Incidencia

En el procesado de la respuesta de Cl@ve2.0 nos está dando un error que no sabemos a que puede ser debido: 2018-09-25 07:54:07,828 ERROR [eu.eidas.auth.engine.xml.opensaml.ResponseUtil] (default task-38) BUSINESS EXCEPTION : audiences [http://localhost:8080/loginibfront/retornoLoginClave/YDIFUIN5-DPJ7NRT8-T8YRVQAD.html] are not allowed ¿Podéis indicarnos cuál puede ser el problema?

25/09/2018 - 08:15:49

Resolución

Buenos días, ¿Podrían facilitar el intercambio de mensajes SAML de petición y respuesta generado contra la pasarela del entorno de Servicios Estables del servicio Cl@ve 2 para su estudio?. Podrán reabrir esta incidencia utilizando el enlace https://ssweb.seap.minhap.es/ayuda/seguimiento, introduciendo 463906 en el campo identificador de consulta o incidencia y 856149 en el número de seguimiento. Reciban un cordial saludo. ---------- Centro de Servicios - Secretaría General de Administración Digital Creación de solicitudes de soporte: https://ssweb.seap.minhap.es/ayuda/consulta/CLAVE http://administracionelectronica.gob.es/ctt/clave

26/09/2018 - 09:05:37

De Tramitador

Reapertura

Enviamos en el zip la petición y respuesta. Donde falla es al procesar la petición de respuesta con el error anteriormente comentado: try { authnResponse = engine.unmarshallResponseAndValidate(decSamlTicket, new URI(config.getPepsUrl()).getHost(), 0, 0, datosSesion.getUrlCallback()); } catch (EIDASSAMLEngineException | URISyntaxException e) { throw new ErrorRespuestaClaveException(e); }

Fichero adjunto: **Clave2.zip**

26/09/2018 - 14:06:25

Resolución

Buenas tardes, El error reportado informa de que la URL situada en "http://localhost:8080/loginibfront/retornoLoginClave/YDIFUIN5-DPJ7NRT8-T8YRVQAD.html" no está permitida en su sistema para recibir y procesar las respuestas devueltas desde el sistema Cl@ve. Según el mensaje de respuesta remitido se observa la URL "http://localhost:8080/loginibfront/retornoLoginClave/VJIFUIQS-O3DNNRT8-T8RZJ0BP.html" como única receptora de los mensajes de respuesta devueltos desde Cl@ve. Esto puede observarse en el atributo Destination de la etiqueta raíz <saml2p:Response/>, así como en el siguiente fragmento XML del mensaje de respuesta: <saml2:Conditions NotBefore="2018-09-26T12:00:21.245Z" NotOnOrAfter="2018-09-26T12:15:21.245Z"> <saml2:AudienceRestriction> <saml2:Audience>http://localhost:8080/loginibfront/retornoLoginClave/VJIFUIQS-O3DNNRT8-T8RZJ0BP.html</saml2:Audience> </saml2:AudienceRestriction> <saml2:OneTimeUse/> </saml2:Conditions> por lo que URLs distintas a la indicada no estarían autorizadas a recibir respuestas de Cl@ve (como ocurre con la URL informada en la apertura de la incidencia "http://localhost:8080/loginibfront/retornoLoginClave/YDIFUIN5-DPJ7NRT8-T8YRVQAD.html"). Por otro lado, analizando el mensaje de petición enviado se observa la existencia del atributo AssertionConsumerServiceURL dentro de la estructura de la etiqueta raíz <saml2p:AuthnRequest /> informando del mismo valor para la URL permitida de recepción de respuestas desde Cl@ve. Rogamos revisen la configuración aplicada en su SP en lo referente a las URLs que podrán recibir y procesar las

respuestas devueltas desde el sistema Cl@ve 2. Podrán reabrir esta incidencia utilizando el enlace https://ssweb.seap.minhap.es/ayuda/seguimiento, introduciendo 463906 en el campo identificador de consulta o incidencia y 856149 en el número de seguimiento. Reciban un cordial saludo. ---------- Centro de Servicios - Secretaría General de Administración Digital Creación de solicitudes de soporte: https://ssweb.seap.minhap.es/ayuda/consulta/CLAVE http://administracionelectronica.gob.es/ctt/clave

