ACER
Agency for the Cooperation of Energy Regulators

REMIT

Agency's REMIT Information System User Manual

For Obtaining ARIS Digital Certificates

Version 1.0

15 January 2019

Agency for the Cooperation of Energy Regulators
Trg republike 3
1000 Ljubljana, Slovenia

Version history

Version	Effective Date
AGENCY'S REMIT INFORMATION SYSTEM USER MANUAL for Obtaining ARIS Digital Certificates Version 1.0	15 January 2019

ACER
Agency for the Cooperation of Energy Regulators

Table of Contents

1 Introduction 5
1.1 Scope and Purpose 5
1.2 Target audience 5
1.3 Glossary 6
1.4 Structure of the document 6
2 Steps for requesting and revoking an ARIS client certificate 7
2.1 Application form to request a certificate 7
2.2 Steps for a client certificate request 10
2.3 Workflow for a client certificate retrieval 17
2.4 Rejection message 21
2.5 Expiration message 21
2.6 Importing the certificate into the Windows certificate store 22
2.7 Importing the certificate into Mozilla Firefox 26
2.8 Importing the certificate into Chrome 29
2.9 Steps for a client certificate revocation 31
3 ARIS machine-to-machine certificate request 35
3.1 Steps for a machine-to-machine certificate request 35
3.2 Steps for a machine-to-machine certificate retrieval 43
3.3 Steps for a machine-to-machine certificate revocation 45

List of Figures

Figure 1: Form for requesting an ARIS User digital certificate for the production environment 8
Figure 2: Form for requesting an ARIS User digital certificate for the test environment 9
Figure 3: Starting page for requesting a certificate for the production environment 10
Figure 4: Starting page for requesting a certificate for the test environment 10
Figure 5: Request page 13
Figure 6: Informative message for successful upload of file 14
Figure 7: Counter increase after uploading files 14
Figure 8: Error message when uploading a file not aligned with requirements 14
Figure 9: Maximum files reached message 15
Figure 10: Edge, Chrome and Firefox process for inserting and saving private key 15
Figure 11: Final step for requesting process of client certificate 16
Figure 12: Rejection message in case of additional request 16
Figure 13: Automatic e-mail after ACER acceptance 17
Figure 14: Accept and retrieve certificate 17
Figure 15: Changed my mind and revocation option 18
Figure 16: Changed my mind and revocation message 18
Figure 17: Changed my mind automatic e-mail 18
Figure 18: Unlock private key in Microsoft Edge, Mozilla Firefox and Google Chrome 19
Figure 19: Download certificate and private key 19
Figure 20: Retrieval of certificate in P12 file and additional options 20
Figure 21: E-mail on successful issuance of client digital certificate 20
Figure 22: Starting page link to the revocation process of client digital certificate 31
Figure 23: Starting page and machine-to-machine selection 36
Figure 24: Initial page in order to insert the details for the machine (Certificate Name) 37
Figure 25: Generate CSR selection 38
Figure 26: Export private key and password insertion for protecting the private key 39
Figure 27: Save the private key 39
Figure 28: Save the private key (workaround for IE) 40
Figure 29: Form upload for machine-to-machine 41
Figure 30: Request for machine-to-machine certificate 42
Figure 31: Request submitted information screen 42
Figure 32: Error message when uploading a file not aligned with requirements 42
Figure 33: Get my certificate e-mail confirmation 43
Figure 34: Certificate retrieval 43
Figure 35: Confirmation e-mail for machine-to-machine certificate 44
Figure 36: Starting page for machine-to-machine revocation 45
Figure 37: Revocation details 46

1 Introduction

1.1 Scope and Purpose

The purpose of this document is to describe the steps that authorised ARIS users must follow in order to request and revoke user and machine-to-machine certificates.

The Certification Authority (CA) which provides the certificates trusted by ARIS is HARICA. The certificates that were issued by the previously used Certification Authority PostarCA and are already enabled in ARIS will remain trusted until they expire or are revoked.

In order to become an authorised user and be able to request a certificate, the domain of the belonging entity should be whitelisted and approved. If you receive an error indicating you are not authorised to request a client or machine-to-machine certificate, please contact the ARIS Central Service Desk (CSD) via servicedesk@support.acer-remit.eu and request to have your organisation (entity) whitelisted.

The presented steps demonstrate the process of issuing certificates from the end-user perspective for both client and machine-to-machine certificates, which are needed to connect to the ARIS Production environment and Test environment.

A user can request only one client certificate per name, surname and email address. A user can request many machine-to-machine certificates with the proviso that he/she has already installed a valid HARICA client certificate.

If a user does not receive any information regarding the rejection or approval of their request within three working days of successfully submitting a request for either a user (client) or machine-to-machine certificate, the user should contact the CSD.

The existing ARIS users with a valid PostarCA certificate do not need to request a HARICA client certificate unless they want to request a new HARICA machine-to-machine certificate or their PostarCA certificate has expired, is about to expire or has been revoked.

1.2 Target audience

The document is intended for ARIS users, i.e. NRA, RRM and ACER staff. This includes entities that want to initiate the RRM registration process to become RRMs.

1.3 Glossary

ACER, Agency – Agency for Cooperation of Energy Regulators

ARIS – Agency's REMIT Information System

CA – Certification Authority

CSD – ARIS Central Service Desk (email address: servicedesk@support.acer-remit.eu)

NRA – National Regulatory Authority

PKI – Public Key Infrastructure

RRM – Registered Reporting Mechanism

1.4 Structure of the document

The document is structured as follows:

1. **Section 2**: Presents the steps for requesting and revoking a client (also referred to as user) certificate. In addition, the process of importing into Windows and specific browsers is described.

