de manera pormenorizada, se realizará la llamada a una URL con protocolo seguro incluyendo un parámetro concreto en dicha llamada.

Para tener acceso a la autenticación a través de certificado electrónico o usuario y contraseña, es necesario, previamente, dar de alta la aplicación a través del módulo de aprovisionamiento de usuarios, teniendo que existir en el LDAP de Autentica los usuarios que van a intentar acceder (existe una opción de registro para aquellos usuarios que no existan en el LDAP, comprobando únicamente el certificado electrónico provisto por el usuario para su acceso. Esta opción solamente se encuentra disponible para accesos a través de certificado electrónico).

2.10.1. URL de acceso

Una vez que la aplicación se ha dado de alta en el sistema, éste enviará a través de correo electrónico el identificador de la aplicación para la composición de la URL a la que será necesario realizar la llamada para el acceso a la página de usuario y contraseña que provee Autentica. Dicha URL se deberá ubicar en la sección de la aplicación encargada de la autenticación de usuarios.

https://autentica.redsara.es/Autentica/servlet/AutenticaServlet?action=goToAutentica&appId=[**IDENTIFICADOR_APLICACIÓN**]

donde el identificador de la aplicación será un valor numérico que se debe proveer desde Autentica. Una vez invocada la URL desde la aplicación por un usuario que desea autenticarse, Autentica tomará el control de la navegación e intentará leer el certificado electrónico del usuario si se encuentra en el repositorio del navegador. En caso contrario, el sistema mostrará la página para informar el usuario y contraseña.

2.10.1.1. Ejemplo de llamada a Autentica

En caso de que para realizar la llamada a Autentica redireccionando desde una tercera página web, se recomienda usar la instrucción JavaScript “replace()”. A continuación se muestran dos ejemplos del uso de esta instrucción:

En el caso de que sea necesario pasar la redirección por una tercera página, se recomienda usar la función replace() de JS:

```
13   <script>
14
15   location.replace("https://pre-autentica.redsara.es/Autentica/servlet/AutenticaServlet?action=goToAutentica&appId=1481")

16   </script>
```

O en el caso de que no exista una página intermedia la llamada se puede realizar usando un “<href>” estándar:

```
1  <html lang="es">
2   <head>
3    <meta charset="ISO-8859-1">
4    <title>Pagina autenticación</title>
5    <meta name="description" content="Test autenticación Autentica">
6   </head>
7    <body>
8      <a href="https://autentica.redsara.es/Autentica/servlet/AutenticaServlet?action=goToAutentica&appId=[IDENTIFICADOR_APLICACIÓN]">
9         Acceso a login
10     </a>
11   </body>
12  </head>
13 </html>
```

2.10.2. URL de respuesta

En el caso de que Autentica valide correctamente el usuario, se redireccionará el flujo de la información a la URL de respuesta que se informa en la configuración de la aplicación.

En este momento, es cuando será posible por parte de la aplicación, recuperar la información que se encuentra en el LDAP de Autentica del usuario que se validó, recogiendo el parámetro "AUTENTICA_USER_XML".

Ejemplo:

String xml_user_autentica = req.getParameter ("AUTENTICA_USER_XML");

De esta forma, la aplicación invocante ya dispondrá de la información del usuario para poder manejarla, la cual viene en formato XML.

2.10.2.1. Varias URL de respuesta en la misma aplicación

Se ha añadido una nueva funcionalidad referida a la posibilidad de que Autentica contemple varias "URLs de respuesta" en función de un parámetro (appParam) enviado en la solicitud previa.

En el campo obligatorio "Url de respuesta por defecto" se indicará la URL a la que se redirigirá Autentica en el caso de que la autenticación del usuario haya sido satisfactoria. Es posible añadir más "URLs de respuesta" asociándolos con el valor introducido en el campo "Identificador URL", cuyo contenido debe ser numérico, de tal forma que en el caso de que un usuario se autentique de forma satisfactoria, y la aplicación haya invocado el acceso con Autentica añadiendo este valor numérico en un parámetro de nombre "appParam", se redirigirá a la URL asociada a dicho valor numérico.

Para más información consulte la documentación del manual de aprovisionamiento de Autentica.

