EUROPEAN COMMISSION
DIRECTORATE-GENERAL
TAXATION AND CUSTOMS UNION
Digital Delivery of Customs and Taxation Policies
Architecture & Digital Operations

UUM&DS[1] – Central Certificates Registration Tool

Manual for Economic Operators

You can find the following information:

[1] Uniform User Management & Digital Signature

General Information

Why registering a certificate?

The Certificate Registration is a self-register process aiming to establish an association between the Identifier of the Economic Operator and the certificate. This registration is a pre-requisite for the signature process, as the registered certificate will be used for signing or sealing the application.
The Economic Operator can register multiple certificates for a given identity.

Who should register a certificate?

Any Economic Operator registered in a Member State - which opted for using the UUMDS Central Certificate Registration Tool - and needs to interact with Customs Central Services requiring digital signatures.

Access and Login

To access Central Certificate Registration Tool you need:

1. Open a web browser;
2. Access the EO Administration tool at the following link : https://customs.ec.europa.eu/taxud/uumds/admin-ext/
3. Make sure to have the necessary Access credentials + Business profile = BP_MANAGE.

About certificates & signatures / seals

What is a digital eIDAS certificate?

Digital certificates are electronic credentials that bind the identity of the certificate owner to a pair of electronic encryption keys, (one public and one private), that can be used to encrypt and sign online communications between an end-users browser and a website. The main purpose of the digital certificate is to ensure that the public key contained in the certificate belongs to the entity to which the certificate was issued. In other words, to verify that a person sending a message is who he or she claims to be, and then to provide the message receiver with the means to decrypt the message.

eIDAS Certificates

The legal European Framework provides specifics for eIDAS certificates for electronic signatures / seals and website authentication in order to meet the requirements of the PSD2 Regulatory Technical Standards (RTS).

- They should respect technical requirements established by ETSI https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.04.01_60/ts_119495v010401p.pdf
- Two level of security are defined for eIDAS certificates:
  - Non-Qualified or advanced certificate
  - Qualified certificate: is a certificate stored on hardware device (HSP, smartcard, USB stick…) with a non-extractable private key.
- Qualified eiDAS certificates are Issued by an eIDAS Trusted Certificate Authorities recognised by a national law or a European Union law https://webgate.ec.europa.eu/tl-browser/#/

What is a digital signature / seal?

A digital signature is a mathematical scheme for verifying the authenticity & integrity of digital messages or documents.
A digital signature is a cryptographic way based on public / private key concept encrypting a document with a private key and decrypting with the public one.
A valid digital signature, where the e satisfied, gives a recipient very strong reason to believe in the authenticity of a known sender and the integrity of the message, which was not altered in transit.

---

eIDAS Signature/Seal

Electronic signatures were first recognised in European legislation through the Directive on a Community framework for electronic signature (eSignature Directive) adopted in 1999. Since 1 July 2016, electronic signatures in the EU are governed by the Electronic Identification and Trust Services (eIDAS) Regulation. eIDAS provides a predictable regulatory environment directly applicable to all EU Member States to enable secure and seamless electronic interactions between businesses, citizens and public authorities (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Introduction+to+e-signature)

- Advanced Electronic Signatures (AdES) (eIDAS Article 3) is an electronic signature which is :
  - uniquely linked to and capable of identifying the signatory;
  - created in a way that allows the signatory to retain control;
  - linked to the document in a way that any subsequent change of the data is detectable.

The most commonly used technology able to provide these features is the use of a public-key infrastructure (PKI), which involves the use of certificates and cryptographic keys.

- Qualified Electronic Signatures (QES) (eIDAS Article 3) is an advanced electronic signature, which is additionally:
  - created by a qualified signature creation device;
  - in addition, is based on a qualified certificate for electronic signatures.
- Signature creation devices come in many forms to protect the electronic signature creation data of the signatory, such as smartcards, SIM cards, and USB sticks. "Remote signature creation devices" can also be used where the device is not in the physical possession of the signatory, but managed by a provider. Those remote qualified signature solutions offer an improved user experience while maintaining the legal certainty offered by qualified electronic signatures.

Trusted Certificate Authorities (CA)

Qualified trust services provided in Europe (e.g. issuance of qualified certificates for electronic signatures or seals, qualified timestamping services) are listed in national 'trusted lists' in all European Union and European Economic Area Member States.

Those lists can be accessed through the List of Trusted List (LOTL) Browser, an online tool provided by the European Commission to ease the process of finding trust services her https://webgate.ec.europa.eu/tl-browser/#/

The trusted lists can include both qualified trust services and non-qualified trust services. Qualified trust services must be included on a national trusted list to be qualified, while it is up to each Member State whether and which non-qualified trust services to list in their trusted list.

European recognition of eIDAS certificates?

A qualified eIDAS signature or sealing based on a qualified eIDAS certificate issued in one Member State shall be recognized as qualified signature in all Member States

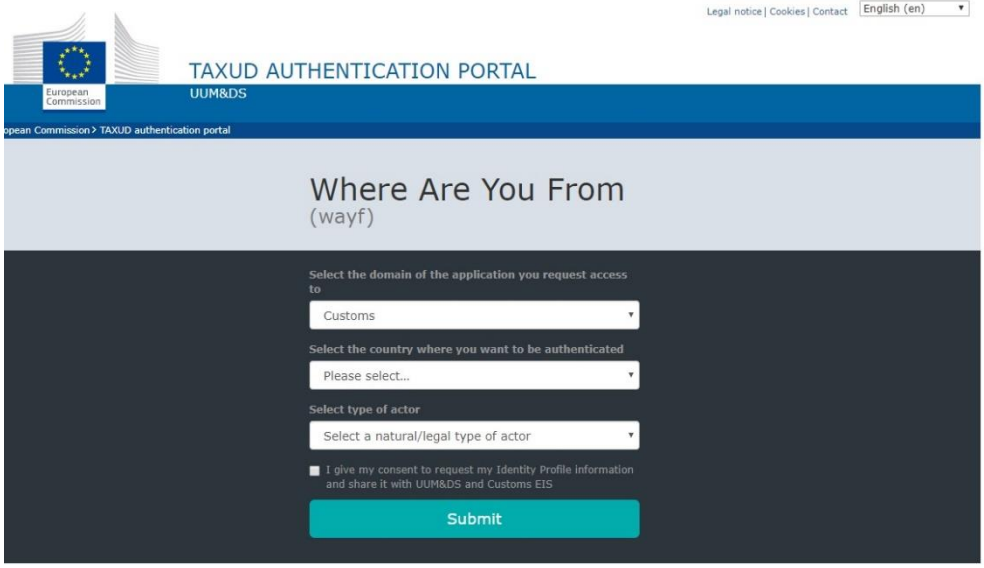
Registration Flows

There are nine flows in the Certificate Management process, which will be described in more detail below:

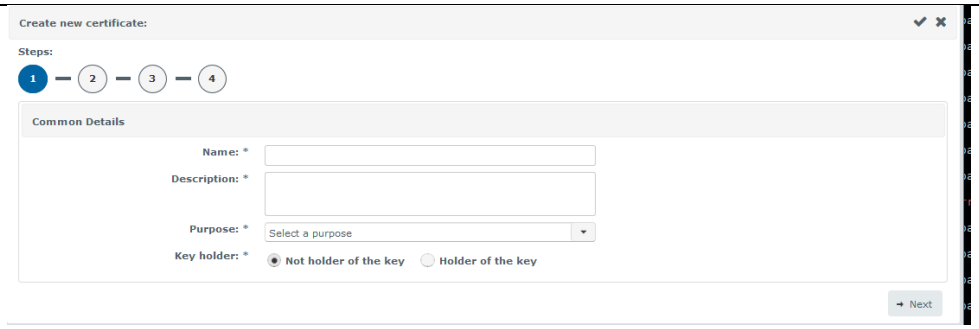
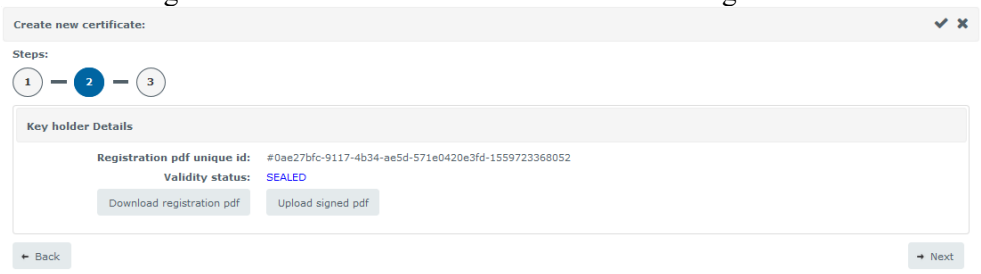
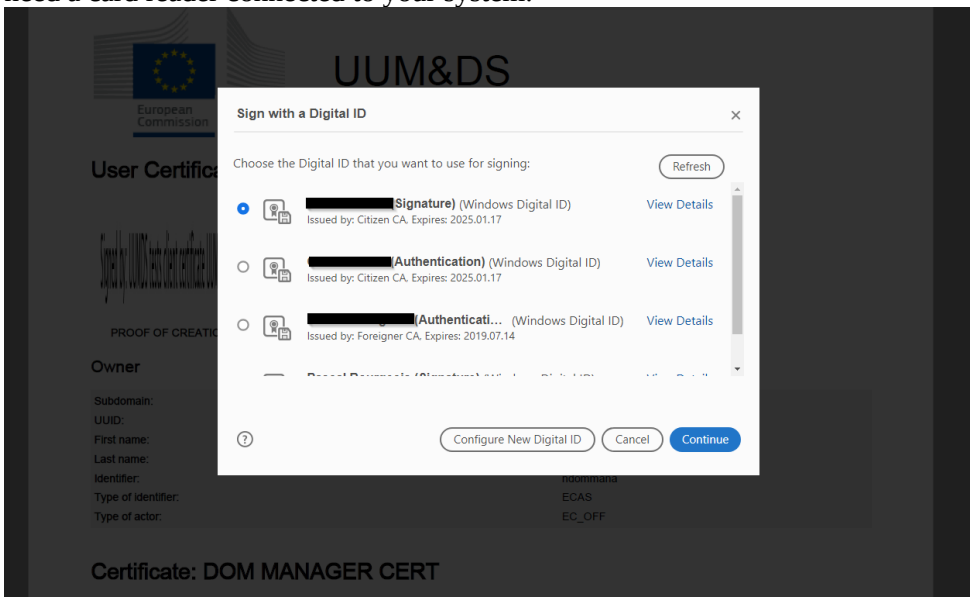
1. **Register Certificate**
    a. **Holder of the key**: An actor registers a certificate for which he is the holder of the private key.
    b. **Not holder of the key**: An actor registers a certificate for which he is not the holder of the private key.
2. **View an Identity Certificate:** An actor can view all his registered certificates and their respective details
3. **Edit an Identity Certificate:** An actor can edit a certificate **only** if it is in DRAFT status
4. **Delete an Identity Certificate:** An actor can delete a certificate only if it is in DRAFT status. Once a certificate is Active, it cannot be deleted, only deactivated.
5. **Activate an Identity Certificate:** An actor should activate a certificate so that he can use it. During activation, validity tests will be performed on the status and time period of the certificate.
6. **Deactivate an Identity Certificate:** An actor can deactivate a registered certificate that is active. The certificate **will not** be deleted from the registry, for historical reasons, but will be unusable. Note that the actor can later reactivate it.
7. **Revoke an Identity Certificate:** A user can revoke a registered certificate. This is possible only if the certificate is in ACTIVE status. **If an actor revokes a certificate this makes the certificate unusable forever**.