2. **Section 3**: Presents the steps for requesting and revoking a machine-to-machine certificate.

2 Steps for requesting and revoking an ARIS client certificate

2.1 Application form to request a certificate

Before initiating a client certificate request, a user should download the required form, available at https://documents.acer-remit.eu/category/remit-reporting-user-package/ within the section *Digital certificate form for physical users*[1]. Depending on the environment that the user intends to use, there are two different application forms: one for the production environment and one for the test environment.

The application form requests specific information divided into two categories. The first part is the data of the legal entity to which the applicant belongs, while the second part pertains to the certificate holder data. The user will upload the form at a later stage of the process, which will enable ACER to validate the eligibility of the request.

Apart from indicating the information that the user should provide, the forms also inform the applicant of the legal statement and the legal basis under which the offered PKI solution issues certificates. Within the links presented, the obligations of the user, the respective regulatory framework and the data retention policy of the service provider can be found.

The application form for the production environment is depicted below (Figure 1), while the respective form for the test environment can be seen underneath (Figure 2):

[1] For machine-to-machine certificates please refer to the section *Digital certificate Form for machine-machine communications*.

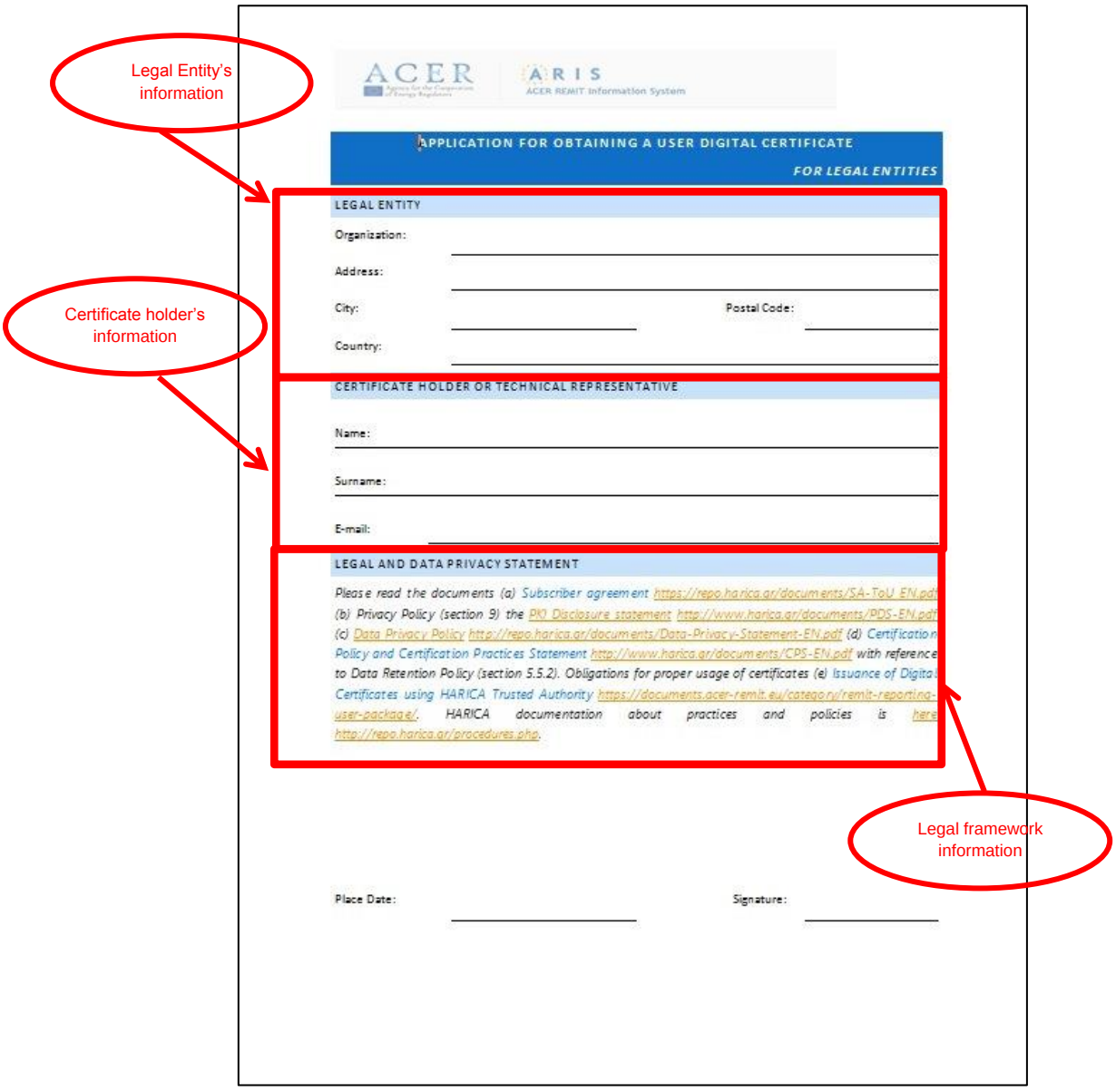
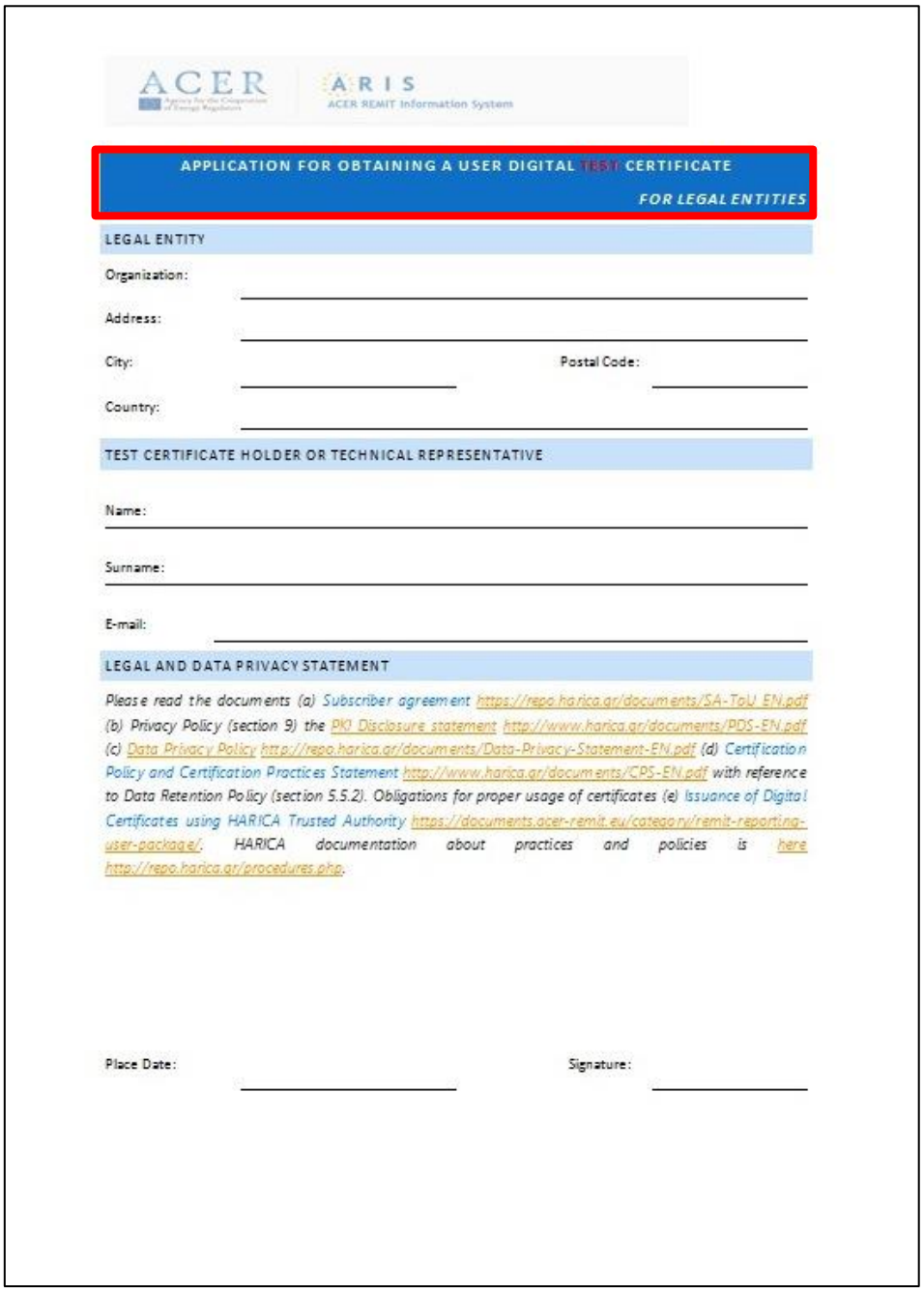