2.10.3. XML de respuesta

A continuación se muestra el XML de respuesta con los datos del usuario recibidos desde Autentica y que deberá gestionar la aplicación invocante:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
- <respuesta>
  <resultado>OK</resultado>
  - <usuario>
    <id>1R</id>
    <userName>1R</userName>
    <isCitizen>false</isCitizen>
    <dir4DocumentID>1R</dir4DocumentID>
    <dir4DocumentType>01</dir4DocumentType>
    <cn>Nombre Ape1 Ape2</cn>
    <givenName>Nombre</givenName>
    <sn>Ape1</sn>
    <dir4LastName>Ape2</dir4LastName>
    <dir4Email>nombreape1@correo.gob.es</dir4Email>
    <dir4UserDateOfBirth>21/02/1972</dir4UserDateOfBirth>
    <dir4UserLocalityCode>1301</dir4UserLocalityCode>
    <dir4UserLocalityEntity>01</dir4UserLocalityEntity>
    <dir4UserLocality>Jaca</dir4UserLocality>
    <dir4UserCountryCode>724</dir4UserCountryCode>
    <dir4UserCountry>España</dir4UserCountry>
    <dir4UserProvinceCode>22</dir4UserProvinceCode>
    <dir4UserProvince>Huesca</dir4UserProvince>
    <dir4UserCCAACode>02</dir4UserCCAACode>
    <dir4UserCCAA>Aragón</dir4UserCCAA>
    <dir4AdministrationLevel>1</dir4AdministrationLevel>
    <dir4OrganizationCode>E00003801</dir4OrganizationCode>
    <dir4OrganizationDesc>Ministerio del Interior</dir4OrganizationDesc>
    <dir4DirCenCode>E00128701</dir4DirCenCode>
    <dir4DirCenDesc>Subsecretaria del Interior</dir4DirCenDesc>
    <dir4JobCentreCode>E03112104</dir4JobCentreCode>
    <dir4JobCentreDesc>S.G. de Tecnologias de la Informacion y las Comunicaciones</dir4JobCentreDesc>
    <dir4OrganicalUnitCodeDir3>E03112104</dir4OrganicalUnitCodeDir3>
    <st>Madrid</st>
    <l>Madrid</l>
    <postalCode>28071</postalCode>
    <street>CALLE Amador de los Ríos</street>
    <employeeType>OTROS</employeeType>
    <telephoneNumber>913434359</telephoneNumber>
    <title>ANALISTA DE SISTEMAS</title>
    <uid>1R</uid>
    <dir4UserName>1R</dir4UserName>
    <dir4LdapBranch>aapp</dir4LdapBranch>
    <dir4OriginSource>Administrador</dir4OriginSource>
    <dir4SystemRegisterDate>05/02/2014 10:24:31</dir4SystemRegisterDate>
    <dir4LastEntryDate>13/06/2017 10:18:08</dir4LastEntryDate>
    <dir4Observations>CERTIFICADO</dir4Observations>
  </usuario>
- - <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  - <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
```

