



EUROPEAN COMMISSION  
DIRECTORATE-GENERAL  
INFORMATICS  
Directorate D - Digital Services  
**Trans-European Services**



# European Commission

## ECAS Technical Guide For ECAS 4.4 and above

Date: 09/10/2018  
Version: 4.5  
Authors: DIGIT ECAS DEVELOPMENT  
Revised by:  
Approved by:  
Public:  
Reference Number:  
Status:

## TABLE OF CONTENTS

<b>1. INTRODUCTION .....</b>	<b>4</b>
1.1. What is ECAS.....	4
1.2. Audience and document scope .....	4
<b>2. ECAS MECHANISM.....</b>	<b>5</b>
2.1. Generic behaviour – basic success scenario .....	5
2.2. Example:.....	8
<b>3. ECAS SERVER .....</b>	<b>19</b>
3.1. ECAS Server URLs .....	19
<b>4. ECAS TICKET VALIDATION .....</b>	<b>20</b>
4.1. Mechanisms to validate ECAS tickets.....	20
4.1.1. CAS Protocol.....	20
4.1.2. Web Services .....	20
4.1.3. Two-way SSL/TLS.....	20
4.2. XML Schema for validation responses.....	20
4.3. ECAS Validation errors.....	22
4.3.1. INVALID_REQUEST .....	22
4.3.2. INVALID_TICKET .....	22
4.3.3. INVALID_SERVICE.....	23
4.3.4. INVALID_USER .....	24
4.3.5. ECAS_PROXY_COMMUNICATION_ERROR .....	24
4.3.6. INVALID_STRENGTH.....	25
4.3.7. INTERNAL_ERROR.....	25
4.4. ECAS Validation success .....	26
4.4.1. AuthenticationSuccess .....	26
<b>5. REFERENCES .....</b>	<b>28</b>
5.1. About the URLs.....	28
5.2. Links .....	29
<b>APPENDIX I: TICKET VALIDATION SCHEMA.....</b>	<b>30</b>
<b>APPENDIX II: TICKET VALIDATION WSDL .....</b>	<b>50</b>

## TABLE OF FIGURES

Figure 1 – The ECAS mechanism.....	5
Figure 2 - The ECAS login screen .....	11
Figure 3 - ECAS redirects the user back to the application .....	13
Figure 4 - The user is authenticated in the application.....	18
Figure 5 - XML Schema for Ticket Validation Responses .....	49
Figure 6 - Ticket Validation WSDL.....	54

## Document History

<i>Ver.</i>	<i>Author</i>	<i>Date</i>	<i>Comment</i>	<i>Mod. Pages</i>
1.0	lauredo	13/02/2007	Reflected changes in ECAS Client 1.3.0.	
2.0	ackxyyo	01/06/2008	Skimmed version of the Developer Kit.	All
3.0	verfade	24/06/2009	Changes for client version 1.9.	All
3.1	ackxyyo	09/09/2009	Reviewed.	All
3.2	ackxyyo	22/09/2009	Technology agnostic, removed ref. to WL except for illustrations purposes. Snapshots updated to ecas-demo. Title/subject adapted. Doc revisions numbers made independent from ECAS version.	
4.0	hordije	16/03/2010	Reflected changes in ECAS Client 1.10.	All
4.1	verfade	19/03/2010	Changes when revising.	
4.2	manalmi	20/03/2012	Changes when revising.	
3.6.3	lauredo	16/12/2013	Reflected changes in ECAS Server 3.6.3	
4.4	lauredo	30/10/2015	Added paragraph about INVALID_STRENGTH. Added the Ticket Validation WSDL annex.	
4.5	lauredo	09/10/2018	Added URL of Ticket Validation schema and WSDL	

## Reference Documents

<i>Code</i>	<i>Title</i>
[ECAS-BASIC]	ECAS Client Installation and Configuration Guide – Basic
[ECAS-ADV]	ECAS Client Installation and Configuration Guide – Advanced
[ECAS-FORGE]	<a href="https://webgate.ec.europa.eu/CITnet/confluence/display/IAM/ECAS+Forge">https://webgate.ec.europa.eu/CITnet/confluence/display/IAM/ECAS+Forge</a> All the above mentioned documents are available at that location.

Contact:

DIGIT-ECAS-DEVELOPMENT@ec.europa.eu

## 1. INTRODUCTION

### 1.1. What is ECAS

ECAS stands for **E**uropean **C**ommission **A**uthentication **S**ervice.

ECAS extends on the Central Authentication Service (CAS) protocol developed at Yale University. CAS became a JA-SIG project in December 2004<sup>1</sup>.

It is an authentication service to protect Web-based applications.

The main features are:

- (1) Protection of the user password: Only ECAS collects the user's password and this only over a secure channel (SSL). This means that the user's password is known only by ECAS and cannot be hijacked by any other application.
- (2) Homogenization of security policies: they are now defined in only one place.
- (3) Web Single Sign-on: the user authenticates only once for all the applications protected via ECAS<sup>2</sup>.

### 1.2. Audience and document scope

This document briefly explains how ECAS works. The intended audience is Java developers (knowledge of Servlets and HTTP will help).

It does not explain how to actually configure your server in order to protect a web application. For complete instructions on how to install and configure for WebLogic, please refer to [ECAS-BASIC] and [ECAS-ADV].

---

<sup>1</sup> See References p. 26, the CAS protocol is available at <http://www.jasig.org/cas/protocol>

<sup>2</sup> The Single Sign-on is only applicable if the user uses the same browser for all the applications.

## 2. ECAS MECHANISM

The mechanism is based on standard features of HTTP and can be used with any Web application in any language (Java, ColdFusion, PHP ...).

Standard mechanisms involved:

1. SSL for confidentiality and integrity
2. HTTP redirections which add request parameters in order to pass information back and forth
3. HTTP Cookie for Web Single Sign-on

### 2.1. Generic behaviour – basic success scenario

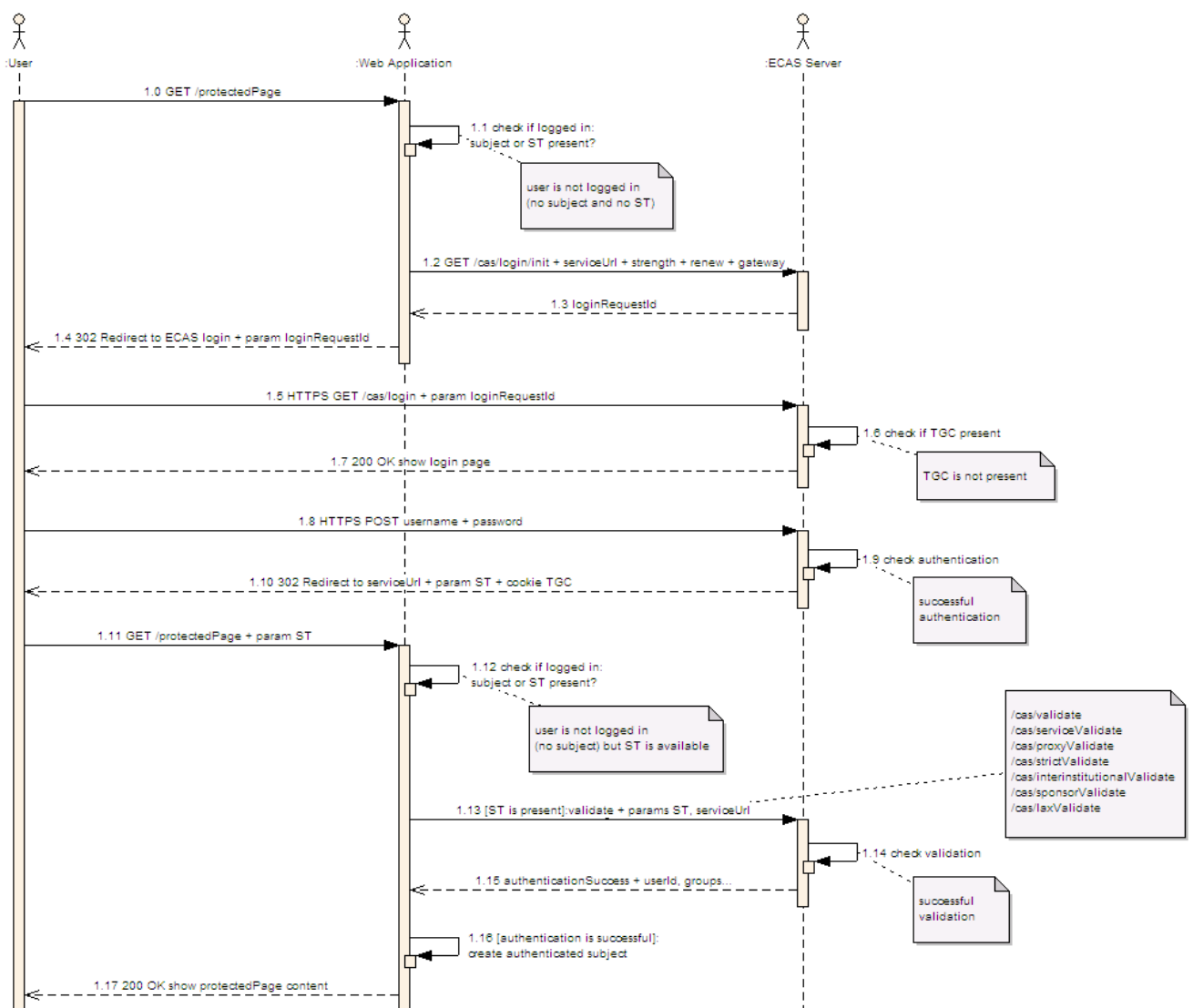


Figure 1 – The ECAS mechanism

- 0) The user requests, through her browser, access to a resource located inside an application protected by ECAS.
- 1) The ECAS Client is a piece of code in front of the application order to protect this application by the European Commission Authentication Service. It checks whether the user is already logged in. It does this by checking if a JEE Security Subject is already present or if the HTTP request contains an ECAS-specific token called a *service ticket* (ST). This ST is used to tell the ECAS Client whether the user has already been authenticated by ECAS or not. As this token is not present in this step in this scenario, the user is going to be redirected to the ECAS Server by the ECAS Client (the actual redirection happens in step 4 and 5).
- 2) The ECAS Client makes a *login initialization request* to the server. It submits the parameters which are necessary to make a secure authentication (strength, renew, gateway) and a parameter called *service* which holds the original request URL where the user must be redirected to after successful authentication.
- 3) The ECAS Server returns a *login request ID*. This ID is used by the server to securely identify which user has which authentication request parameters.
- 4) The ECAS Client redirects the user to the secured ECAS login screen. The ECAS Client adds the login request ID to the redirection URL.
- 5) The user's browser follows the redirection URL and requests the ECAS login screen via HTTPS.
- 6) The user enters ECAS. The ECAS Server checks whether a *ticket granting cookie* (TGC) is present (see also step 10). In this scenario it is not.
- 7) Based on the login request ID and the authentication request parameters it represents, the user is presented a login form to enter her username and password.
- 8) The user enters her username and password and submits the form to ECAS for authentication. The form is submitted using HTTPS.
- 9) The ECAS authentication service checks the given credentials. In this scenario the credentials are valid.
- 10) The ECAS Server redirects the user to the URL which is retrieved from the service parameter (see step 2). The Server adds the service ticket to the redirection URL.

The ECAS Server also sets an ECAS cookie called a *Ticket Granting Cookie* (TGC). This is a secure (only sent via SSL/TLS), context-specific (valid only for the ECAS context) cookie stored in memory (not stored on the hard drive). It is this cookie that allows the *Web single sign-on* (SSO) mechanism. ECAS looks for this cookie and does not present the login form if it finds it.
- 11) The user's browser follows the redirection URL and requests the original resource (from step 0) but now there is an ST parameter in the HTTP request.
- 12) Similar to step 1. The ECAS Client checks whether the user is already logged in. It does this by checking if a JEE Security Subject is already present or if the HTTP request contains an ST. This time the ST is present and the ECAS Client extracts this new ticket from the request query string.
- 13) The ECAS Client validates the ST by querying the ECAS Server through a secure connection (HTTPS). The service parameter is also sent along to validate that it is the legitimate (original) ECAS Client requesting the validation.
- 14) The ECAS Server checks the ST and service parameter. The ST is valid only once and only for a short period of time. In this scenario, the ST is valid.
- 15) The ECAS Server replies with an *authentication successful* message. The response also contains:

- The *user unique id* (also called uid or user ID). This is not to be confused with the *user moniker* (= *username*) which is not returned.
  - The *user login date and time* which was recorded when the TGC was obtained by entering the password in the ECAS login form (steps 8, 9 and 10).
  - The *strength* of the authentication mechanism. This property allows different levels of authentication strengths such as “BASIC”, “STRONG”, “NTLM” or “CLIENT\_CERT”. At the moment only “STRONG” and “NTLM” are used.
  - The user’s *CUD*<sup>3</sup> *groups* requested by the application.
- 16) The ECAS Client constructs a Security Subject for the application server it protects, allowing the user to be authenticated with the standard mechanisms of the container<sup>4</sup>.
- 17) If the *authorization* succeeds, the original requested resource is presented to the user. If it fails, the authenticated user is redirected to the error page specified in the application’s deployment descriptor.