Figure 1: Form for requesting an ARIS User digital certificate for the production environment



ACER ARIS
ACER REMIT Information System

APPLICATION FOR OBTAINING A USER DIGITAL TEST CERTIFICATE
FOR LEGAL ENTITIES

LEGAL ENTITY

Organization: _____

Address: _____

City: _____ Postal Code: _____

Country: _____

TEST CERTIFICATE HOLDER OR TECHNICAL REPRESENTATIVE

Name: _____

Surname: _____

E-mail: _____

LEGAL AND DATA PRIVACY STATEMENT

Please read the documents (a) Subscriber agreement https://repo.harica.gr/documents/SA-ToU_EN.pdf (b) Privacy Policy (section 9) the PKI Disclosure statement http://www.harica.gr/documents/PDS-EN.pdf (c) Data Privacy Policy http://repo.harica.gr/documents/Data-Privacy-Statement-EN.pdf (d) Certification Policy and Certification Practices Statement http://www.harica.gr/documents/CPS-EN.pdf with reference to Data Retention Policy (section 5.5.2). Obligations for proper usage of certificates (e) Issuance of Digital Certificates using HARICA Trusted Authority https://documents.acer-remit.eu/category/remit-reporting-user-package/. HARICA documentation about practices and policies is here http://repo.harica.gr/procedures.php.

Place Date: _____ Signature: _____

Figure 2: Form for requesting an ARIS User digital certificate for the TEST environment

2.2 Steps for a client certificate request

A. For the production environment visit https://www.acer-remit.eu/certificates and select the link under the client (user) certificates tab (Figure 3).