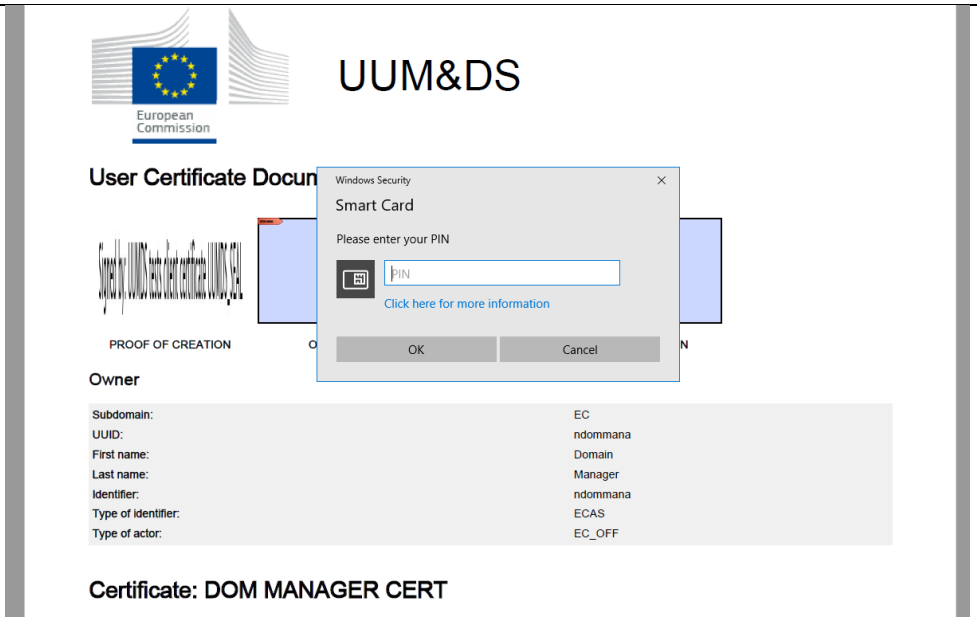
Flow 1: Register an Identity Certificate

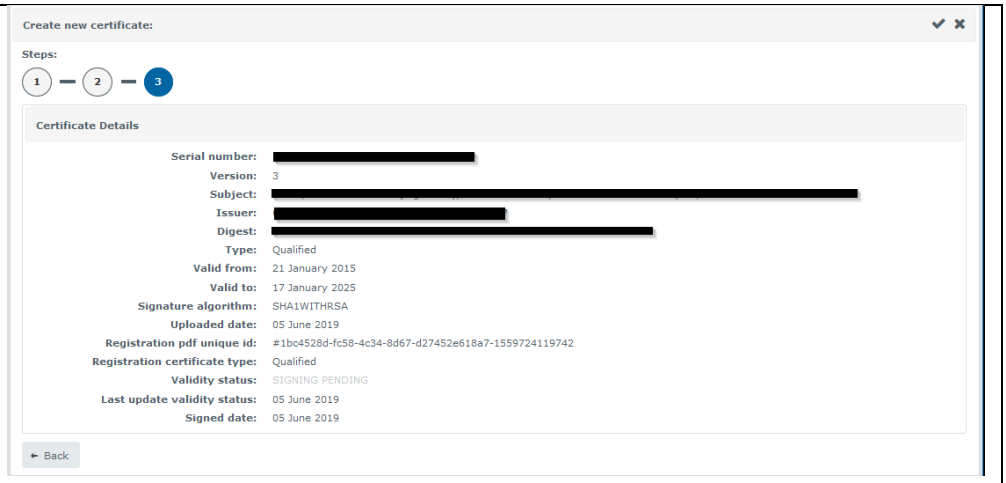
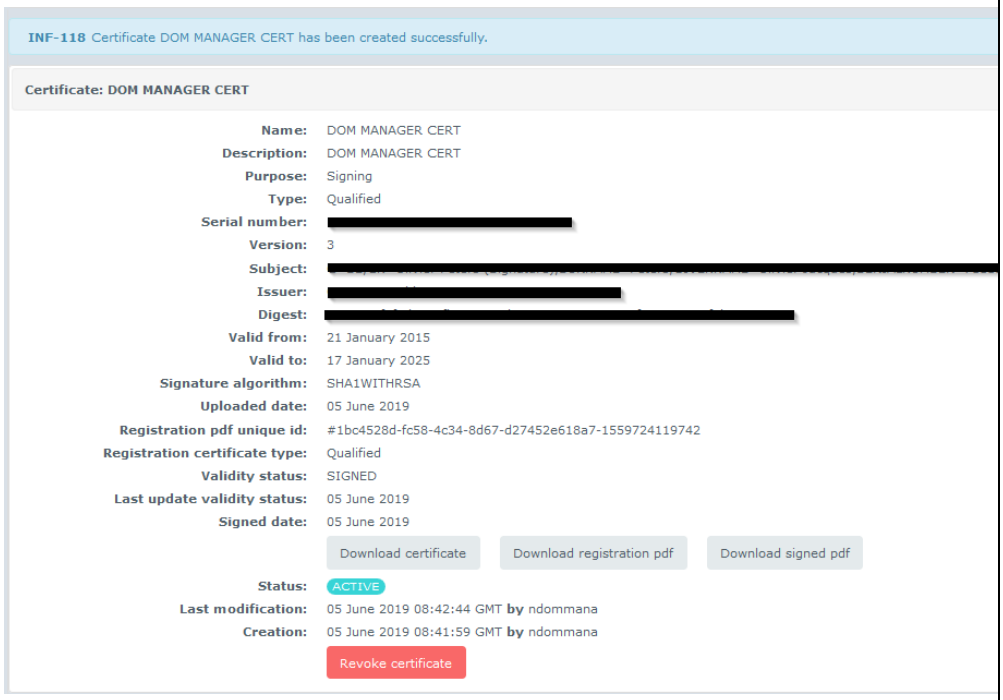
This flow describes the registration of an identity certificate with UUM&DS. It has two sub-flows, the first one when the actor is the holder of the private key and the second one when the actor is not the holder of the private key.

<table>
<tr><th colspan="2">Flow 1a when actor is holder of the private key</th></tr>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>Pre-requisite</td><td>The actor needs to have the Business Profile = BP_MANAGE assigned in UUMDS to his identity</td></tr>
<tr><td>1</td><td>The actor should open a browser and access the following address:
https://customs.ec.europa.eu/taxud/uumds/admin-ext/
He will authenticate by acting on his own behalf.
He needs to have the Business Profile = BP_MANAGE assigned to his identity</td></tr>
<tr><td>2</td><td>Complete the data in the page below (Where Are You From - WAYF) as following
 

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Domain</td><td>Customs is the only selection currently available</td></tr>
<tr><td>Identification Country</td><td>Select your country</td></tr>
<tr><td>Type of actor</td><td>Select your correct type of actor (in this case, Economic operator)</td></tr>
<tr><td>Act on behalf</td><td>Select that you want to act on behalf of Myself</td></tr>
<tr><td>Give your consent</td><td>Tick the box to confirm that you give consent to share your Identity Profile information.</td></tr>
</table>
Press Submit.</td></tr>
<tr><td>3</td><td>In the welcome screen, select View in the left panel under My User Identity.</td></tr>
<tr><td>4</td><td>From the list of user identity certificates click on the + Icon</td></tr>
<tr><td>5</td><td>The certificate creation wizard is displayed to allow entering the certificate info.</td></tr>
</table>

	 Fill in the user certificate details with the certificate's • Name • Description • Purpose - Signature tick the Holder of the key button and click Next
6	The PDF registration document is generated and the sealing is launched. The validity status is '**Sealing pending**'. Once the PDF document sealed, click on 'Download registration PDF' to download the document to sign 
7	Open the document and sign it using your digital ID by clicking in the "OWNER" box and save the signed PDF file. To sign it with your personal PIN code you will need a card reader connected to your system. 