---

<sup>3</sup> CUD: the Central User Database of the Commission

<sup>4</sup> These are standard Servlet API methods: [getRemoteUser\(\)](#), [getUserPrincipal\(\)](#), [isUserInRole\(String role\)](#) from [HttpServletRequest](#)



## 2.2. Example:

We will examine the HTTP requests and responses using the sample Java Web application `ecas-demo.ear` deployed on a WebLogic Server.

The user wants to access `http://myserver:7001/ecas-demo/protected/?param=123`

The “**protected**” context of the “**ecas-demo**” application is protected by ECAS and by a security authorization constraint in the `web.xml` and `weblogic.xml` deployment descriptors.

In the case of WebLogic Server, the ECAS Client consists in a WebLogic SSPI mechanism (an `AuthProvider` and `IdentityAsserterV2`).

Note that the numbering used below does not follow the numbering of the basic successful scenario.

(1) The user wants to access a resource protected by ECAS.

### HTTP Request:

```
http://myserver:7001/ecas-demo/protected/?param=123

GET /ecas-demo/protected/?param=123 HTTP/1.1
Host: myserver:7001
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: lang=en
```

### HTTP Response (delayed until the completion of step (2)):

```
HTTP/1.x 303 ECAS Authentication Required
Cache-Control: no-cache="Set-Cookie"
Transfer-Encoding: chunked
Location: https://ecas.cc.cec.eu.int:7002/cas/login?loginRequestId=
        ECAS_LR-2-npEzItoEL7h2gQyA5cCq7DLvxPCu6SRlppRVPvrszk7W-LdqaJcrzRYZ
        SU3kdplatzy-cuiYv2LnbMIztULLpui5e8
Content-Type: text/html; charset=utf-8
Set-Cookie: JSESSIONID=Q1YTKNfdJ3JJcWnD4RbwtM5hctty0BXNyQGfrTnpvk6GTh1l
        3D19!938862237; path=/ecas-demo
```

Since the ECAS Client did not find a *service ticket* granting access to this protected resource, it redirects to the ECAS login page for authentication.

- (2) As the ECAS Client didn't find a service ticket in the request, the user is redirected to the ECAS Server (previous step). But first, the ECAS Client must make a *login initialization request* to the server.

#### HTTP Request:

```
https://ecas.cc.cec.eu.int:7002/cas/login/init
```

```
POST /cas/login/init HTTP/1.1
Content-type: application/x-www-form-urlencoded;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
User-Agent: EcasHttpClient/1.9.0.0 (20090616181624) (Java/1.6.0_05;
  OS/Windows XP; Host/MYSERVER; IP/127.0.0.1) Java/1.6.0_05
Host: ecas.cc.cec.eu.int:7002
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Proxy-Connection: keep-alive
Content-Length: 133

service=http%3A%2F%2Fmyserver%3A7001%2Fecas-demo%2Fprotected
  %2Findex.jsp%3Fparam%3D123&acceptStrengths=PASSWORD%2CCCLIENT_CERT&
```

#### HTTP Response:

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Cache-Control: no-store
Pragma: no-cache
Content-Type: text/xml; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Length: 302

<?xml version="1.0" encoding="utf-8"?>
<loginRequest xmlns="https://ecas.ec.europa.eu/cas/schemas">
  <loginRequestSuccess>
    <loginRequestId>ECAS_LR-2-npEzItoEL7h2gQyA5cCq7DLvxPCu6SR1ppRVPvrsz
      k7W-LdqaJcrzRYZSU3kdplatzy-cuiYv2LnBMIztULLpui5e8</loginRequestId>
    </loginRequestSuccess>
  </loginRequest>
```

Among other parameters, a *service* request parameter is submitted. It contains the URLEncoded URL of the resource the user wanted to access. In our example, this is `<http://myserver:7001/ecas-demo/protected/index.jsp?param=123>` which is URLEncoded into `<http%3A%2F%2Fmyserver%3A7001%2Fecas-demo%2Fprotected%2Findex.jsp%3Fparam%3D123>`

- (3) As the ECAS Client doesn't find a service ticket in the request, it redirects to the ECAS login screen.

HTTP Request:

```
https://ecas.cc.cec.eu.int:7002/cas/login?loginRequestId=
ECAS_LR-2-npEzItoEL7h2gQyA5cCq7DLvxPCu6SRlppRVPvrszk7W-LdqaJcrzRYZ
SU3kdplatzy-cuiYv2LnbMIztULLpui5e8


GET /cas/login?loginRequestId=ECAS_LR-2-npEzItoEL7h2gQyA5cCq7DLvxPCu6S
RlppRVPvrszk7W-LdqaJcrzRYZSU3kdplatzy-cuiYv2LnbMIztULLpui5e8
HTTP/1.1
Host: ecas.cc.cec.eu.int:7002
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB;
rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: lang=en; MyEcasDomain=eu.europa.ec
```

HTTP Response:

```
HTTP/1.x 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Set-Cookie: CAS_SESSIONID=KhpkKNfSGB2ZDcmB6h2nvXYbg8kVb92mKywybLGC31FhN
7h6Hlrk!938862237; path=/cas; secure
```

- (4) The user has been redirected to ECAS and is presented the login screen:

Contact | Privacy Statement | English (en)




EUROPEAN COMMISSION AUTHENTICATION SERVICE (ECAS)

European Commission

Intracomm > Authentication Service > Login

[Login](#)
[New password](#)
[Sign Up](#)
[Help](#)



( authenticates your identity on European Commission websites )

**Login** [Not registered yet](#)

Is the selected domain correct?  
[European Commission](#) [Change it](#)

Username or e-mail address \*

Password \*




[More options...](#)

[Login!](#) [Lost your password?](#)

\* Required fields

---

Or log in with your

 [Mobile phone](#)
 [Token](#)
 [eID](#)

**Figure 2 - The ECAS login screen**

(5) The user submits the ECAS login form containing her credentials to the ECAS Server:

HTTP Request:

```
https://ecas.cc.cec.eu.int:7002/cas/login?loginRequestId=ECAS_LR-2-npEzItoEL7h2gQyA5cCq7DLvxPCu6SRlppRVPvrszk7W-LdqaJcrzRYZSU3kdplatzy-cuiYv2LnbMIztULLpui5e8

POST /cas/login?loginRequestId=ECAS_LR-2-npEzItoEL7h2gQyA5cCq7DLvxPCu6SRlppRVPvrszk7W-LdqaJcrzRYZSU3kdplatzy-cuiYv2LnbMIztULLpui5e8
HTTP/1.1
Host: ecas.cc.cec.eu.int:7002
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: https://ecas.cc.cec.eu.int:7002/cas/login?loginRequestId=ECAS_LR-2-npEzItoEL7h2gQyA5cCq7DLvxPCu6SRlppRVPvrszk7W-LdqaJcrzRYZSU3kdplatzy-cuiYv2LnbMIztULLpui5e8
Cookie: CAS_SESSIONID=KhpkKNfSGB2ZDcmB6h2nvXYbg8kVb92mKywybLGC31FhN7h6Hlrk!938862237; lang=en; MyEcasDomain=eu.europa.ec
Content-Type: application/x-www-form-urlencoded
Content-Length: 151

domain=eu.europa.ec&lt=LT-4-zifxzclDTi2zcWVlXuOTzyeJigGGP1VXGzul7qUwUESlG-LdqaJcrzRYZSU3kdplatzy-rMzqebcXiSN78yOf1U93Be&username=usertest&password=xxxx
```

### HTTP Response:

```
HTTP/1.x 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Set-Cookie: CASTGC=ECAS_TGC-2-xdj6BU8YziejD7U8k0YhgH7qYYI089hIKE2ds1CgH
    qRxqkhzZ07yQ1wp39fFOZyMaGl3QzOcnMMfaIPTWDM3xUG-LdqaJcrzRYSU3kdpla
    tzy-okGEgzkNbRUJYnnkrzTlmM; version=1; path=/cas; secure; discard;
    httpOnly
Refresh: 0; url=/cas/redirecting-to/ecas-demo?loginRequestId=ECAS_LR-2-
    npEzItoEL7h2gQyA5cCq7DLvxPCu6SRlppRVPvrszk7W-LdqaJcrzRYSU3kdplatz
    y-cuiYv2LnbMIztULLpui5e8
```

The response contains the *ticket granting cookie* (TGC) for *single sign-on* (SSO), and client-side redirection mechanisms (*meta refresh*, *window.location.href*) that redirect the browser to the page responsible for the actual HTTP redirection to our *ecas-demo* application. This two-phase redirection was introduced to inform users about what application they are waiting for.

(6) The response is displayed by the browser, while the user is about to be redirected.

As a result of a successful authentication, a *redirection page* is presented shortly to the user indicating that she has been authenticated successfully and that she is about to be redirected to the requested resource.



**Figure 3 - ECAS redirects the user back to the application**

(7) The second part of the two-phase redirection.

#### HTTP Request:

```
https://ecas.cc.cec.eu.int:7002/cas/redirecting-to/ecas-demo
?loginRequestId=ECAS_LR-2-npEzItoEL7h2gQyA5cCq7DLvxPCu6SR1ppRVPvrs
zk7W-LdqaJcrzRYZSU3kdplatzy-cuiYv2LnbMIztULLpui5e8

GET /cas/redirecting-to/ecas-demo?loginRequestId=ECAS_LR-2-npEzItoEL7h2
gQyA5cCq7DLvxPCu6SR1ppRVPvrszk7W-LdqaJcrzRYZSU3kdplatzy-cuiYv2LnbM
IztULLpui5e8 HTTP/1.1
Host: ecas.cc.cec.eu.int:7002
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB;
rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: https://ecas.cc.cec.eu.int:7002/cas/login?loginRequestId=
ECAS_LR-2-npEzItoEL7h2gQyA5cCq7DLvxPCu6SR1ppRVPvrszk7W-LdqaJcrzRYZ
SU3kdplatzy-cuiYv2LnbMIztULLpui5e8
Cookie: CAS_SESSIONID=KhpKKNfSGB2ZDcmB6h2nvXYbg8kVb92mKywybLGC31FhN7h6H
lrk!938862237; CASTGC=ECAS_TGC-2-xdj6BU8YziejD7U8k0YhgH7qYYI089hIK
E2ds1CgHqRxqkhzZ07yQ1wp39fOZyMaGl3QzOcnMMfaIPTWDM3xUG-LdqaJcrzRYZ
SU3kdplatzy-okGEgzkNbRUJYnnkrzTlmM; lang=en;
MyEcasDomain=eu.europa.ec
```

#### HTTP Response:

```
HTTP/1.x 303 See Other
Cache-Control: no-cache, no-store
Pragma: no-cache
Location: http://myserver:7001/ecas-demo/protected/index.jsp?param=123
&ticket=ECAS_ST-2-xLbqlpoBUzV2MQvXiKHcsUilaMQWyzhTUnZabdkQ0iUm-Ld
qaJcrzRYZSU3kdplatzy-zNbjVUnJh0GzGJzUB1KkKm
Content-Length: 455
Content-Type: text/html; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT
```

The user is redirected to the original URL, which in this example is our *ecas-demo* sample application. Observe the *ticket* parameter in the redirection URL (see the *Location* header).

Note: if the request uses HTTP/1.1, the response status code is “303”, if the request uses HTTP/1.0, it is “302”. The reason behind that is to avoid ambiguity in the browser behaviour because, here, we are redirecting after an HTTP POST to an HTTP GET (thus modifying the HTTP verb, which is stated as forbidden in HTTP/1.0 but correctly made by all modern browsers).

An HTTP “303” status code, unambiguously tells the browser to use HTTP GET to access to the redirected location and not to resend the posted FORM parameters.

(8) The browser follows the redirection, with a ticket parameter in the redirection URL.

HTTP Request:

```
http://myserver:7001/ecas-demo/protected/index.jsp
?param=123&ticket=ECAS_ST-2-xLbqlpoBUzV2MQvXiKHcsUIlaMQWyzhTUnZab
dkQ0iUm-LdqaJcrzRYZSU3kdplatzy-zNbjVUnJJh0GzGJzUB1KkKm

GET /ecas-demo/protected/index.jsp?param=123&ticket=ECAS_ST-2-xLbqlpoBU
zV2MQvXiKHcsUIlaMQWyzhTUnZabdkQ0iUm-LdqaJcrzRYZSU3kdplatzy-zNbjVUn
JJh0GzGJzUB1KkKm HTTP/1.1
Host: myserver:7001
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB;
rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

HTTP Response (delayed until after completion of step (9)):

```
HTTP/1.x 200 OK
Cache-Control: no-cache="Set-Cookie"
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1
Set-Cookie: JSESSIONID=4sVrKNffYHzJrT3M0JmpPSZ46L5vSsdJ2F6ttkks0NnV4dyM
Ltkd!938862237; path=/ecas-demo
```

As before, the application server redirects the browser to */ecas-demo/protected*, which is protected by the ECAS Client but this time there is a *ticket* parameter in the URL.