```
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    - <Reference URI="">
      - <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>GIuvZt8mOoVGs+E4IxvZIHnCKTo=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>KWRGET+DG7IQReqW1gGU3pqZsgBoO3gmOjIC1MnekH4wWjmemF6W7wf64+6TQJOmGHPlJ+E720vH
      RbZo+CgpbCHjnFnv81cRfDMGBZCbpETN7r7vp6rat1YP67K5lDWEtr9CxbgTwxBU+2Iq4pl9UQDD
      HovzTqlgIAeJhMlERtaW07pGDzhh+rOLLMaSpW+0Q6dsT5fkcfn4gSmgfXbhAACm84Kvn2VNHJkI
      I4Q5zUrWwGWPQVBrVMVsCMdop42wq+Y6r3RVkRTJOHXeckEqoOo/sUWicVSNiYy13IkpoY1MA5cW
      v009FE0l3RRi7tS+2TovhSRoyaTmfbBSgKhkgg==</SignatureValue>
  - <KeyInfo>
    - <X509Data>
        <X509SubjectName>CN=AUTENTICA,OU=DTIC,O=DTIC,L=MAD,ST=MAD,C=ES</X509SubjectName>
        <X509Certificate>MIIDXjCCAkagAwIBAgIBQDANBgkqhkiG9w0BAQsFADCBiTELMAkGA1UEBhMCRVMxDzANBgNVBAgT
          Bk1BRFJJRDEPMA0GA1UEBxMGTUFEUklEMQwwCgYDVQQKEwNNUFIxFjAUBgNVBAsTDVNBUkEgU0lT
          VEVNQVMxDTALBgNVBAMTBFNBUkExIzAhBgkqhkiG9w0BCQEWFHNpc3RlbWFzLXNncGRAbXByLmVz
          MB4XDTE2MDEyNjE2MzIwMFoXDTI5MDEyNjE2MzIwMFowWzELMAkGA1UEBhMCRVMxDDAKBgNVBAgT
          A01BRDEMMAoGA1UEBxMDTUFEMQ0wCwYDVQQKEwREVElDMQ0wCwYDVQQLEwREVElDMRIwEAYDVQQD
          EwlBVVRFTlRJQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDzIi1nGPOk0a2GM5/8
          vMqVk4IuxOw9xETEVRojf5YfBcAlrGEodFp3+qfV+McD+5cEah9Gkkm+LC0rEnu7aa4leDs0pMS2 /VnQToAtSFYA2cwpLOyrXkjK7EFSIOqoYpYXL6OM71MWqqasWIdlN
          DFGiECIjsI6YUrMXaUoY6sjyu1+O5mVb6Dv/F6olcNibnGCfVS3ZN2rhITLflfIewH8g8iUSD9sl
          Gc4qi5l1gHFMfHmOVAEaAr0wrRA2XLEVqiY2DsRIgPMHik1go/yREKHWlxtYyqgDFqzowDeP2icP
          p/Qc0dn5qFz2Zep4gliDAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAHVEE1814THH+LyVDfQIqqXG
          Q5Dw6ZojVsKM9+3E+SY4OKK51sIaY7GMcRHQ1fcpgiF+Rm8g3M3N8fAVplMBbJb554QVa/u8bOgV
          ooGKn5j51lsJ705Rwvs8r/1nB0LSN5XDBcGD1SbsBnjw1qZrsw/DghobMcqOV8FpRQvdht0rAiEl
          COuho8Ow2BOCY8EJTof5nS87cn3G7HKYq7k1TQhffj8qeAisTjcrn8u5DQhjIXyjmfGWwbrr3hei
          TPa6DS7bDYXKpvVOKMhG+qOdC6WyJqNuhT63xFcRlU6sSvpb80+GGY6IPZVzUXMFQOelo/vsVmbD K/LeTdxrDs4zy0k=</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
</respuesta>
```

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<respuesta>
  <resultado>OK</resultado>
  <usuario>
        <id>1R</id>
        <userName>1R</userName>
         <isCitizen>false</isCitizen>
         <dir4DocumentID>1R</dir4DocumentID>
         <dir4DocumentType>01</dir4DocumentType>
         <cn>Nombre Ape1 Ape2</cn>
         <givenName>Nombre</givenName>
         <sn>Ape1</sn>
         <dir4LastName>Ape2</dir4LastName>
         <dir4Email>nombreape1@correo.gob.es</dir4Email>
         <dir4UserDateOfBirth>21/02/1972</dir4UserDateOfBirth>
          <dir4UserLocalityCode>1301</dir4UserLocalityCode>
          <dir4UserLocalityEntity>01</dir4UserLocalityEntity>
          <dir4UserLocality>Jaca</dir4UserLocality>
          <dir4UserCountryCode>724</dir4UserCountryCode>
          <dir4UserCountry>España</dir4UserCountry>
          <dir4UserProvinceCode>22</dir4UserProvinceCode>
          <dir4UserProvince>Huesca</dir4UserProvince>
          <dir4UserCCAACode>02</dir4UserCCAACode>
          <dir4UserCCAA>Aragón</dir4UserCCAA>
          <dir4AdministrationLevel>1</dir4AdministrationLevel>
          <dir4OrganizationCode>E00003801</dir4OrganizationCode>
          <dir4OrganizationDesc>Ministerio del Interior</dir4OrganizationDesc>
          <dir4DirCenCode>E00128701</dir4DirCenCode>
          <dir4DirCenDesc>Subsecretaria del Interior</dir4DirCenDesc>
          <dir4JobCentreCode>E03112104</dir4JobCentreCode>
          <dir4JobCentreDesc>S.G. de Tecnologias de la Informacion y las
  Comunicaciones</dir4JobCentreDesc>
          <dir4OrganicalUnitCodeDir3>E03112104</dir4OrganicalUnitCodeDir3>
          <st>Madrid</st>
           <l>Madrid</l>
```

```
            <postalCode>28071</postalCode>
            <street>CALLE Amador de los Ríos</street>
            <employeeType>OTROS</employeeType>
            <telephoneNumber>913434359</telephoneNumber>
            <title>ANALISTA DE SISTEMAS</title>
            <uid>1R</uid>
            <dir4UserName>1R</dir4UserName>
            <dir4LdapBranch>aapp</dir4LdapBranch>
            <dir4OriginSource>Administrador</dir4OriginSource>
            <dir4SystemRegisterDate>05/02/2014 10:24:31</dir4SystemRegisterDate>
            <dir4LastEntryDate>13/06/2017 10:18:08</dir4LastEntryDate>
            <dir4Observations>CERTIFICADO</dir4Observations>
    </usuario>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
          <SignedInfo>
             <CanonicalizationMethod  Algorithm="http://www.w3.org/TR/2001/REC-
    xml-c14n-20010315" />
            <SignatureMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
           <Reference URI="">
          <Transforms>
         <Transform  Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
    signature" />
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
     <DigestValue>GIuvZt8mOoVGs+E4IxvZIHnCKTo=</DigestValue>
    </Reference>
    </SignedInfo>

    <SignatureValue>KWRGET+DG7IQReqW1gGU3pqZsgBoO3gmOjIC1MnekH4wWjm
    emF6W7wf64+6TQJOmGHPlJ+E720vH
    RbZo+CgpbCHjnFnv81cRfDMGBZCbpETN7r7vp6rat1YP67K5lDWEtr9CxbgTwxBU
    +2Iq4pl9UQDD
    HovzTqlgIAeJhMlERtaW07pGDzhh+rOLLMaSpW+0Q6dsT5fkcfn4gSmgfXbhAACm
    84Kvn2VNHJkI
    I4Q5zUrWwGWPQVBrVMVsCMdop42wq+Y6r3RVkRTJOHXeckEqoOo/sUWicVSNi
    Yy13IkpoY1MA5cW
    v009FE0l3RRi7tS+2TovhSRoyaTmfbBSgKhkgg==</SignatureValue>
<KeyInfo>
```

