Access Management through UUM&DS

Your passport to EU Applications

Version **0.20**

Contents

1. Economic Operator (EO) Management

Before using any of the Applications an Economic Operator has to be registered in MS IAM that federates UUM&DS. Depending on the type of the authenticating Member State the process that should be followed is described in the following paragraphs.

For a description of Member state Types please refer to the Definitions Table

1.1. EO Account Registration

1.1.1. Member States Type A/B/C

Member states currently belonging to this type are: AT, BE, BG, CY, CZ, DK, ES, FI, GR, HR, HU, IE, IT, LT, LV, NL, PL, PT, SE and SI.
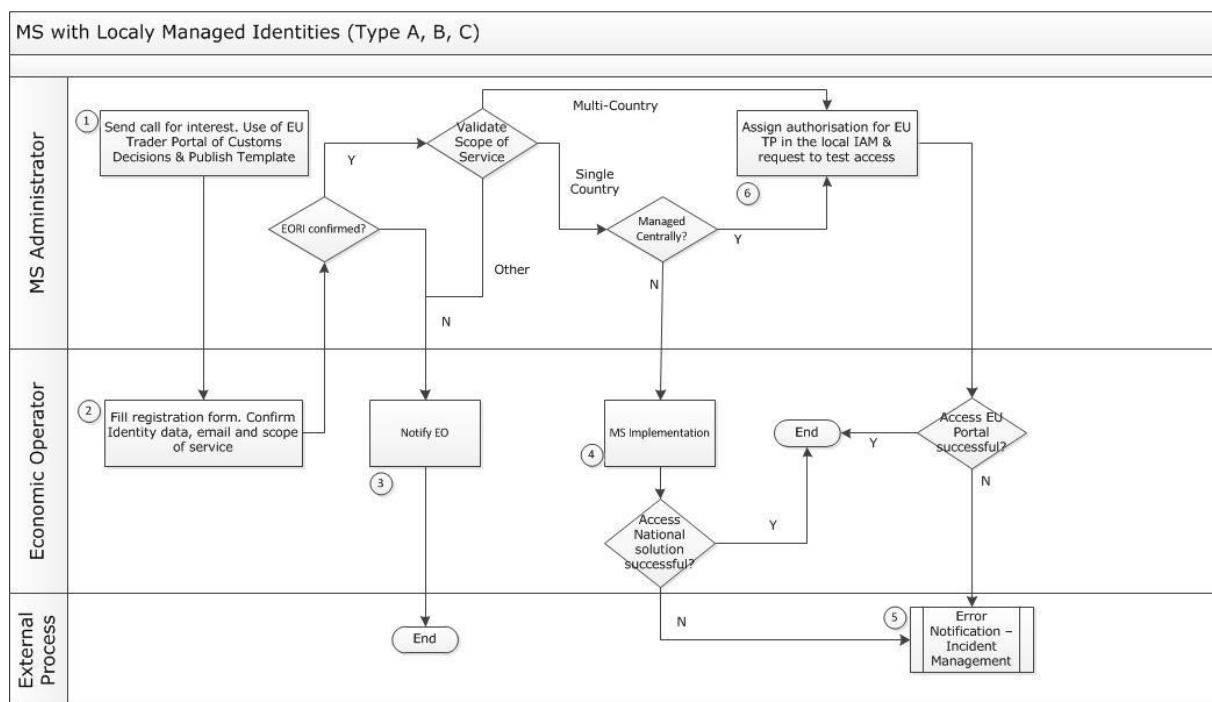

Table 1 Registration Process for Type A/B/C

Process description

Step1: MS Administration calls for interest and publishes application template for the usage of EU Trader Portal.

Step2: Each Economic Operator fills in the application and sends it back to the MS Administrator. In the application the following data are confirmed:

- Identity Data (EORI, Name etc.) It is very important that the EO gives his consent in accordance with the applicable personal data protection laws and regulations. See also the WAYF page in the next slide.
- Email address which is very important since all communications (password change requests etc.) will use this email!
- Scope of Service.

Access management through UUM&DS

Step 3: MS Administrator checks EORI validity. If the EORI is not confirmed, the Economic Operator is informed and the current process ends. The EO must initialise the process providing the correct EORI information.

Step 4& 5: If the EORI is valid, the scope of service is validated. For the types of applications of authorisations that are managed locally by the MS systems and not by the central CDS Trader Portal System, the EO request is serviced by the MS application following the MS specific processes.

Step 6: For the cases that the EO submits his applications for EU authorisations using the central EU Portal of Customs Decisions (EU Portal of CDS) access to the service is managed by UUM&DS.MS administration assigns the appropriate business profiles to the EO in the MS IAM system enabling the access to the EU Portal of CDS , following the request of the EO.

1.1.2.   Member States Type D

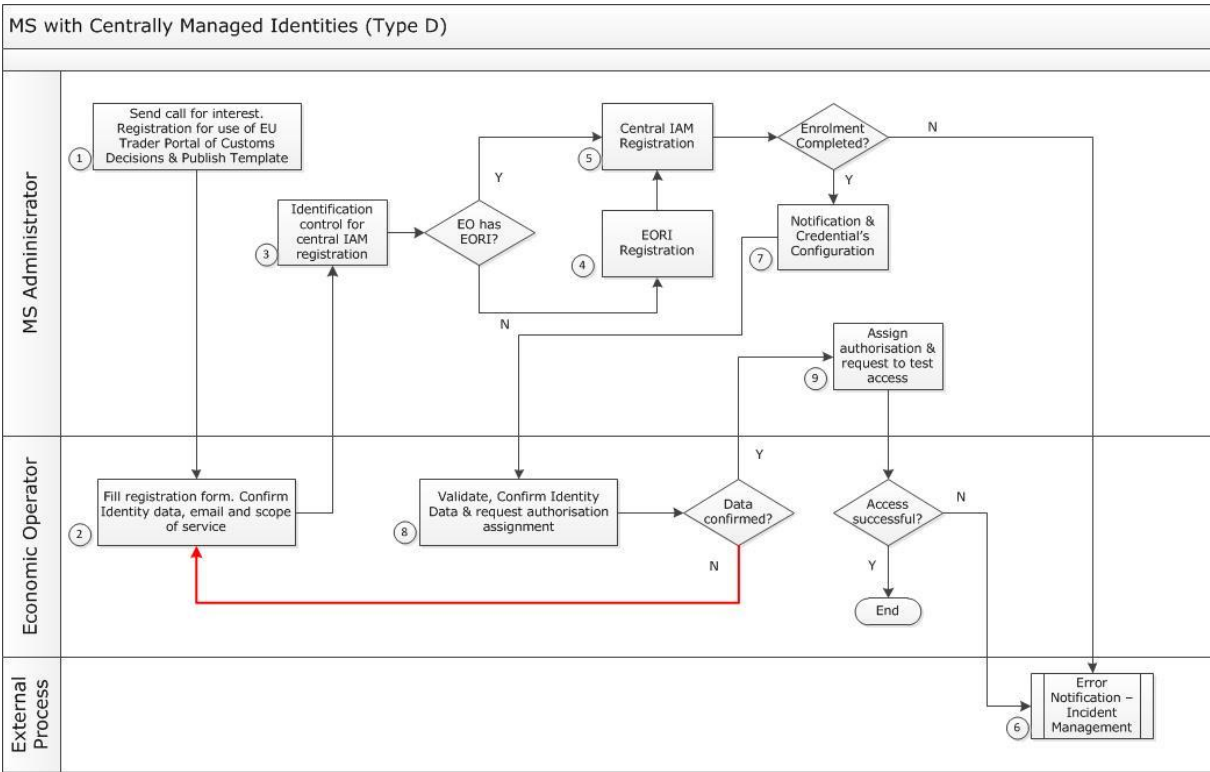Member states currently belonging to this type are: DE, EE, FR, LU, MT, RO, SK and UK.

Table 2 Registration Process for Type D

Process Description

Step 1: MS Administrator sends call for interest and publishes the application template for using EU Trader Portal.

Step 2: Each Economic Operator fills in the application and sends it back to the MS Administrator. In the application the following data are confirmed:

- Identity Data (EORI, Name etc.) It is very important that the EO gives his consent in accordance with the applicable personal data protection laws and regulations. See also the WAYF page in the next slide.

- Email address which is very important since all communications (password change requests etc.) will use this email!
- Scope of Service.

Step 3: MS Administrator performs identification control for central registration

Step 4& 5: In case the EO has no EORI, registration takes place and then the EO is registered in the Central IAM.

Step 6: If the enrolment is not completed an error notification is sent and incident management is started.

Step 7: If the enrolment is complete, a notification is generated and credential's configuration takes place.

Step 8: EO receives the notification and confirms Identity Data (EORI, Name etc.) Then EO requests authorisation assignment.
In case Identity data are not confirmed, EO fills again the registration form and repeats the process from step 2 else

Step 9: EO receives the notification and confirms Identity Data (EORI, Name etc.) Then EO requests authorisation assignment.
In case Identity data are not confirmed, EO fills again the registration form and repeats the process from step 2 else the EO tests the access to the Trader Portal of CDS using the provided credentials and reports the result back to the MS IAM administration for EO.

1.2.   EO Account Change

If a change is required for an EO account the following process will be followed:

- EO will submit a Change Request Form to their identifying National Authority
- National Authority will validate the request and forward it to
- The Sub-Domain Administrator (for Type D member states) or
- The MS-IAM team (for Types A/B/C)
- The responsible team will fulfil the request and report back to the National Authority which in turn
- Will inform the requester for the completion of their request.

1.3.   EO Account Deactivation

Customs or the EO can request the deactivation or termination of an account; the following process will be followed:

- Deactivation request can be received from as a Change Request Form by
- An EO, in case they wish to discontinue using the system
- Customs Officer
- Internal Audit, in case a security issue has been identified

Access management through UUM&DS

- Inactivity report (an account has been inactive for an extended period of time)
- National Authority will validate the request and forward it to
- The Sub-Domain Administrator (for Type D member states) or
- The MS-IAM team (for Types A/B/C)
- The responsible team will fulfil the request and report back to the National Authority which in turn
- Will inform the requester for the completion of their request.

2. Access management (Authentication)

2.1. Authentication

Before using any of the Applications secured by UUM&DS, the users should identify themselves (authenticate).

Users should **always** access the Application URL and not the WAYF URL. Users will be redirected to the WAYF page automatically!

User requests access to a specific Application by visiting its main page (i.e. https://customs.ec.europa.eu/tpui-cdms-web/ for Trader Portal) and is redirected to the Where Are You From (WAYF) page. At this point the user defines in what capacity they will access the application i.e. acting on their own behalf (no delegation), acting on behalf of someone else (first level delegation) or acting under a mandate on behalf of someone representing someone else (second level delegation). The form is submitted. An authentication request is created and validated by UUM&DS containing:

- The domain
- The list of attributes to provide and for each of them a flag indicating if it is mandatory or optional.

The request is signed and UUM&DS redirects the user:

For Type A,B,C: to the MS IAM authentication portal with the signed request. MS IAM validates the request and displays the authentication page. The User submits the MS IAM authentication form after providing the following information:

- Authentication method,
- Credentials: depending on the MS, this could be a password, an ID card, an optional OTP.

A signed and encrypted request is sent to the MS IAM to authenticate the user.

A signed and encrypted response is sent by the MS IAM to UUM&DS to verify if access to the system should be granted.

UUM&DS redirects the user to the Application with a ticket. The central service performs fine-grained authorisation and displays the central Application page.

For Type D: to the TAXUD CAS authentication where he submits the form providing the following information:

- Type of identifier,
- Identifier,
- Credentials

TAXUD CAS redirects the user to the UUM&DS system which verifies the user respects the condition to access the service. UUM&DS redirects the user to the Application with a ticket which performs fine-grained-authorisation and displays the central Application page.

Access management through UUM&DS

Authentication Failure:

There are two possible cases for authentication failure: Wrong credentials, i.e. user id and password, or insufficient authority to access the specific application.

Authentication is valid for any application of the same Domain, in this case Customs. If the user requests to access an application of a different Domain or requests to represent another entity or act as a different Type of Actor, they must first log out from the current session opened through the UUM&DS system and request a new session to be opened again through UUM&DS.

2.2.   Authentication without delegation for MS Type A/B/C

Member states currently belonging to this type are: AT, BE, BG, CY, CZ, DK, ES, FI, GR, HR, HU, IE, IT, LT, LV, NL, PL, PT, SE and SI.

Scenario: A Trader or Economic Operator (EO) needs to access the Application. He requests the Application page and is redirected to the UUM&DS as in Figure 1.
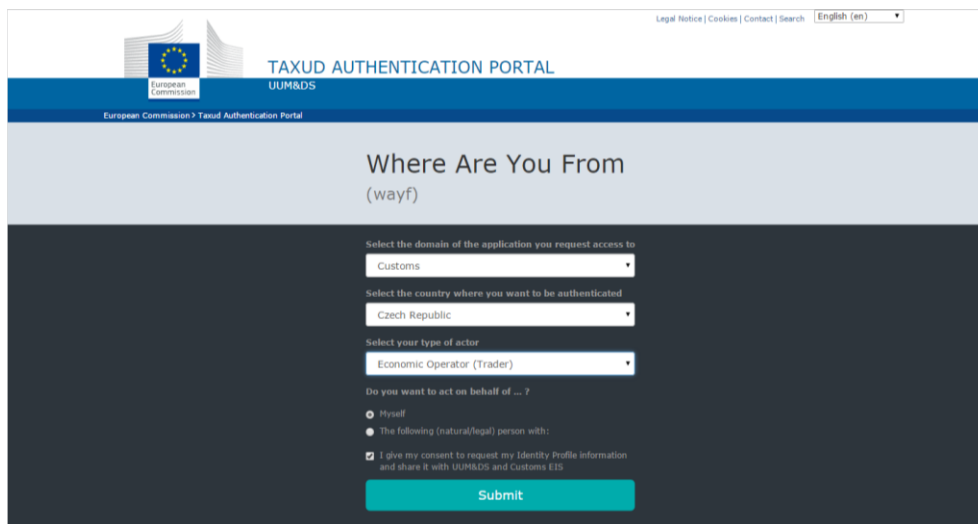
Figure 1: WAYF for EO and MS type A, B and C

On the WAYF page, provides the following information:

- The Domain, which is **Customs** in the above example;

- The place where you want to be authenticated, (i.e. the country for the trader);

- The Type of Actor (the list of available Types of Actors may change according to UUM&DS Reference Data).