- (9) The ECAS Client finds the ticket and validates it by opening a direct HTTPS connection to ECAS Validation URL and by sending the **ticket** and the **service** to be validated. Optionally, the application may want to receive some CUD groups the user belongs to, by adding a parameter called “groups”. The application also needs to specify the authentication strengths it accepts when validating tickets:

#### HTTP Request:

```
https://ecas.cc.cec.eu.int:7002/cas/strictValidate
```

```
POST /cas/strictValidate HTTP/1.1
Content-type: application/x-www-form-urlencoded;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
User-Agent: EcasHttpClient/1.9.0.0 (20090616181624) (Java/1.6.0_05;
  OS/Windows XP; Host/MYSERVER; IP/127.0.0.1) Java/1.6.0_05
Host: ecas.cc.cec.eu.int:7002
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Proxy-Connection: keep-alive
Content-Length: 252

service=http%3A%2F%2Fmyserver%3A7001%2Fecas-demo%2Fprotected
%2Findex.jsp%3Fparam%3D123&ticket=ECAS_ST-2-xLbqlpoBUzV2MQvXiKHcsU
IlaMQWyzhTUnZabdkQ0iUm-LdqaJcrzRYZSU3kdplatzy-zNbjVUnJJh0GzGJzUBlK
kKm&groups=MY_CUD_GROUP_FOR_USERS%2CMY_CUD_GROUP_FOR_ADMINS&accepts
trengths=PASSWORD%2CCCLIENT_CERT
```

#### HTTP Response:

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Cache-Control: no-store
Pragma: no-cache
Content-Type: text/xml; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Length: 470

<cas:serviceResponse xmlns:cas="https://ecas.ec.europa.eu/cas/schemas"
  server="ECAS Server version 3.6.0 - 04/09/2013"
  date="2013-09-04T19:17:19.321+02:00"
  version="3.6">
  <cas:authenticationSuccess>
    <cas:user>usertest</cas:user>
    <cas:groups number="2">
      <cas:group>MY_CUD_GROUP_FOR_USERS</cas:group>
      <cas:group>MY_CUD_GROUP_FOR_ADMINS</cas:group>
    </cas:groups>
    <cas:strengths number="1">
      <cas:strength>PASSWORD</cas:strength>
    </cas:strengths>
    <cas:loginDate>2009-06-30T16:03:27.885+02:00</cas:loginDate>
  </cas:authenticationSuccess>
</cas:serviceResponse>
```

The ticket validation response contains the username, her groups, the strength level of the login and the date when the actual authentication was performed.

In our example, “ecas-demo” queried ECAS for membership to CUD groups “MY\_CUD\_GROUP\_FOR\_USERS” and “MY\_CUD\_GROUP\_FOR\_ADMINS”, which the authenticated user possesses as those groups are returned in the validation XML response.

(10) The ECAS Client now creates a JEE Subject to run-as and redirects the user to the resource she requested in the first place.

JEE servlet security-constraints are checked against the ECAS-authenticated Subject. As the user belongs to the groups specified in the security constraints, the application server grants her access.

If she had not been authorized to enter the requested resource, she would have been redirected to the error page specified in the form-based login-info of **web.xml**.

But as she was authorized, the requested resource “*http://myserver:7001/ecas-demo/protected/index.jsp?param=123*” is displayed in her browser:

## ecas-demo: Protected Zone

You are authorized to see this page because you have the J2EE role: "**ecasTestRole**" which was mapped from the CUD group: "**INTERNET**" returned by ECAS or mapped from the extra group returned by this application's ExtraGroupHandler

Test the following features to validate your ECAS client installation and configuration:

- [Anonymous Zone](#) ⓘ
- [Authenticated Zone \(no role required\)](#) ⓘ
- [Protected Zone \(requires group: INTERNET\)](#) ⓘ
- [Admin Zone \(requires group: LIVENEWS\)](#) ⓘ
- [Domain-protected Zone \(requires role: EuropeanCommissionRole\)](#) ⓘ
- [EmployeeType-protected Zone \(requires role: intramurosRole\)](#) ⓘ
- [Unauthorized Zone](#) ⓘ
- [Sample Renewal Page \(confirmation\) \(requires group: INTERNET\)](#) ⓘ
- [Sample Gateway Page \(peek\) \(no role required\)](#) ⓘ
- [Signature Zone](#) ⓘ
- [Re-POST to Protected Form Example](#) ⓘ
- [Change Language for Language Propagation](#) ⓘ
- [Deprecated CAS 1.0 validation for legacy systems](#) ⓘ
- [Logout](#) ⓘ

Servlet Security Methods	Result
<code>request.getRemoteUser()</code>	hordije
<code>request.getUserPrincipal()</code>	hordije
<code>((DetailedUser)request.getUserPrincipal()).getFirstName()</code>	Jerome
<code>((DetailedUser)request.getUserPrincipal()).getLastName()</code>	HORDIES
<code>((DetailedUser)request.getUserPrincipal()).getDomain()</code>	eu.europa.ec (i.e. European Commission)
<code>((DetailedUser)request.getUserPrincipal()).getDomainUsername()</code>	hordije
<code>((DetailedUser)request.getUserPrincipal()).getEmail()</code>	Jerome.HORDIES@ext.ec.europa.eu
<code>((DetailedUser)request.getUserPrincipal()).getTelephoneNumber()</code>	54318
<code>((DetailedUser)request.getUserPrincipal()).getDepartmentNumber()</code>	DIGIT.A.3.001
<code>((DetailedUser)request.getUserPrincipal()).getEmployeeType()</code>	x
<code>((DetailedUser)request.getUserPrincipal()).getEmployeeNumber()</code>	70001549
<code>((DetailedUser)request.getUserPrincipal()).getUserManager()</code>	null
<code>request.isUserInRole("ecasTestRole")</code>	true
<code>request.isUserInRole("adminRole")</code>	true
<code>request.isUserInRole("EuropeanCommissionRole")</code>	true
<code>request.isUserInRole("intramurosRole")</code>	true
<i>Authentication Data retrieved via the <a href="#">Servlet API</a>.</i>	

**Figure 4 - The user is authenticated in the application**

### 3. ECAS SERVER

ECAS service is offered via a JEE server containing the authentication application. It is meant to achieve high availability and high performance.

#### 3.1. ECAS Server URLs

The important URLs of ECAS Server:

**-login:**

<https://ecas.ec.europa.eu/cas/login>

This is the URL users use in order to log in

**-validating:**

<https://ecas.cc.cec.eu.int:7002/cas/strictValidate>

This is the default URL used for validating tickets.

(An application protected by ECAS needs to validate a token issued by ECAS (a *ticket*) to be able to know the identity of the user. The validating call is not done by the user's browser but by the application behind the scenes.)

The strictValidate URL only accepts internal Commission users. For other user populations, you need to use other validation URLs. For instance for interinstitutional users, you need to use *interinstitutionalValidate*, or for self-registered users, you have to use *laxValidate* (more details about the validationUrl in [ECAS-ADV]).

**-logout:**

<https://ecas.ec.europa.eu/cas/logout>

This is the URL users (or applications) can use to log out from ECAS.

Redirecting the user to this URL will log her out and will end her Single Logon session. It is recommended not to use it.

## 4. ECAS TICKET VALIDATION

### 4.1. Mechanisms to validate ECAS tickets

Tickets can only be validated over a secure transport (using TLS).

Tickets can only be validated once.

The validation consumes the ticket.

Tickets stay valid only for a limited amount of time (typically 5 minutes) after which they expire and are no longer available.

#### 4.1.1. CAS Protocol

Tickets can be validated using the CAS protocol, which uses an HTTP POST to send request parameters to the ECAS server and receives an XML response back.

The ticket validation XML response is specified by an XML schema (see 4.2 XML Schema for validation responses).

#### 4.1.2. Web Services

Tickets can also be validated using Web Services.

You can find the corresponding WSDL at

<https://ecas.ec.europa.eu/cas/ws/TicketValidationService?wsdl>

Available bindings are HTTP GET, HTTP POST, SOAP 1.1 and SOAP 1.2.

All available input parameters are documented in the [WSDL](#).

#### 4.1.3. Two-way SSL/TLS

One-way TLS is usually used (only the ECAS server is authenticated by the connecting application) but two-way TLS (mutual authentication) can also be used.

When two-way TLS is used, no Proxy-Granting-Ticket callback URL is required when requesting Proxy Granting Tickets as the service application is already authenticated by the TLS connection itself. So in this case, ProxyGrantingTickets are directly sent back in the XML response without performing a callback to the service application.

Please also note that when two-way TLS is attempted with the ECAS servers, they perform a DNS reverse lookup to ensure that the connecting peer owns the domain name corresponding to the client certificate presented in the TLS connection. A DNS reverse lookup failure results in a ticket validation failure.

## 4.2. XML Schema for validation responses

The XML Schema for XML messages returned by ECAS validation Servlet can be found at:

<https://ecas.ec.europa.eu/cas/schemas>

For your convenience, it is reproduced in APPENDIX I: Ticket Validation Schema

The optional "version" parameter in the validation request allows clients to specify the version of the protocol and XML Schema they want to receive in the XML response.

If no version parameter is sent by the client, we send the latest XML Schema.

#### Examples:

-Request with version 1.3:

```
GET /cas/strictValidate?version=1.3&ticket=ECAS_ST-13-  
DtujAkLF5FbgPOKVmr1z HTTP/1.1
```

```
Host: ecas.cc.cec.eu.int:7002
Connection: keep-alive
```

-Response:

```
HTTP/1.x 200 OK
Cache-Control: no-store
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/xml; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT

<?xml version="1.0" encoding="utf-8"?>
<cas:serviceResponse xmlns:cas="https://www.cc.cec/cas/schemas/1.3">
  <cas:authenticationFailure code='INVALID_REQUEST'>
    'service' and 'ticket' parameters are both required
  </cas:authenticationFailure>
</cas:serviceResponse>
```

-Request with version 1.9:

```
GET /cas/strictValidate?version=1.9&ticket=ECAS_ST-13-
DtujAkLF5FbgPOKVMrlz HTTP/1.1
Host: ecas.cc.cec.eu.int:7002
Connection: keep-alive
```

-Response:

```
HTTP/1.x 200 OK
Cache-Control: no-store
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/xml; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT

<?xml version="1.0" encoding="utf-8"?>
<cas:serviceResponse xmlns:cas="https://www.cc.cec/cas/schemas/1.9">
  <cas:authenticationFailure code='INVALID_REQUEST'>
    'service' and 'ticket' parameters are both required
  </cas:authenticationFailure>
</cas:serviceResponse>
```

-Request with no version specified:

```
GET /cas/strictValidate?ticket=ECAS_ST-13-DtujAkLF5FbgPOKVMrlz HTTP/1.1
Host: ecas.cc.cec.eu.int:7002
Connection: keep-alive
```

-Response:

```
HTTP/1.x 200 OK
Cache-Control: no-store
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/xml; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT

<?xml version="1.0" encoding="utf-8"?>
<cas:serviceResponse xmlns:cas="https://ecas.ec.europa.eu/cas/schemas">
  <cas:authenticationFailure code='INVALID_REQUEST'>
    'service' and 'ticket' parameters are both required
  </cas:authenticationFailure>
</cas:serviceResponse>
```

### 4.3. ECAS Validation errors

#### 4.3.1. INVALID\_REQUEST

If the validation request does not contain a *ticket* AND a *service* parameter, ECAS replies by an INVALID\_REQUEST error code within an authenticationFailure tag.

Example:

-Request:

```
GET /cas/strictValidate?ticket=ECAS_ST-13-DtujAkLF5FbgPOKVMrlz HTTP/1.1
Host: ecas.cc.cec.eu.int:7002
Connection: keep-alive
```

-Response:

```
HTTP/1.x 200 OK
Cache-Control: no-store
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/xml; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT

<?xml version="1.0" encoding="utf-8"?>
<cas:serviceResponse xmlns:cas="https://ecas.ec.europa.eu/cas/schemas">
  <cas:authenticationFailure code='INVALID_REQUEST'>
    'service' and 'ticket' parameters are both required
  </cas:authenticationFailure>
</cas:serviceResponse>
```

#### 4.3.2. INVALID\_TICKET

If the service ticket has already been used once or has expired or is malformed or was not created by ECAS, the validation Servlet replies by an authenticationFailure with code INVALID\_TICKET.

Example:

**-Request:**

```
GET
/cas/strictValidate?service=https%3A%2F%2F158.166.132.216%3A7002%2Fappl
icationA%2Flogin&ticket=ECAS_ST-13-DtujAkLF5FbgPOKVMr1U HTTP/1.1
Host: ecas.cc.cec.eu.int:7002
Connection: keep-alive
```

**-Response:**

```
HTTP/1.x 200 OK
Cache-Control: no-store
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/xml; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT

<?xml version="1.0" encoding="utf-8"?>
<cas:serviceResponse xmlns:cas="https://ecas.ec.europa.eu/cas/schemas">
  <cas:authenticationFailure code='INVALID_TICKET'>
    ticket 'ECAS_ST-13-DtujAkLF5FbgPOKVMr1U' not recognized
  </cas:authenticationFailure>
</cas:serviceResponse>
```

#### 4.3.3. INVALID SERVICE

If the service the protected application sent along with the service ticket does not match the service ECAS stored when creating the service ticket, ECAS Validation Servlet replies by an authenticationFailure with code INVALID\_SERVICE.

Example:

**-Request:**