<X509Data>

<X509SubjectName>**CN=AUTENTICA,OU=DTIC,O=DTIC,L=MAD,ST=MAD,C=ES**</X509SubjectName>

<X509Certificate>**MIIDXjCCAkagAwIBAgIBQDANBgkqhkiG9w0BAQsFADCBiTELMAkGA1UEBhMCRVMxDzANBgNVBAgT**
Bk1BRFJJRDEPMA0GA1UEBxMGTUFEUklEMQwwCgYDVQQKEwNNUFIxFjAUBgNVBAsTDVNBUkEgU0lT
VEVNQVMxDTALBgNVBAMTBFNBUkExIzAhBgkqhkiG9w0BCQEWFHNpc3RlbWFzLXNncGRAbXByLmVz
MB4XDTE2MDEyNjE2MzIwMFoXDTI5MDEyNjE2MzIwMFowWzELMAkGA1UEBhMCRVMxDDAKBgNVBAgT
A01BRDEMMAoGA1UEBxMDTUFEMQ0wCwYDVQQKEwREVElDMQ0wCwYDVQQLEwREVElDMRIwEAYDVQQD
EwlBVVRFTlRJQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDzIi1nGPOk0a2GM5/8
vMqVk4IuxOw9xETEVRojf5YfBcAlrGEodFp3+qfV+McD+5cEah9Gkkm+LC0rEnu7aa4leDs0pMS2
/VnQToAtSFYA2cwpLOyrXkjK7EFSIOqoYpYXL6OM71MWqqasWIdlND7dH8L4Vy4FUHndYNv815/E
DFGiECIjsI6YUrMXaUoY6sjyu1+O5mVb6Dv/F6olcNibnGCfVS3ZN2rhITLflfIewH8g8iUSD9sl
Gc4qi5l1gHFMfHmOVAEaAr0wrRA2XLEVqiY2DsRIgPMHik1go/yREKHWlxtYyqgDFqzowDeP2icP
p/Qc0dn5qFz2Zep4gliDAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAHVEE1814THH+LyVDfQIqqXG
Q5Dw6ZojVsKM9+3E+SY4OKK51sIaY7GMcRHQ1fcpgiF+Rm8g3M3N8fAVplMBbJb554QVa/u8bOgV
ooGKn5j51lsJ705Rwvs8r/1nB0LSN5XDBcGD1SbsBnjw1qZrsw/DghobMcqOV8FpRQvdht0rAiEl
COuho8Ow2BOCY8EJTof5nS87cn3G7HKYq7k1TQhffj8qeAisTjcrn8u5DQhjIXyjmfGWwbrr3hei
TPa6DS7bDYXKpvVOKMhG+qOdC6WyJqNuhT63xFcRlU6sSvpb80+GGY6IPZVzUXMFQOelo/vsVmbD K/LeTdxrDs4zy0k=</X509Certificate>

</X509Data>

</KeyInfo>

</Signature>

</respuesta>

El XML de respuesta irá firmado con certificado electrónico, por lo que se recomienda, en base a consideraciones de seguridad, verificar la autenticidad de dicha firma en todas las llamadas que se hagan a Autentica.