- Tick the box giving consent and click **Submit.**

Afterwards, the user will be redirected to the authentication portal where he will perform the actual authentication. Once authenticated, you will be redirected to the service if the PDP has granted you access, or to a UUM&DS error page if the access is denied.

If the authenticating country is of type D (users that are provisioned), information additional to that described in the previous cases is provided in the WAYF page:

- The user's type of identifier;

Access management through UUM&DS
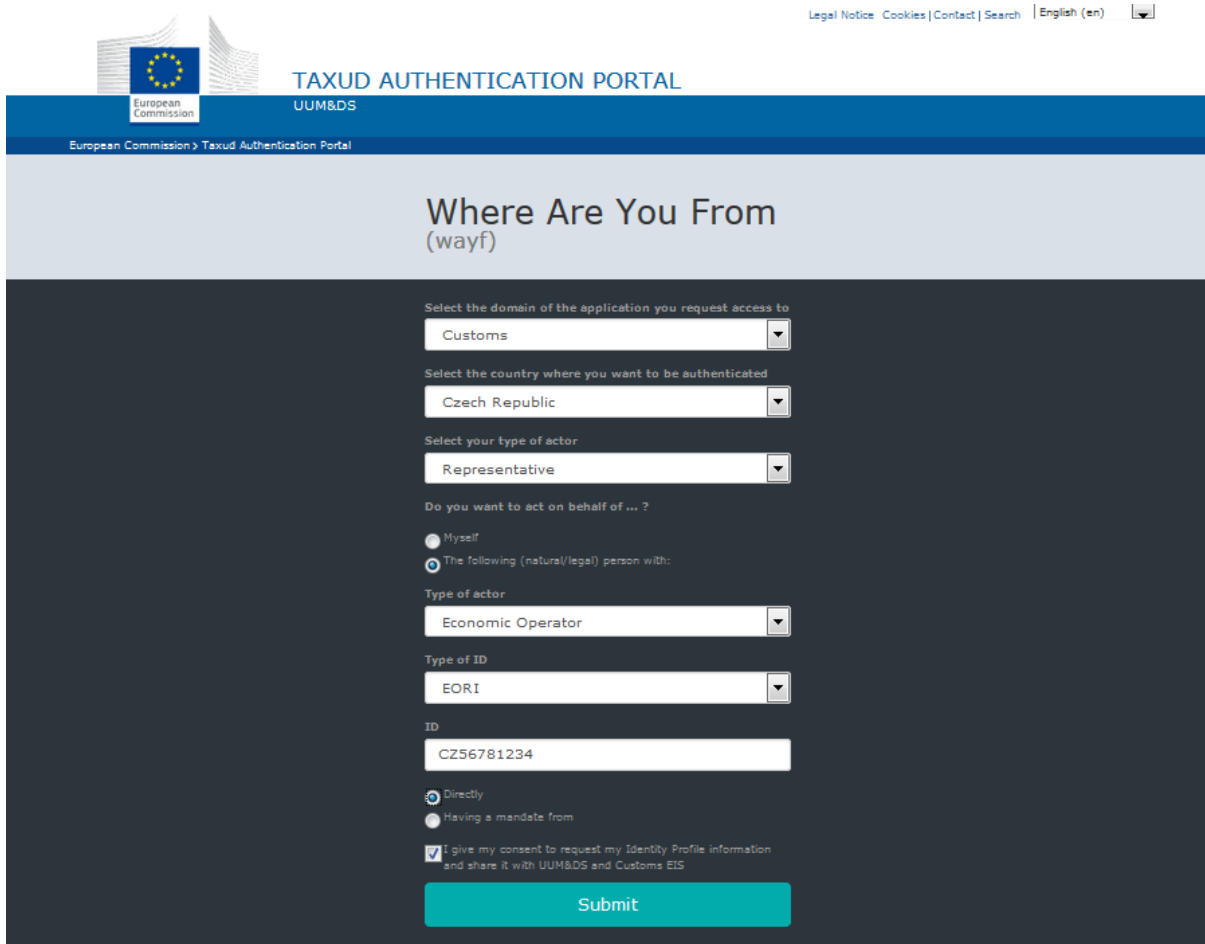
- The user's identifier.

Figure 2 WAYF for Type D countries

2.3. Authentication with delegation for MS Type A/B/C

First level

Scenario 1: A Customs Representative (CR) represents an Economic Operator (EO) for specific tasks. CR requests the Application page and is redirected to the UUM&DS in Figure 1. There he uses the option to act on behalf of someone else and the page in Figure 3 appears.

Figure 3: WAYF - Authentication with delegation – First level

Here, in addition to the normal authentication without delegation (as discussed in section 2.2 — *Authentication without delegation*) you need to provide the **Type of Actor**, **Type of ID** and **ID** of the delegator, either for a central or a local delegation. The list of possible **Types of Actor** and **Type of ID** may vary depending on the delegation authorised and the supported Types of Actors for the country where you want to be authenticated.

Scenario 2: An Employee (EMPL) is mandated by an Economic Operator (EO) for specific tasks. EMPL requests the Application page and is redirected to the UUM&DS in Figure 1. There he uses the option to act on behalf of someone else and the page in Figure 4 appears.
Please be aware that **Employees cannot** have EORI numbers!

Figure 4: WAYF first level delegation for EMPL

Second level

Scenario: An Employee (EMPL or Mandated Person) of a Customs Representative (CR) is acting on behalf of an Economic Operator (EO). The employee requests the Application page and is redirected to the UUM&DS in Figure 5.

The Mandated Person provides the following information of the WAYF page

- The country where he will be authenticated,
- The domain to which the application belongs to,
- The type of actor he wants to act as,
- Checks the box specifying he wants to act on behalf of a natural or legal person (delegation),
- The type of ID of the Delegator,
- The ID of the Delegator,
- Checks the box specifying he has a mandate from,
- The type of ID of the Delegate,
- The ID of the Delegate,
- Checks the legal disclaimer abiding to the rules of the provided service.

The Mandated Person submits the form. A SAML authentication request is created and validated by UUM&DS containing:

- The domain,

- The list of attributes to provide and for each of them a flag indicating if it is mandatory or optional

The authentication request is signed and UUM&DS redirects the user to the MS IAM authentication portal.

MS IAM validates the authentication request and displays the authentication page. The Mandated Person submits the MS IAM authentication form after providing the following information:

- Authentication method,

- Credentials: depending on the MS, this could be a password, an ID card, an optional OTP.

MS IAM validates, encrypts and signs the SAML assertion. MS IAM redirects the Mandated Person to the UUM&DS authentication portal (WAYF) with the encrypted SAML assertion.

UUM&DS checks the delegation and roles assignments authorisations. MS IAM is responsible to check the Delegator rights and send a valid list of business profiles.

UUM&DS redirects the Mandated Person to the Application with a ticket and displays the Application page.

The Mandated Person gains accesses to the Application.

Figure 5: WAYF - Authentication with delegation – Second level

2.4. Authentication without delegation for MS Type D

Member states currently belonging to this type are: DE, EE, FR, LU, MT, RO, SK and UK.

EO registered in these countries will follow the process as described below:

UUM&DS intercepts the request and redirects the user to the UUM&DS WAYF page (Figure 2) User provides the following information of the WAYF page:

- TAXUD CAS authentication system,
- The domain to which the application belongs to,
- The type of actor he wants to act as and the type of identifier.
- Check the box specifying he wants to act for himself (no delegation),
- Check the legal disclaimer abiding to the rules of the provided service as regards the consent to sharing his/hers identification and authorisation data with central services.

Access management through UUM&DS

The user submits the form and UUM&DS redirects the user to the TAXUD CAS authentication portal where the user provides the following information:

- Type of identifier,
- Identifier,
- Credentials

TAXUD CAS redirects the user to the UUM&DS system which verifies that the user respects the condition to access the service. Then UUM&DS redirects the user to the Application with a ticket which performs fine-grained-authorisation and the Application page is displayed.

Figure 6: Authentication TAXUD CAS

2.5. Authentication with delegation for MS Type D

There are two possible scenarios:

Scenario 1: A Customs Representative (CR) represents an Economic Operator (EO) for specific tasks. CR requests the Application page and is redirected to the UUM&DS in Figure 2. There he uses the option to act on behalf of someone else and the page in Figure 7 appears.

Figure 7: WAYF (type D) - CR representing an EO

Scenario 2: An Employee (EMPL) is mandated by an Economic Operator (EO) for specific tasks. EMPL requests the Application page and is redirected to the UUM&DS in Figure 2. There he uses the option to act on behalf of someone else and the page in Figure 8 appears.

Figure 8: WAYF (type D) - EMPL representing an EO

2.6. Authentication MS-IAM

After completing the WAYF page, if the authenticating country has their own IAM, the user is redirected to the respective country's IAM system. An example can be seen in Figure 9 below.

User provides the following information of the WAYF page:

- The country where he will be authenticated,
- The domain to which the application belongs to,
- The type of actor he wants to act as,
- Checks the legal disclaimer abiding to the rules of the provided service as regards the consent to sharing his/hers identification and authorisation data with central services.

User submits the form. An authentication request is created and validated by UUM&DS containing:

- The domain,
- The list of attributes to provide and for each of them a flag indicating if it is mandatory or optional.

The authentication request is signed and UUM&DS redirects the user to the MS IAM authentication portal.

MS IAM validates the authentication request and displays the authentication page. The User submits the MS IAM authentication form after providing the following information:

- Authentication method,
- Credentials: depending on the MS, this could be a password, an ID card, an optional OTP.

MS IAM validates, encrypts and signs the request, then redirects the user to the UUM&DS authentication portal (WAYF)

UUM&DS verifies the request and verifies that the user respects the condition to access the service, then it redirects the user to the Application with a ticket.

The Application performs fine-grained authorisation and displays its main page.

Figure 9: Authentication MS-IAM

2.7.   Successful Login

After completing the authentication process, the user will be directed to the main page of the requested Application. In Figure 10 below you can find an example of a UUM&DS secured Application.

**Figure 10: Trader Portal Application**

2.8. SSO (Single Sign-On)

This function allows a user, already authenticated with UUM&DS to access another Application without re-authenticating. UUM&DS intercepts access to the Application, and redirects the user to his national authentication portal. Once authenticated, UUM&DS verifies that the user is authorised to access this Application and provides access.

2.9. Logging out

To logout from UUM&DS, several options are provided:

- The most reliable option is to close the browser, this not only closes the session with UUM&DS but also with the authentication portal.

- From the application (Admin for example), click the logout option in the right corner, for example:
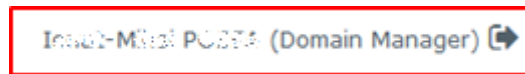
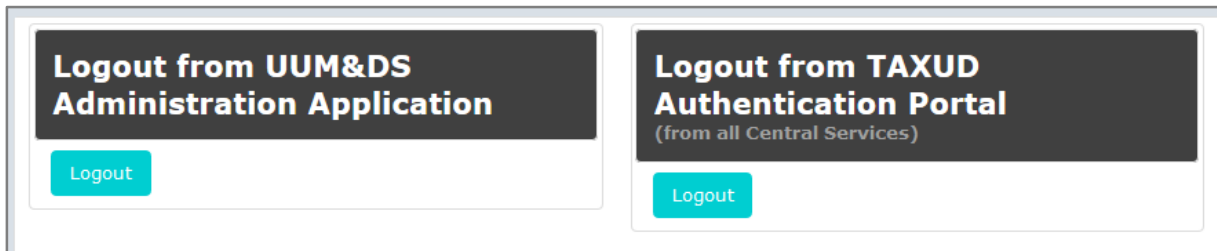- You will be prompted to confirm if you want to logout locally from the application or fully from UUM&DS:

Figure 11: Logout options

- **Logout from UUM&DS Administration Application** will only terminate the session of the Admin application. The single sign-on is still active and if you reconnect to the application you will re-enter it without the need to authenticate. For further information related to single sign-on, refer to the ECAS wiki at https://webgate.ec.europa.eu/CITnet/confluence/pages/viewpage.action?spaceKey=IAM&title=ECAS.

- **Logout from TAXUD Authentication Portal** will terminate the session of the Admin application and from UUM&DS. If you reconnect to the application you will be redirected to the WAYF. You may select a different place to perform the authentication and different delegation or Type of Actors. Bear in mind that a logout from UUM&DS does not have any effect with the session done with Corporate EU Login or MS National Authentication Portal. In other words, if the national portal has a single sign-on, it may not ask you to re-authenticate. There is also no guarantee that the new parameter taken from the WAYF page is taken into consideration, especially concerning the Type of Actor and delegation.

Note: It is strongly recommended to always close the browser in order to perform a full logout. This is the most secure way to be sure that nobody will be able to access your application without having to re-authenticate, and that the new parameters of the WAYF are correctly taken into account in a new authentication process.