```
GET /cas/strictValidate?
service=https%3A%2F%2Fwrong.service%3A7002%2FapplicationA%2Findex.jsp&t
icket=ECAS_ST-2-uVQeZF3gDduNCSQFh7Ve HTTP/1.1
Host: ecas.cc.cec.eu.int:7002
Connection: keep-alive
```

**-Response:**

```
HTTP/1.x 200 OK
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Content-Type: text/xml; charset=UTF-8
Content-Length: 9335
Proxy-Connection: Keep-Alive
Connection: Keep-Alive

<?xml version="1.0" encoding="utf-8"?>
<cas:serviceResponse xmlns:cas="https://ecas.ec.europa.eu/cas/schemas">
  <cas:authenticationFailure code='INVALID_SERVICE'>
    ticket 'ECAS_ST-2-uVQeZF3gDduNCSQFh7Ve' does not match supplied
    Service
  </cas:authenticationFailure>
</cas:serviceResponse>
```



#### 4.3.4. INVALID\_USER

The user was authenticated successfully but does not belong to the accepted population based on the validation URL. Please see [ECAS-ADV] for all available validation URLs and user populations. In the examples below, strictValidate will only accept internal Commission users.

##### Example:

##### -Request:

```
GET /cas/strictValidate?
service=https%3A%2F%2F158.166.132.216%3A7002%2FapplicationA%2Flogin
&ticket=ECAS_ST-2-uVQeZF3gDduNCSQFh7Ve HTTP/1.1
Host: ecas.cc.cec.eu.int:7002
Connection: keep-alive
```

##### -Response:

```
HTTP/1.x 200 OK
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Content-Type: text/xml; charset=UTF-8
Content-Length: 9335
Proxy-Connection: Keep-Alive
Connection: Keep-Alive

<?xml version="1.0" encoding="utf-8"?>
<cas:serviceResponse xmlns:cas="https://ecas.ec.europa.eu/cas/schemas">
  <cas:authenticationFailure code='INVALID_USER'>
    user 'nverfade' is an external user
  </cas:authenticationFailure>
</cas:serviceResponse>
```

#### 4.3.5. ECAS\_PROXY\_COMMUNICATION\_ERROR

This error code is thrown when your application uses ECAS Proxy Tickets and the configured PGT URL (the callback URL in your application used to receive Proxy Tickets from the ECAS Server) cannot be accessed.

This can be either because:

Your PGT URL is not reachable from the ECAS Server (network issue)

Your PGT URL is invalid (typo, wrong value)

Your PGT URL does not use HTTPS with an accepted certificate. For production, only SSL certificates issued by the Commission's PKI: CommisSign are accepted (a.k.a "SSLPeerUnverifiedException").

Your PGT URL is served using an invalid SSL Certificate, e.g. the CN (common name) does not match the hostname of your server (a.k.a. "hostname verification failed").

Your PGT URL is wrongly protected by a security-constraint. In that case, the ECAS Server is requested to authenticate to send the PGT, which it cannot do on its own. The PGT URL must be accessible without authentication.

#### Example:

##### **-Request:**

```
GET
/cas/strictValidate?service=https%3A%2F%2F158.166.132.216%3A7002%2Fappl
icationA%2Flogin&ticket=ECAS_ST-2-
uVQeZF3gDduNCSQFh7Ve&pgtUrl=https%3A%2F%2F158.166.132.216%3A7002%2Fappl
icationA%2FecasProxy HTTP/1.1
Host: ecas.cc.cec.eu.int:7002
Keep-Alive: 300
Connection: keep-alive
```

##### **-Response:**

```
HTTP/1.x 200 OK
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Content-Type: text/xml; charset=UTF-8
Content-Length: 9335
Proxy-Connection: Keep-Alive
Connection: Keep-Alive

<?xml version="1.0" encoding="UTF-8"?>
<cas:serviceResponse xmlns:cas="https://ecas.ec.europa.eu/cas/schemas">
  <cas:authenticationFailure code="ECAS_PROXY_COMMUNICATION_ERROR">
    Unable to access your requested callback URL:
    "https://158.166.132.216:7002/applicationA/ecasProxy"
    (javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated)
  </cas:authenticationFailure>
</cas:serviceResponse>
```

#### 4.3.6. INVALID\_STRENGTH

This error code is thrown when the application is requesting an authentication strength which is not available in the connected ECAS server environment (for instance, because the requested strength exists in TEST but does not exist in PRODUCTION).

Or this error code is sent when the application specifies the ***acceptStrengths*** request parameter with the comma-separated list of authentication it accepts but the ticket being validated corresponds to a User who was not authenticated with any of the accepted strengths.

For instance, if the User was authenticated during her SSO session using PASSWORD\_SMS and NTLM, and if the application requested authentication strengths consisting in PASSWORD\_TOKEN and STORK, the validation of the ticket would produce an INVALID\_STRENGTH error since there are no strength in common between the requested ones and the ones having authenticated the user.

If the application does not send any ***acceptStrengths*** request parameter, the validation of the authentication strengths **MUST** be handled client-side in the ECAS client logic since the ECAS server will return the list of all the strengths having authenticated the user.

In particular, the ECAS client logic **MUST** compare the strengths configured in the application configuration files as acceptable to the one returned by the ECAS server in the ticket validation XML response and **MUST** reject validation responses which do not meet the authentication requirements of the protected application.

#### 4.3.7. INTERNAL\_ERROR

This error code is thrown when an unexpected internal server error occurs at the ECAS server-side. There is nothing you can do about this kind of errors apart from contacting the support to report the incident.

## 4.4. ECAS Validation success

### 4.4.1. AuthenticationSuccess

If the user was successfully authenticated by ECAS and if the ticket is valid and matches the supplied service parameter, the response is an AuthenticationSuccess which contains the username, the groups the user belongs to from those the client application asked, the strength level of the performed authentication and its timestamp.

#### Example 1:

-Request:

```
GET /cas/TicketValidationService?service=
http%3A%2F%2F158.166.132.216%3A7001%2FapplicationA%2Findex.jsp
&ticket=ECAS_ST-208-JNZ7OzT8aaRav12I6kIF&groups=MY_CUD_GROUP1,
MY_CUD_GROUP2&service=https%3A%2F%2Fd02di1022041dit%3A7002%2Fhelloworld
%2Fprotected%2FhelloFriends&ticketTypes=SERVICE&acceptStrengths=PASSWOR
D HTTP/1.1
Host: ecast.cc.cec.eu.int:7002
Connection: keep-alive
```

-Response:

```
HTTP/1.x 200 OK
Cache-Control: no-store
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/xml; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT

<cas:serviceResponse server="ECAS TEST version 3.6.3.20595 - 12/12/2013
- 11:36" date="2013-12-12T14:43:22.477+02:00">
  <cas:authenticationSuccess>
    <cas:user>donydgr</cas:user>
    <cas:groups number="2">
      <cas:group>MY_CUD_GROUP1</cas:group>
      <cas:group>MY_CUD_GROUP2</cas:group>
    </cas:groups>
    <cas:strengths number="1">
      <cas:strength>PASSWORD</cas:strength>
    </cas:strengths>
    <cas:authenticationFactors number="1">
      <cas:moniker>donydgr</cas:moniker>
    </cas:authenticationFactors>
    <cas:loginDate>2012-09-14T14:41:50.350+02:00</cas:loginDate>
    <cas:ticketType>SERVICE</cas:ticketType>
  </cas:authenticationSuccess>
</cas:serviceResponse>
```

**Example 2:** The application may also request the user details. In that case the exchange looks as follows:

-Request:

```
GET /cas/TicketValidationService?ticket=ECAS_ST-369693-
fKo5rCGtrvozXAkdxpFfRBZZaLVpQovPJjzc9wewmJO0-CDPpTLiluVzlMEIdfbszzjW-
qtLv40lRGQgH7WJQqzTEo0&service=https%3A%2F%2Fd02di1022041dit%3A7002%2Fh
elloworld%2Fprotected%2FhelloFriends
&userDetails=true&ticketTypes=SERVICE&acceptStrengths=PASSWORD HTTP/1.1
Host: ecast.cc.cec.eu.int:7002
Connection: keep-alive
```

-Response:

```
HTTP/1.x 200 OK
Cache-Control: no-store
Date: Mon, 21 Sep 2009 19:00:25 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/xml; charset=utf-8
Expires: Wed, 31 Dec 1969 23:59:59 GMT
X-Powered-By: Servlet/2.4 JSP/2.0

1 <?xml version="1.0" encoding="utf-8"?>
2 <cas:serviceResponse
xmlns:cas="https://ecas.ec.europa.eu/cas/schemas"
3         server="ECAS TEST version 3.1.2.10595 -
12/09/2012 - 11:36"
4         date="2012-09-12T18:00:44.099+02:00">
5     <cas:authenticationSuccess>
6         <cas:user>donydgr</cas:user>
7         <cas:departmentNumber>DIGIT.A.3.001</cas:departmentNumber>
8         <cas:email>Gregory.DONY@ext.ec.europa.eu</cas:email>
9         <cas:employeeNumber>90037440</cas:employeeNumber>
10        <cas:employeeType>x</cas:employeeType>
11
12        <cas:firstName>Gregory</cas:firstName>
13        <cas:lastName>DONY</cas:lastName>
14        <cas:domain>eu.europa.ec</cas:domain>
15        <cas:domainUsername>donydgr</cas:domainUsername>
16        <cas:telephoneNumber>93819</cas:telephoneNumber>
17        <cas:locale>en</cas:locale>
18
19        <cas:assuranceLevel>40</cas:assuranceLevel>
20        <cas:uid>donydgr</cas:uid>
21        <cas:orgId>231651</cas:orgId>
22        <cas:strength>STRONG</cas:strength>
23        <cas:authenticationFactors number="1">
24            <cas:moniker>donydgr</cas:moniker>
25
26        </cas:authenticationFactors>
27        <cas:loginDate>2012-09-12T18:00:00.878+02:00</cas:loginDate>
28        <cas:ticketType>SERVICE</cas:ticketType>
29    </cas:authenticationSuccess>
30 </cas:serviceResponse>
```

## 5. REFERENCES

### 5.1. About the URLs

Please adapt the links for ECAS to your environment:

From within the European Commission, please use:

either <https://ecas.cc.cec.eu.int:7002/cas>

or <https://ecas.ec.europa.eu/cas>

or <https://www.cc.cec/ecas/>

or <https://intragate.ec.europa.eu/cas>

From outside and for trusted contractors, please use

<https://webgate.ec.europa.eu/cas>

From other European Institutions using the TESTA II network, please use:

<https://webgate.ec.testa.eu/cas>

## 5.2. Links

### CAS:

CAS authentication mechanism, developed at Yale University is now a JA-SIG project:

<http://www.jasig.org/cas>

<http://www.jasig.org/cas/protocol>

### HTTP/1.1:

<http://www.w3.org/Protocols/rfc2616/rfc2616.html>

### ECAS:

ECAS project home page on Wiki:

<https://webgate.ec.europa.eu/CITnet/confluence/display/IAM/ECAS>

ECAS Forge: <https://webgate.ec.europa.eu/CITnet/confluence/display/IAM/ECAS+Forge>

ECAS Forum: <https://webgate.ec.europa.eu/CITnet/modules/newbb/viewforum.php?forum=35>

ECAS issue tracker (JIRA): <https://webgate.ec.europa.eu/CITnet/jira/browse/ECAS>

ECAS repository (Subversion): <https://webgate.ec.europa.eu/CITnet/svn/ecas-public>

ECAS fisheye: <https://webgate.ec.europa.eu/CITnet/fisheye/browse/ECAS>

# APPENDIX I: TICKET VALIDATION SCHEMA

The Ticket Validation schema is available at: <https://ecas.ec.europa.eu/cas/schemas/ecas.xsd>

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="https://ecas.ec.europa.eu/cas/schemas" xmlns="https://ecas.ec.europa.eu/cas/schemas"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified" version="5.8.0" xml:lang="EN">
  <xsd:attributeGroup name="ecasServerAttributeGroup">
    <xsd:annotation>
      <xsd:documentation>ECAS Server environment and date-time information</xsd:documentation>
      <xsd:appinfo>since 3.1.0</xsd:appinfo>
    </xsd:annotation>
    <xsd:attribute name="server" type="xsd:string">
      <xsd:annotation>
        <xsd:documentation>
          The ECAS Server environment such as PRODUCTION, TEST, LOAD, DEVELOPMENT, etc plus the version
          and build information.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:attribute>
    <xsd:attribute name="date" type="xsd:dateTime">
      <xsd:annotation>
        <xsd:documentation>The ECAS Server date and time.</xsd:documentation>
      </xsd:annotation>
    </xsd:attribute>
    <xsd:attribute name="version" type="xsd:string">
      <xsd:annotation>
        <xsd:documentation>
          The ECAS protocol version used in this message.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:attribute>
  </xsd:attributeGroup>
  <xsd:element name="serviceResponse">
    <xsd:annotation>
      <xsd:documentation>ECAS response to a Ticket validation request or a ProxyTicket obtention request
      </xsd:documentation>
      <xsd:appinfo>version 4.5.0</xsd:appinfo>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:choice>
        <xsd:element name="authenticationSuccess" type="authenticationSuccessType">
          <xsd:unique name="authenticationSuccess-group-uniqueness">
            <xsd:annotation>
              <xsd:documentation>
                The group name must be unique within the authenticationSuccess element.
              </xsd:documentation>
            </xsd:annotation>
            <xsd:selector xpath="groups"/>
            <xsd:field xpath="group"/>
          </xsd:unique>
          <xsd:unique name="authenticationSuccess-proxy-uniqueness">
            <xsd:annotation>
              <xsd:documentation>
                The proxy value must be unique within the authenticationSuccess element.
              </xsd:documentation>
            </xsd:annotation>
            <xsd:selector xpath="proxies"/>
            <xsd:field xpath="proxy"/>
          </xsd:unique>
          <xsd:unique name="authenticationSuccess-extendedAttribute-uniqueness">
            <xsd:annotation>
              <xsd:documentation>
                Each dynamicAttribute must be unique within the authenticationSuccess element.
              </xsd:documentation>
            </xsd:annotation>
            <xsd:selector xpath="extendedAttributes/extendedAttribute"/>
            <xsd:field xpath="@name"/>
          </xsd:unique>
        </xsd:element>
      </xsd:choice>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```