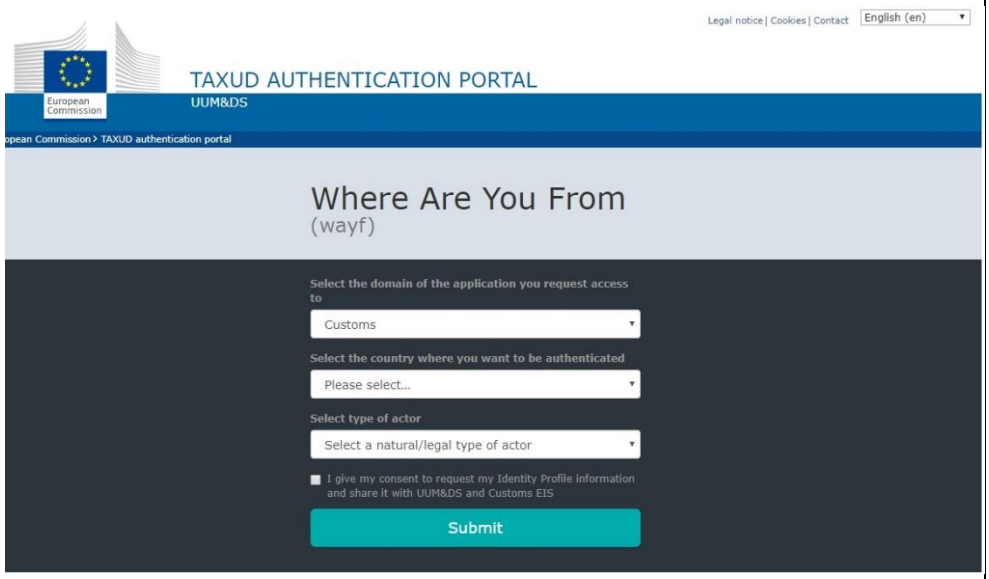
	 
8	Click on 'Upload signed PDF' to upload the signed document just saved at the previous step. Once the signed PDF uploaded, the validity status of the certificate becomes **Signing pending.** This means that the signed document has been sent to be sealed by the EU Sealing Service.

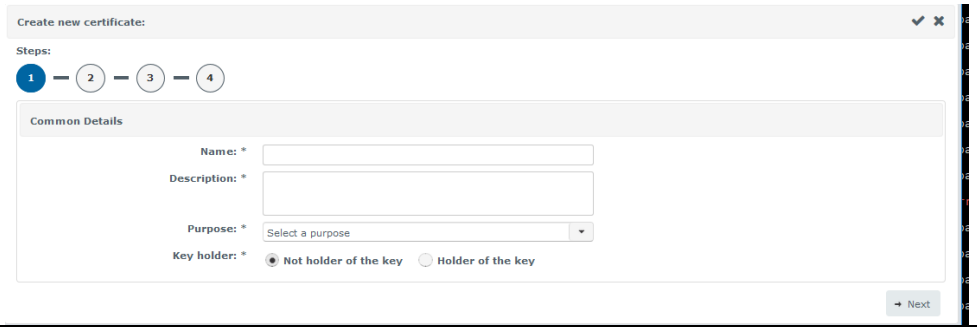
	 The certificate is activated and the details of the certificate are displayed.  At this point, the certificate status becomes **Active**.
End	This concludes the Add an Identity Certificate (Holder of the key) flow.

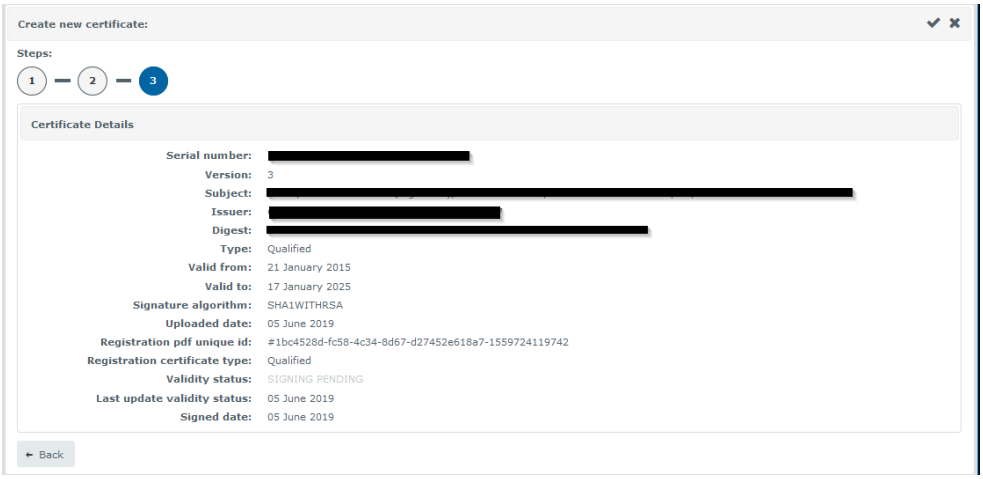
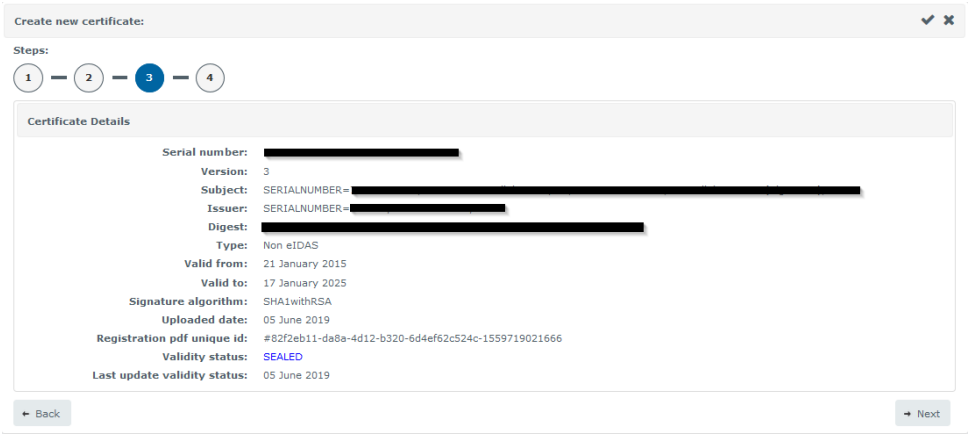
Flow 1b when actor is not holder of the private key without delegation	
Pre-requisites	• The actor has the public key of the certificate he wants to register. • The actor needs to have the Business Profile = **BP_MANAGE** assigned in UUMDS to his identity

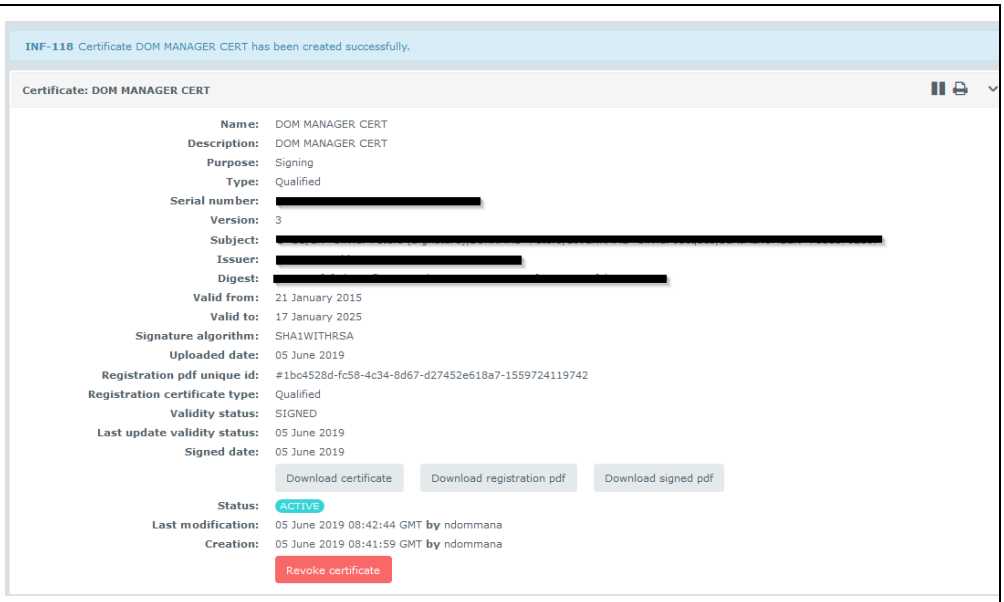
<table>
<tr><td></td><td>

- The actor has already registered his own certificate

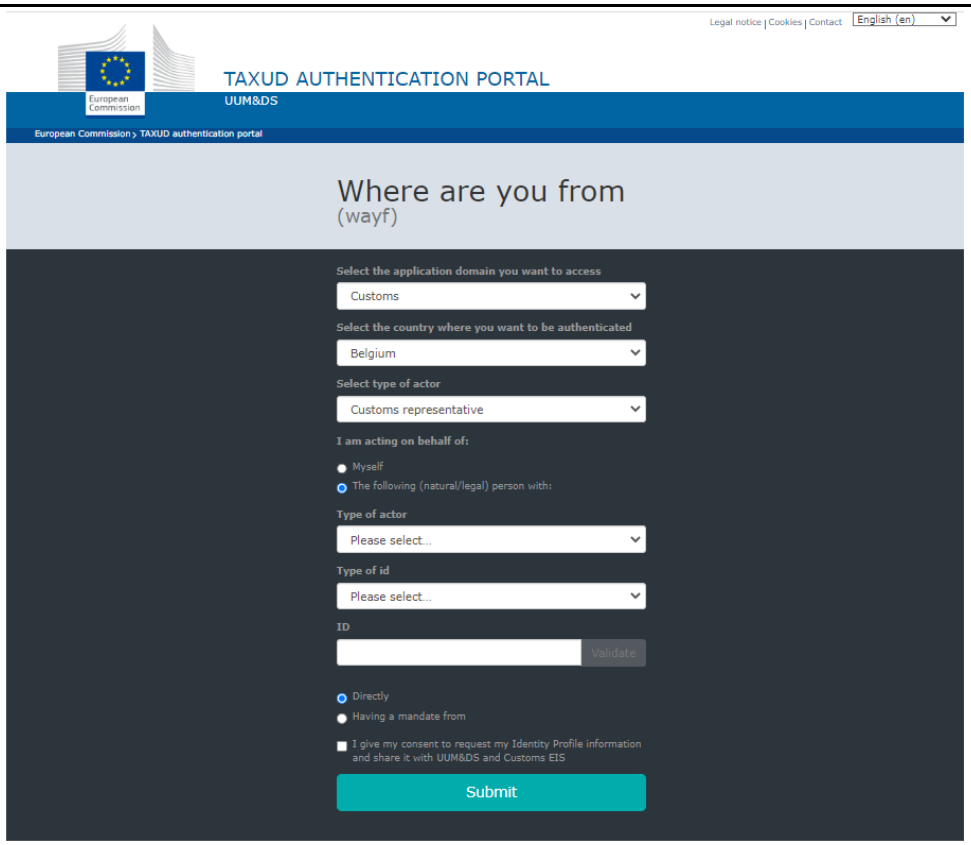
</td></tr>
<tr><td>Step</td><td>Description</td></tr>
<tr><td>1</td><td>The actor should open a browser and access the following address:
https://customs.ec.europa.eu/taxud/uumds/admin-ext/
He logs in to the owner of the certificate account.</td></tr>
<tr><td>2</td><td>Complete the data in the page below (Where Are You From - WAYF) as following
 

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Domain</td><td>Customs is the only selection currently available</td></tr>
<tr><td>Identification Country</td><td>Select your country</td></tr>
<tr><td>Type of actor</td><td>Select your correct type of actor (in this case, Economic operator)</td></tr>
<tr><td>Give your consent</td><td>Tick the box to confirm that you give consent to share your Identity Profile information.</td></tr>
</table>
Press Submit.</td></tr>
<tr><td>3</td><td>In the welcome screen, select View in the left panel under My User Identity.</td></tr>
<tr><td>4</td><td>From the list of user identity certificates click on ‘+’ Icon</td></tr>
<tr><td>5</td><td>The user certificate wizard is displayed to allow retrieving the certificate info.
 