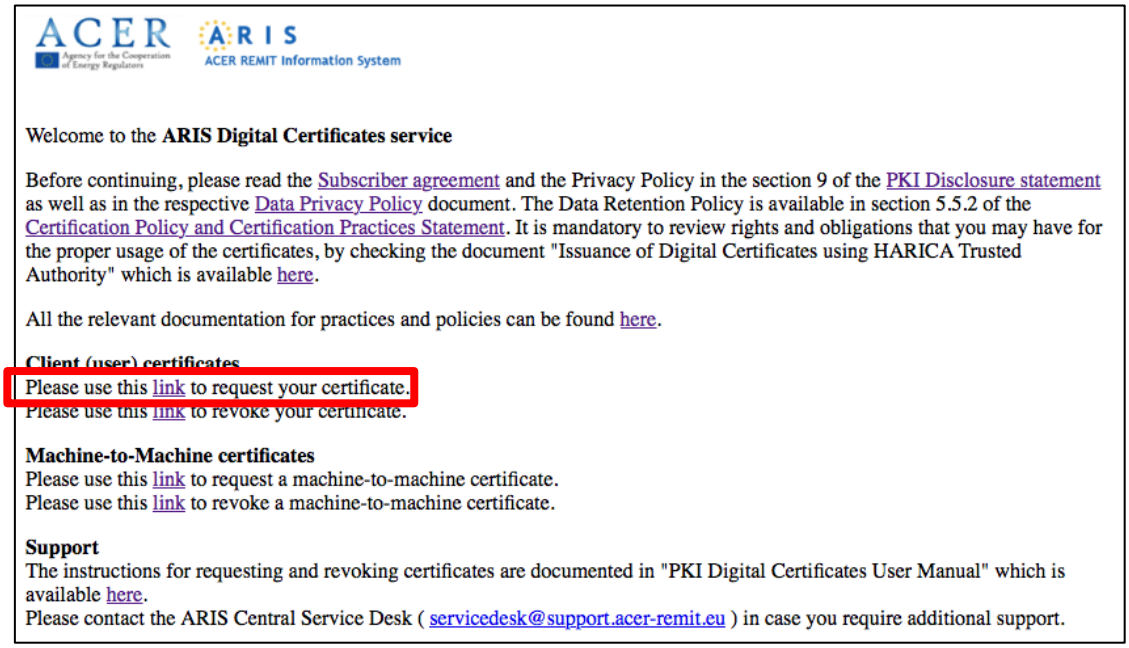


Figure 3: Starting page for requesting a certificate for the production environment

B. For the test environment visit https://pilot.test-acer-remit.eu/certificates and select the link under the client (user) certificates tab (Figure 4).

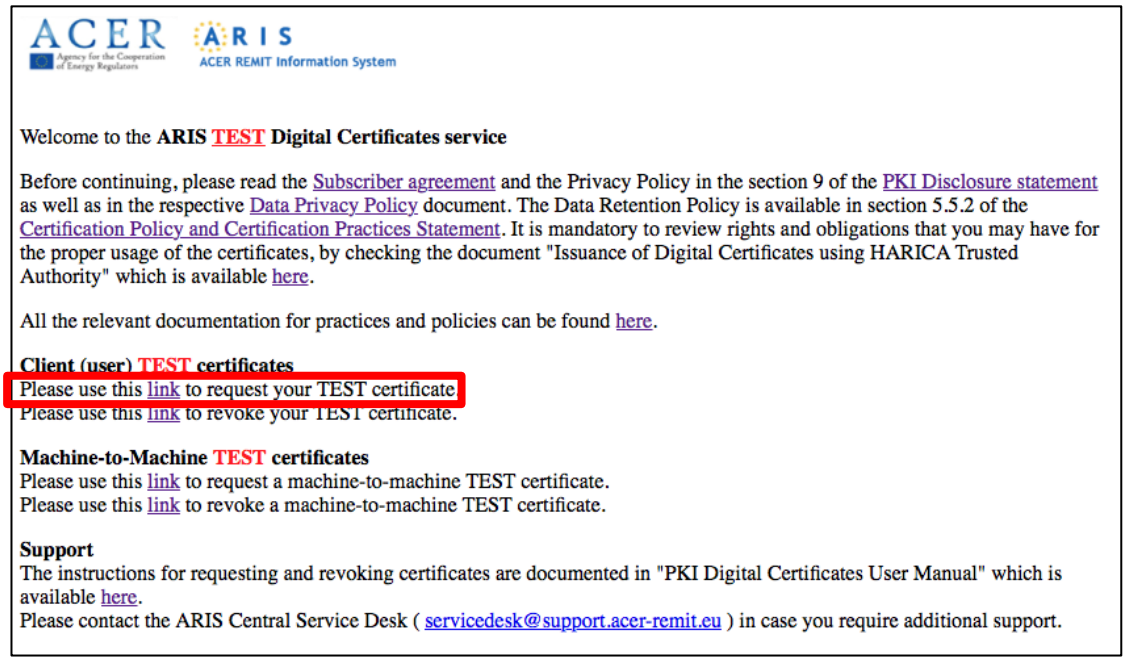


Figure 4: Starting page for requesting a certificate for the test environment

Important notice:

You are kindly requested to use the same internet browser on the same computer where you would like to install the certificate throughout the whole process.