2.10. Delegation management (Delegation CD)

This chapter describes the basic nominal flows for delegation creation and approval. Economic Operators that are authorised in Member States that use Central Delegation (currently CY, DE, EE, FR, GR, IE, LU, RO, SK and UK) can use the following paragraphs to define and manage Delegations. You may find the supported delegations for every Member State in Table Delegation Options by MS

2.10.1. Creating a delegation by delegator

This section describes the steps you need to take in order to create first level delegation using the UUM&DS Admin interface in the central UUMDS service.

2.10.1.1. Step 1 — Enter WAYF user details

Figure 12 Where Are You From page

Complete the page with the following information:

- Select the Customs Domain.
- Select your country.
- Select your correct type of actor (Economic operator).
- Select who you want to act on behalf of (e.g. Myself).

Access management through UUM&DS

- Tick the box to confirm that you give consent to share your Identity Profile information.
- Click **Submit** to send the data to the TAXUD CAS.

2.10.1.2. Step 2 — Add the delegation
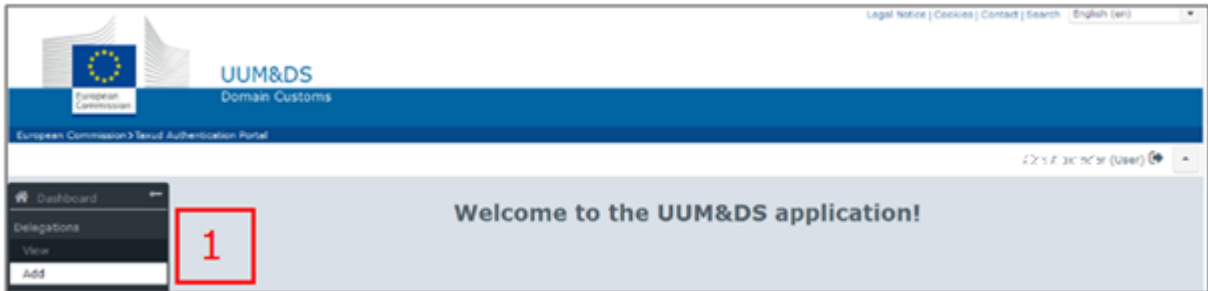
The UUM&DS welcome page opens.

Figure 13 Welcome page

- In the Dashboard, select **Delegations > Add**.

    The Add delegation page opens.
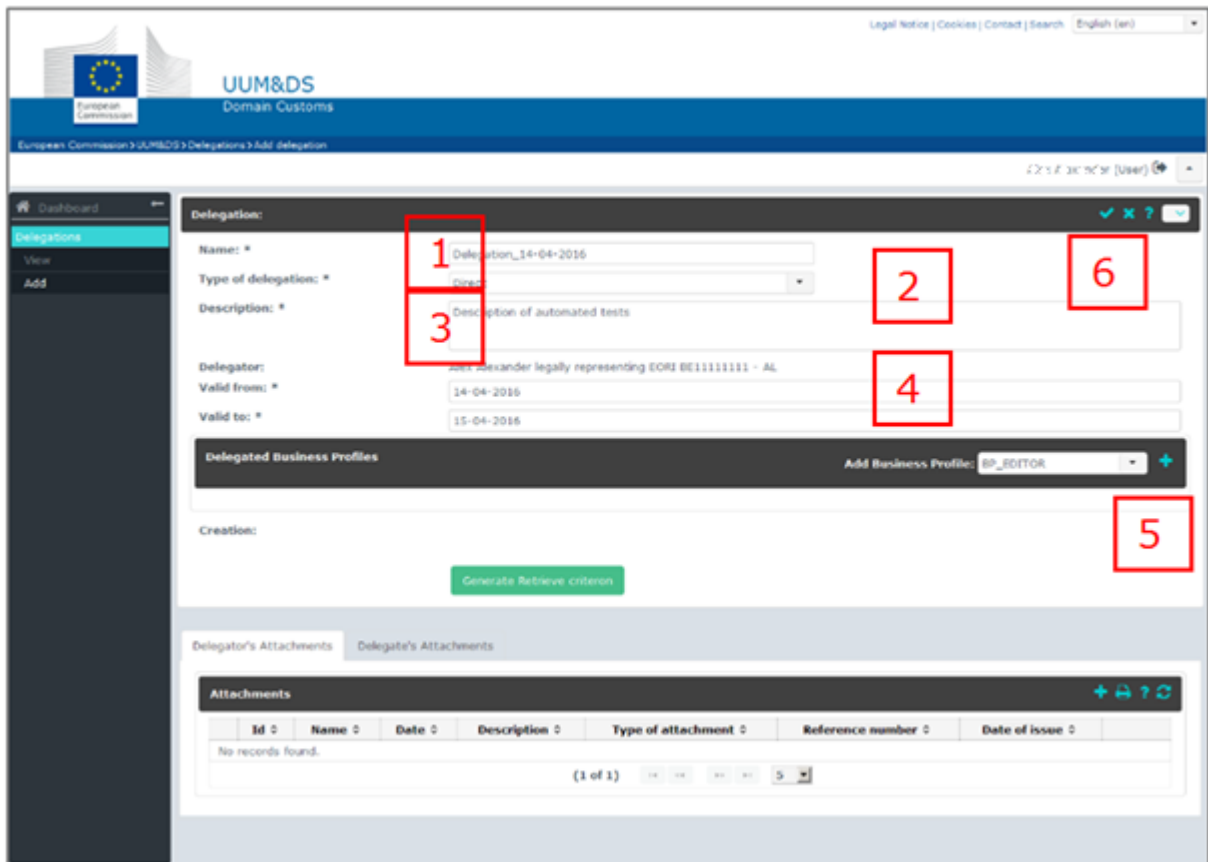
2.10.1.3. Step 3 — Complete the Add delegation details

Figure 14 Delegation page

Complete the Add delegation page details:

- Enter **Name** of delegation (e.g. Delegation_14-04-2016).
- Select **Type of delegation** (e.g. Direct) 📝
- Enter a Description.
- Enter the **Valid from** date and **Valid to** dates.
- Select **Add Business Profile** (e.g. BP_EDITOR) and click ➕.
- Click ✅ to save.

2.10.1.4. Step 4 — Select applications

The lists of **Available applications** and **Selected applications** open.
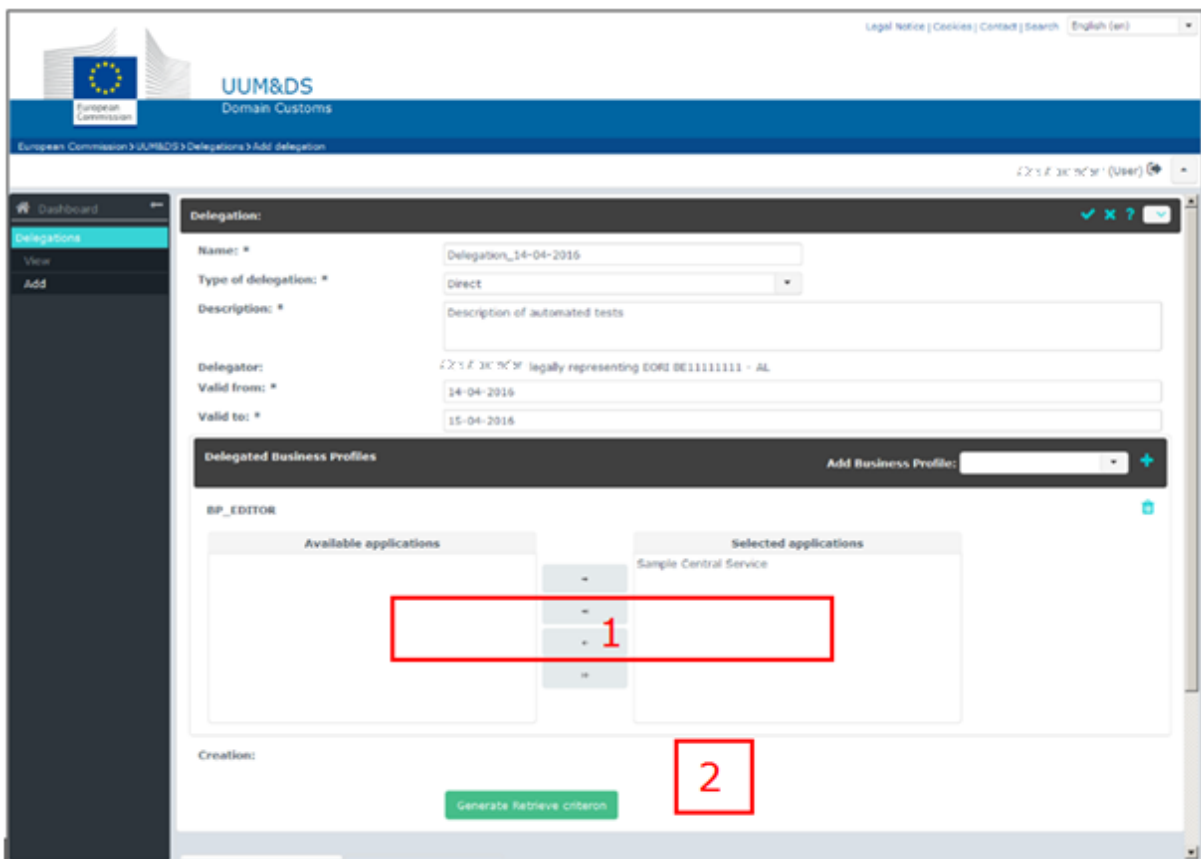
Figure 15 Delegation page – Applications

- To select or deselect an application, choose the application and click → or ← to move the application to the appropriate list.
- Click **Generate Retrieve Criterion**. This automatically saves the delegations and generates a unique criterion that will be used to retrieve the delegation request.

  The Generated Delegation Request Retrieve Criterion page opens containing the generated token.

Access management through UUM&DS

Figure 16 Token page

- Communicate this token to the delegate.

  The delegate now needs to accept the delegation as shown in section .

2.10.2. Creating a second level delegation by delegator

This section describes the steps you need to take in order to create second level delegations using the UUMDS Admin interface in the central UUMDS service.
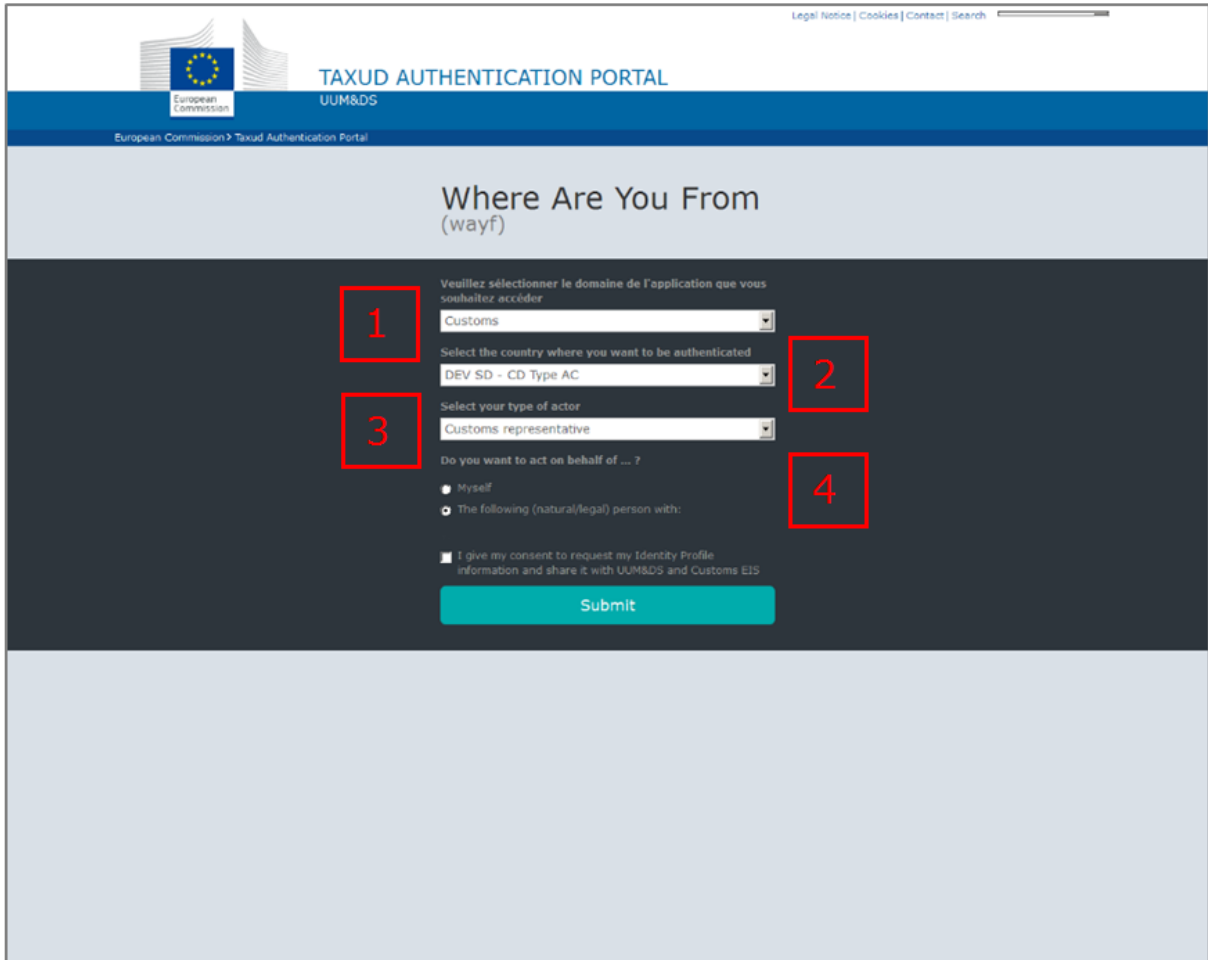
2.10.2.1. Step 1 — Enter WAYF user details

Figure 17 Where Are You From page - for 2nd level delegation

Access management through UUM&DS

Complete the page with the following information:

- Select the Customs Domain.
- Select your country.
- Select your correct type of actor (e.g. Customs representative).
- Select who you want to act on behalf of (e.g. The following (natural/legal) person with:)

  Additional fields open.