</td></tr>
</table>

	Fill in the user certificate common part with the certificate's • Name • Description • Purpose tick the **Not** Holder of the key button and click Next
6	Click on the **Upload certificate** button; select the certificate from the Open menu and click **Open**
7	An information message is displayed during the verification of the certificate that is currently uploaded; information displayed related to the uploaded certificate and a registration PDF document with a unique id is generated. The sealing is launched and the validity status of the certificate is **'Sealing pending'**;
8	 Once the PDF document sealed, click **Next** button to sign the document. 

	
9	Click on the **Download registration PDF** button to download the document to sign; open the document and sign the document using your digital entity by clicking in the **OWNER** box
10	Follow Step 7 - 8 of Flow 1a
End	This concludes the Add an Identity Certificate (**Not Holder of the key without delegation**) flow.

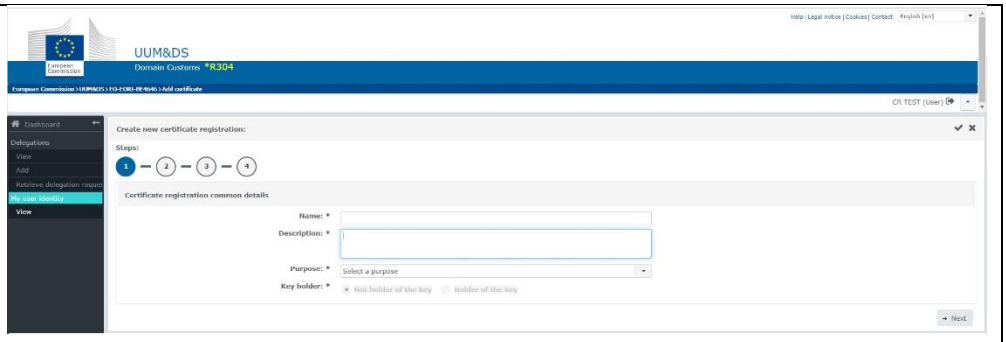
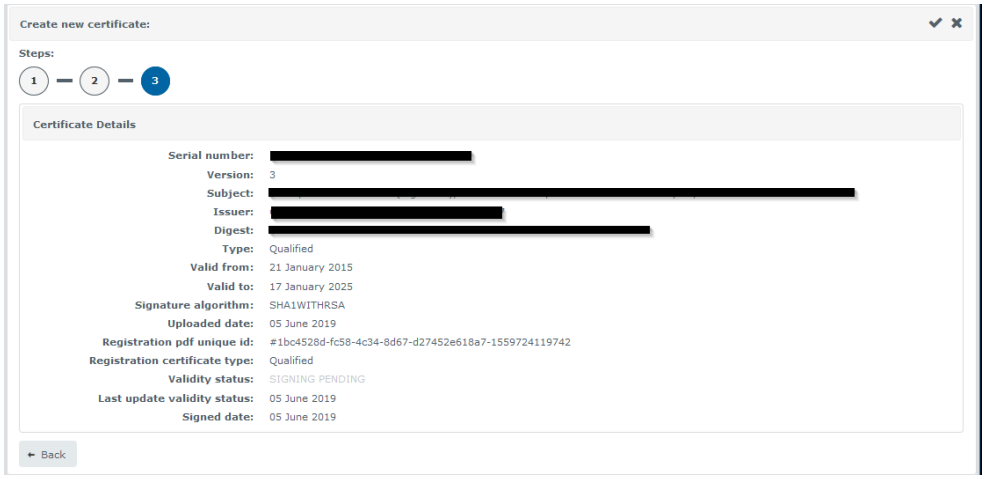
Flow 1c when actor is not holder of the private key using delegation	
Pre-requisites	• The actor has a valid delegation with the entity/company for which he wants to register the certificate • The actor has the public key of the certificate he wants to register. • The actor needs to have the Business Profile = **BP_MANAGE** assigned in UUMDS to his identity • The actor has already registered his own certificate
Step	**Description**
1	The actor should open a browser and access the following address: https://customs.ec.europa.eu/taxud/uumds/admin-ext/ He acts on behalf of the entity/company for which certificate he wants to register the certificate
2	Complete the data in the page below (Where Are You From - WAYF) as following

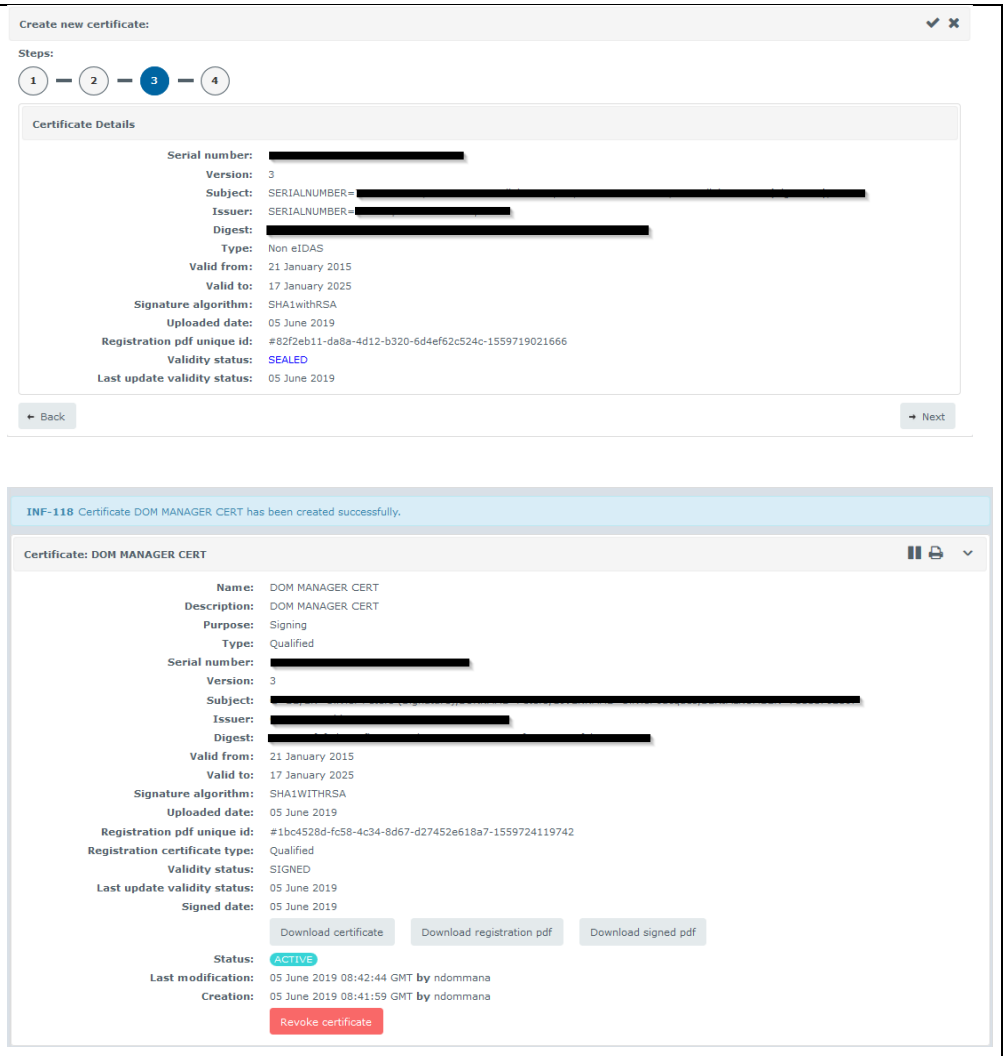


Field	Description
Domain	Customs is the only selection currently available
Identification Country	Select your country
Type of actor	Select your correct type of actor (in this case, Economic operator)
Act on behalf	Select that you want to act on behalf of another entity
Give your consent	Tick the box to confirm that you give consent to share your Identity Profile information.

Press Submit.

3	In the welcome screen, select **View** in the left panel under My User Identity.
4	From the list of user identity certificates click on '+' Icon
5	The user certificate wizard is displayed to allow retrieving the certificate info.

