SAML

Table of Contents

Introduction to SAML in ECAS

ECAS offers support for the Security Assertion Markup Language (SAML) protocol. SAML is a standardised means for conveying authentication data from a system capable of authenticating a user (an identity provider) and a system that consumes user authentication data (a service provider).

SAML defines both the message protocols, that is, the flows between the systems, and the message contents. The SAML message format is based on XML. It is enrichened with necessary security data such as a digital signature of the message content. The blocks of information which regroup information about an authenticated user and which are passed to the service provider are called *assertions*. Each assertion contains a number of *attributes*, which are the actual bits of user information.

The examples section shows a sample SAML response, such as it is currently provided by ECAS.

Currently, ECAS interacts with several service provider partners in SAML. One of those service providers is the *Juniper VPN* - commonly known as the myremote portal.

Supported versions and profiles

ECAS supports the SAML versions **1.1 and 2.0**.

The currently implemented profiles are:

SAML 1.1	SAML 2.0
Browser/POST	Web Browser SSO

How to register a SAML Service Provider in ECAS

First of all we invite you to configure your acceptance application with ECAS acceptance. The public URL of ECAS acceptance is https://ecas.acceptance.ec.europa.eu/cas/login.

The SAML metadata file for ECAS acceptance is accessible via HTTP : https://ecas.acceptance.ec.europa.eu/cas/saml/metadata.xml

ECAS is not a standard SAML product so it is not able to upload a SAML metadata file and magically work with your service provider.

Therefore, to use ECAS as an Identity Provider you have to provide the following information to EC-IAM-SERVICE-DESK@ec.europa.eu :

1. The issuer URI (aka entity ID) of your application. It has to correspond to the value of the *<saml2p:Issuer/>* node in the SAML request received by ECAS.
2. The assertion consumer URL. The registered assertion consumer URL is a fallback if no consumer URL is defined is the SAML request received by ECAS.
3. One or more authentication strenght(s) accepted by your application. Strengths currently compatible with SAML are PASSWORD, PASSWORD_SMS, PASSWORD_TOKEN and STORK.
4. If you want activate the strength upgrade functionality (only possible if at least one multi-factor strength and at least one single-factor strength are accepted)
5. The attributes you want to receive in the SAML response and the mapping with supported user details
6. If you want to force authentication (renew mode), we recommend to use the attribute ForceAuthn="1" in the SAML Request. However, we also have a fallback on server side if your SAML client doesn't support that attribute.

ECAS IdP accepts signed SAML requests as well as unsigned SAML requests. We highly recommend to use digital signature in order to ensure the integrity of your SAML requests. If you want to sign the SAML request we need the public key to verify the digital signature.

Information required by ECAS	Corresponding entry in ECAS SAML 2.0 metadata file
Issuer URI	<md:EntityDescriptor ID="_683bc631-4bab-44b4-98d3-73667b03f128" entityID="***https://ecas.acceptance.ec.europa.eu/cas/login***">
Assertion consumer URL	<md:SPSSODescriptor ...> ... <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="***https://ecas.acceptance.ec.europa.eu/cas/login***" index="0" isDefault="true" xsi:type="md:IndexedEndpointType"/> </md:SPSSODescriptor>
Public key used to verify signature	<md:SPSSODescriptor ...> <md:KeyDescriptor use="signing"> <ds:KeyInfo> <ds:X509Data> ... <ds:X509Certificate> ***MIIGXjCCBEagAwIBAgIQakKwl057ulV/ACZihKf91zANBgkqhkiG9w0BAQ0FADCBzzELMAkGA1UE*** ***ThisIsThePublicKey*** ***wac8ukKIPUJfVGYOIiPm3zyv4jxk1BH9+YmaA1eA1IIRZGH1w+mKVZ5EJfQ/1rBZEWhk17QFOXTu*** ***iX9eYGdGf3xQvVwKYJOBfSZTfWtAHQIofsl3swKXiBBlTnU5ayk=*** </ds:X509Certificate> </ds:X509Data> </ds:KeyInfo> </md:KeyDescriptor> </md:SPSSODescriptor>

Table 1: ECAS metadata file as an example of how to find useful information to act as a SAML Service provider

Supported User Details

The user information that ECAS can put the SAML response, is defined in the `authenticationSuccessType` in `ecas.xsd`, found at https://ecas.ec.europa.eu/cas/schemas/ecas.xsd.

SAML 2.0 message examples

Sample unsigned SAML request

The following shows a sample unsigned SAML 2.0 request; communication flow: Service Provider -> ECAS.