Figure 18 WAYF page – Additional fields

- Select the type of actor that you are representing (e.g. Economic Operator)
- Select the Type of ID (e.g. EORI).
- Enter the ID (e.g. BE11111111)
- Select **Directly**.
- Tick the box to confirm that you give consent to share your Identity Profile information.
- Click **Submit** to send the data to the TAXUD CAS.

2.10.2.2.   Step 2 — Add the delegation

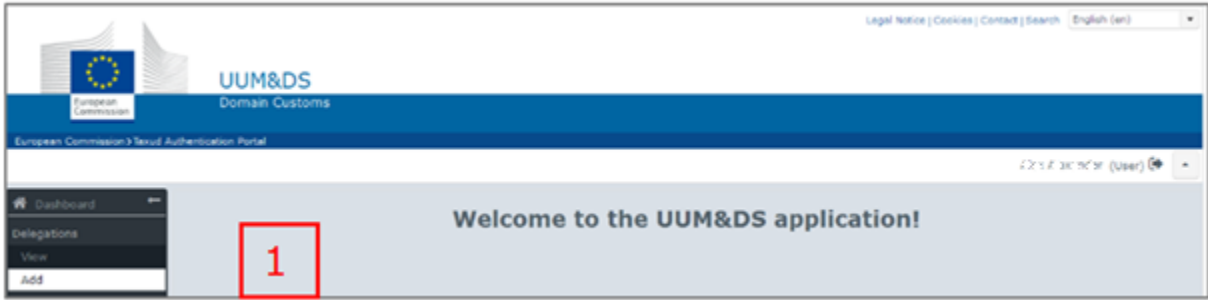The UUM&DS welcome page opens.

Figure 19 Welcome page

- In the Dashboard, select **Delegations > Add**.

  The Add delegation page opens.

2.10.2.3. Step 3 — Complete the Add delegation details
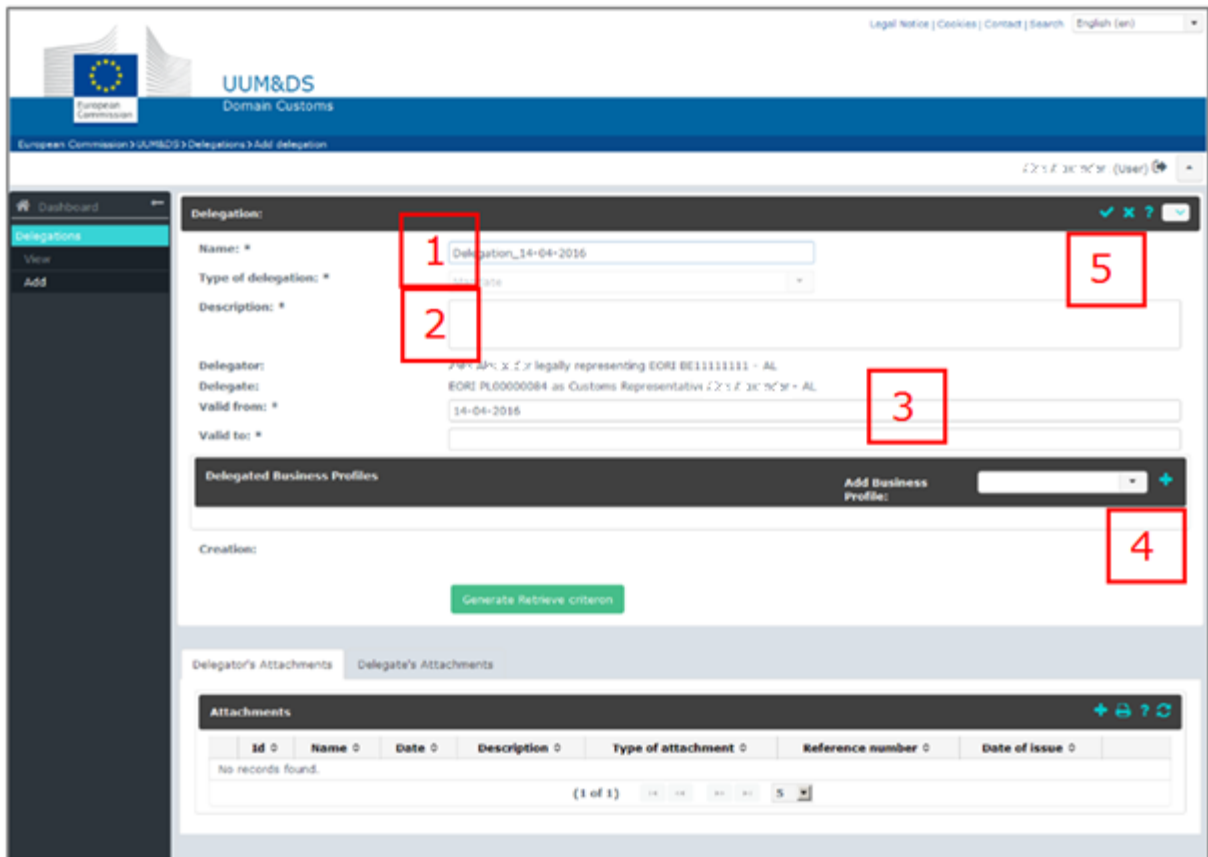

Figure 20 Delegation page

Complete the Add delegation page details:

- Enter **Name** of delegation (e.g. Delegation_14-04-2016).
- Enter a Description.

Access management through UUM&DS

- Enter the **Valid from** date and **Valid to** dates.

- Select **Add Business Profile** (e.g. BP_EDITOR) and click ➕.

- Click ✔ to save.

2.10.2.4. Step 4 — Select applications

The lists of **Available applications** and **Selected applications** open.
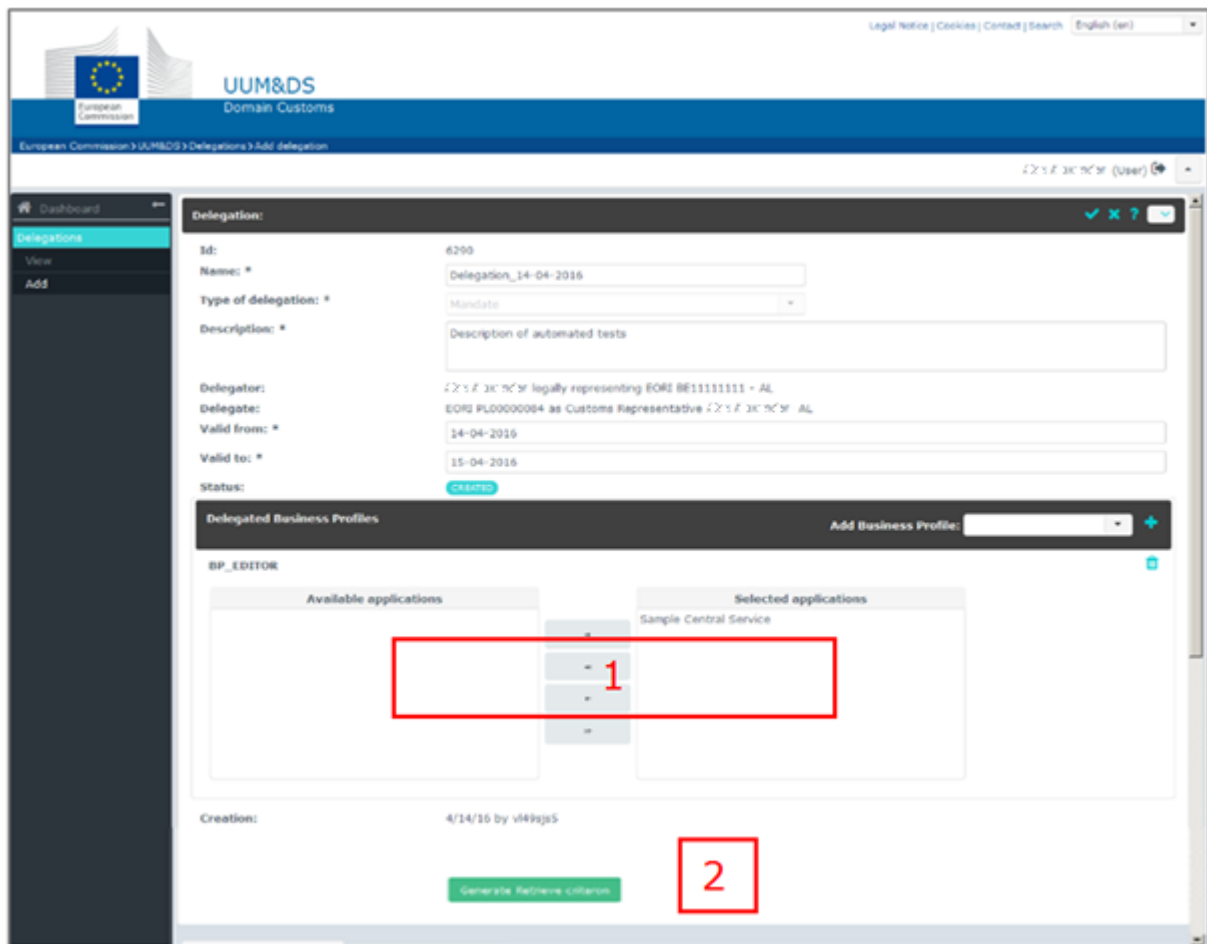
Figure 21 Application page

- To select, or to remove an application from the list of selected applications, choose the application and click → or ← to move the application to the appropriate list.

- Click **Generate Retrieve Criterion**.

  The Generated Delegation Request Retrieve Criterion page opens containing the generated token.

Figure 22 Token page

- Communicate this token to the delegate.

  The delegate now needs to accept the delegation as described below.

2.10.3. Delegation Retrieval, Acceptance or Rejection

This section describes the steps to be followed to retrieve accept or reject delegations using the UUMDS Admin interface in the central UUMDS service.

2.10.3.1. Step 1 — Enter WAYF user details

Figure 23 WAYF page

Complete the page with the following information:

Access management through UUM&DS

- Select the Customs Domain.
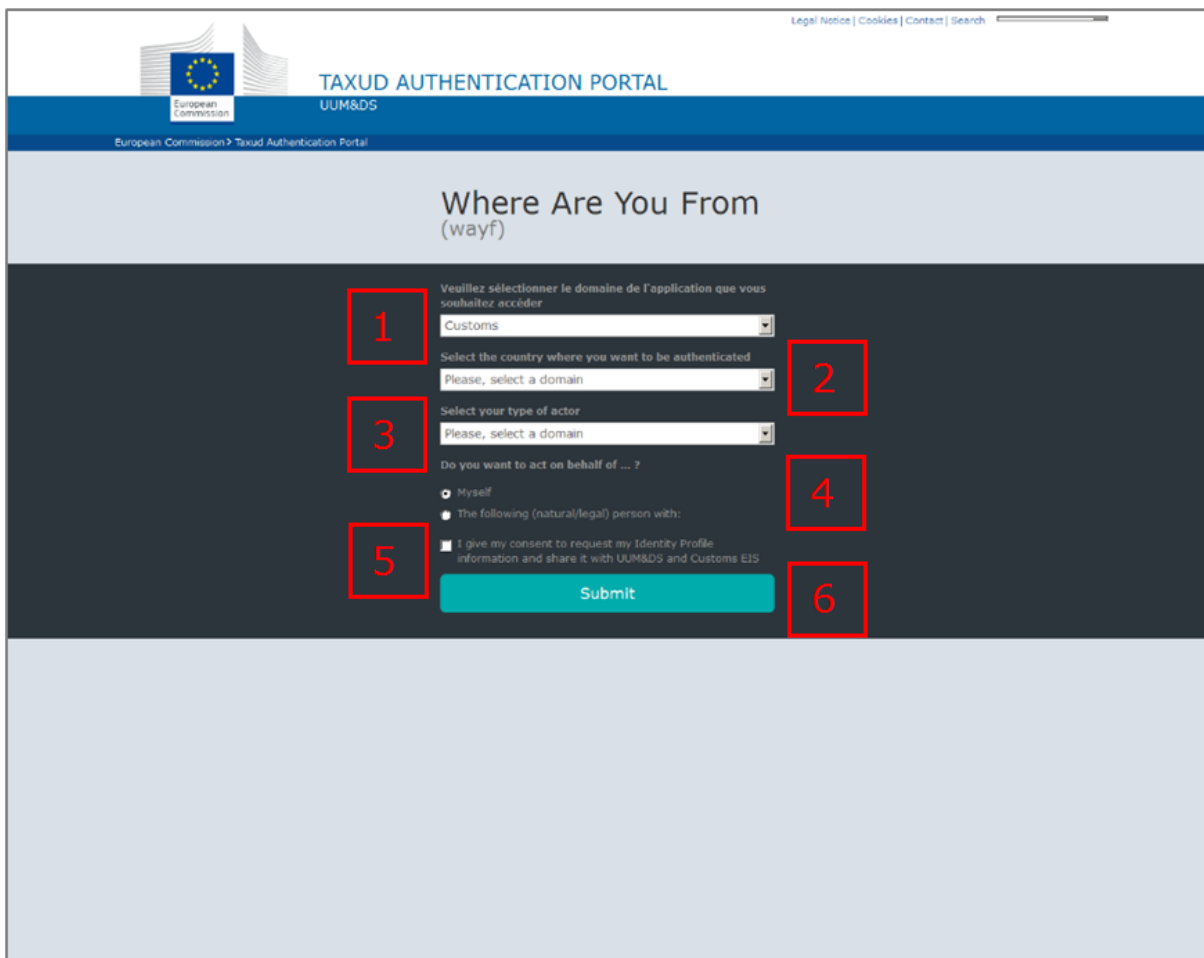- Select your country.
- Select your correct type of actor (e.g. Customs representative).
- Select who you want to act on behalf of (e.g. Myself).
- Tick the box to confirm that you give consent to share your Identity Profile information.
- Click **Submit** to send the data to the TAXUD CAS.