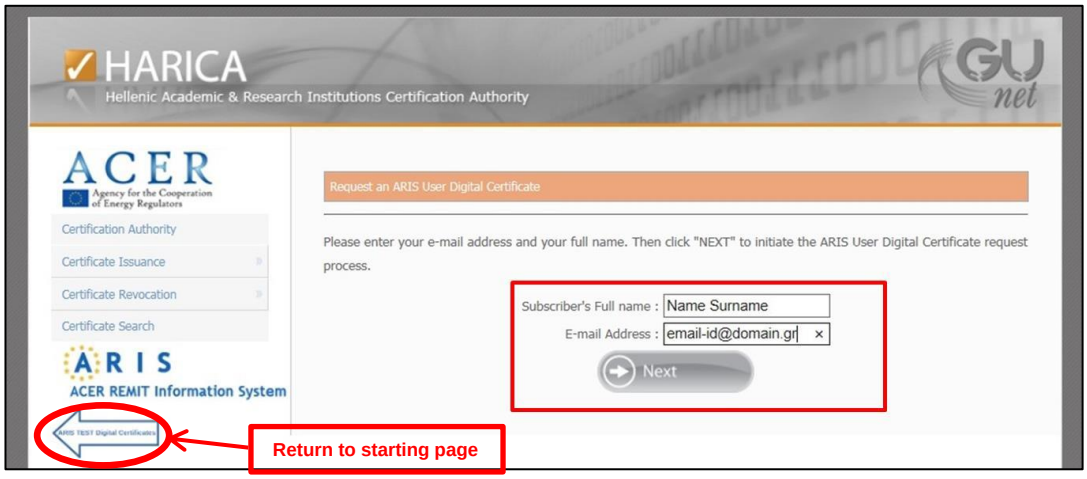
The procedure for obtaining production and test certificates is essentially the same, which is why only the flow for production certificates is presented in this manual.

ONLY FOR TEST CERTIFICATES: In order for the client computer to consider the test certificates as trusted, the test root CA certificate has to be manually installed as a 'Trusted Root Certification Authority' certificate. The test root CA certificate can be obtained from this link:

https://www.dev.harica.gr/certs/StagingHaricaRootCA2015.der

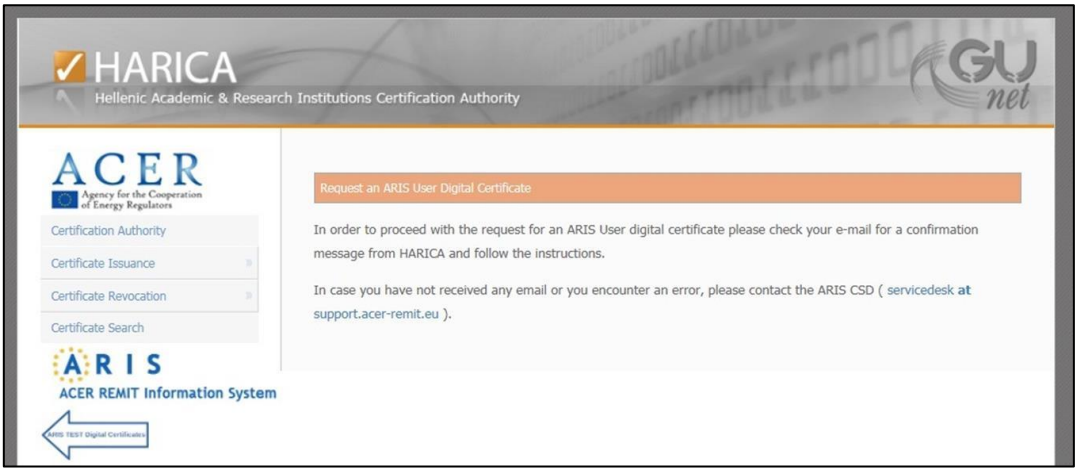
Please note that on some computers specific user privileges may be required to install the test root CA certificate.

Step 1 : Enter your full name (as indicated on your national ID/Passport) and your email address. The provided domain within your email must be authorised and whitelisted for requesting a certificate for ARIS. Press **Next**.



You can always return to the initial page by selecting **ARIS Digital Certificates** or **ARIS TEST Digital Certificates**.

Step 2 : The following message will appear on the screen. You will receive an email. Please check your email and confirm the validity of your email address by clicking on **Request Confirmation Link**.



Dear Sir/Madam,

Please follow the link below in order to continue with your request.

- Request Confirmation Link

If you did not initiate the request for an ARIS User digital certificate please report this to the ARIS CSD (servicedesk@support.acer-remit.eu).

Please do not reply to this e-mail. In case of any questions please contact the ARIS CSD (servicedesk@support.acer-remit.eu)

HARICA Public Key Infrastructure

Step 3 : Upload a digital copy of your national ID/ Passport as well as the required form and then press **Request**. The form is available here: https://documents.acer-remit.eu/category/remit-reporting-user-package/. See also Section 2.1 of this manual.
Within this step, as depicted in Figure 5, the client is informed about the proper and accepted format/type of document to upload, as well as on the accepted size and resolution of the uploaded data. A notice is included, containing the following text:

Please click 'Browse' to upload a scan (in 1 or multiple files) of your official photo ID for Identity validation (Passport/ID) and the filled in APPLICATION FOR OBTAINING A USER TEST DIGITAL CERTIFICATE. Scanned documents must have a resolution of at least 400x400px and must not exceed 2MB in size. The ID must clearly display the full name (in Latin) and the picture of the Applicant. IDs that do not display the full name in Latin will not be accepted and the request will be denied.
Note: Uploading a valid photo ID scan and a correctly filled form is **mandatory** in order to request a certificate.