26/09/2018 - 16:41:29

De Tramitador

Reapertura

La url de retorno de Cl@ve que estamos indicando varía según la petición ya que usamos la url para identificar la sesión de login: http://localhost:8080/loginibfront/retornoLoginClave/<id-sesion>.html Por tanto la url variará para cada intento de login en Clave. Si se fijan en las petición / respuesta que se pasan en el zip las urls coinciden entre la petición y la respuesta: - Petición: <saml2p:AuthnRequest ... AssertionConsumerServiceURL="http://localhost:8080/loginibfront/retornoLoginClave/VJIFUIQS-O3DNNRT8-T8RZJ0BP.html" > - Respuesta: <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"> <saml2:SubjectConfirmationData Address="10.252.131.21" InResponseTo="_GlPJOw5Jb2NpNsMPk4ydINWeaG3cjL7toU7Zciid-mRMxJ8EnB7MjvZeM2eS9_l" NotOnOrAfter="2018-09-26T12:15:21.245Z" Recipient="http://localhost:8080/loginibfront/retornoLoginClave/VJIFUIQS-O3DNNRT8-T8RZJ0BP.html"/> </saml2:SubjectConfirmation> Por tanto según lo que comentan no debería dar el error que comentan (la descripción del error variará para cada petición). En el caso anterior sería: BUSINESS EXCEPTION : audiences [http://localhost:8080/loginibfront/retornoLoginClave/VJIFUIQS-O3DNNRT8-T8RZJ0BP.html] are not allowed

26/09/2018 - 16:56:56

Resolución

Buenos días, ¿Es posible que en su sistema se estén dando situaciones de cacheo de sesiones entre procesos de autenticación independientes?. Según han detallado, si las URLs de retorno se generan de forma dinámica por cada inicio de sesión en su entorno, las URLs siguientes http://localhost:8080/loginibfront/retornoLoginClave/YDIFUIN5-DPJ7NRT8-T8YRVQAD.html http://localhost:8080/loginibfront/retornoLoginClave/VJIFUIQS-O3DNNRT8-T8RZJ0BP.html deben corresponderse con inicios de sesión independientes. ¿Podrían revisar si las sesiones de autenticación para diferentes usuarios están siendo cacheadas de alguna forma en sus sistemas?. Podrán reabrir esta incidencia utilizando el enlace https://ssweb.seap.minhap.es/ayuda/seguimiento, introduciendo 463906 en el campo identificador de consulta o incidencia y 856149 en el número de seguimiento. Reciban un cordial saludo. ---------- Centro de Servicios - Secretaría General de Administración Digital Creación de solicitudes de soporte: https://ssweb.seap.minhap.es/ayuda/consulta/CLAVE http://administracionelectronica.gob.es/ctt/clave

01/10/2018 - 09:33:45

De Tramitador

Reapertura

Buenas, No es el caso. No se producen cacheo de sesiones. Cada intento de inicio de sesión tiene su URL específica (http://localhost:8080/loginibfront/retornoLoginClave/<id_sesion>.html) En los intentos de inicio de sesión con Clave2.0, las peticiones y respuestas hacen referencia a la sesión específica, por lo que son coherentes. Pero en la validación de la respuesta que se hace

(engine.unmarshallResponseAndValidate) da el error comentado: BUSINESS EXCEPTION : audiences [http://localhost:8080/loginibfront/retornoLoginClave/<id_sesion>.html] are not allowed Por tanto, la petición y respuesta son referentes a la misma URL, pero al validar la respuesta se genera error.