2.10.3.2. Step 2 — User retrieves delegation

Figure 24 Welcome page

- In the Dashboard, select **Delegations > Retrieve** delegation request.
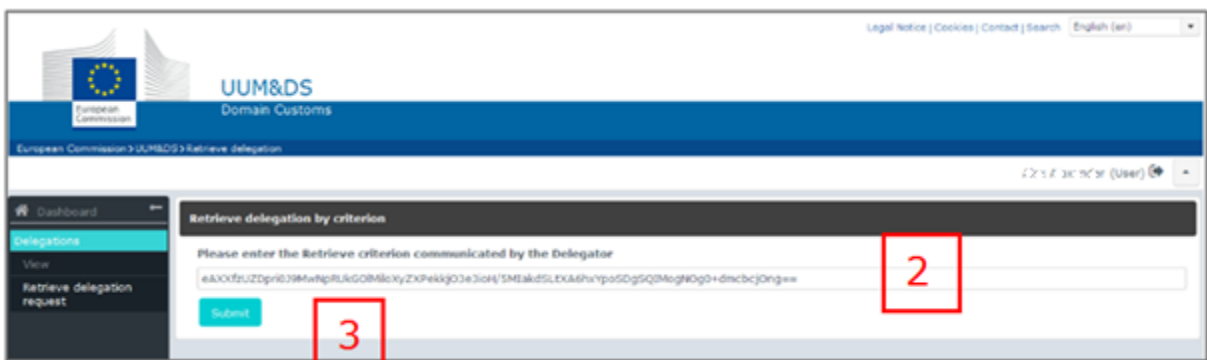
Figure 25 Retrieve Delegation

- Enter the token as received from the delegator.
- Click **Submit**.

  The delegation is displayed.

Access management through UUM&DS

2.10.3.3. Step 2 — User accepts delegation

Figure 26 Delegation acceptance

- Examine the delegation and click **Accept**.
- A comment box opens; verify the Delegation number (e.g. 6281).
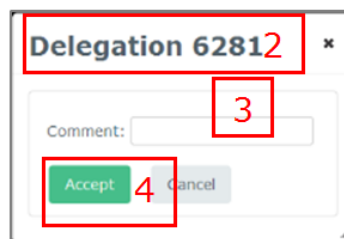
Figure 27 Comment box

- Enter a **Comment**.
- Click **Accept**.

2.10.3.4. Step 2 — User rejects delegation

The user has the option to Reject the delegation instead of Accept. In this case, the delegation is rejected and cannot be applied anymore.

Access management through UUM&DS

Figure 28 Delegation Rejection
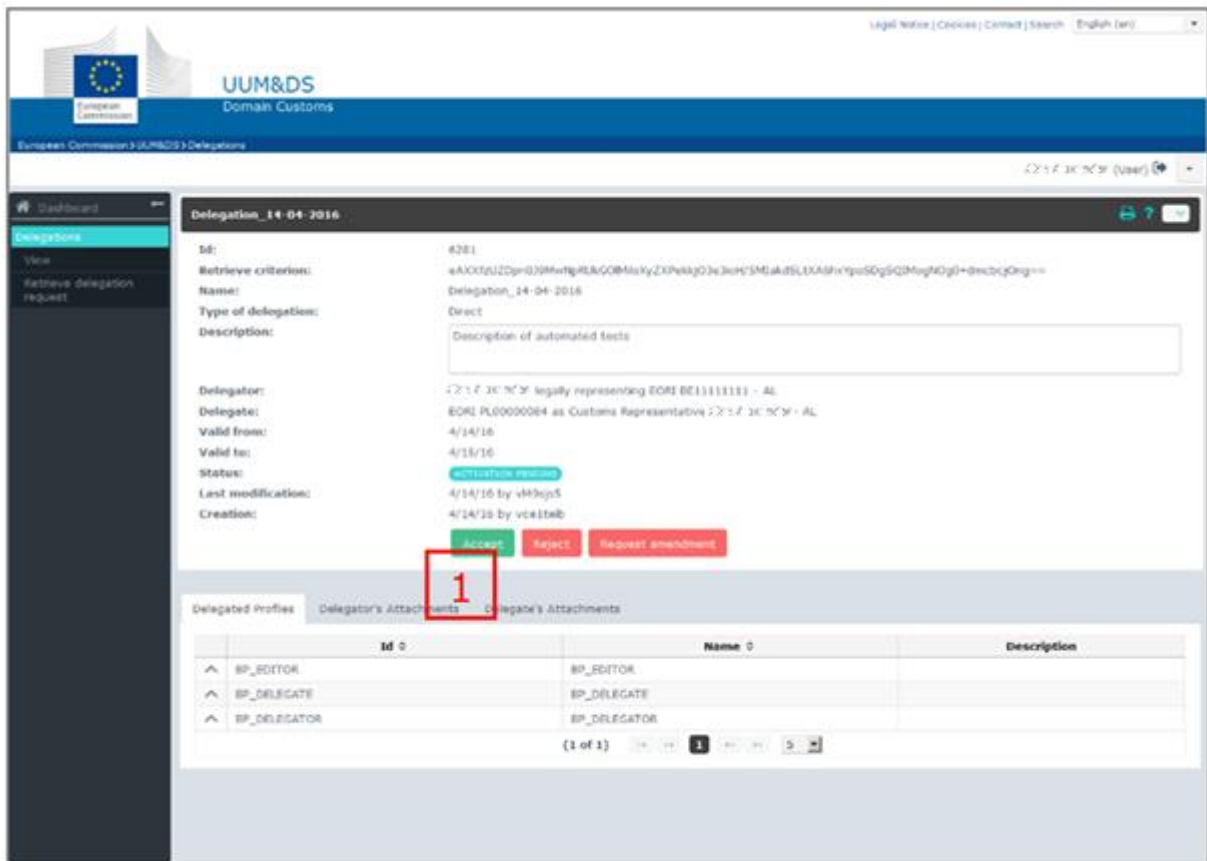
- Examine the delegation and click **Reject**.
- A comment box opens, verify the Delegation number (e.g. 6281).

Figure 29 Comment Box

- Enter a **Comment**.
- Click **Reject**.

The delegator is notified and can see in his dashboard that the delegation has been rejected.
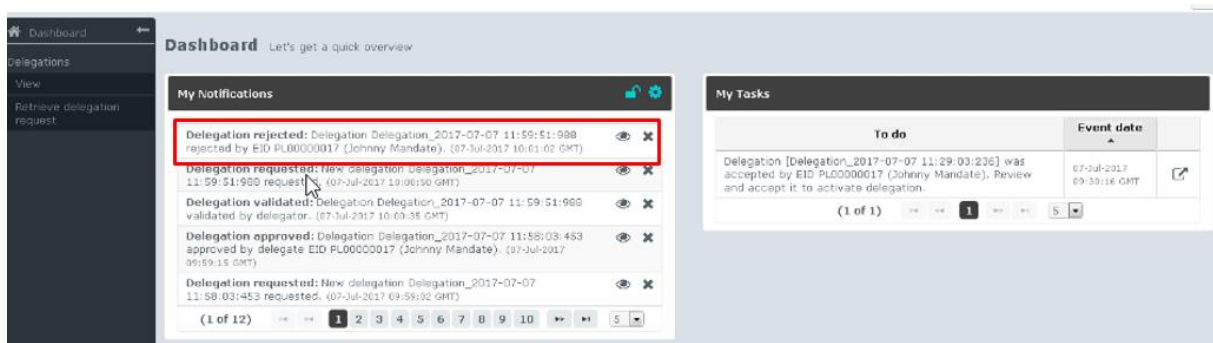
Figure 30 Dashboard with delegation rejection

2.10.4. Delegation amendment

The user has the option to request an amendment for the delegation instead of Accept. In this case, the user asks the delegator to amend the delegation as described in the amendment comment.
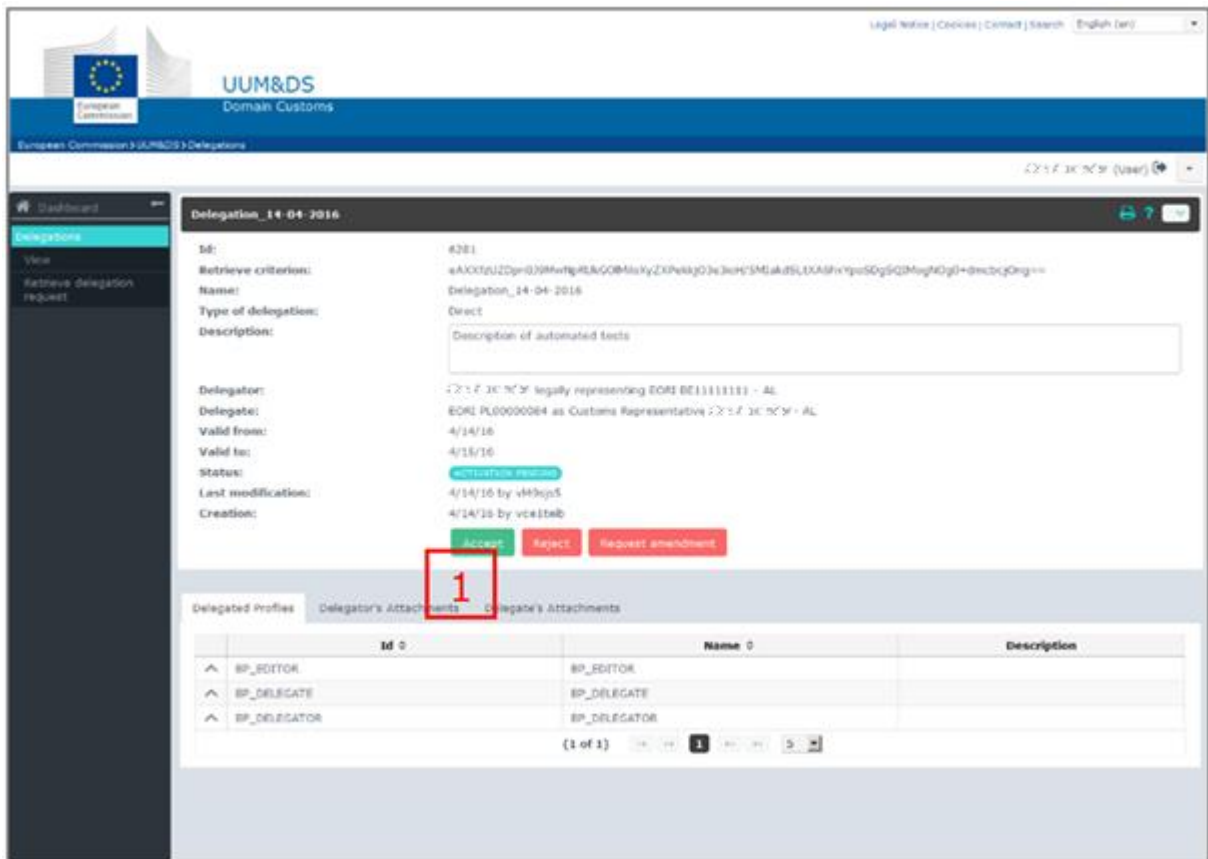
Figure 31 Delegation amendment

- Examine the delegation and click **Request amendment**.
- A comment box opens; verify the Delegation number (e.g. 6281).

Figure 32 Comment box

- Enter a **Comment** which is the requested change(s).
- Click Request amendment.