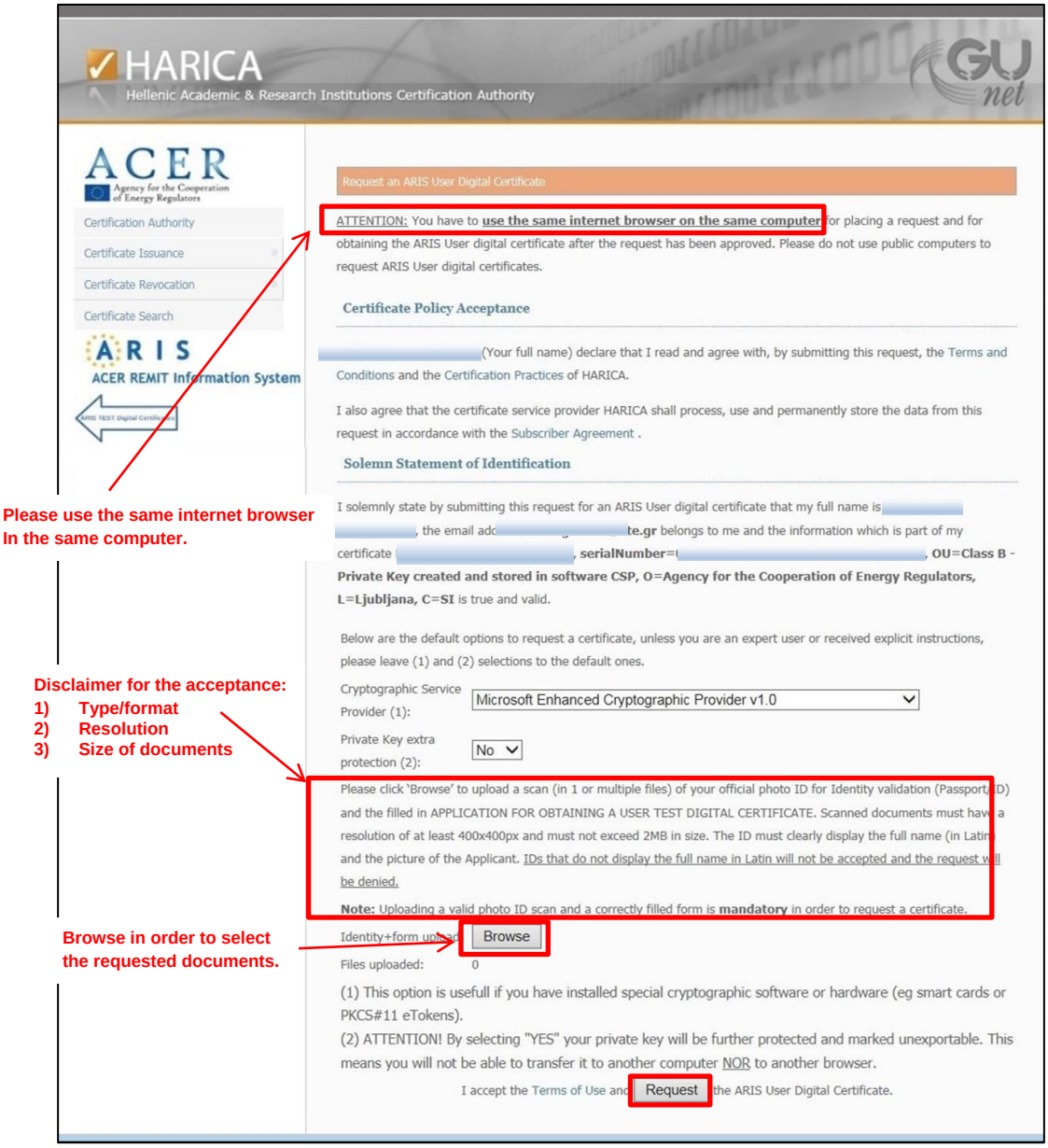


Figure 5: Request page

To upload a file you should click on **Browse**. If the upload was successful, the following window will pop up (Figure 6).

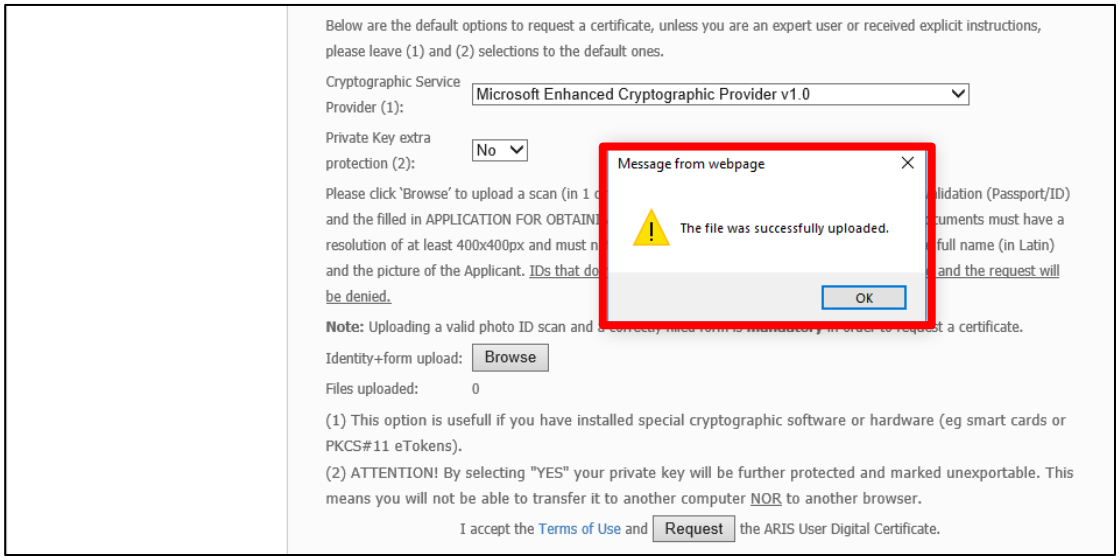


Figure 6: Informative message for successful upload of file

After pressing **OK**, the counter will be increased as depicted below (Figure 7).

Figure 7: Counter increase after uploading files

In case the user tries to upload a file that does not comply with the requirements (regarding resolution or size), the following pop-up window will appear (Figure 8).