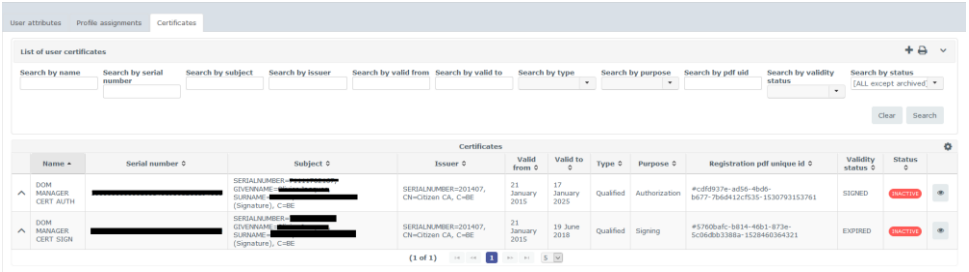
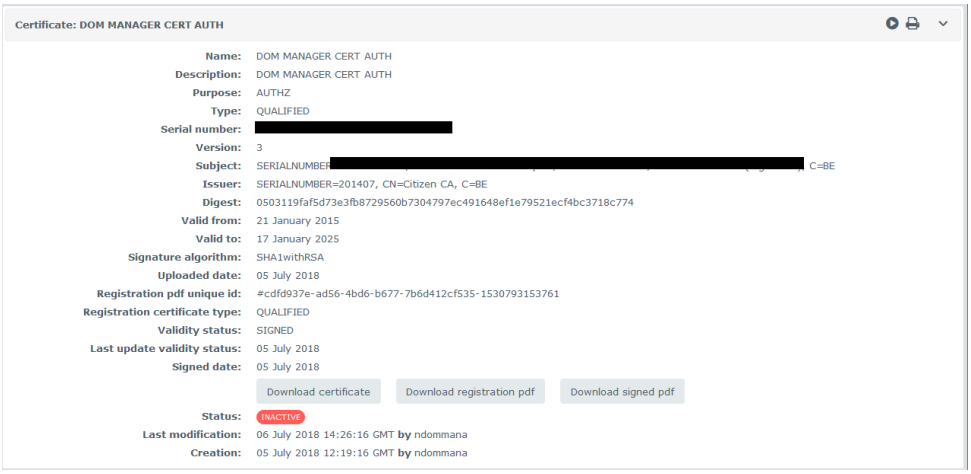
	 Fill in the user certificate common part with the certificate's • Name • Description • Purpose As you can see the options of **Holder if the key** and **Not holder of the key** are greyed out. This is because you act on behalf of an EO and therefore you cannot be the holder of the key. The option **Not holder of the key** is selected by default. Click Next
6	Click on the **Upload certificate** button; select the certificate from the Open menu and click **Open**
7	An information message is displayed during the verification of the certificate that is currently uploaded; information displayed related to the uploaded certificate and a registration PDF document with a unique id is generated. The sealing is launched and the validity status of the certificate is **'Sealing pending'**;
8	 Once the PDF document sealed, click **Next** button to sign the document.

	
9	Click on the **Download registration PDF** button to download the document to sign; open the document and sign the document using your digital entity by clicking in the **OWNER** box
10	Follow Step 7 - 8 of Flow 1a
End	This concludes the Add an Identity Certificate (**Not Holder of the key with delegation**) flow.

Flow 2: View an Identity Certificate

This flow describes how an actor can view his certificate, download it, download the registration PDF created during the upload process, and the signed registration PDF document. (The last button is only available when the signed PDF has been uploaded see **Flow 1a** and **1b** for an explanation on uploading a signed PDF).

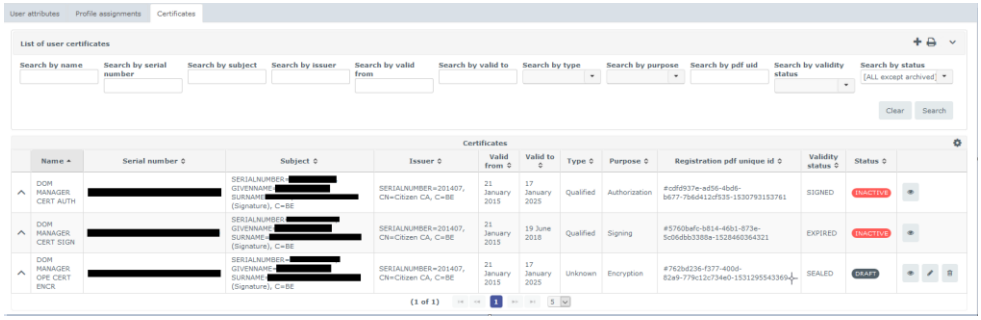
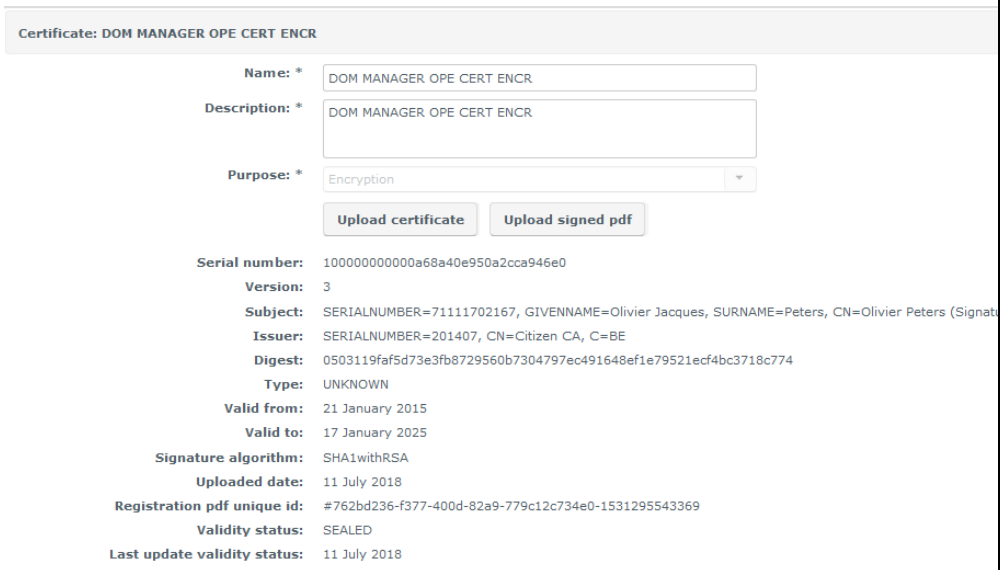
Step	Description
1-2	Follow the **Login Steps** in **Flow 1a**

3	In the welcome screen, select **View** in the left panel under My User Identity.
4	From the list of user identity certificates click on the eye Icon on the right. 
5	The selected registered certificate details are displayed with the following buttons to download:  • The certificate; • The registration PDF document generated during the certificate upload; • The registration PDF document signed. This button is available only after the signed PDF is uploaded see Flow 1a steps 7 and 8 for explanation on uploading signed PDF.
End	This concludes the View an Identity Certificate flow.

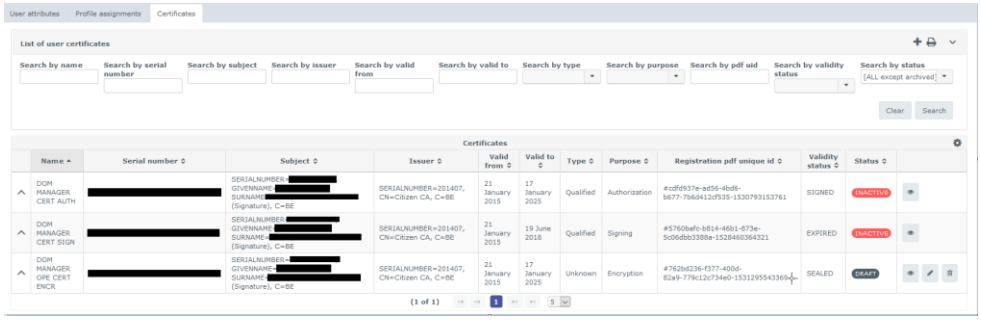
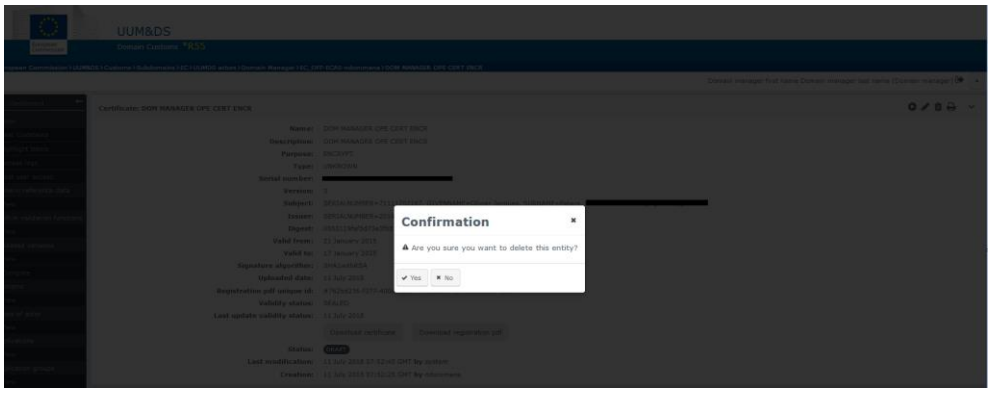
Flow 3: Edit an Identity Certificate

This flow describes how an actor can edit a certificate. Please note that this option is **only** available if the certificate is in DRAFT status.
You can modify the name, description and the certificate for the selected registration.

Step	Description

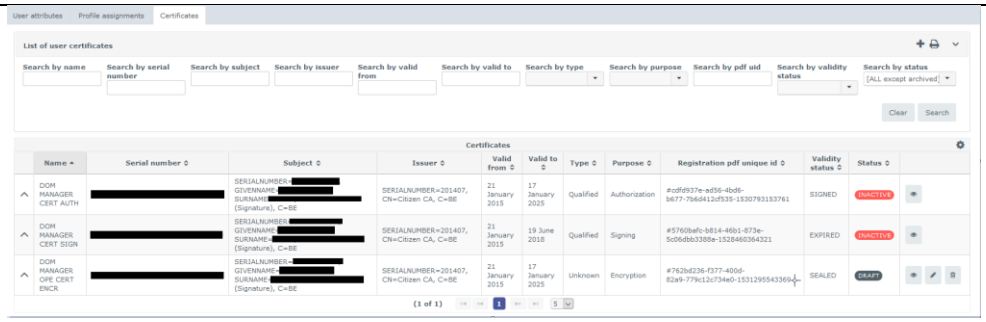
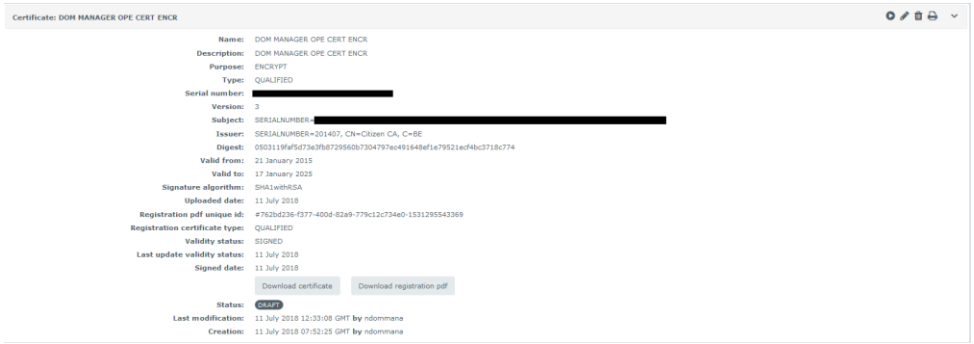
1-2	Follow the **Login Steps** in **Flow 1a**
3	In the welcome screen, select **View** in the left panel under My User Identity.
4	From the list of user identity certificates select the one you want to edit and click on the pen Icon located on the right 
5	The following elements can be modified : Name, Description and Certificate  • Name should be unique • Certificate can be updated by clicking on the Upload certificate button and follow steps 6 – 8 of Flow 1a. • An information message is displayed during the verification of the signed registration PDF document that is currently uploaded
End	This concludes the Edit an Identity Certificate flow.