Para el tratamiento de este XML se encuentra disponible en el PAe la librería (aut-sdk), la cual procesa dicho XML de manera muy sencilla.

2.11. Varias URL de respuesta en la misma aplicación

Se ha añadido una nueva funcionalidad referida a la posibilidad de que Autentica contemple varias "URLs de respuesta" en función de un parámetro (appParam) enviado en la solicitud previa.

En el campo obligatorio "Url de respuesta por defecto" se indicará la URL a la que se redirigirá Autentica en el caso de que la autenticación del usuario haya sido satisfactoria. Es posible añadir más "URLs de respuesta" asociándolos con el valor introducido en el campo "Identificador URL", cuyo contenido debe ser numérico, de tal forma que en el caso de que un usuario se autentique de forma satisfactoria, y la aplicación haya invocado el acceso con Autentica añadiendo este valor numérico en un parámetro de nombre "appParam", se redirigirá a la URL asociada a dicho valor numérico.

Para más información consulte la documentación del manual de aprovisionamiento de Autentica.

2.12. Elemento de puestos

A continuación se explican con más detalle los campos descriptivos de los puestos:

En primer lugar, aunque se distinga entre primer puesto y restantes según la posición en donde se encuentren del XML de respuesta, no significa que haya un puesto principal del usuario y otros secundarios, ya que todos están al mismo nivel de importancia.

2.12.1. Primer puesto del usuario

Contiene los siguientes campos obligatorios:

- dir4AdministrationLevel: indica el tipo de unidad orgánica
  - 1 → AGE
  - 2 → CCAA
  - 3 → EELL
  - 4 → Universidades
  - 5 → Otras instituciones

Nivel 1 de la unidad orgánica

- dir4OrganizationCode: Código del organismo
- dir4OrganizationDesc: Descripción del organismo

- dir4OrganicalUnitCodeDir3: Código de DIR3 del último nivel guardado de un usuario

- dir4OrganicalUnitCCAA: CCAA de la unidad orgánica

A continuación se indican los campos no obligatorios:

Nivel 2 de la unidad orgánica

- dir4DirCenCode: Código del centro directivo
- dir4DirCenDesc: Centro directivo

Nivel 3 de la unidad orgánica

- dir4JobCentreCode: Código del centro de destino
- dir4JobCentreDesc: Centro de destino

Los siguientes elementos del XML indican la dirección del último nivel guardado de un usuario.

- stateOrProvinceName: Provincia de la unidad orgánica
- localityName: Localidad de la unidad orgánica
- postalCode: Código postal de la unidad orgánica
- street: Dirección de la unidad orgánica

Indica el puesto o cargo del usuario dentro de la unidad orgánica a la que pertenece.

- Title: Puesto o cargo

2.12.2. Resto de puestos

Si el usuario tiene más puestos vienen en el XML bajo el elemento “puestos”, cada uno de ellos dentro del elemento “puesto”. Los elementos serían los mismos que en el primer puesto y con el mismo tipo de obligatoriedad.

2.13. Autorización

Autentica dispone de servicios de autorización. El uso de estos servicios se encuentra reflejado en el manual de autorización de Autentica, disponible en el portal del PAE en su sección de descargas.