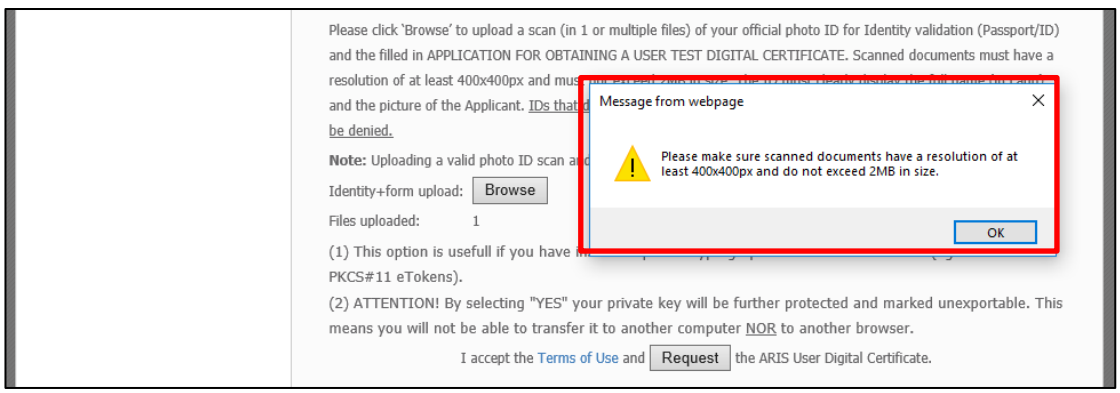


Figure 8: Error message when uploading a file not aligned with requirements

In order to upload another file, you can click on **Browse** again and select a second file. You will be informed of the number of uploaded files. Press **Request** when you wish to proceed to the next step.

Important notice:

The maximum number of files that a client can upload is four (4). Trying to upload a fifth (5) file will result in the error message, as depicted in Figure 9.

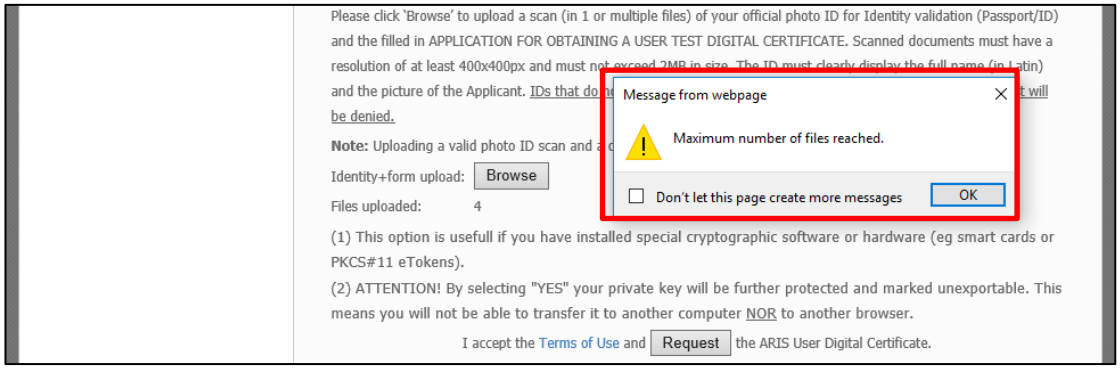


Figure 9: Maximum files reached message

Alternatively, a single zip file containing all the required files can be uploaded.

Important notice:

If you are using Internet explorer, you will be automatically directed to Step 6. If you are using Microsoft Edge, Google Chrome or Mozilla Firefox, you will be directed to Step 5 before completing the process and proceeding to Step 6. Step 5 is the generation of the private key for the certificate.

Step 4 : You will be prompted to enter a password to protect your certificate's private key. Confirm the password and press **Save private key** (Figure 10).

Figure 10: Edge, Chrome and Firefox process for inserting and saving private key

Step 5 : At this point, ACER will check the provided information and approve or deny the issuing of a certificate for ARIS (Figure 11).

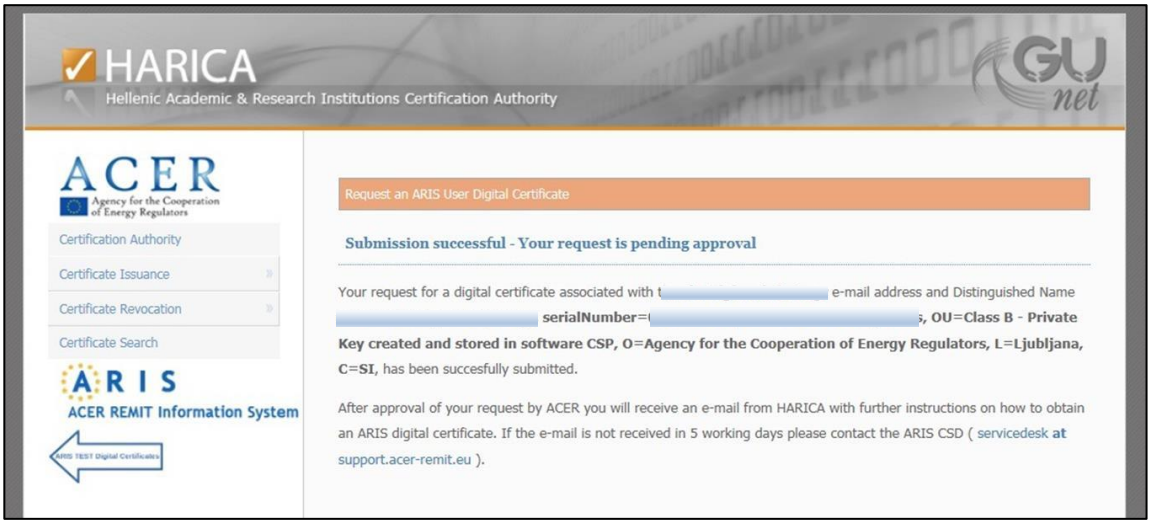


Figure 11: Final step for requesting process of client certificate

If the user requesting a certificate is already in possession of a valid HARICA certificate or has another request already pending validation, the following message will be shown and the request will be rejected. In order to request a new certificate while the old one is still active, the user should first revoke the old certificate and only then proceed with the new request.