```

</xsd:element>
<xsd:element name="authenticationFailure" type="authenticationFailureType"/>
<xsd:element name="proxySuccess" type="proxySuccessType"/>
<xsd:element name="proxyFailure" type="proxyFailureType"/>
</xsd:choice>
<xsd:attributeGroup ref="ecasServerAttributeGroup"/>
</xsd:complexType>
</xsd:element>
<xsd:complexType name="authenticationSuccessType">
  <xsd:annotation>
    <xsd:documentation>ECAS body response when authentication succeeded</xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="user" type="userType">
      <xsd:annotation>
        <xsd:documentation>The name of the user authenticated by ECAS, this is the uid, the unique user ID.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:sequence id="userDetails" minOccurs="0">
      <xsd:element name="registrationLevelVersion" minOccurs="0" maxOccurs="unbounded">
        <xsd:complexType>
          <xsd:annotation>
            <xsd:documentation>The version of the user's credentials used in the authentication method
            for the requested application security level.
            </xsd:documentation>
          </xsd:annotation>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="level" type="registrationLevelType" use="required">
                <xsd:annotation>
                  <xsd:documentation>The application security level for the version of the user's
                  credentials
                  </xsd:documentation>
                </xsd:annotation>
              </xsd:attribute>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="departmentNumber" type="xsd:string" minOccurs="0">
        <xsd:annotation>
          <xsd:documentation>The user's department number</xsd:documentation>
        </xsd:annotation>
      </xsd:element>
      <xsd:element name="email" type="xsd:string" minOccurs="0">
        <xsd:annotation>
          <xsd:documentation>The user's email</xsd:documentation>
        </xsd:annotation>
      </xsd:element>
      <xsd:element name="employeeNumber" type="xsd:string" minOccurs="0" nillable="true">
        <xsd:annotation>
          <xsd:documentation>
            The user's employee number, if she belongs to the European Commission.
            Null for external users.
            Some other Institutions may also provide an employee number.
            The employee number is the PER_ID (unique ID from COMREF).

            This is different from the ecSysperNumber which is the pers_number, registration number and
            SYSPER number; ecSysperNumber = pers_number = registration number = SYSPER number. The
            ecSysperNumber is not returned by ECAS.
          </xsd:documentation>
          <xsd:appinfo>since 1.9.1</xsd:appinfo>
        </xsd:annotation>
      </xsd:element>
      <xsd:element name="employeeType" type="employeeTypeType" minOccurs="0">
        <xsd:annotation>
          <xsd:documentation>The user's employeeType</xsd:documentation>
        </xsd:annotation>
      </xsd:element>
      <xsd:element name="firstName" type="xsd:string" minOccurs="0">
        <xsd:annotation>
          <xsd:documentation>The user's firstName</xsd:documentation>
        </xsd:annotation>
      </xsd:element>
    </xsd:sequence>
  </xsd:sequence>

```



```

</xsd:element>
<xsd:element name="lastName" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>The user's lastName</xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="domain" type="domainType" minOccurs="0">
  <xsd:annotation>
    <xsd:appinfo>The domain replaces the organisation</xsd:appinfo>
    <xsd:documentation>The user's domain</xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="domainUsername" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The user's name in her domain or organisation.
      (This can be different from the "user" value, which is the unique user id at the
      Commission's.
      The pair domain and domainUsername is unique within the Commission's.)
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="telephoneNumber" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>The user's telephoneNumber</xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="userManager" type="xsd:string" minOccurs="0" nillable="true">
  <xsd:annotation>
    <xsd:documentation>The user's manager. May be null.</xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="timeZone" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The user's timeZone e.g. &quot;GMT+01:00&quot;.
      This user's attribute is informational and may be inaccurate.
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="locale" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The user's locale e.g. &quot;en&quot;.
      This user's attribute is informational and may be inaccurate.
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="assuranceLevel" type="assuranceLevelType" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The user's identity assurance level.
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="uid" type="userType">
  <xsd:annotation>
    <xsd:documentation>
      The uid is the user's unique ID. It has the same value as the value of the "user" element
      (see above).
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="orgId" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The orgId is the ID of the user's organisation in the HR system.
    </xsd:documentation>
    <xsd:appinfo>since 2.5.0</xsd:appinfo>
  </xsd:annotation>
</xsd:element>
<xsd:element name="teleworkingPriority" type="xsd:boolean" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>

```

A "true" value indicates that the user has priority in teleworking.

A "false" value indicates that the user does not have priority in teleworking.

```
</xsd:documentation>
<xsd:appinfo>since 4.5.0</xsd:appinfo>
</xsd:annotation>
</xsd:element>
<xsd:element name="extendedAttributes" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>The user's additional attributes, which can come from an extension for
    specific needs of a target application.
    </xsd:documentation>
    <xsd:appinfo>since 4.0.0</xsd:appinfo>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="extendedAttribute" type="attributeType" maxOccurs="unbounded">
        <xsd:annotation>
          <xsd:documentation>An additional attribute.</xsd:documentation>
          <xsd:appinfo>since 4.0.0</xsd:appinfo>
        </xsd:annotation>
      </xsd:element>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
</xsd:sequence>
<xsd:element name="groups" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>The list of CUD groups the user belongs to</xsd:documentation>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="group" type="xsd:string" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="number" type="xsd:nonNegativeInteger" use="required"/>
  </xsd:complexType>
</xsd:element>
<xsd:element name="strengths">
  <xsd:annotation>
    <xsd:documentation>
      The list of authentication strengths the user is currently authenticated with in her SSO session
      matching the strengths accepted by the target application.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="strength" type="strengthType" maxOccurs="unbounded">
        <xsd:annotation>
          <xsd:documentation>
            A strength with which the user was authenticated by ECAS in her SSO
            session matching one of the strengths requested by the target application.
          </xsd:documentation>
        </xsd:annotation>
      </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="number" type="xsd:nonNegativeInteger" use="required"/>
  </xsd:complexType>
</xsd:element>
<xsd:element name="authenticationFactors" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>The list of authentication factors in multi-factor authentications
  </xsd:documentation>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:sequence>
      <xsd:choice maxOccurs="unbounded">
        <xsd:element name="mobilePhoneNumber" type="xsd:string">
          <xsd:annotation>
            <xsd:documentation>The mobile phone number used as second authentication factor when
            using multi-factor authentication including an SMS challenge
          </xsd:documentation>
        </xsd:annotation>
      </xsd:element>
      <xsd:element name="moniker" type="xsd:string">
        <xsd:annotation>
```

```

        <xsd:documentation>The username in a username/password authentication
      </xsd:documentation>
    </xsd:annotation>
  </xsd:element>
  <xsd:element name="storkId" type="xsd:string">
    <xsd:annotation>
      <xsd:documentation>The STORK identifier when the STORK authentication is used
    </xsd:documentation>
    </xsd:annotation>
  </xsd:element>
  <xsd:element name="tokenCramId" type="xsd:string">
    <xsd:annotation>
      <xsd:documentation>The serial number of the CRAM hardware token used as second
        authentication factor when using multi-factor authentication including a
        CRAM hardware token
      </xsd:documentation>
      <xsd:appinfo>since 4.3.0</xsd:appinfo>
    </xsd:annotation>
  </xsd:element>
  <xsd:element name="tokenId" type="xsd:string">
    <xsd:annotation>
      <xsd:documentation>The serial number of the hardware token used as second
        authentication factor when using multi-factor authentication including a
        hardware token
      </xsd:documentation>
    </xsd:annotation>
  </xsd:element>
  <xsd:element name="mobileDevice" type="mobileDeviceType">
    <xsd:annotation>
      <xsd:documentation>The mobile device used as second authentication factor when
        using multi-factor authentication including a Mobile Device
      </xsd:documentation>
      <xsd:appinfo>since 5.8.0</xsd:appinfo>
    </xsd:annotation>
  </xsd:element>
</xsd:choice>
</xsd:sequence>
<xsd:attribute name="number" type="xsd:nonNegativeInteger" use="required"/>
</xsd:complexType>
</xsd:element>
<xsd:element name="loginDate" type="xsd:dateTime" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>The timeStamp when the user last authenticated to ECAS by supplying her password
  </xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="sso" type="xsd:boolean">
  <xsd:annotation>
    <xsd:documentation>
      A "true" value indicates that the authentication comes from Web Single Sign-On (SSO).
      A "false" value indicates that the authentication comes from the first
      authentication of the end-user or from the renewal of the authentication.
    </xsd:documentation>
    <xsd:appinfo>since 4.4.0</xsd:appinfo>
  </xsd:annotation>
</xsd:element>
<xsd:element name="ticketType" type="ticketType" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The type of the ticket being validated. For instance, the ticket can be a ServiceTicket,
      a ProxyTicket or a DesktopProxyTicket.
    </xsd:documentation>
    <xsd:appinfo>since 1.11.0</xsd:appinfo>
  </xsd:annotation>
</xsd:element>
<xsd:element name="proxyGrantingProtocol" type="proxyGrantingProtocolType" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The Proxy Granting Protocol used to obtain Proxy Granting Tickets.
      For instance, PGT_URL to use a callback URL, CLIENT_CERT to use 2-way SSL and
      a client X.509 certificate, DESKTOP to request a DesktopProxyGrantingTicket for
      a desktop application.
    </xsd:documentation>
    <xsd:appinfo>since 1.11.0</xsd:appinfo>
  </xsd:annotation>

```

```

    </xsd:annotation>
  </xsd:element>
  <xsd:element name="proxyGrantingTicket" type="xsd:string" minOccurs="0">
    <xsd:annotation>
      <xsd:documentation>The ProxyGrantingTicket IOU for ECAS proxies (pgtIOU)</xsd:documentation>
    </xsd:annotation>
  </xsd:element>
  <xsd:element name="proxies" minOccurs="0">
    <xsd:annotation>
      <xsd:documentation>The list of ECAS proxies in the chain</xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="proxy" type="xsd:string" minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
      <xsd:attribute name="number" type="xsd:nonNegativeInteger" use="optional"/>
    </xsd:complexType>
  </xsd:element>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="authenticationFailureType">
  <xsd:annotation>
    <xsd:documentation>ECAS body response when authentication failed</xsd:documentation>
  </xsd:annotation>
  <xsd:simpleContent>
    <xsd:extension base="xsd:string">
      <xsd:attribute name="code" type="xsd:string" use="required">
        <xsd:annotation>
          <xsd:documentation>The error code thrown by ECAS</xsd:documentation>
        </xsd:annotation>
      </xsd:attribute>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
<xsd:complexType name="proxySuccessType">
  <xsd:annotation>
    <xsd:documentation>ECAS body response when a ProxyTicket request succeeds</xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="proxyTicket" type="xsd:string">
      <xsd:annotation>
        <xsd:documentation>The value of the ProxyTicket generated by ECAS</xsd:documentation>
      </xsd:annotation>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="proxyFailureType">
  <xsd:annotation>
    <xsd:documentation>ECAS body response when a ProxyTicket request fails</xsd:documentation>
  </xsd:annotation>
  <xsd:simpleContent>
    <xsd:extension base="xsd:string">
      <xsd:attribute name="code" type="xsd:string" use="required">
        <xsd:annotation>
          <xsd:documentation>The error code thrown by ECAS</xsd:documentation>
        </xsd:annotation>
      </xsd:attribute>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
<xsd:simpleType name="userType">
  <xsd:annotation>
    <xsd:documentation>The username should be at least 7-character long</xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="7"/>
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="errorCode">
  <xsd:annotation>
    <xsd:documentation>Possible error codes thrown by ECAS</xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">

```