Flow 4: Delete an Identity Certificate	This flow describes how an actor can delete a certificate. A user certificate can be deleted **only** while it is in DRAFT status. Indeed, a certificate that has been active at some point **cannot** be deleted; it stays in the system to keep the historical record and enable tracing its usage during its life cycle.

Step	Description
1-2	Follow the **Login Steps** in **Flow 1a**
3	In the welcome screen, select **Delete** in the left panel under My User Identity.
4	From the list of user identity certificates select the one you want to delete and click on the trash Icon on the right. 
5	Click on Yes to confirm deletion. 
End	This concludes the Delete an Identity Certificate flow.

Flow 5: Activate / Reactivate an Identity Certificate	This flow describes how to activate a certificate. To use a certificate, you have to activate it. During activation the validity status and validity period of the certificate are checked. A certificate that has been deactivated can also be reactivated, so that it can be used again for the specific purpose (Authorisation, Signing, etc…). The reactivation is only possible if a certificate is in INACTIVE status

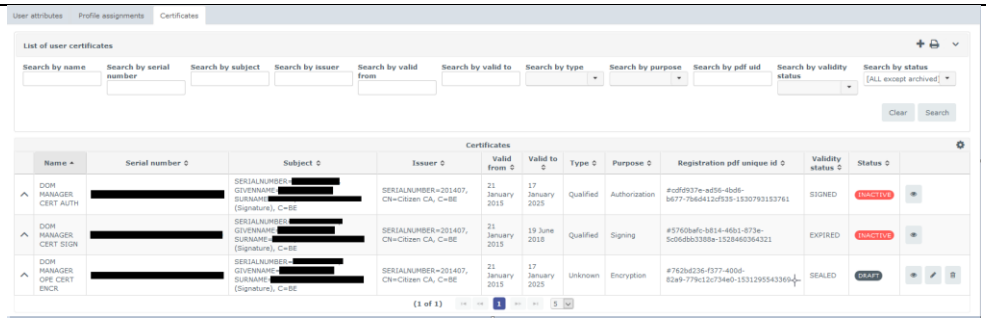
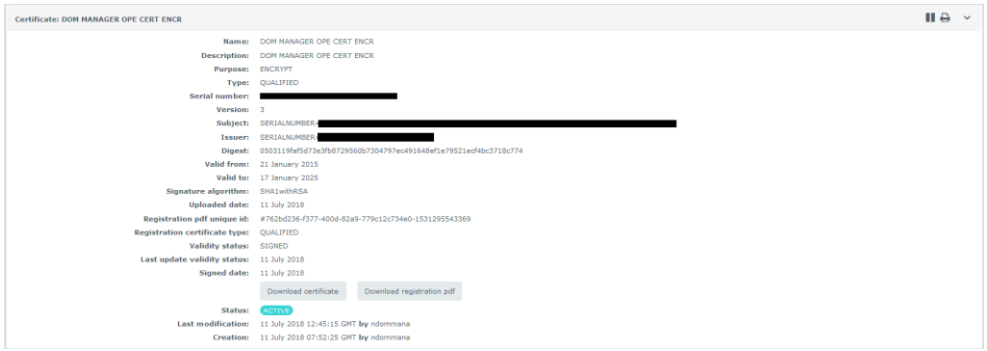
Step	Description
1-2	Follow the **Login Steps** in **Flow 1a**
3	In the welcome screen, select **View** in the left panel under My User Identity.
4	From the list of user identity certificates select the one you want to activate and click on the eye Icon on the right.

	
5	The selected registered certificate details are displayed. Click on the arrow icon (top right) to activate the certificate and set its status to ACTIVE.  The following buttons are available also • Download the certificate; • Download the registration PDF document generated during the certificate upload;
End	This concludes the Activate an Identity Certificate flow.

Flow 6: Deactivate an Identity Certificate

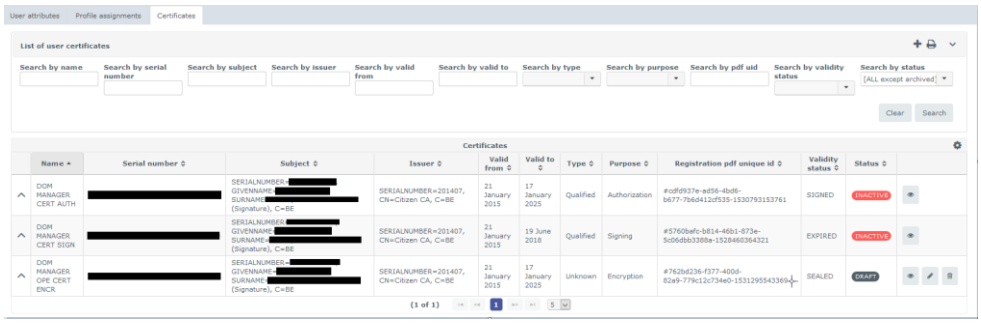
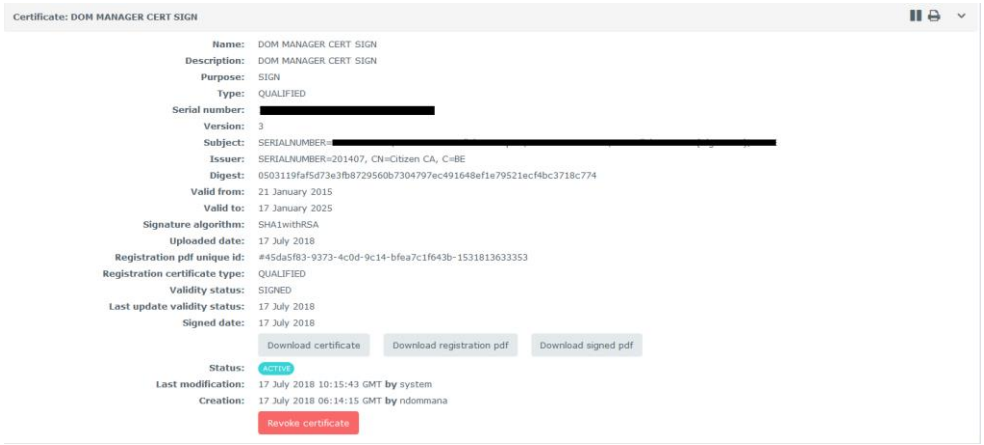
This flow describes how an actor can disable temporarily a user certificate to prevent using its usage for the purpose (Authorisation, Signing, etc…). An actor can deactivate a certificate **only** if it is in ACTIVE status.

Step	Description
1-2	Follow the **Login Steps** in **Flow 1a**
3	In the welcome screen, select **View** in the left panel under My User Identity.
4	From the list of user identity certificates select the one you want to deactivate and click on the eye Icon on the right,

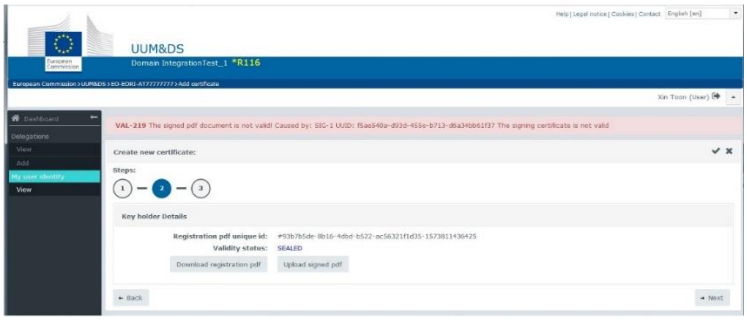
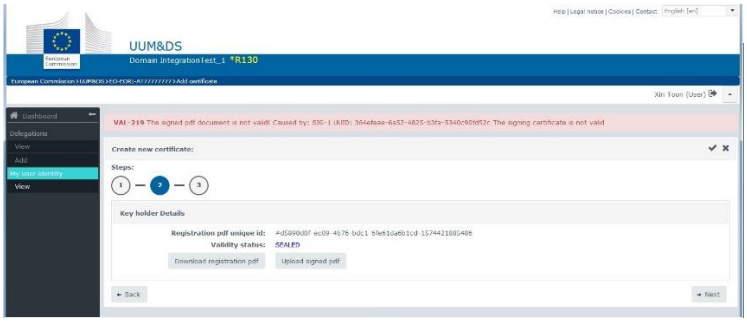
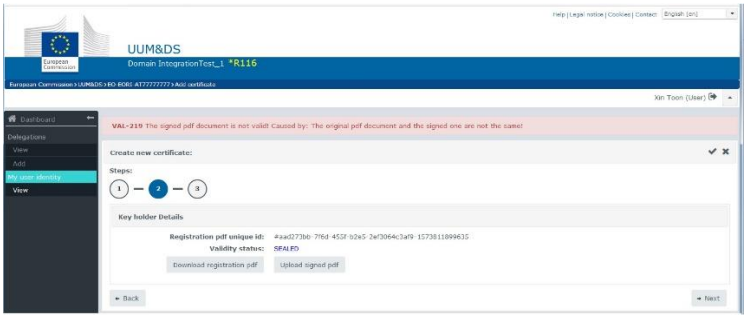
	
5	The selected registered certificate details are displayed. Click on the pause icon (top right) ⏸ to deactivate the certificate and set the certificate status to INACTIVE.  The following buttons are available also • Download the certificate; • Download the registration PDF document generated during the certificate upload;
End	This concludes the Deactivate an Identity Certificate flow.