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    Destination="https://ecasd.cc.cec.eu.int:7002/cas/login"
                    ForceAuthn="false"
                    ID="_0xe010f8d9875b05b4f95a7806210b0be2"
                    IsPassive="false"
                    IssueInstant="2014-12-09T11:30:41.732Z"
                    Version="2.0"
                    >
    <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">d02di1022041dit</saml:Issuer>
</samlp:AuthnRequest>
```

Sample signed SAML request

The following shows a sample signed SAML 2.0 request; communication flow: Service Provider -> ECAS.

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    Destination="https://ecasd.cc.cec.eu.int:7002/cas/login"
                    ForceAuthn="false"
                    ID="_0x14956c887e664bdb71d7685b89b70619"
                    IsPassive="false"
                    IssueInstant="2014-12-09T11:38:29.418Z"
                    Version="2.0"
                    >
    <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">d02di1022041dit</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/2000/09/xmldsig#rsa-sha1"
/>
            <ds:Reference URI="#_0x14956c887e664bdb71d7685b89b70619">
                <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#WithComments">
                        <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                                                PrefixList="ds saml samlp"
                                                />
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<ds:DigestValue>GHmWZ3x+Ba+2YQS+BRx70st4DiuYlKZ4C6ZeidlST8Y=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
XYDBDIb4ft1uqSBcEtwQ9UdELbjfzObkIhzEA2pB2AEqvbZLp3bI7vrIzesImIXqL8iWtp5VBAqW
UsWvMOtXI+wliNC013rUNiKM9q4Z5lF0lyAcrVH3RpSfrkKOVxYHAVwk3ipewFHPJcacK6UuEpI7
YDYz+vsnfm1xXK/nWY8ABzNb4ZPkPvKagIhP86Cu8iRf+kHgawLJvX7kqQ8Dd4dlnFDKpE+3ypiu
ocCw5Yy/jhzG/uEYny/cSYjntdfMb9VhxuIMIgH9kGP17DArwGEct9yevdlQXxkC0q18fKs+FEra
0E14dlpm5/OGmlaPv219DHCsJmmySrD1IyfyIw==
</ds:SignatureValue>
    </ds:Signature>
</samlp:AuthnRequest>
```

Sample SAML request with the AssertionConsumerServiceURL attribute

The following shows a sample unsigned SAML 2.0 request containing the AssertionConsumerServiceURL attribute ; communication flow: Service Provider -> ECAS.

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

AssertionConsumerServiceURL="https://webgate.d02di1022041dit.ec.europa.eu/saml/sso"
     Destination="https://ecasd.cc.cec.eu.int:7002/cas/login"
                    ForceAuthn="false"
                    ID="_0xe010f8d9875b05b4f95a7806210b0be2"
                    IsPassive="false"
                    IssueInstant="2014-12-09T11:30:41.732Z"
                    Version="2.0"
                    >
    <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">d02di1022041dit</saml:Issuer>
</samlp:AuthnRequest>
```

ECAS uses the value of the SAML attribute as the destination of the SAML response (i.e. https://webgate.d02di1022041dit.ec.europa.eu/saml/sso) instead of the value registered in ECAS.

Sample SAML response

The following is a sample SAML 2.0 response; communication flow: ECAS -> Service Provider.

```
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
Consent="urn:oasis:names:tc:SAML:2.0:consent:obtained"
Destination="https://myremote.ec.europa.eu/dana-na/auth/saml-consumer.cgi"
ID="_74dba72f-47ba-4ab5-94a2-7fe5abc56768"
InResponseTo="_76358f4621f1944be270f68e9b8e9300"
IssueInstant="2012-10-23T06:42:30.267Z" Version="2.0">
    <saml2:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://ecas.cc.cec.eu.int:7
002/cas/login</saml2: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="#_74dba72f-47ba-4ab5-94a2-7fe5abc56768">
                <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#">
                        <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xs"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>JyrRua/49aFjNXPJoYWFSxZhBbJwevCYJoWNhnTmMvo=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>

<ds:SignatureValue>aP1+3Tey9leMqAUb8oECOaWVzG2CG0GGHpG0WYhE2fB838PCdyo3GZrN0Hmn0PLZy9p
8Y86Vl79XMETiu5KnvDaKGtw1IN19BnYqyRgytDjb/sqfzHl124EpyYSUGelFi/dIlUjP9wBm7k1rjrDp7uVj6
UlBo1iRvFS+iGEmFKPMm1UHMMW7KqKteUtcVbA1pma/xffmOXxlyZcFhe5dmPMiPJ1DtbfxjvW3snbCoR2NhfM
```