```

<xsd:enumeration value="BAD_PGT">
  <xsd:annotation>
    <xsd:documentation>
      Error code thrown when a ProxyGrantingTicket is not recognized.
      This may be because the user logged out of ECAS or because the PGT is invalid.
    </xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="ECAS_PROXY_COMMUNICATION_ERROR">
  <xsd:annotation>
    <xsd:documentation>
      Error code thrown when the proxy service callback URL cannot be reached by the ECAS server.
      This may be because the callback URL is not available (503 or 404) or
      because this callback URL is wrongly under a security constraint (401) or
      because the callback URL uses an SSL certificate which is not trusted by the ECAS server or
      because the callback URL did not reply correctly (HTTP 200 + proxySuccess tag in the body).
    </xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="INTERNAL_ERROR">
  <xsd:annotation>
    <xsd:documentation>Error code thrown when an internal error occurred in the ECAS server itself.
  </xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="INVALID_PROXY_CALLBACK_URL">
  <xsd:annotation>
    <xsd:documentation>
      Error code thrown when the specified ProxyGrantingTicket Callback URL is invalid,e.g. because it
      is malformed.
    </xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="INVALID_REQUEST">
  <xsd:annotation>
    <xsd:documentation>Error code thrown when the request is invalid e.g. because parameters are
      missing.
    </xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="INVALID_SERVICE">
  <xsd:annotation>
    <xsd:documentation>Error code thrown when the service given at validation does not match with the
      service used at authentication.
    </xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="INVALID_STRENGTH">
  <xsd:annotation>
    <xsd:documentation>
      Error code thrown when the requested authentication strength cannot be provided by the targeted
      ECAS Server,
      for example because it does not exist on that environment.
    </xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="INVALID_TICKET">
  <xsd:annotation>
    <xsd:documentation>
      Error code thrown when the ticket is not recognized either because it was not emitted
      by this ECAS server environment, or because it expired, or because it has already been
      validated.
    </xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="INVALID_USER">
  <xsd:annotation>
    <xsd:documentation>
      Error code thrown when the user does not meet the requirements for the application e.g.
      because she is self-registered whilst the application only accepts internal users.
    </xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
</xsd:restriction>

```

```

</xsd:simpleType>
<xsd:simpleType name="strengthType">
  <xsd:annotation>
    <xsd:documentation>Possible values for the strength parameter</xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="BASIC">
      <xsd:annotation>
        <xsd:documentation>
          Authentication strength used by the ECAS mock-up server.
          This strength will never be used against a production environment.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="CLIENT_CERT">
      <xsd:annotation>
        <xsd:documentation>
          Authentication strength representing 2-way SSL with a client X.509 certificate.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="PASSWORD">
      <xsd:annotation>
        <xsd:documentation>
          Default authentication strength in ECAS, using a username/password scheme.
          Same as the deprecated STRONG strength.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="PASSWORD_SMS">
      <xsd:annotation>
        <xsd:documentation>
          Multi-factor authentication strength using PASSWORD and SMS.
          Replaces the deprecated STRONG_SMS strength.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="PASSWORD_TOKEN">
      <xsd:annotation>
        <xsd:documentation>
          Multi-factor authentication strength using PASSWORD and a hardware-token challenge (OTP).
          Replaces the deprecated STRONG_TOKEN strength.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="PASSWORD_TOKEN_CRAM">
      <xsd:annotation>
        <xsd:documentation>
          Multi-factor authentication strength composed of the ECAS password plus a Challenge-Response
          Authentication Mechanism (CRAM) performed via a hardware token or "DigiPass".
        </xsd:documentation>
      <xsd:annotation>
        <xsd:appinfo>since 4.3.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="PASSWORD_SOFTWARE_TOKEN">
      <xsd:annotation>
        <xsd:documentation>
          Multi-factor authentication strength using PASSWORD and a challenge-response OTP generated by
          the ECAS Mobile app via a QR code.
        </xsd:documentation>
      <xsd:annotation>
        <xsd:appinfo>since 3.10.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="PASSWORD_MOBILE_APP">
      <xsd:annotation>
        <xsd:documentation>
          Multi-factor authentication strength using PASSWORD and the ECAS Mobile app.
        </xsd:documentation>
      <xsd:annotation>
        <xsd:appinfo>since 3.10.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="MOBILE_APP">
      <xsd:annotation>
        <xsd:documentation>

```

Authentication strength using the ECAS Mobile app to authenticate and access an ECAS-protected resource on the device.

```
</xsd:documentation>
<xsd:appinfo>since 3.10.0</xsd:appinfo>
</xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="MDM_CERT">
  <xsd:annotation>
    <xsd:documentation>
      Authentication strength using the Mobile-Device-Management (MDM) client software certificate.
    </xsd:documentation>
    <xsd:appinfo>since 4.0.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="SOCIAL_NETWORKS">
  <xsd:annotation>
    <xsd:documentation>
      Authentication strength via federation with a social network such as Facebook, Google, Twitter,
      etc.
      Reserved for future use.
    </xsd:documentation>
    <xsd:appinfo>since 3.2.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="STORK">
  <xsd:annotation>
    <xsd:documentation>
      Authentication strength used by the STORK project, which is the federation of European national
      eIDs.
    </xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="WINDOWS">
  <xsd:annotation>
    <xsd:documentation>
      Authentication strength representing the Microsoft Windows authentication method from within the
      Commission's network.
    </xsd:documentation>
    <xsd:appinfo>since 1.16.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="STRONG">
  <xsd:annotation>
    <xsd:documentation>
      Default authentication strength in ECAS.
      Deprecated, please use PASSWORD instead.
    </xsd:documentation>
    <xsd:appinfo>Deprecated since 3.1.0, use PASSWORD instead.</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="STRONG_SMS">
  <xsd:annotation>
    <xsd:documentation>
      Multi-factor authentication strength using PASSWORD and SMS.
      Deprecated, please use PASSWORD_SMS instead.
    </xsd:documentation>
    <xsd:appinfo>since 1.18.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="STRONG_TOKEN">
  <xsd:annotation>
    <xsd:documentation>
      Multi-factor authentication strength using PASSWORD and TOKEN.
      Deprecated, please use PASSWORD_TOKEN instead.
    </xsd:documentation>
    <xsd:appinfo>since 1.19.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="NTLM">
  <xsd:annotation>
    <xsd:documentation>
      Authentication strength representing the legacy Microsoft NTLM protocol against the NET1 domain
      inside the Commission's network.
      This strength is deprecated and is going to be phased out in the near future.
```

```

        </xsd:documentation>
        <xsd:appinfo>deprecated since 1.16.0</xsd:appinfo>
    </xsd:annotation>
</xsd:enumeration>
<xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="ticketType">
    <xsd:annotation>
        <xsd:documentation>Legal types of tickets.</xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="SERVICE">
            <xsd:annotation>
                <xsd:documentation>Represents a ServiceTicket</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
        <xsd:enumeration value="PROXY">
            <xsd:annotation>
                <xsd:documentation>Represents a ProxyTicket</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
        <xsd:enumeration value="DESKTOP">
            <xsd:annotation>
                <xsd:documentation>Represents a DesktopProxyTicket</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
        <xsd:enumeration value="UNKNOWN">
            <xsd:annotation>
                <xsd:documentation>Reserved for future use</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="employeeTypeType">
    <xsd:annotation>
        <xsd:documentation>Possible values for the employeeType parameter</xsd:documentation>
        <xsd:appinfo>since 1.9</xsd:appinfo>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="f">
            <xsd:annotation>
                <xsd:documentation>Full employee</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
        <xsd:enumeration value="x">
            <xsd:annotation>
                <xsd:documentation>Intramuros external user</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
        <xsd:enumeration value="e">
            <xsd:annotation>
                <xsd:documentation>Extramuros external user</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
        <xsd:enumeration value="n">
            <xsd:annotation>
                <xsd:documentation>Extramuros named external user</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
        <xsd:enumeration value="r">
            <xsd:annotation>
                <xsd:documentation>Retired</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
        <xsd:enumeration value="d">
            <xsd:annotation>
                <xsd:documentation>Beneficiary</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
        <xsd:enumeration value="i">
            <xsd:annotation>
                <xsd:documentation>Other institution employee</xsd:documentation>
            </xsd:annotation>
        </xsd:enumeration>
    </xsd:restriction>

```



```

</xsd:enumeration>
<xsd:enumeration value="s">
  <xsd:annotation>
    <xsd:documentation>Trainee</xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="c">
  <xsd:annotation>
    <xsd:documentation>Direct contract</xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="g">
  <xsd:annotation>
    <xsd:documentation>Guest</xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="j">
  <xsd:annotation>
    <xsd:documentation>Job</xsd:documentation>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="v">
  <xsd:annotation>
    <xsd:documentation>
      Virtual.
      Employee type for virtual users, used in federated identities.
      Virtual users automatically created from Federated third parties such as STORK eIDs or social networks.
    </xsd:documentation>
    <xsd:appinfo>since 3.9.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="q">
  <xsd:annotation>
    <xsd:documentation>
      XF Statutory Link.
      The XF statutory link type was created by DG HR to cater for all the different types of exceptions such as
      stagiaires from countries that are less trusted, pensioners that remain active as advisors, etc.
    </xsd:documentation>
    <xsd:appinfo>since 4.0.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
</xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="domainType">
  <xsd:annotation>
    <xsd:documentation>Possible values for the domain parameter</xsd:documentation>
    <xsd:appinfo>since 1.9</xsd:appinfo>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="eu.europa.acer">
      <xsd:annotation>
        <xsd:documentation>Agency for the Cooperation of Energy Regulators</xsd:documentation>
        <xsd:appinfo>since 3.1.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="eu.europa.artemis">
      <xsd:annotation>
        <xsd:documentation>Artemis Joint Undertaking</xsd:documentation>
        <xsd:appinfo>since 3.6.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="eu.europa.berec">
      <xsd:annotation>
        <xsd:documentation>The BEREC Office</xsd:documentation>
        <xsd:appinfo>since 3.1.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="eu.europa.cdt">
      <xsd:annotation>
        <xsd:documentation>Translation Centre</xsd:documentation>
        <xsd:appinfo>since 1.0.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="eu.europa.cedefop">

```

```

<xsd:annotation>
  <xsd:documentation>European Centre for the Development of Vocational Training</xsd:documentation>
  <xsd:appinfo>since 3.1.0</xsd:appinfo>
</xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.cepol">
  <xsd:annotation>
    <xsd:documentation>European Police College</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.cleansky">
  <xsd:annotation>
    <xsd:documentation>Clean Sky Joint Undertaking</xsd:documentation>
    <xsd:appinfo>since 3.10.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.consilium">
  <xsd:annotation>
    <xsd:documentation>Council of the European Union</xsd:documentation>
    <xsd:appinfo>since 1.0.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.cor">
  <xsd:annotation>
    <xsd:documentation>Committee of the Regions</xsd:documentation>
    <xsd:appinfo>since 1.0.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.cpvo">
  <xsd:annotation>
    <xsd:documentation>Community Plant Variety Office</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.curia">
  <xsd:annotation>
    <xsd:documentation>Court of Justice of the European Union</xsd:documentation>
    <xsd:appinfo>since 1.0.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.easa">
  <xsd:annotation>
    <xsd:documentation>European Aviation Safety Agency</xsd:documentation>
    <xsd:appinfo>since 1.19.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.easo">
  <xsd:annotation>
    <xsd:documentation>European Asylum Support Office</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eba">
  <xsd:annotation>
    <xsd:documentation>European Banking Authority</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.ec">
  <xsd:annotation>
    <xsd:documentation>European Commission</xsd:documentation>
    <xsd:appinfo>since 1.0.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eca">
  <xsd:annotation>
    <xsd:documentation>European Court of Auditors</xsd:documentation>
    <xsd:appinfo>since 1.0.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.ecb">
  <xsd:annotation>

```

```

    <xsd:documentation>European Central Bank</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.ecdc">
  <xsd:annotation>
    <xsd:documentation>European Centre for Disease Prevention and Control</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.echa">
  <xsd:annotation>
    <xsd:documentation>European Chemicals Agency</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.ecsel">
  <xsd:annotation>
    <xsd:documentation>ECSEL JU</xsd:documentation>
    <xsd:appinfo>since 3.10.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eda">
  <xsd:annotation>
    <xsd:documentation>European Defence Agency</xsd:documentation>
    <xsd:appinfo>since 3.10.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.edps">
  <xsd:annotation>
    <xsd:documentation>European Data Protection Supervisor</xsd:documentation>
    <xsd:appinfo>since 1.15.3</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eea">
  <xsd:annotation>
    <xsd:documentation>European Environment Agency</xsd:documentation>
    <xsd:appinfo>since 3.1.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eeas">
  <xsd:annotation>
    <xsd:documentation>European External Action Service</xsd:documentation>
    <xsd:appinfo>since 1.15.3</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eesc">
  <xsd:annotation>
    <xsd:documentation>European Economic and Social Committee</xsd:documentation>
    <xsd:appinfo>since 1.0.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.efca">
  <xsd:annotation>
    <xsd:documentation>European Fisheries Control Agency</xsd:documentation>
    <xsd:appinfo>since 3.1.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.efsa">
  <xsd:annotation>
    <xsd:documentation>European Food Safety Authority</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eige">
  <xsd:annotation>
    <xsd:documentation>European Institute for Gender Equality</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eiopa">
  <xsd:annotation>
    <xsd:documentation>European Insurance and Occupational Pensions Authority</xsd:documentation>

```