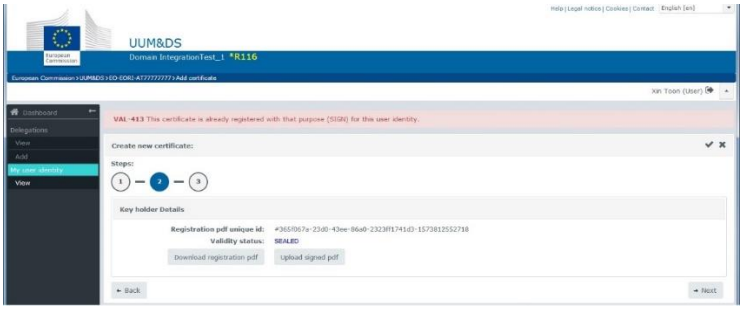
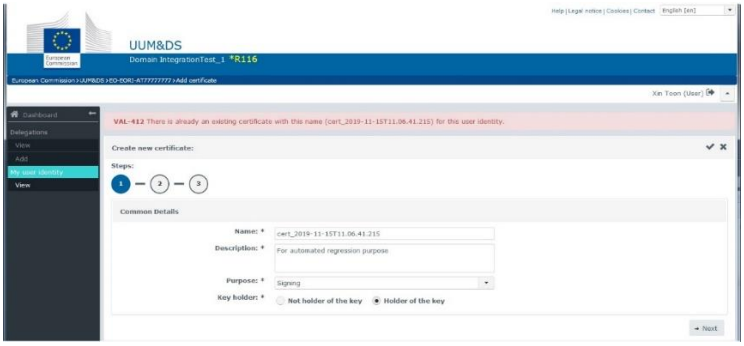
Flow 7: Revoke an Identity Certificate	This flow describes how an actor can revoke a user certificate to prevent using this certificate for a purpose (Authorisation, Signing, etc…). The revocation is **only** possible on a certificate in ACTIVE status. **A revoked user certificate cannot be used anymore, it is unusable forever.** If you need to suspend the usage of a certificate, but be able to use it again later, please use the Deactivate an Identity Certificate flow.

Step	Description
1-2	Follow the **Login Steps** in **Flow 1a**
3	In the welcome screen, select **View** in the left panel under My User Identity.

4	From the list of user identity certificates select the one you want to reactivate and click on the eye Icon on the right. 
5	The selected registered certificate details are displayed. Click on the Revoke button (bottom centre) to reactivate the certificate and set its status to REVOKED.  The following buttons are available also to download • the certificate; • the registration PDF document generated during the certificate upload; • the registration PDF document signed.
End	This concludes the Revoke an Identity Certificate flow.

What can go wrong?

Anomaly Type	Display behaviour	What to do?
The certificate is not trusted or not valid	If the certificate • is not issued by a trusted CA (member of the LOTL or member of the UUM&DS Customs Alternate List) or • the date is outside the validity period of the certificate (earlier than the start valid or later than the end valid date) the following error page is displayed 	Obtain a certificate from a CA that is a member in the LOTL or in the UUMDS Customs Alternate List.
The certificate used for signing is not the same as the one used to register.	UUM&DS detects that the signing certificate is not the same that the one previously uploaded for this registration and the following screen is displayed. 	Please sign the PDF with the same certificate you are in the process of registering.
The registration PDF has been altered or is not corresponding to the original one.	UUM&DS detects that the uploaded document has been altered or does not correspond to the original registration and the following screen is displayed. 	Please use the original PDF you have downloaded for signing without alterations.

Duplicate registration.	UUM&DS detects that the certificate is a. already registered in UUM&DS or b. the identity and purpose used for the registration are the same with an already registered certificate. One of the following screens is displayed Screen for error a.  Screen for error b  	For case a, please use a different certificate. For case b, either use a different certificate or register the certificate for a different purpose.

In case you need assistance National Service Desks

In case you need assistance, please contact your National Service Desk. You can find contact details for all Member States in the table below.

Contact information of National Service Desks (NSD) for UUM&DS and Trader Portal						
Code	**Country**	**e-Mail**	**Main Phone number**	**Fax (optional)**	**Business Days**	**Business Hours (CET)**
AT	Austria	info@usp.gv.at	+43 502 337 33	N/A	Monday – Thursday Friday	08:00 – 16:00 08:00 – 14:30
BE	Belgium	servicedesk.pub@minfin.fed.be	+32(0)257 636 36	N/A	Monday – Sunday	00:00 – 24:00
BG	Bulgaria	servicedesk@customs.bg	+359 298 594 980	N/A	Monday – Friday	08:00 – 16:30
CY	Cyprus	helpdesk.cyprus@customs.mof.gov.cy	+357 226 018 63 +357 226 018 68 +357 226 018 88	+357 226 027 67	Monday – Friday	07:30 – 16:00
CZ	Czech	ecrhelpdesk@cs.mfcr.cz	+420 261 331 998 +420 724 013 014	N/A	Monday – Friday Monday – Sunday	07:00 – 15:30 00:00 – 24:00
DE	Germany	servicedesk@itzbund.de	+49 692 097 154 5	N/A	Monday – Sunday	00:00 – 24:00
DK	Denmark	servicedesk@skat.dk	+45 701 573 01	N/A	Monday – Friday	08:00 – 17:00
EE	Estonia	tolliinfo@emta.ee	+37 288 008 14	N/A	Monday – Thursday	07:30 – 15:30

					Friday	07:30 – 14:30
ES	Spain	proced.simpli.adu@correo.aeat.es	N/A	N/A		09:00 – 15:00
FI	Finland	cd@tulli.fi	+358 295 5200	N/A	Monday – Friday	06:00 – 14:15
FR	France	fr-nsd-uumds@douane.finances.gouv.fr	+33 157 534 291	N/A	Monday – Friday	09:00 – 18:00
GR	Greece	uumds.helpdesk@aade.gr	+30 210 480 249 6	+30 210 480 244 6	Monday – Friday	06:30 – 15:00
HR	Croatia	helpdesk@carina.hr	+385 165 118 88	+385 165 118 89	Monday – Sunday	00:00 – 24:00
HU	Hungary	init_rsz_vfeft_o@nav.gov.hu	+36 147 041 95	N/A	Monday – Thursday	08:00 – 16:30
IE	Ireland	ecustoms@revenue.ie	+353 1 738 3677	+353 676 33 97	Monday – Friday	10:00 – 18:00
IT	Italy	dogane.helpdesk.eu@agenziadogane.it	N/A	N/A	Monday – Friday	09:00 – 15:00
LT	Lithuania	helpdesk@lrmuitine.lt	+370 523 623 02	+370 523 623 38	Monday – Sunday	00:00 – 24:00
LU	Luxembourg	cds@do.etat.lu	N/A	N/A	Monday – Sunday	08:30 – 17:00
LV	Latvia	CDMS.help@vid.gov.lv	+371 671 208 69 +371 671 208 77	N/A	Monday – Friday	08:00 – 16:00
MT	Malta	compsec.customs@gov.mt	+ 356 25 992 777	N/A	Monday – Sunday	08:00 – 17:00
NL	Netherlands	BCA.UDO.EU@belastingdienst.nl	+31 88 156 66 55	N/A	Monday – Friday	07:00 – 17:00
PL	Poland	helpdesk-eclo@mf.gov.pl https://puesc.gov.pl/web/puesc/helpdesk-sc	+48 33 483 20 55	N/A	Monday – Friday	08:00 – 16:00

PT	Portugal	pt-uumdscd-nsd@at.gov.pt	N/A	N/A	Monday – Friday	10:00 – 18:30
RO	Romania	ro_nsdcd@customs.ro	N/A	N/A	Monday – Thursday Friday	07:30 – 16:00 07:30 – 13:30
SE	Sweden	it-support@tullverket.se	+46 771 520 520	N/A	Monday – Friday	08:00 – 16:30
SI	Slovenia	sd.fu@gov.si	+386 5 297 68 00	+386 5 297 67 64	Monday – Friday	08:00 – 18:00
SK	Slovakia	https://www.financnasprava.sk/sk/kontakt/ako-s-nami-komunikovat	+421 48 4317 222	N/A	Monday – Sunday	00:00 – 24:00
UK	United Kingdom	admin.uum@hmrc.gsi.gov.uk	+44 3000 528005	N/A	Monday – Friday	08:00 – 14:00