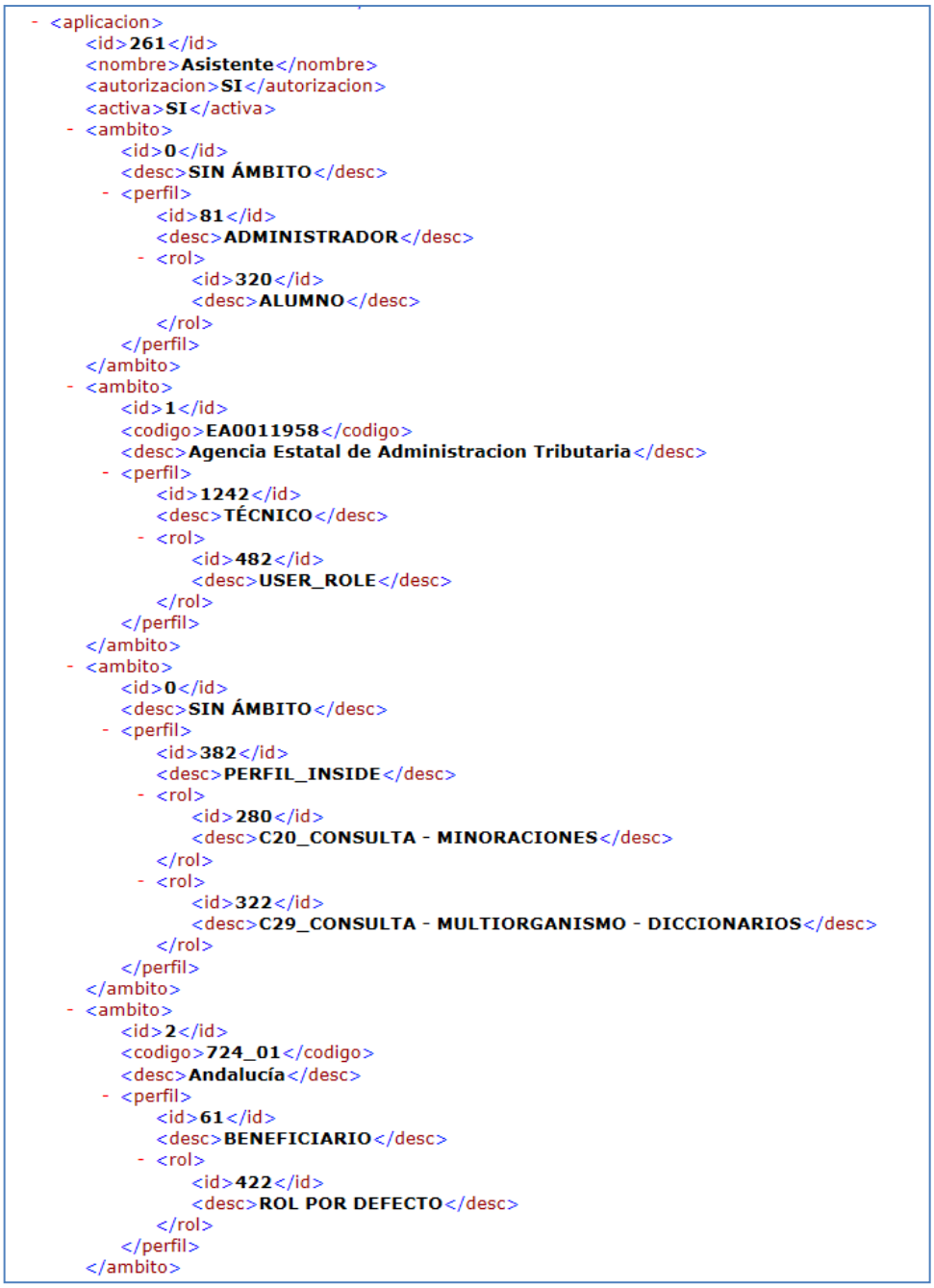
2.13.1. Ubicación de los atributos relativos a la autorización en el XML de respuesta

Dentro del XML de respuesta que Autentica provee cuando se realiza una autenticación de un usuario en una aplicación integrada, existe un conjunto de atributos donde se define la autorización

asociada a dicho usuario y aplicación, si procede. La etiqueta que contiene esta información se denomina <aplicacion>.

Si el usuario no tuviera asociado ningún tipo de autorización, la etiqueta <aplicacion> no se mostrará en el XML de respuesta.

En caso de que el usuario tuviera asociado algún tipo de autorización, la etiqueta <aplicacion> se mostrará de esta manera:



Donde existirán varias etiquetas dependientes de <aplicacion> que contendrán la información relativa a la autorización del usuario.

Dependiendo del entorno, los campos tendrán distinto identificador y la descripción corresponderá a la que se haya definido en cada entorno:

- **Aplicación**
    - **ID**: define el identificador de la aplicación.

- **Nombre**: define el nombre de la aplicación.
- **Autorización**: define si se ha asociado autorización a la aplicación.
- **Activa**: define si la autorización asociada a la aplicación está en modo activo o inactivo. En caso de esta en modo inactivo, la etiqueta <aplicacion> no se mostrará.
- **Ámbito**: define el ámbito de cada perfil/rol. Todos los perfiles/roles deben tener un ámbito. El ámbito por defecto es SIN ÁMBITO.
    - **ID**: define el identificador del ámbito. Es un código interno de Autentica. En caso de ser SIN ÁMBITO, el identificador es 0.
    - **DESC**: define la descripción del ámbito.
        - **Perfil:** define el perfil asociado
            - **ID:** define el identificador del perfil asociado. Es un código interno de Autentica.
            - **DESC:** define la descripción del perfil asociado.
                - **ROL:** define el rol asociado
                - **ID:** define el identificador del rol asociado. Es un código interno de Autentica.
                - **DESC:** define la descripción del rol asociado.