```

    <xsd:appinfo>since 3.1.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eit">
  <xsd:annotation>
    <xsd:documentation>European Institute of Innovation and Technology</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.ema">
  <xsd:annotation>
    <xsd:documentation>European Medicines Agency</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.emcdda">
  <xsd:annotation>
    <xsd:documentation>European Monitoring Centre for Drugs and Drug Addiction</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.emsa">
  <xsd:annotation>
    <xsd:documentation>European Maritime Safety Agency</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eniac">
  <xsd:annotation>
    <xsd:documentation>ENIAC Joint Undertaking</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.enisa">
  <xsd:annotation>
    <xsd:documentation>European Union Agency for network and information security</xsd:documentation>
    <xsd:appinfo>since 3.10.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.era">
  <xsd:annotation>
    <xsd:documentation>European Railway Agency</xsd:documentation>
    <xsd:appinfo>since 1.17.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.esma">
  <xsd:annotation>
    <xsd:documentation>European Securities and Markets Authority</xsd:documentation>
    <xsd:appinfo>since 3.1.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.ETF">
  <xsd:annotation>
    <xsd:documentation>European Training Foundation</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eui">
  <xsd:annotation>
    <xsd:documentation>European University Institute</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eulisa">
  <xsd:annotation>
    <xsd:documentation>eu-LISA</xsd:documentation>
    <xsd:appinfo>since 3.10.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eurofound">
  <xsd:annotation>
    <xsd:documentation>European Foundation for the Improvement of Living and Working Conditions
  </xsd:documentation>

```

```

    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.eurojust">
  <xsd:annotation>
    <xsd:documentation>Eurojust</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.europarl">
  <xsd:annotation>
    <xsd:documentation>European Parliament</xsd:documentation>
    <xsd:appinfo>since 1.0.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.european-council">
  <xsd:annotation>
    <xsd:documentation>European Council</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.europol">
  <xsd:annotation>
    <xsd:documentation>European Police Office</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.f4e">
  <xsd:annotation>
    <xsd:documentation>European Joint Undertaking for ITER and the Development of Fusion Energy
    </xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.fch">
  <xsd:annotation>
    <xsd:documentation>Joint Undertaking «Fuel Cells and Hydrogen»</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.fra">
  <xsd:annotation>
    <xsd:documentation>European Union Agency for Fundamental Rights</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.frontex">
  <xsd:annotation>
    <xsd:documentation>Frontex | European Union Agency</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.gsa">
  <xsd:annotation>
    <xsd:documentation>European GNSS Agency</xsd:documentation>
    <xsd:appinfo>since 1.0.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.imi">
  <xsd:annotation>
    <xsd:documentation>IMI Joint Undertaking</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.ohim">
  <xsd:annotation>
    <xsd:documentation>Office for Harmonization in the Internal Market</xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
</xsd:enumeration>
<xsd:enumeration value="eu.europa.ombudsman">
  <xsd:annotation>
    <xsd:documentation>European Ombudsman</xsd:documentation>

```

```

        <xsd:appinfo>since 3.1.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="eu.europa.osha">
      <xsd:annotation>
        <xsd:documentation>European Agency for Safety and Health at Work</xsd:documentation>
        <xsd:appinfo>since 3.6.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="eu.europa.sesar">
      <xsd:annotation>
        <xsd:documentation>SESAR Joint Undertaking</xsd:documentation>
        <xsd:appinfo>since 3.6.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="external">
      <xsd:annotation>
        <xsd:documentation>External (people who do not work for the Commission nor any other registered
interinstitutional body)
        </xsd:documentation>
        <xsd:appinfo>since 1.0.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:enumeration>
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="proxyGrantingProtocolType">
  <xsd:annotation>
    <xsd:documentation>Legal values for the Proxy Granting Protocol.</xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="PGT_URL">
      <xsd:annotation>
        <xsd:documentation>Protocol using a callback URL accessed in SSL.</xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="CLIENT_CERT">
      <xsd:annotation>
        <xsd:documentation>Protocol using a client X.509 certificate in 2-way SSL.</xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="DESKTOP">
      <xsd:annotation>
        <xsd:documentation>Protocol for desktop applications.</xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="assuranceLevelType">
  <xsd:annotation>
    <xsd:documentation>Identity Assurance Levels.</xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:unsignedShort">
    <xsd:enumeration value="0">
      <xsd:annotation>
        <xsd:documentation>NO_ASSURANCE</xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="10">
      <xsd:annotation>
        <xsd:documentation>LOW</xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="20">
      <xsd:annotation>
        <xsd:documentation>MEDIUM</xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="30">
      <xsd:annotation>
        <xsd:documentation>HIGH</xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="40">

```

```

    <xsd:annotation>
      <xsd:documentation>TOP</xsd:documentation>
    </xsd:annotation>
  </xsd:enumeration>
</xsd:restriction>
</xsd:simpleType>
<xsd:element name="userConfirmationSignatureRequest">
  <xsd:annotation>
    <xsd:documentation>ECAS response to a UserConfirmation Signature request</xsd:documentation>
    <xsd:appinfo>since 1.5</xsd:appinfo>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:choice>
      <xsd:element name="signatureRequestId" type="xsd:string"/>
      <xsd:element name="signatureRequestFailure" type="signatureRequestFailureType"/>
    </xsd:choice>
    <xsd:attributeGroup ref="ecasServerAttributeGroup"/>
  </xsd:complexType>
</xsd:element>
<xsd:complexType name="signatureRequestFailureType">
  <xsd:annotation>
    <xsd:documentation>ECAS body response when the Signature request failed</xsd:documentation>
  </xsd:annotation>
  <xsd:simpleContent>
    <xsd:extension base="xsd:string">
      <xsd:attribute name="code" type="errorCode" use="required">
        <xsd:annotation>
          <xsd:documentation>The error code thrown by ECAS</xsd:documentation>
        </xsd:annotation>
      </xsd:attribute>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
<xsd:element name="messageAuthenticationSignature">
  <xsd:annotation>
    <xsd:documentation>ECAS response to a Message Authentication Signature request</xsd:documentation>
    <xsd:appinfo>since 1.5</xsd:appinfo>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="messageAuthenticationFailure" type="messageAuthenticationFailureType"/>
    </xsd:sequence>
    <xsd:attributeGroup ref="ecasServerAttributeGroup"/>
  </xsd:complexType>
</xsd:element>
<xsd:complexType name="messageAuthenticationFailureType">
  <xsd:annotation>
    <xsd:documentation>ECAS body response when the message authentication Signature failed</xsd:documentation>
  </xsd:annotation>
  <xsd:simpleContent>
    <xsd:extension base="xsd:string">
      <xsd:attribute name="code" type="errorCode" use="required">
        <xsd:annotation>
          <xsd:documentation>The error code thrown by ECAS</xsd:documentation>
        </xsd:annotation>
      </xsd:attribute>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
<xsd:element name="userConfirmationSignature">
  <xsd:annotation>
    <xsd:documentation>ECAS response to a User Confirmation Signature</xsd:documentation>
    <xsd:appinfo>since 1.5</xsd:appinfo>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="signatureFailure" type="signatureFailureType"/>
    </xsd:sequence>
    <xsd:attributeGroup ref="ecasServerAttributeGroup"/>
  </xsd:complexType>
</xsd:element>
<xsd:complexType name="signatureFailureType">
  <xsd:annotation>

```



```

<xsd:documentation>ECAS body response when the User Confirmation Signature failed</xsd:documentation>
</xsd:annotation>
<xsd:simpleContent>
  <xsd:extension base="xsd:string">
    <xsd:attribute name="code" type="errorCode" use="required">
      <xsd:annotation>
        <xsd:documentation>The error code thrown by ECAS</xsd:documentation>
      </xsd:annotation>
    </xsd:attribute>
  </xsd:extension>
</xsd:simpleContent>
</xsd:complexType>
<xsd:element name="loginRequest">
  <xsd:annotation>
    <xsd:documentation>
      ECAS response to a Login Transaction Request.
      Client applications initiate login transaction by sending all their login parameters prior to
      the redirection to the ECAS login page.
      They receive in return a login request ID and a transaction secret.
      The login request ID is passed in the query string when redirecting to the ECAS login page.
      This prevents accidental tampering of the ECAS login URL.
      The transaction secret is used at validation time to prevent man-in-the-middle attacks.
    </xsd:documentation>
    <xsd:appinfo>since 1.9</xsd:appinfo>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:choice>
      <xsd:element name="loginRequestSuccess" type="loginRequestSuccessType"/>
      <xsd:element name="loginRequestFailure" type="loginRequestFailureType"/>
    </xsd:choice>
    <xsd:attributeGroup ref="ecasServerAttributeGroup"/>
  </xsd:complexType>
</xsd:element>
<xsd:complexType name="loginRequestSuccessType">
  <xsd:annotation>
    <xsd:documentation>
      ECAS body response with the Login Transaction Request content
      i.e. the loginRequestId and the transaction secret
    </xsd:documentation>
    <xsd:appinfo>since 1.9</xsd:appinfo>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="loginRequestId" type="xsd:string"/>
    <xsd:element name="loginResponseId" type="xsd:string" minOccurs="0"/>
    <xsd:element name="privateServiceTicket" type="xsd:string" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="loginRequestFailureType">
  <xsd:annotation>
    <xsd:documentation>ECAS body response when the Login Transaction Request failed</xsd:documentation>
    <xsd:appinfo>since 1.9</xsd:appinfo>
  </xsd:annotation>
  <xsd:simpleContent>
    <xsd:extension base="xsd:string">
      <xsd:attribute name="code" type="errorCode" use="required">
        <xsd:annotation>
          <xsd:documentation>The error code thrown by ECAS</xsd:documentation>
        </xsd:annotation>
      </xsd:attribute>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
<xsd:simpleType name="registrationLevelType">
  <xsd:annotation>
    <xsd:documentation>The application security level for the version of the user's credentials.
  </xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:unsignedShort">
    <xsd:enumeration value="0">
      <xsd:annotation>
        <xsd:documentation>No application security</xsd:documentation>
      </xsd:annotation>
    </xsd:enumeration>
    <xsd:enumeration value="10">

```



```

    <xsd:annotation>
      <xsd:documentation>Low application security</xsd:documentation>
    </xsd:annotation>
  </xsd:enumeration>
  <xsd:enumeration value="20">
    <xsd:annotation>
      <xsd:documentation>Medium application security</xsd:documentation>
    </xsd:annotation>
  </xsd:enumeration>
  <xsd:enumeration value="30">
    <xsd:annotation>
      <xsd:documentation>High application security</xsd:documentation>
    </xsd:annotation>
  </xsd:enumeration>
  <xsd:enumeration value="40">
    <xsd:annotation>
      <xsd:documentation>Top application security</xsd:documentation>
    </xsd:annotation>
  </xsd:enumeration>
</xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="IPv4AddressType">
  <xsd:annotation>
    <xsd:documentation>
      IPv4 address in the dotted-decimal notation.
    </xsd:documentation>
    <xsd:appinfo>since 3.1.2</xsd:appinfo>
  </xsd:annotation>

  <xsd:restriction base="xsd:string">
    <xsd:pattern
      value="((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|1-9[0-9][0-9])\.){3}(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|1-9[0-9][0-9])"/>
  </xsd:restriction>
</xsd:simpleType>
<xsd:complexType name="attributeType">
  <xsd:annotation>
    <xsd:documentation>An attribute, which can have one or more values.</xsd:documentation>
    <xsd:appinfo>since 4.0.0</xsd:appinfo>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="attributeValue" type="xsd:string" maxOccurs="unbounded">
      <xsd:annotation>
        <xsd:documentation>One of the values of this attribute.</xsd:documentation>
        <xsd:appinfo>since 4.0.0</xsd:appinfo>
      </xsd:annotation>
    </xsd:element>
  </xsd:sequence>
  <xsd:attribute name="name" type="xsd:string" use="required">
    <xsd:annotation>
      <xsd:documentation>The name of this attribute.</xsd:documentation>
      <xsd:appinfo>since 4.0.0</xsd:appinfo>
    </xsd:annotation>
  </xsd:attribute>
  <xsd:anyAttribute namespace="##other" processContents="lax"/>
</xsd:complexType>
<xsd:complexType name="mobileDeviceType">
  <xsd:annotation>
    <xsd:documentation>
      The mobile device used as second authentication factor when using multi-factor
      authentication including a mobile device such as a smartphone or a tablet.
    </xsd:documentation>
    <xsd:appinfo>since 5.8.0</xsd:appinfo>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="deviceName" type="xsd:string" minOccurs="0">
      <xsd:annotation>
        <xsd:documentation>The mobile device "friendly" name as chosen by the end-user.</xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="deviceIdentifier" type="xsd:string">
      <xsd:annotation>
        <xsd:documentation>The unique identifier assigned by EU Login to this mobile device.</xsd:documentation>
      </xsd:annotation>
    </xsd:element>
  </xsd:sequence>

```

```

<xsd:element name="mobileOs" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>The mobile device operating system (OS).</xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="deviceManufacturer" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>The mobile device manufacturer.</xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="deviceModel" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>The mobile device model.</xsd:documentation>
  </xsd:annotation>
</xsd:element>
</xsd:sequence>
<xsd:anyAttribute namespace="##targetNamespace"/>
</xsd:complexType>
</xsd:schema>

```

**Figure 5 - XML Schema for Ticket Validation Responses**

## APPENDIX II: TICKET VALIDATION WSDL

The Ticket Validation WSDL is available at:

<https://ecas.ec.europa.eu/cas/ws/TicketValidationService.wsdl>