The delegator is notified and can see in his dashboard that the delegation has been rejected for amendment.
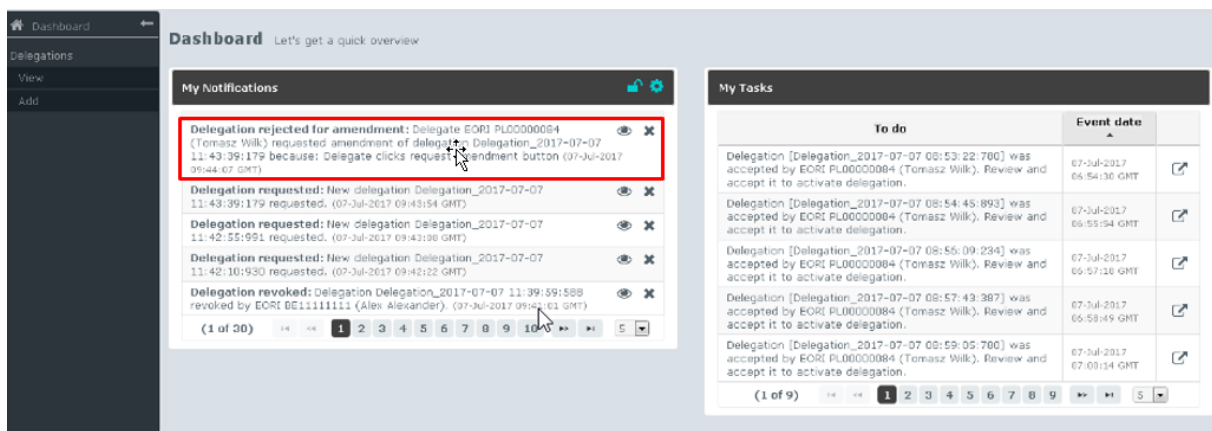
Figure 33 Dashboard with delegation amendment

2.10.5. Delegation Revocation

The user or the delegator has the option to revoke a delegation which is already active or that has been accepted. In this case, the delegation is revoked and cannot be applied anymore. This is an optional step that allows a delegation to end.
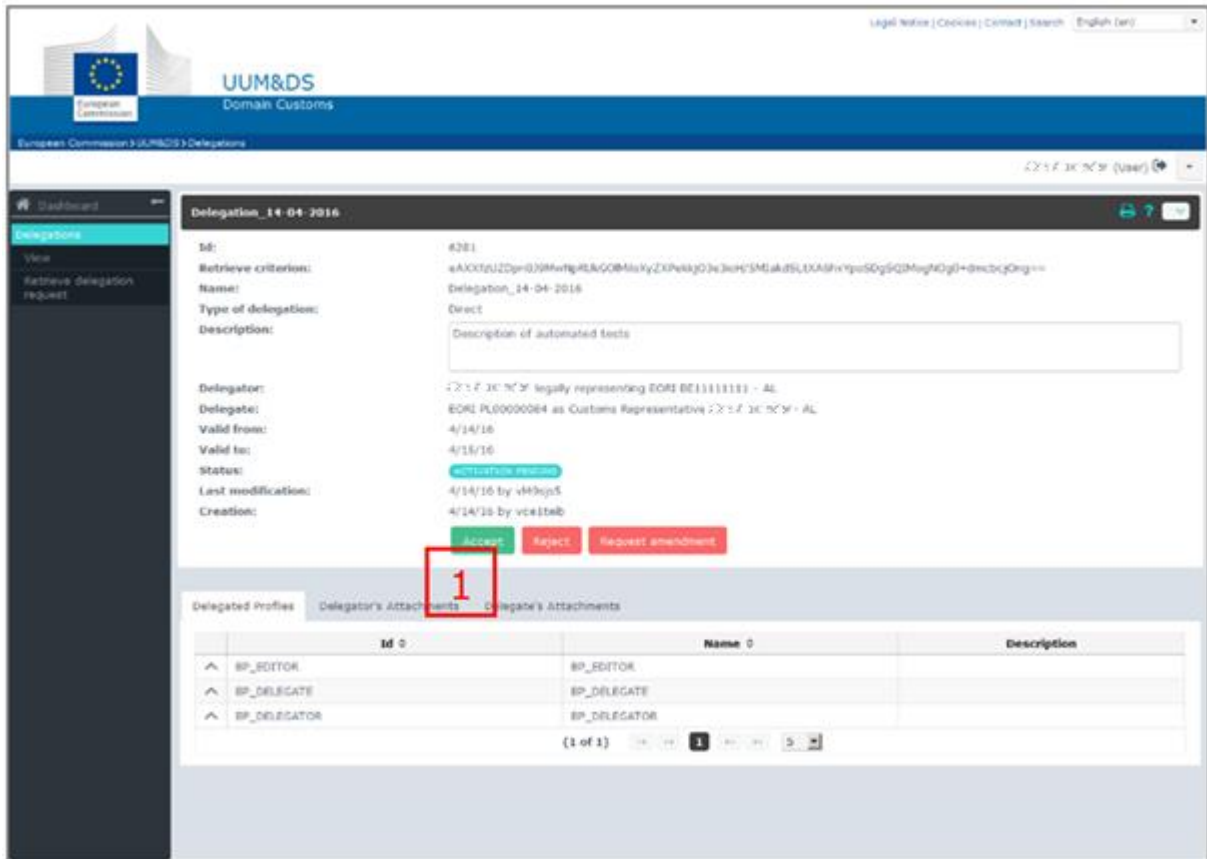
Figure 34 Delegation revocation

- Select the delegation and click **Revoke**.
- A comment box opens; verify the Delegation number (e.g. 6281).

Figure 35 Comment box

- Enter a **Comment** – i.e. the reason for the revocation.
- Click **Revoke**.

The delegator is notified and can see in his dashboard that the delegation has been revoked.

Access management through UUM&DS
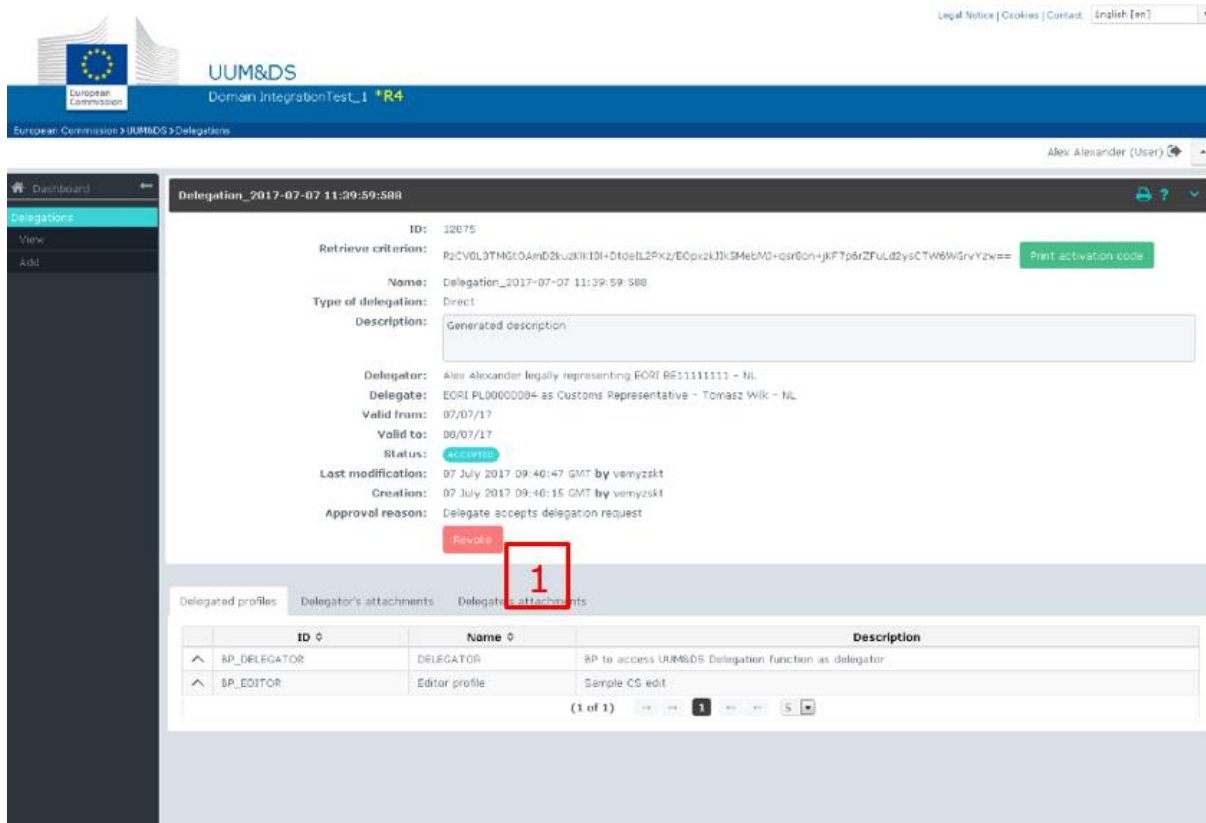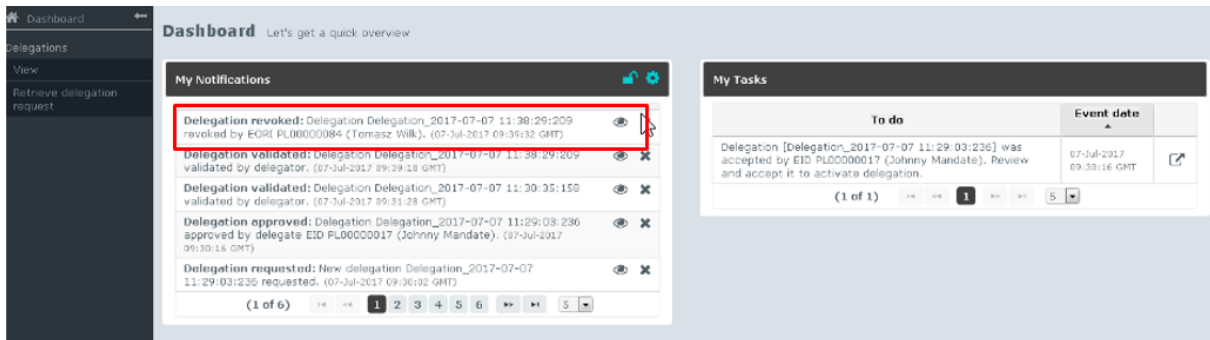
Figure 36 Dashboard with delegation revocation

2.10.6. Delegation Expiration

When a delegation is expired or will be expired in few days[1] (number of days configurable), a notification is sent to the both delegation partners. It means that for a first level of delegation, the delegator and the delegate are notified and for a second level delegation, the delegated and the mandate are notified.

This notification is sent by mail and also appears in the dashboard of the delegation partners.
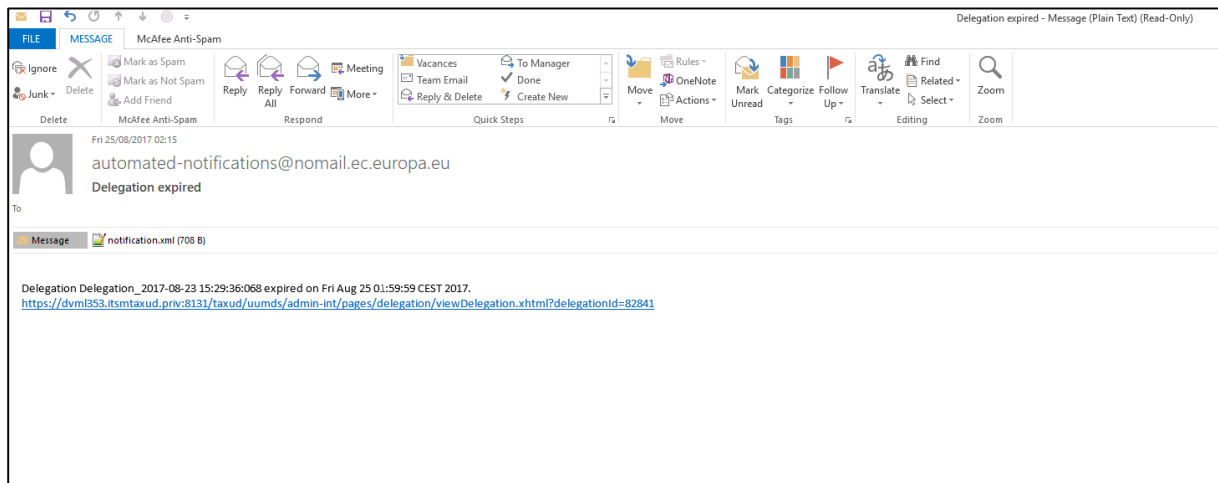
Figure 37: Example of e-mail sent when delegation has expired