2.14. Módulo de interoperabilidad

Autentica dispone de un módulo de interoperabilidad a través de servicios web. El uso de este módulo se encuentra reflejado en el manual de integración con servicios web de Autentica, disponible en el portal del PAE en su sección de descargas.

2.15. Opciones de cierre de sesión

2.15.1. Opción Logout

Se puede indicar una URL logout propia de la aplicación, de tal forma que, al igual que la URL de respuesta, será invocada desde Autentica cuando desde la aplicación invocante se invoque una acción de logout de Autentica indicando el id de la aplicación que lo está invocando, como por ejemplo:

- Se indica para la aplicación 3469 la siguiente URL de Logout, la cual se guarda en la ficha de la aplicación:

  https://aplicacion.redsara.es/app3469/servlet/App3469Servlet?action=logoutPage&type=JSP

- Se invoca desde la aplicación 3469 la siguiente URL:

  https://autentica.redsara.es/Autentica/logout?appId=3469

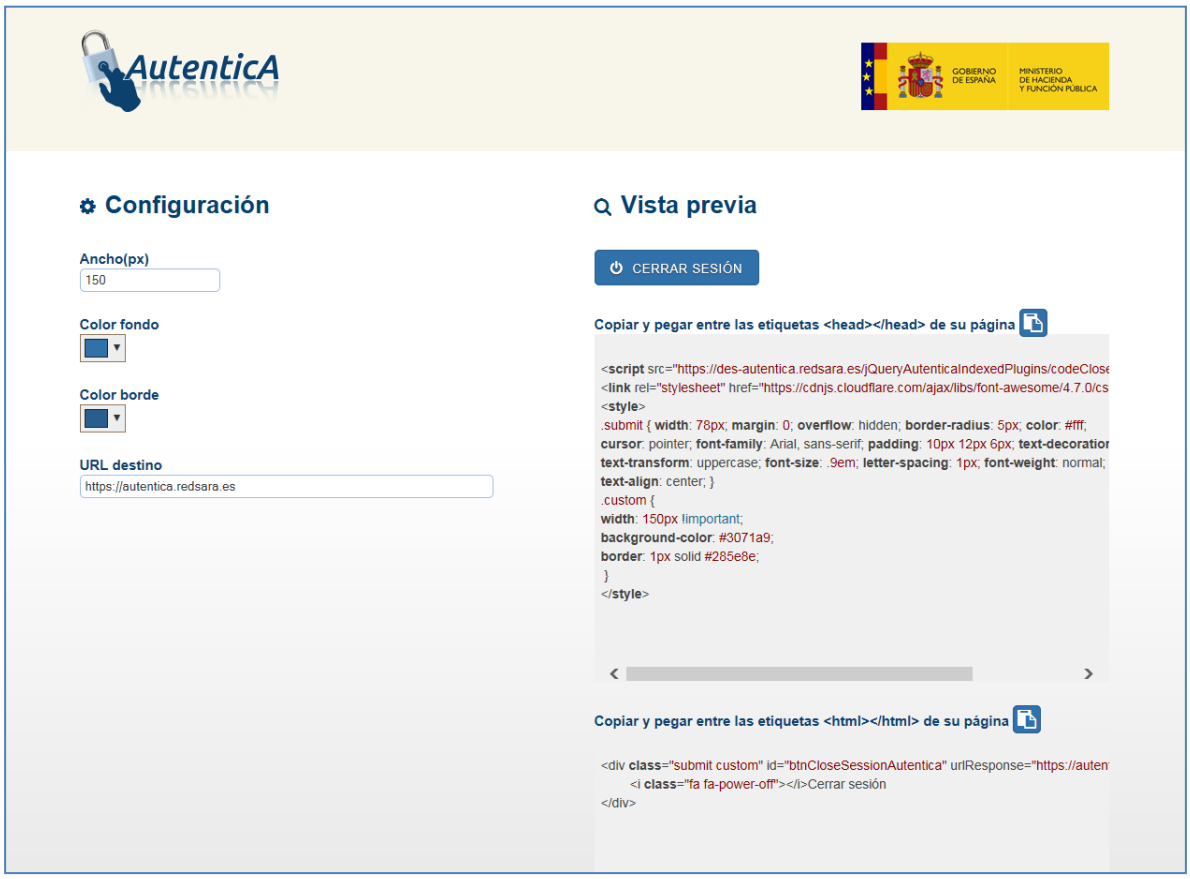
- Se redirecciona desde Autentica a la URL de logout indicada en el punto 1.