```
<?xml version='1.0' encoding='UTF-8'?>
<wsdl:definitions name="TicketValidationService" targetNamespace="https://ecas.ec.europa.eu/cas/schemas"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns="https://ecas.ec.europa.eu/cas/schemas"
  xmlns:ecas="https://ecas.ec.europa.eu/cas/schemas"
  xmlns:soap11="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
  xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <wsdl:types>
    <xsd:schema targetNamespace="https://ecas.ec.europa.eu/cas/schemas"
      elementFormDefault="qualified" attributeFormDefault="unqualified" version="3.6.0" xml:lang="EN">
      <xsd:include schemaLocation="https://ecas.ec.europa.eu/cas/schemas/ecas.xsd"/>
      <xsd:element name="serviceRequest">
        <xsd:annotation>
          <xsd:documentation>Request to ECAS to validate a Service- or a Proxy-Ticket</xsd:documentation>
          <xsd:appinfo>version 1.9.2</xsd:appinfo>
        </xsd:annotation>
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="service" type="xsd:string">
              <xsd:annotation>
                <xsd:documentation>
                  The service is the protected URL the user wants to access.
                  It is also the URL where the ECAS server has to redirect the user to after successful authentication.
                </xsd:documentation>
              </xsd:annotation>
            </xsd:element>
            <xsd:element name="ticket" type="xsd:string">
              <xsd:annotation>
                <xsd:documentation>
                  The ticket is a token returned by the ECAS server.
                  It uniquely identifies a user.
                  It is only valid once and for a short period of time.
                  It is associated to one service and cannot be validated for another service.
                </xsd:documentation>
              </xsd:annotation>
            </xsd:element>
            <xsd:element name="renew" type="xsd:boolean" minOccurs="0" default="false">
              <xsd:annotation>
                <xsd:documentation>
                  The renew parameter can be used to disable Single-Sign-On and force users to
                  authenticate again (entering their credentials again).
                  It can be used to confirm the user's identity for a sensitive transaction (electronic sign-off) or
                  by sensitive applications that wish not to participate in the Web Single-Sign-On session.
                </xsd:documentation>
              </xsd:annotation>
            </xsd:element>
            <xsd:element name="pgtUrl" type="xsd:anyURI" minOccurs="0">
              <xsd:annotation>
                <xsd:documentation>
                  The ProxyGrantingTicket URL is the callback URL to which the ECAS server connects to send Proxy-
                  Granting-Tickets.
                  This must be an httpS URL using a CommisSign PKI certificate.
                  It must acknowledge PGT submissions with a proxySuccess message.
                </xsd:documentation>
              </xsd:annotation>
            </xsd:element>
            <xsd:element name="groups" minOccurs="0">
              <xsd:annotation>
                <xsd:documentation>
                  The groups parameter is the sequence of the CUD groups the application wants ECAS to check and return.
                  If the groups parameter is omitted, ECAS does not return any group.
                </xsd:documentation>
              </xsd:annotation>
            </xsd:element>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:schema>
    </wsdl:types>
  </wsdl:definitions>
```

```

    <xsd:sequence>
      <xsd:element name="group" type="xsd:string" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="userDetails" type="xsd:boolean" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      If set to true, ECAS returns user attributes.
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="clientFingerprint" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The client fingerprint is an MBUN token sent by the client application to prevent man-in-the-middle attacks.
      It is used when login transactions are initiated.
      (Only used in login transactions).
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="sessionId" type="xsd:string" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The sessionId is a digest used in login transactions to identity session loss.
      (Only used in login transactions).
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="version" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The version parameter specifies which version of the ECAS protocol to use.
      If omitted, the latest protocol is used.
      It can be used by custom clients that targetted a specific protocol version with a given XML namespace.
      Note that this WSDL is also constrained by its requested version and that you must query it
      by adding the version to it to see other values (e.g. adding "?version=1.3" to the WSDL URL).
    </xsd:documentation>
  </xsd:annotation>
  <xsd:simpleType>
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="CURRENT"/>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="ticketTypes">
  <xsd:annotation>
    <xsd:documentation>
      The "ticketTypes" property is the sequence of ECAS ticket-types accepted by the application.
      If users try to access the application with other ticket types than the ones specified here,
      an INVALID_TICKET error code is returned by ECAS.
    </xsd:documentation>
    <xsd:appinfo>since 1.11.0</xsd:appinfo>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="ticketType" type="ecas:ticketType" maxOccurs="3" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="assuranceLevel" type="ecas:assuranceLevelType">
  <xsd:annotation>
    <xsd:documentation>
      The "assuranceLevel" property is the level of assurance in the user's identity
      the application requires to grant access.
      If users with assurance levels lower than the one configured here try to access the application,
      an INVALID_USER error code is returned by ECAS.
    </xsd:documentation>
    <xsd:appinfo>since 1.11.0</xsd:appinfo>
  </xsd:annotation>
</xsd:element>
<xsd:element name="proxyGrantingProtocol" type="ecas:proxyGrantingProtocolType" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>

```

The "proxyGrantingProtocol" property is used to specify the protocol to be used to obtain ProxyGrantingTickets (PGT).

```

</xsd:documentation>
<xsd:appinfo>since 1.11.0</xsd:appinfo>
</xsd:annotation>
</xsd:element>
<xsd:element name="userAddress" type="ecas:IPv4AddressType" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>
      The "userAddress" property is used to specify the IP v4 Address of the end user
      actually at the origin of the ticket validation request.
      This information is needed for audit or forensics capabilities.
    </xsd:documentation>
    <xsd:appinfo>since 3.1.2</xsd:appinfo>
  </xsd:annotation>
</xsd:element>
<xsd:element name="singleSignOut" type="xsd:boolean" minOccurs="0" default="false">
  <xsd:annotation>
    <xsd:documentation>
      The "singleSignOut" parameter is used to specify that the Single-Sign-Out protocol of
      CAS 3 is supported for this Ticket validation.
      If the user logs out of ECAS, a Single-Sign-Out message will be sent to the
      target service to indicate the end of the Single-Sign-On session.
      The official ECAS client supports this feature.
      See the ECAS Client Advance Guide for details.
      See https://wiki.jasig.org/display/CASUM/Single+Sign+Out and
      https://wiki.jasig.org/display/CASC/Configuring+Single+Sign+Out
      for the original CAS documentation.
      Note that if the client technology is known to support this feature, this
      parameter can be omitted.
    </xsd:documentation>
    <xsd:appinfo>since 1.20.0</xsd:appinfo>
  </xsd:annotation>
</xsd:element>
<xsd:element name="acceptStrengths">
  <xsd:annotation>
    <xsd:documentation>
      The "acceptStrengths" property is the sequence of ECAS authentication strengths
      accepted by the client application.
      If users try to access the application with other strengths than the ones specified
      here, an INVALID_STRENGTH error usually occurs at the level of the ECAS Client.
    </xsd:documentation>
    <xsd:appinfo>since 3.6.0</xsd:appinfo>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="strength" type="ecas:strengthType" maxOccurs="unbounded" />
    </xsd:sequence>
  </xsd:complexType>
  <xsd:unique name="serviceRequest-acceptStrengths-strength-uniqueness">
    <xsd:annotation>
      <xsd:documentation>
        The strengthType name must be unique within the acceptStrengths in the serviceRequest.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:selector xpath="acceptStrengths"/>
    <xsd:field xpath="strength"/>
  </xsd:unique>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
<xsd:unique name="serviceRequest-group-uniqueness">
  <xsd:annotation>
    <xsd:documentation>
      The group name must be unique within the serviceRequest.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:selector xpath="groups"/>
  <xsd:field xpath="group"/>
</xsd:unique>
<xsd:unique name="serviceRequest-ticketType-uniqueness">
  <xsd:annotation>
    <xsd:documentation>
      The ticketType name must be unique within the serviceRequest.
    </xsd:documentation>
  </xsd:annotation>

```

```

        </xsd:documentation>
        </xsd:annotation>
        <xsd:selector xpath="ticketTypes"/>
        <xsd:field xpath="ticketType"/>
    </xsd:unique>
</xsd:element>
</xsd:schema>
</wsdl:types>
<wsdl:message name="validateIn">
    <wsdl:part element="serviceRequest" name="serviceRequestPart"/>
</wsdl:message>
<wsdl:message name="validateOut">
    <wsdl:part element="serviceResponse" name="serviceResponsePart"/>
</wsdl:message>
<wsdl:message name="httpRequest">
    <wsdl:part name="service" type="xsd:string"/>
    <wsdl:part name="ticket" type="xsd:string"/>
    <wsdl:part name="pgtUrl" type="xsd:string"/>
    <wsdl:part name="groups" type="xsd:string"/>
    <wsdl:part name="renew" type="xsd:string"/>
    <wsdl:part name="userDetails" type="xsd:string"/>
    <wsdl:part name="clientFingerprint" type="xsd:string"/>
    <wsdl:part name="sessionId" type="xsd:string"/>
    <wsdl:part name="version" type="xsd:string"/>
    <wsdl:part name="ticketTypes" type="xsd:string"/>
    <wsdl:part name="assuranceLevel" type="xsd:string"/>
    <wsdl:part name="proxyGrantingProtocol" type="xsd:string"/>
    <wsdl:part name="userAddress" type="xsd:string"/>
    <wsdl:part name="singleSignOut" type="xsd:string"/>
    <wsdl:part name="acceptStrengths" type="xsd:string"/>
</wsdl:message>
<wsdl:portType name="TicketValidationIntf">
    <wsdl:operation name="validate">
        <wsdl:input message="validateIn"/>
        <wsdl:output message="validateOut"/>
    </wsdl:operation>
</wsdl:portType>
<wsdl:portType name="TicketValidationHttpPostIntf">
    <wsdl:operation name="validate">
        <wsdl:input message="httpRequest"/>
        <wsdl:output message="validateOut"/>
    </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="TicketValidationServiceSoap11Binding" type="TicketValidationIntf">
    <wssoap11:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="validate">
        <wssoap11:operation style="document"/>
        <wsdl:input>
            <wssoap11:body use="literal"/>
        </wsdl:input>
        <wsdl:output>
            <wssoap11:body use="literal"/>
        </wsdl:output>
    </wsdl:operation>
</wsdl:binding>
<wsdl:binding name="TicketValidationServiceSoap12Binding" type="TicketValidationIntf">
    <wssoap12:binding style="document" transport="http://www.w3.org/2003/05/soap/bindings/HTTP"/>
    <wsdl:operation name="validate">
        <wssoap12:operation style="document"/>
        <wsdl:input>
            <wssoap12:body use="literal"/>
        </wsdl:input>
        <wsdl:output>
            <wssoap12:body use="literal"/>
        </wsdl:output>
    </wsdl:operation>
</wsdl:binding>
<wsdl:binding name="TicketValidationServiceHttpPostBinding" type="TicketValidationHttpPostIntf">
    <http:binding verb="POST"/>
    <wsdl:operation name="validate">
        <http:operation location="/post"/>
        <wsdl:input>
            <mime:content type="application/x-www-form-urlencoded"/>

```

```

    </wsdl:input>
    <wsdl:output>
      <mime:mimeXml part="serviceResponsePart"/>
    </wsdl:output>
  </wsdl:operation>
</wsdl:binding>
<wsdl:service name="TicketValidationService">
  <wsdl:port binding="TicketValidationServiceSoap11Binding" name="TicketValidationServiceSoap11Port">
    <soap11:address location="https://ecas.ec.europa.eu/cas/ws/TicketValidationService/soap/1.1"/>
  </wsdl:port>
  <wsdl:port binding="TicketValidationServiceSoap12Binding" name="TicketValidationServiceSoap12Port">
    <soap12:address location="https://ecas.ec.europa.eu/cas/ws/TicketValidationService/soap/1.2"/>
  </wsdl:port>
  <wsdl:port binding="TicketValidationServiceHttpPostBinding" name="TicketValidationServiceHttpPostPort">
    <http:address location="https://ecas.ec.europa.eu/cas/ws/TicketValidationService/http"/>
  </wsdl:port>
  <wsdl:port binding="TicketValidationServiceSoap11Binding" name="TicketValidationService2WaySSLSoap11Port">
    <soap11:address location="https://ecas.cc.cec.eu.int:7003/cas/ws/TicketValidationService/soap/1.1"/>
  </wsdl:port>
  <wsdl:port binding="TicketValidationServiceSoap12Binding" name="TicketValidationService2WaySSLSoap12Port">
    <soap12:address location="https://ecas.cc.cec.eu.int:7003/cas/ws/TicketValidationService/soap/1.2"/>
  </wsdl:port>
  <wsdl:port binding="TicketValidationServiceHttpPostBinding"
name="TicketValidationService2WaySSLHttpPostPort">
    <http:address location="https://ecas.cc.cec.eu.int:7003/cas/ws/TicketValidationService/http"/>
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>

```

**Figure 6 - Ticket Validation WSDL**