---

[1] Feature available from FAT5 release
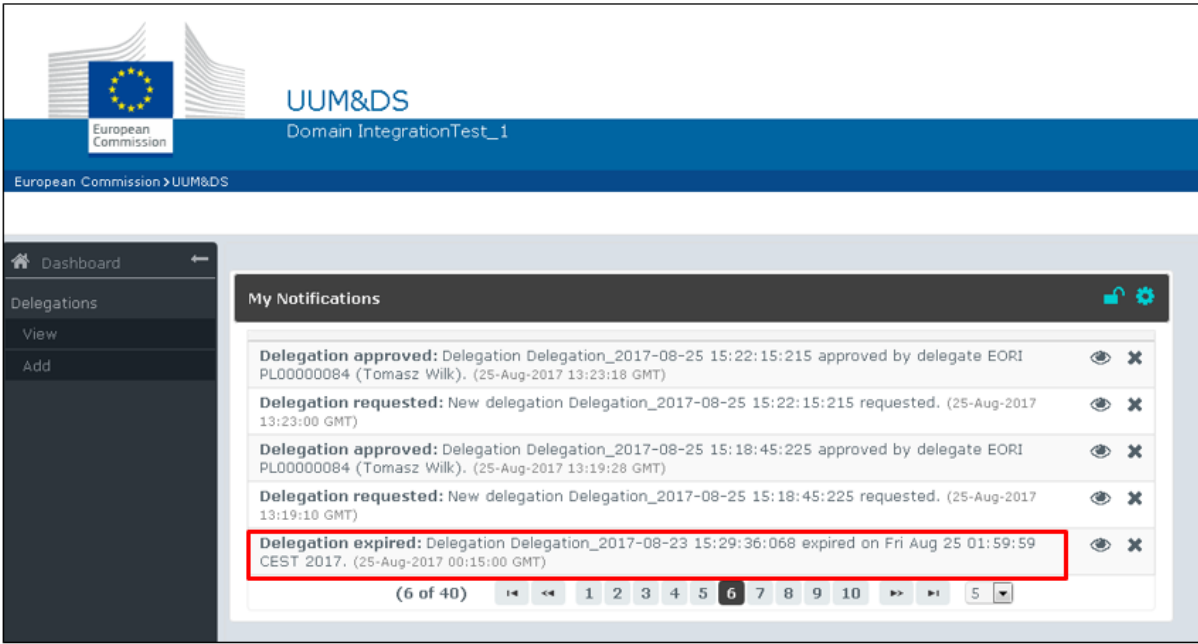
Figure 38: Dashboard with expired delegation
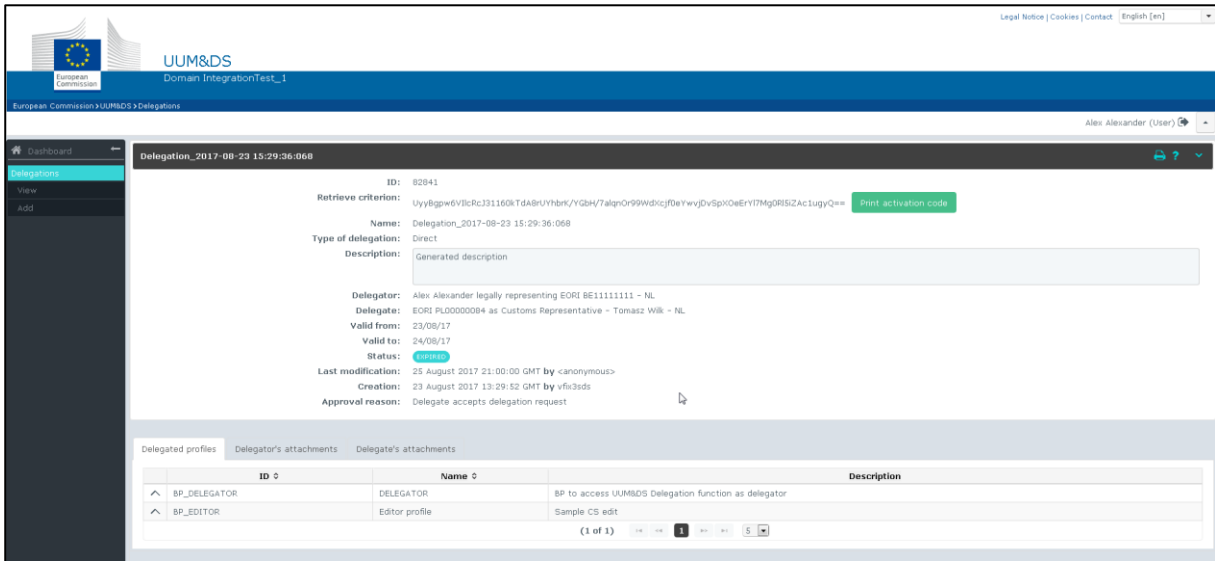
Figure 39: Expired delegation content
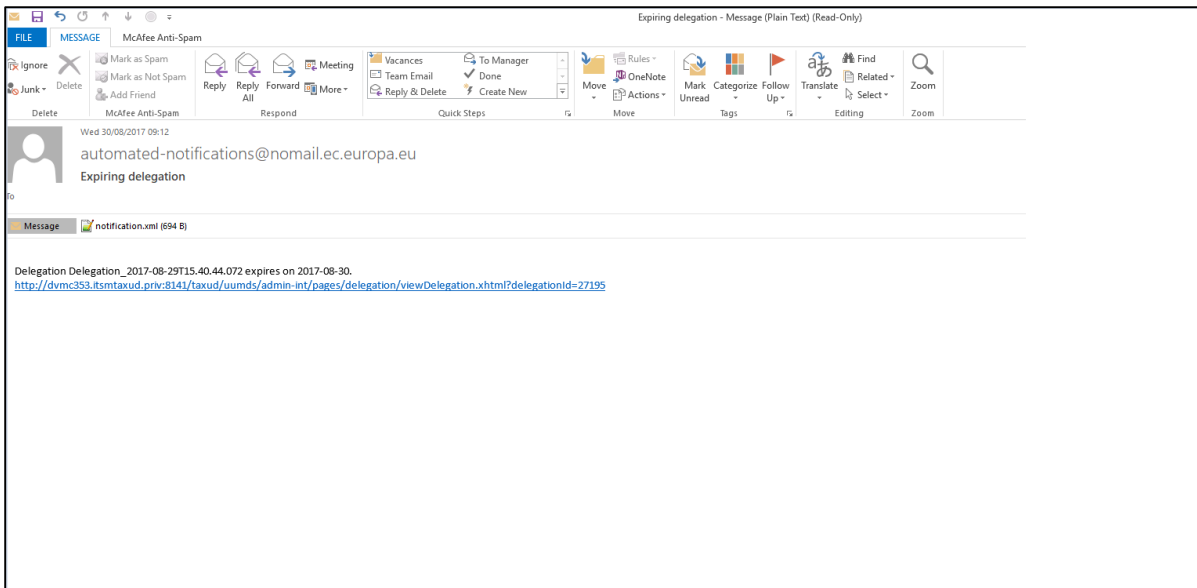
Figure 40: Example of e-mail sent when delegation is about to expire[2]
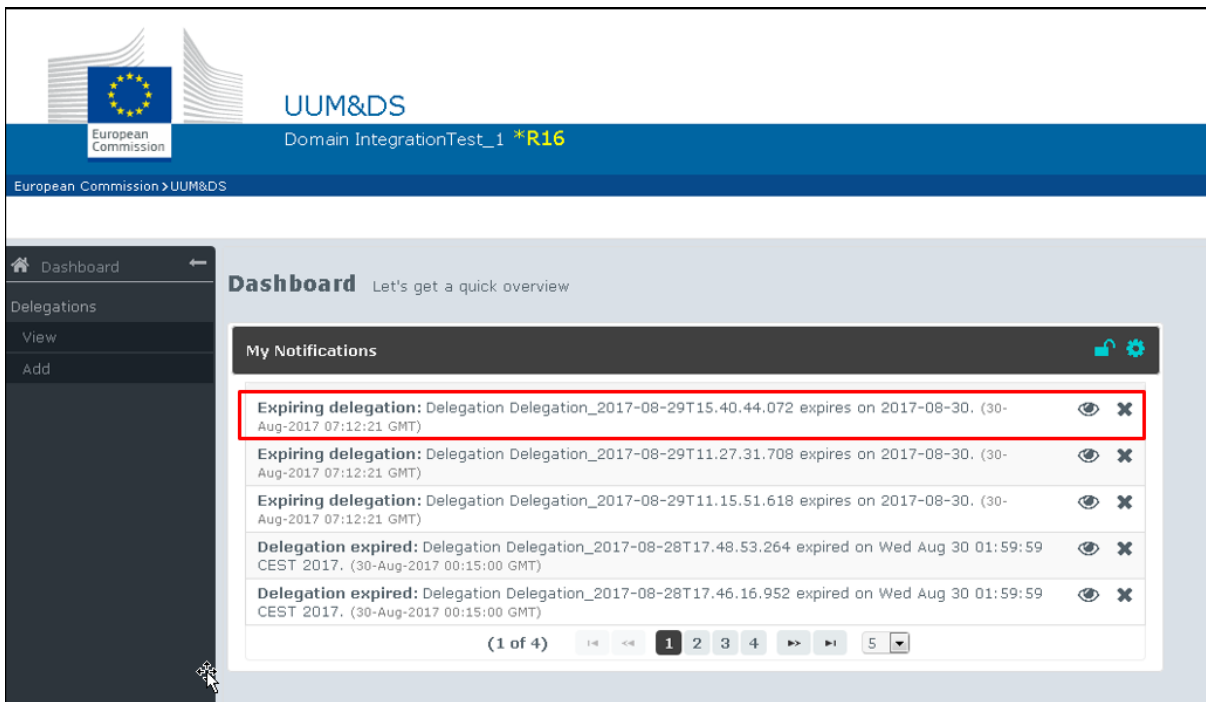
Figure 41: Dashboard with delegations about to expire[2]

---

2 Feature available from FAT5 release

Access management through UUM&DS
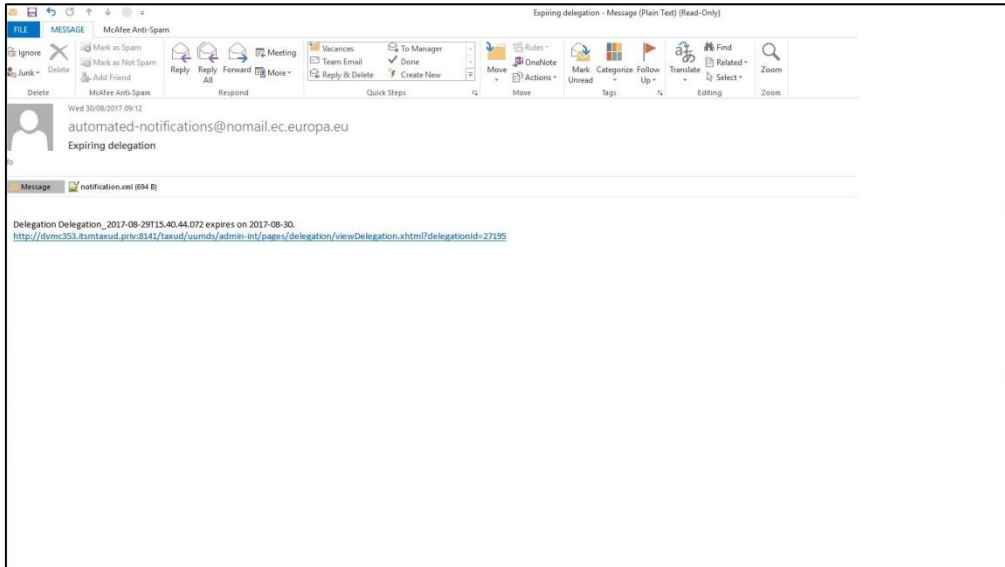
Figure 42: The content of the delegation about to expire

Remark: The user needs to subscribe to the 'Expiring delegation' event to receive notifications about delegation that will expire in few days.**3**

Figure 43: Subscription to Expiring delegation event[3]

---

3 Feature available from FAT5 release

2.11. Notification management

Users can use Notifications to be informed by the system for specific events i.e. Delegation requested, Delegations Approved, Delegation Rejected etc. Delegation Notifications can be managed by clicking on the gear wheel in the **My Notifications** panel of the dashboard.

Figure 44 Notifications page

The page lists all possible notifications.

2.11.1. Subscribe to notifications

To subscribe to a notification:

- Select a line of the table.

- Click the selected

- Enter one or more **Email addresses** separated by commas.

Subscribing to a notification does not ensure that you are eligible to receive it.

A sample view of the dashboard is attached below (Figure 45) as well as a sample notification e-mail, informing on reference data changes (Figure 46).
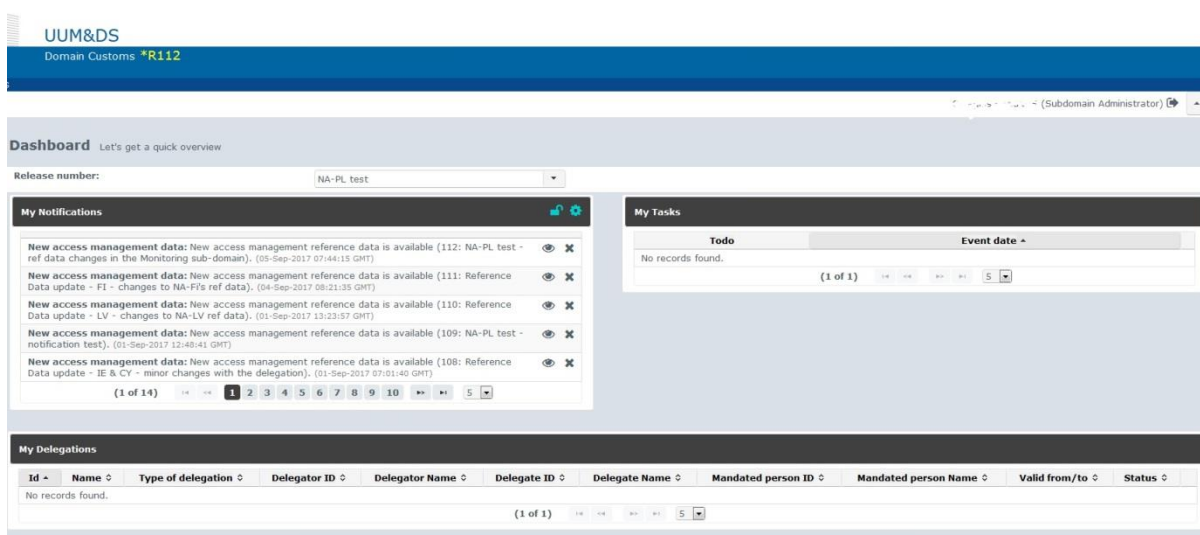
Figure 45: Dashboard containing notifications

New access
management data.ms

Figure 46: Sample Notification mail

2.11.2. Unsubscribe from notifications

To unsubscribe, please follow the same process but remove all the e-mail addresses from the subscription.

3. What can go wrong?

3.1. Access management failure

The following two cases may lead to Authentication failure:

- Authentication fails because the National Authentication Portal has reported invalid credentials i.e. wrong user id or password or both. In that case, a UUM&DS session is not established and you need to repeat the full authentication cycle.