2.15.2. Cierre de sesión

Con objeto de proporcionar de manera activa un mecanismo que asegure el cierre de sesión iniciada a través de certificado electrónico (ver el punto Otras consideraciones de seguridad) y otras dependencias de sesión adicionales en aquellas aplicaciones integradas con Autentica, se ha habilitado un módulo para la configuración de botones de cierre de sesión con la finalidad de que sea posible su implantación en dichas aplicaciones. El acceso a este modulo se realizará a través del siguiente enlace:

https://autentica.redsara.es/DIR4/servlet/Dir4Servlet?action=customButtonCloseSession

Con el prefijo (pre-) y (se-) en caso de acceder al entorno de preproducción y servicios estables respectivamente.



A continuación se detallan las opciones para su correcta configuración:

- **Ancho**: configurará el tamaño en pixeles del ancho que tendrá el botón
- **Color fondo**: configurará el color de fondo del botón
- **Color borde**: configurará el color del borde del botón
- **URL destino**: será la URL que tomará el control de la navegación una vez se hayan cerrado las sesiones activas. Adicionalmente esta URL deberá servir para cerrar las sesiones abiertas de la propia aplicación integrada y llevar al usuario a un punto neutral en dicha aplicación en su navegación.

Una vez configurado el botón a través de la vista previa, se copiará el código resultante:

- La porción de código destinado a copiar entre las etiquetas <head>, en concreto la parte que se refiere al estilo del botón y se recomienda que se incluya en el CSS global de la aplicación, en aras de mantener la accesibilidad y modularidad en el código. La parte que se refiere a JS, se ubicará con normalidad dentro de la etiqueta <head>

2.15.2.1. Supuesto especial para el navegador Firefox

Dadas las peculiaridades del navegador Firefox, se puede realizar la siguiente configuración a modo de ejemplo, dado que el botón de cierre de sesión indicado en el punto anterior no termina de cerrarla.

Añadimos un enlace:

```
<a href="javascript:logout();">Cerrar sesión</a>
```

Definimos la función javascript donde se invoca un servlet de la propia aplicación.

```
<script>
	function logout(){
		var alertResponse = confirm("¿Seguro que quiere cerrar su sesión?");
		if(alertResponse){
			document.location.href = "../servlet/AppServlet?action=logoutPRO";
		}
	}
</script>
```

Se invoca Autentica, señalando en [AUTENTICA_URL] el entorno en el que nos encontramos (por ejemplo, https://autentica.redsara.es para el entorno de producción) e invocando la acción “logout” con el parámetro appId para especificar el identificador de la aplicación a partir de la cual se va a obtener la URL de logout de la aplicación invocante a la que se redireccionará una vez cerrada la sesión.

```
public String logoutPRO(HttpServletResponse res){
        try {
                String sRedirect = "[AUTENTICA_URL]/Autentica/logout?appId=2944";
                res.sendRedirect(sRedirect);
                return "OK";
        }catch (Exception e) {
                log.error("LogoutHandler.logoutPRO.Exception:" + e.toString());
                return null;
        }
 }
```

2.16. Otras consideraciones de seguridad

La eliminación de la sesión de certificado electrónico históricamente ha acarreado algunos problemas debido a que, por la funcionalidad nativa de los navegadores, estos conservan su ciclo de vida mientras la instancia siga en memoria, o lo que es lo mismo, mientras no se cierre el navegador completamente (incluyendo las pestañas abiertas).

Con este mecanismo se consigue evitar este extremo en la mayoría de los navegadores, no obstante se han encontrado problemas en el navegador Mozilla Firefox, por lo que se recomienda que en este dispositivo se complete la funcionalidad cerrando el navegador de manera deliberada por parte del usuario.

Esta acción, aunque no es imprescindible en otros navegadores, no deja de ser una buena práctica y asegura de manera fehaciente la destrucción completa de la sesión de certificado electrónico.

Cuando se use esta funcionalidad con el navegador Mozilla Firefox el sistema mostrará una ventana recordando al usuario que debe cerrar el navegador para completar la acción y proceder al cierre de sesión de manera segura.

Las pruebas se han realizado sobre los siguientes navegadores:

- Internet Explorer
- Google Chrome

- Mozilla Firefox