```
wIbPkQCl4B2oNoSe0zAk4WDpfUsxB16J9MHxlK90Au6ybBswsbZoYezE6TWlhI5YY0UUKAC7+pRIOLxSRu9Yan
1uhZ1jx7ecP4HR5Qw==</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>

<ds:X509SubjectName>CN=ecas-prod-sts,1.2.840.113549.1.9.1=#162344494749542d454341532d4
44556454c4f504d454e544065632e6575726f70612e6575,OU=DIGIT,O=European
Commission,L=Brussels,C=BE</ds:X509SubjectName>

<ds:X509Certificate>MIIGeTCCBGGgAwIBAgIQVtSzs2ZsuMRXGcttBnBlfjANBgkqhkiG9w0BAQUFADCB5D
ELMAkGA1UE
...
Qy0Gt8gWsjs=</ds:X509Certificate>

<ds:X509Certificate>MIIHXjCCBUagAwIBAgIBATANBgkqhkiG9w0BAQUFADCB5DELMAkGA1UEBhMCQkUxET
APBgNVBAgM
...
Qlq5pIka4rlm</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        <saml2p:StatusMessage>Successful ECAS authentication</saml2p:StatusMessage>
    </saml2p:Status>
    <saml2:Assertion ID="_79ba7d43-dc55-430d-8c55-ff363b735bf2"
IssueInstant="2012-10-23T06:42:30.267Z" Version="2.0">
        <saml2:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://ecas.cc.cec.eu.int:7
002/cas/login</saml2:Issuer>
        <saml2:Subject>
            <saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">keschma</saml2:NameID>
            <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml2:SubjectConfirmationData
InResponseTo="_76358f4621f1944be270f68e9b8e9300"
NotOnOrAfter="2012-10-23T07:12:30.267Z"
Recipient="https://myremote.ec.europa.eu/dana-na/auth/saml-consumer.cgi"/>
            </saml2:SubjectConfirmation>
        </saml2:Subject>
        <saml2:Conditions NotBefore="2012-10-23T06:12:30.267Z"
NotOnOrAfter="2012-10-23T07:12:30.267Z">
            <saml2:AudienceRestriction>

<saml2:Audience>https://myremote.ec.europa.eu/dana-na/auth/saml-endpoint.cgi?p=sp1</sa
ml2:Audience>
            </saml2:AudienceRestriction>
            <saml2:OneTimeUse/>
            <saml2:ProxyRestriction Count="0"/>
        </saml2:Conditions>
        <saml2:AuthnStatement AuthnInstant="2012-10-23T06:42:30.267Z"
SessionIndex="_d4a2eb81-4ee9-45f9-b0c8-cfd252317c0e"
SessionNotOnOrAfter="2012-10-23T07:12:30.267Z">
            <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml2:Aut
hnContextClassRef>
            </saml2:AuthnContext>
        </saml2:AuthnStatement>
        <saml2:AttributeStatement>
            <saml2:Attribute FriendlyName="User Identifier" Name="user"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">keschma</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Email" Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Martin.HOFFMANN@ec.europa.eu</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Organisation" Name="domain"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">eu.europa.ec</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Organisation Username"
Name="domainUsername" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">keschma</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="First Name" Name="firstName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Martin</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Last Name" Name="lastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">HOFFMANN</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Groups" Name="groups"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">DIGIT_WEB_ALL</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">INTERNET</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">LIVENEWS</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">DG_DIGIT</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SDT_VISTA</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">EUROPOL</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
xsi:type="xs:string">SG_CISNET</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">PRICEFIX</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">DIGIT_ITBOS</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">DIGIT_VLE_P</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">OXAN</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">DIGIT_ECAS_A</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">ARES_USERS</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">DEV_IQSG</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">OPOCE_LEXAADM</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">OIB_KW_PARENT</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">RAPIDW</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">DANTE</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">PRICEMOB</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">CELEXW</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">OIB_KIDDYWEB</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">RAEPLUS</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">RELEX_TARIQAEC</saml2:AttributeValue>
                <saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SLWF</saml2:AttributeValue>
            </saml2:Attribute>
```