  This will result to a screen similar to Figure 47, with a message coming from the National Authentication Portal (in this case TAXUD CAS).
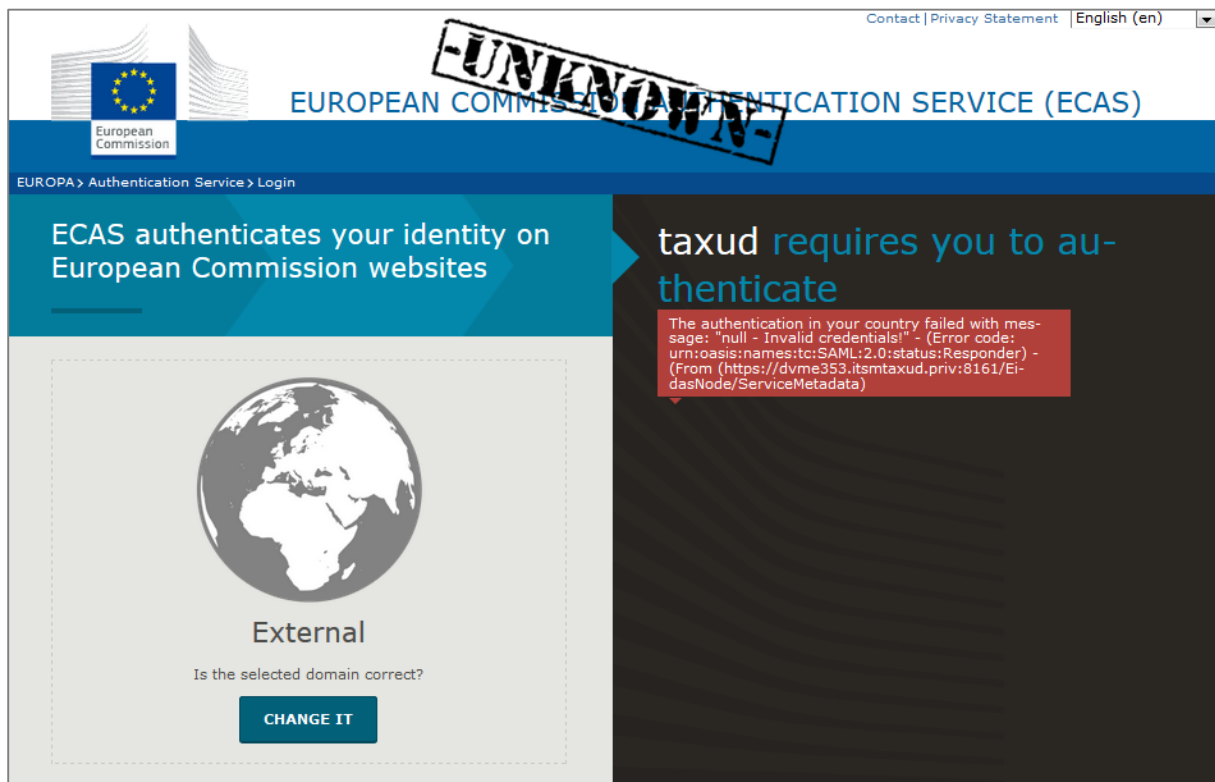
Figure 47: National Portal - Authentication failed

- Authentication fails as a result of an access denial decision by the PDP. Although the user is correctly authenticated but does not have the privilege for accessing the service i.e. wrong or missing business profile assignment. In that case, the single sign-on session is established but the access to the application is denied. In this case a screen similar to Figure 48 is shown. The user can try to access another application, or to re-authenticate using a different user identifier, Type of Actor or delegation.
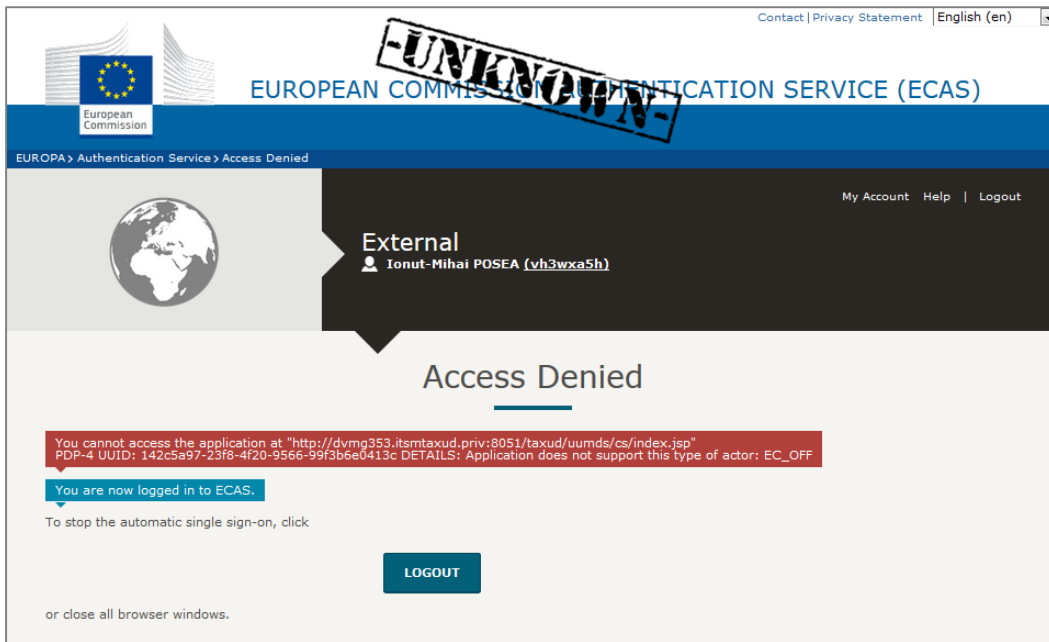
Figure 48: Access Denied — Type of Actor not supported

3.2. Insufficient authorisation

User authorisation is accomplished using business profiles. The combination of the proper business profiles authorises user's access to Applications and resources. A user may not be able to access an Application due to lack or mismatch of business profiles. The error page received in these cases can be found in Figure 49.
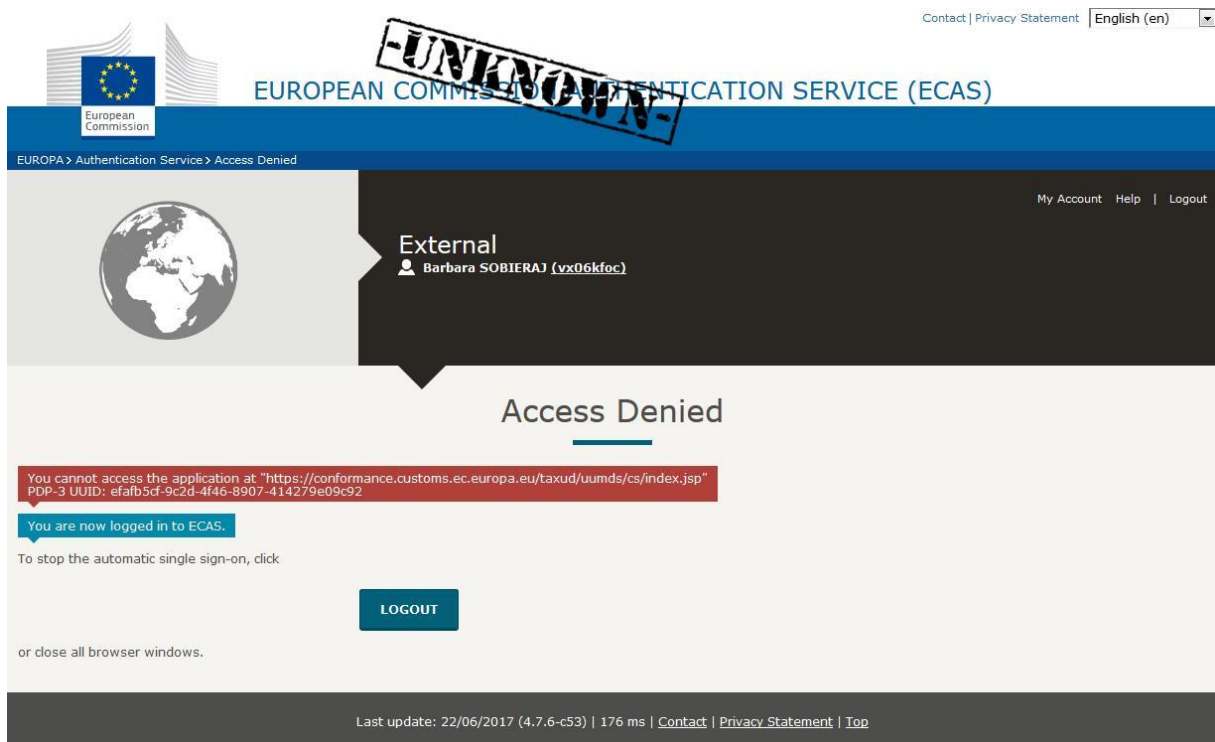
Figure 49 Business profile / Authorisation problem

Access management through UUM&DS

3.3.   Delegation Problems

In the case of Customs Representatives and Employees accessing the Applications, there may be a problem with delegation. If a delegation is not valid or has expired, the user will receive the page in Figure 50 even though he has the proper credentials.

Figure 50 Invalid / Expired delegation

3.4.   Session timeout

For security reasons, there is an inactivity timeout set to 5 minutes in the WAYF page. This means that if the user stays inactive in this page for more than 5 minutes, he cannot log into the system, even having proper credentials. To solve this, the user should close the browser window and retry in a new one. The page displayed in this occasion can be seen in Figure 51.

Figure 51: Session Timeout

4. Definitions

Term	Definition
Applications	Applications in UUM&DS are meta-data about a Central Service. These meta-data are used to manage the security and access of the Central Service.
ATTR-PEPS	**Attribute PEPS**. This is a component for MS IAM of Type B in charge of providing to UUM&DS the authorisation information for a given user through a SAML interface.
ATTR-WS	**Attribute WS**. This is a component for MS IAM of Type B in charge of providing to UUM&DS the authorisation information for a given user through a SOAP web service.
CED	CED is the Commission European Directory and it is used to know the ECAS account name of EC Officials. This is needed when creating assignments or delegations for EC officials.
Central Service	A Central Service is a component that is protected by UUM&DS and hosted at DG TAXUD. This component is not part of UUM&DS and is usually a Central Customs European Information System.
Delegate/Representative	The person who is assigned the authorisation(s) by the delegator
Delegation	The delegation is the action of a person (legal or natural) to assign to another natural or legal person to act on his behalf by delegating one or more of his authorisations defined as business profiles. The scope of the delegated business profiles (scoped by application) can be the same or a subset of the one of the original business profile.
Delegation Partner	User involved into a delegation
Delegator	The person who owns the authorisations and decides to assign -all or part of- them to another natural or legal person (delegate).
Direct Representation	The EO is responsible for the actions performed by the Customs Representative (delegated entity) on the name of the EO
ECAS	ECAS is the European Commission Authentication portal. It is federated by UUM&DS to authenticate EC Officials.
EC Mail Gateway	EC Mail gateway is a European Commission system for sending e-mails to other people. In UUM&DS, it is used for notifying Economic Operator or UUM&DS Admins about an action (delegation, application's approvals, …)
EC/NA Official	EC/NA Officials are in charge of managing UUM&DS users and their authorisations.
First Level delegation	The first level delegation is the action of a person (legal or natural), who owns the authorisations, to assign to another natural or legal person to act on his behalf, by delegating one or more of his authorisations defined as business profiles to another natural or legal person.
Indirect Representation	The Customs Representative (delegated entity) is responsible for the actions performed by him on the name of the EO

Term	Definition
Mandate	The action of a person (legal or natural) to assign an authorisation to a natural person (i.e. employee) in order to act on his behalf. The EO /CR is responsible for the actions performed by his employee (delegated entity) on the name of the EO/CR
Mandated Person	Natural person who has been mandated either by the delegator who owns the authorisations or by the Delegated person, who has been assigned a set of authorisations, to act on his behalf but the responsibility for his actions remains to the originator of the mandate.
MS IAM	MS IAM is a Customs IT system which offers authentication services to Economic Operators and provides a set of user's attributes such as business profiles to central services through UUM&DS. It can also manage EO delegations to other entities. The MS IAM system provides access to national Customs IT systems and is extended to enable access to central Customs European Information Systems for EO.
MS IAM of Type A	MS IAM in the Customs domain is one consolidated system for the authentication and authorisation of users that can be directly interfaced with the UUM&DS system.
MS IAM of Type B	MS IAM in the Customs domain consists of two systems, one for the authentication and another for the provision of additional attributes. UUM&DS requests and retrieves authentication and authorisation information from one system in the MS which the Single Point Of Contact (SPOC) withh UUM&DS.
MS IAM of Type C	MS IAM in the Customs domain consists of multiple IAMs for the authentication and the authorisation of users. MS shall provide a unified IAM with a common authentication portal in order to interface with the UUM&DS system.
MS IAM of Type D	The MS has no IAM that can be federated with UUM&DS. Consequently, it will provision identities and authorisations into the central UUM&DS system.
SAML Adapter	This is the component which is responsible to make the integration between the MS PEPS and the MS IAM.
Second level Delegation	The action of a delegate (legal or natural person) to further delegate his or hers delegated authorisation(s) to another person (natural or legal).For UUM&DS central delegation service second level delegation shall implement second level delegation from a natural or legal person only to a natural person which is equivalent to a mandate.
STORK	STORK is the set of PEPS deployed for each MS, in charge of federating and integrating each MS IAM. In this document, we present STORK into two sub-components: MS PEPS (PEPS deployed for the MS) and TAXUD PEPS (PEPS deployed for DG TAXUD).
UUM&DS Admin	UUM&DS Administrators are in charge of managing UUM&DS meta-data, such as the registration of Central Services. There are different kinds of administrators with specific tasks.

Table 3 Definitions Table

Access management through UUM&DS

5. Supported Delegations by MS

MS	Delegation Type	No Delegation	1st level (CR)	1st level (EMPL)	2nd level
AT	Local		X		X
BE	--	X			
BG	Local		X	X	X
CY	Central		X		
CZ	Local		X		
DE	Central		X		
DK	Local	X			
EE	Central		X	X	
ES	Local		X	X	X
FI	Local	X			
FR	Central			X	
GR	Central		X	X	X
HR	Local		X	X	X
HU	Local		X	X	X
IE	Central		X		
IT	Local		X	X	X
LT	Local		X	X	X
LU	Central		X	X	
LV	Local			X	
MT	--	X			
NL	--	X			
PL	Local		X	X	X
PT	Local		X		
RO	Central		X	X	
SE	--	X			

Access management through UUM&DS

SI	Local			X	
SK	Central			X	
UK	Central		X	X	