Appendix 1 – Registration flow and status chart

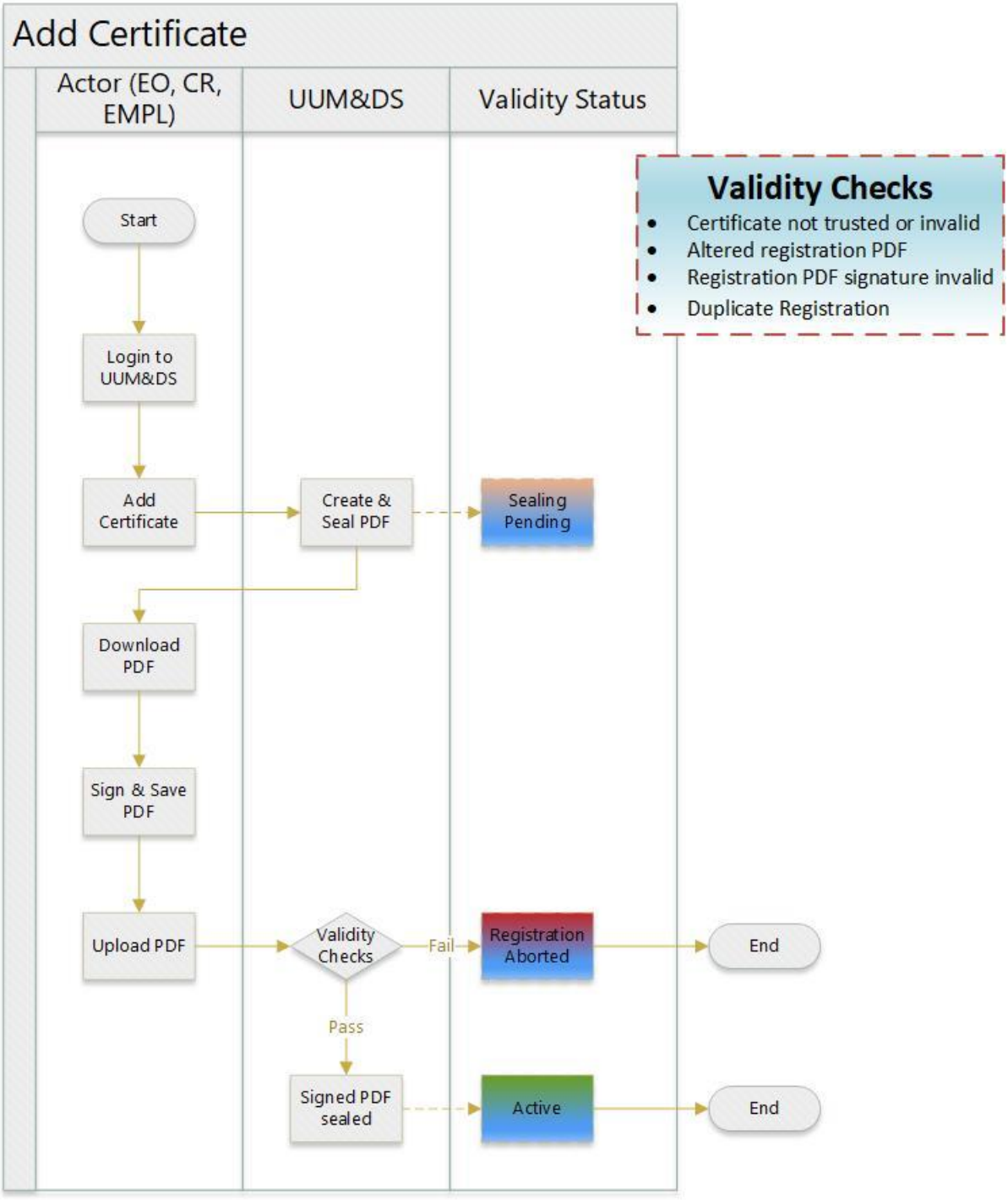
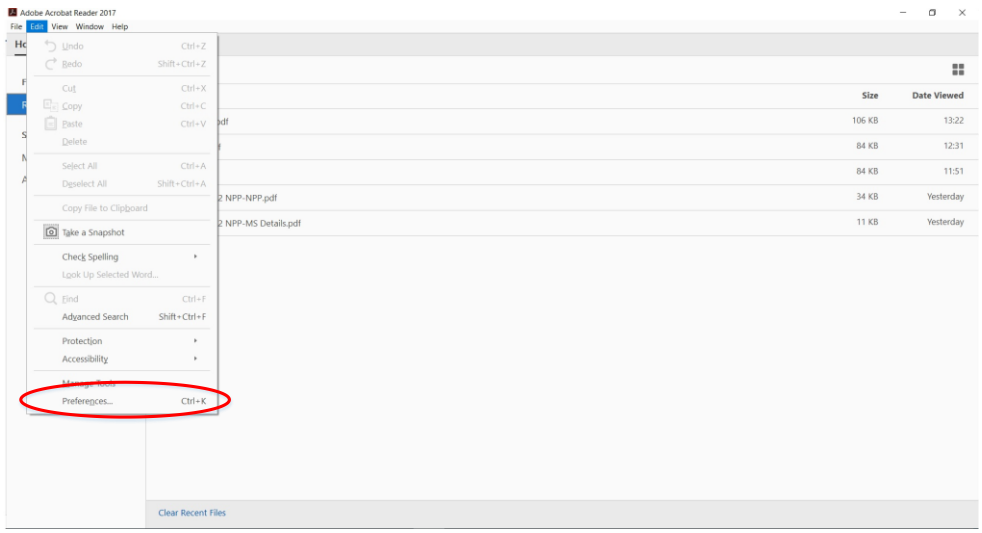
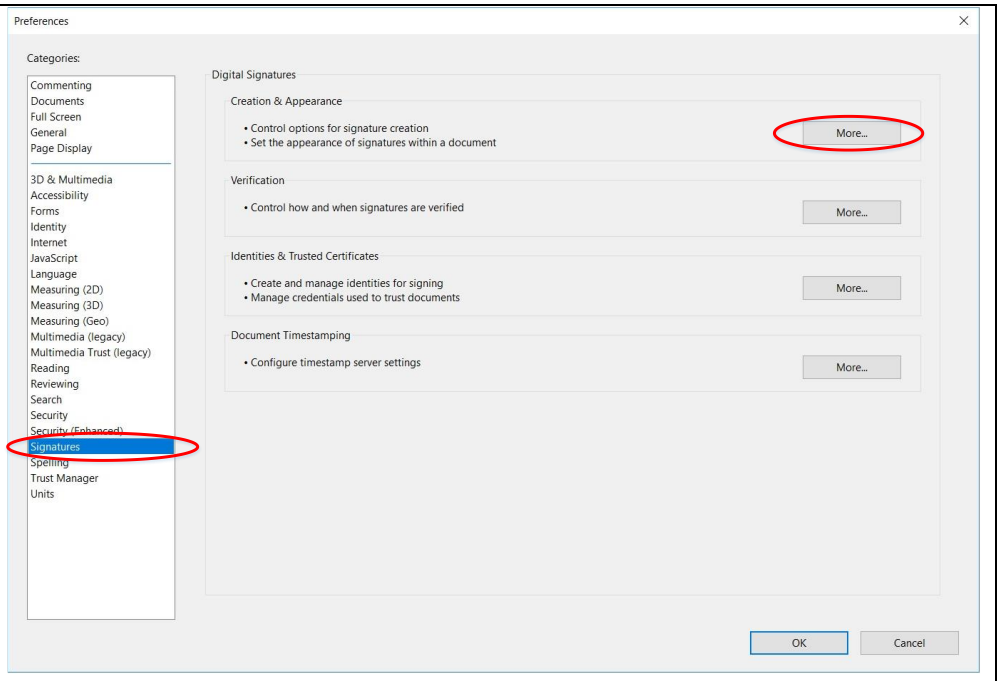


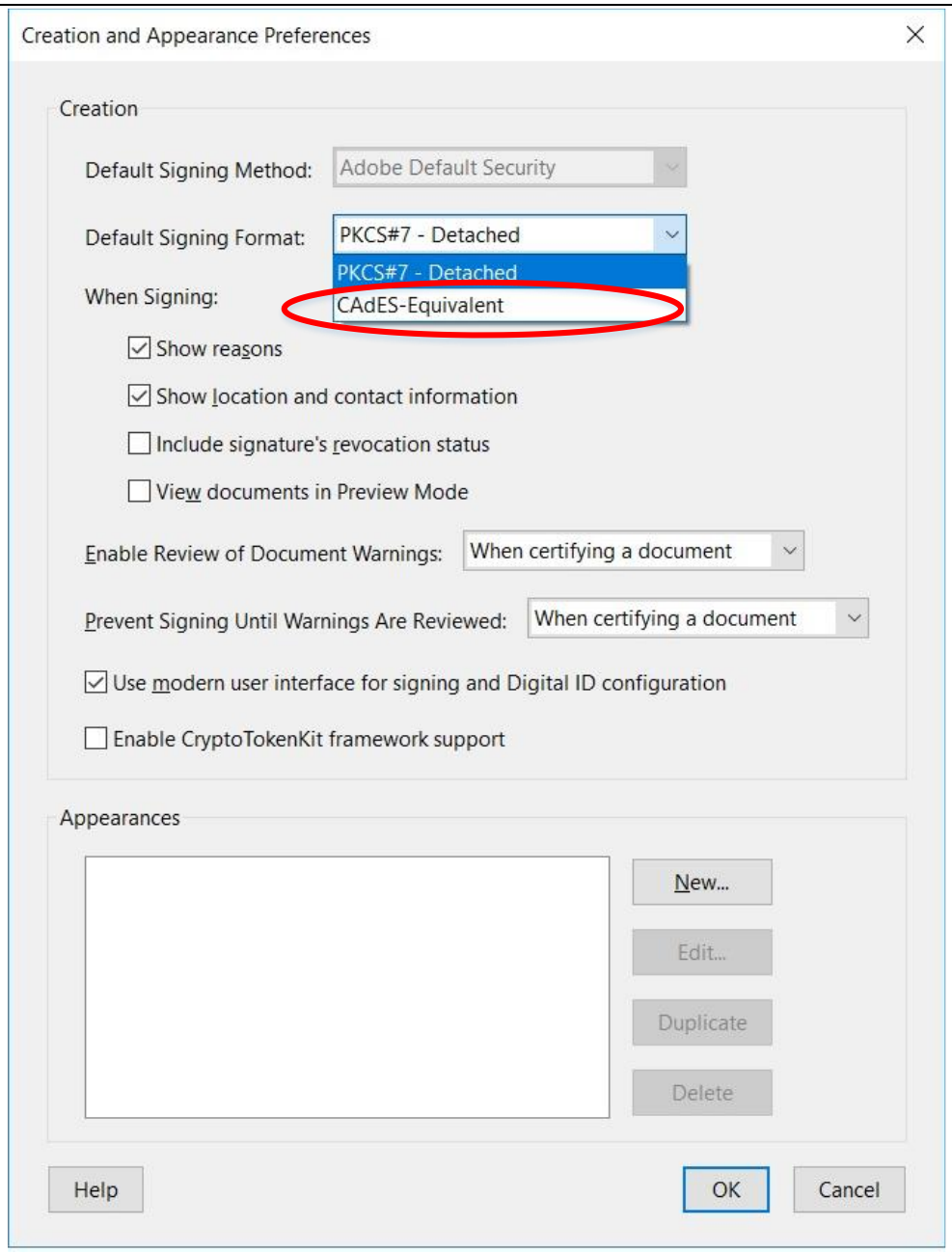
Figure 1 Add Certificate process

Appendix 2 – Adobe Acrobat setup

If you are going to use Adobe Acrobat during the certificate registration, please follow this setup before you start.

Step	Description
1	Open Adobe Acrobat Reader.
2	Click Edit → Preferences as below 
3	In the Preferences tab that appears, please click on Signatures in the left panel and then More at the Creation & Appearance part of the page.

	
4	At the Default Signing Format drop-down menu, please select CAdES-Equivalent and click OK.

	
5	Click OK at the Preferences screen.
End	The Adobe Acrobat Reader setup is complete

END OF DOCUMENT