```
        </saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>
```

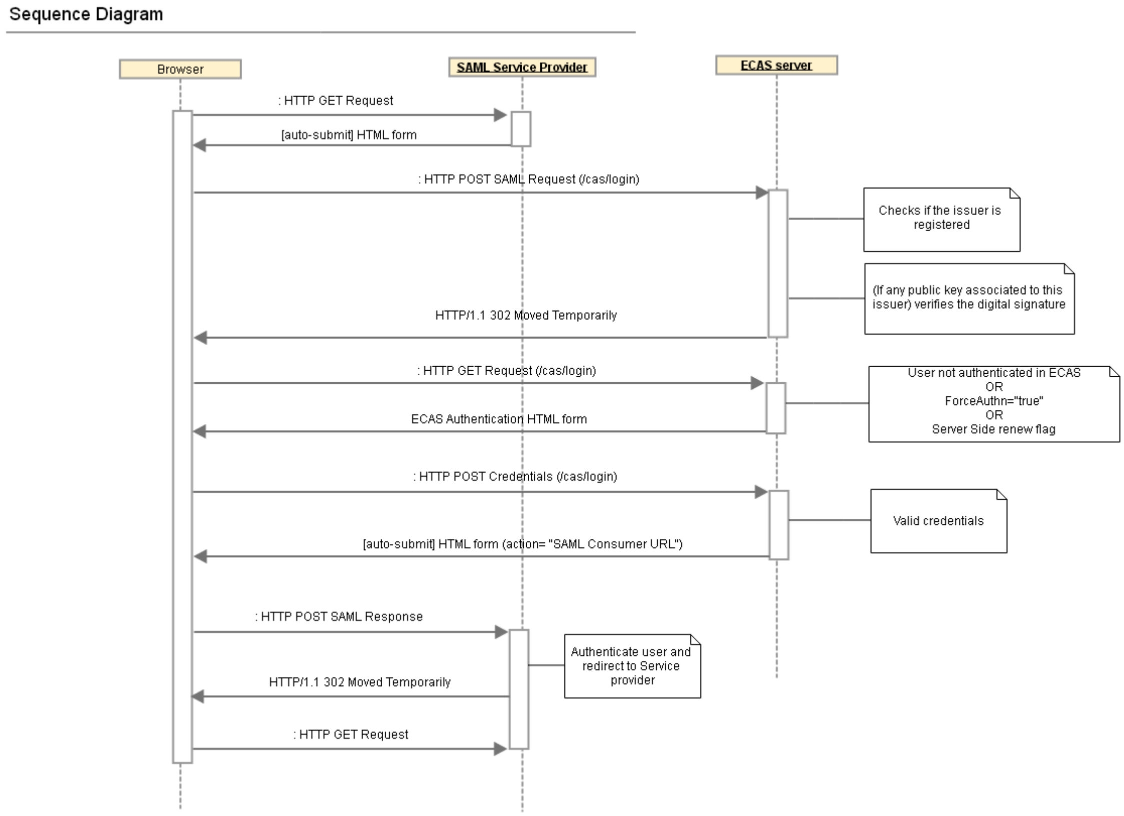
FAQ

User gets an error when she is redirected to ECAS login page.

- *"SAML AuthnRequest must contain an Issuer."* : the SAML requests doesn't contain any <saml:Issuer/> entry.
- *"The requested relying party is not registered (SAML). Please register your application with the IAM (Identity and Access Management) service." :* the value within <saml:Issuer/> doens't correspond to any issuer URI registered in ECAS.
- *"Invalid SAML AuthnRequest signature."* : the verification of the digital signature failed. Check if the private key used to signed and the public key registered in ECAS are parts of the same valid key pair.
- "*Unsigned SAML AuthnRequest while ECAS is expecting a signed SAML AuthnRequest. "* A public key is linked to the current issuer in ECAS but the SAML request is not signed.

Note: If ECAS receives a signed SAML request but no public key is linked to the issuer URI, the signature is not verified but the SAML request is accepted by ECAS and the authentication web flow continues.

Annex


Sequence Diagram
Browser
SAML Service Provider
ECAS server
: HTTP GET Request
[auto-submit] HTML form
: HTTP POST SAML Request (/cas/login)
Checks if the issuer is registered
(If any public key associated to this issuer) verifies the digital signature
HTTP/1.1 302 Moved Temporarily
: HTTP GET Request (/cas/login)
User not authenticated in ECAS OR ForceAuthn="true" OR Server Side renew flag
ECAS Authentication HTML form
: HTTP POST Credentials (/cas/login)
Valid credentials
[auto-submit] HTML form (action= "SAML Consumer URL")
: HTTP POST SAML Response
Authenticate user and redirect to Service provider
HTTP/1.1 302 Moved Temporarily
: HTTP GET Request