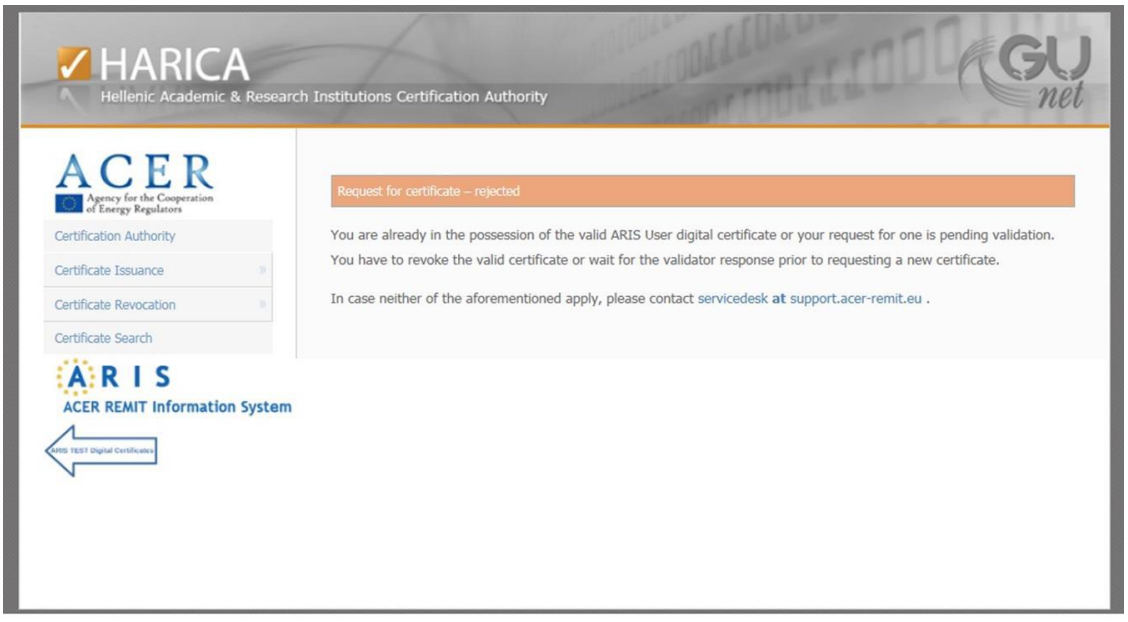
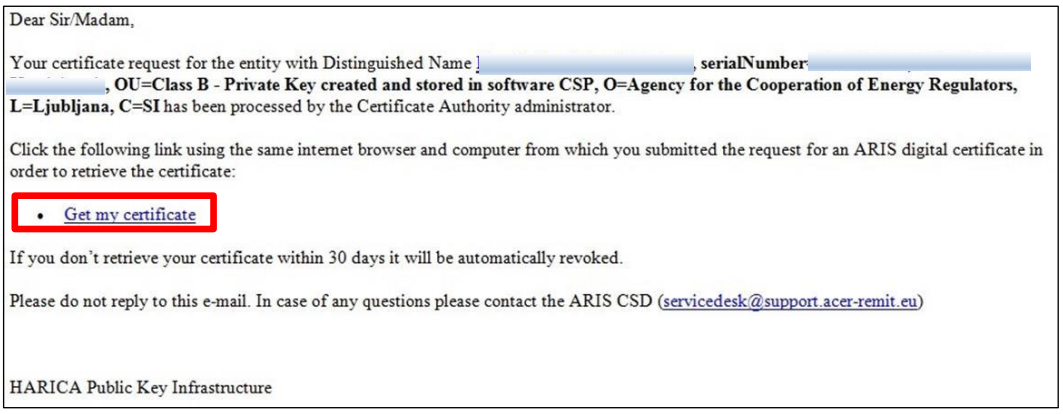


Figure 12: Rejection message in case of additional request

2.3 Workflow for a client certificate retrieval

This section describes the steps for certificate retrieval following the approval of ACER. In case there is a rejection from ACER, the user will be shown the screen that is presented in Section 2.4.

Step 1. After the approval of your request, you will receive an email in order to proceed with the certificate retrieval. Click on **Get my certificate**.



Dear Sir/Madam,

Your certificate request for the entity with Distinguished Name [redacted], **serialNumber**[redacted], **OU=Class B - Private Key created and stored in software CSP, O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI** has been processed by the Certificate Authority administrator.

Click the following link using the same internet browser and computer from which you submitted the request for an ARIS digital certificate in order to retrieve the certificate:

- Get my certificate

If you don't retrieve your certificate within 30 days it will be automatically revoked.

Please do not reply to this e-mail. In case of any questions please contact the ARIS CSD (servicedesk@support.acer-remit.eu)

HARICA Public Key Infrastructure

Figure 13: Automatic e-mail after ACER's acceptance

Step 2. At this stage you have two options. Select:

A. I accept and want to retrieve my certificate link (Figure 14) if you want to proceed and retrieve your certificate**.**

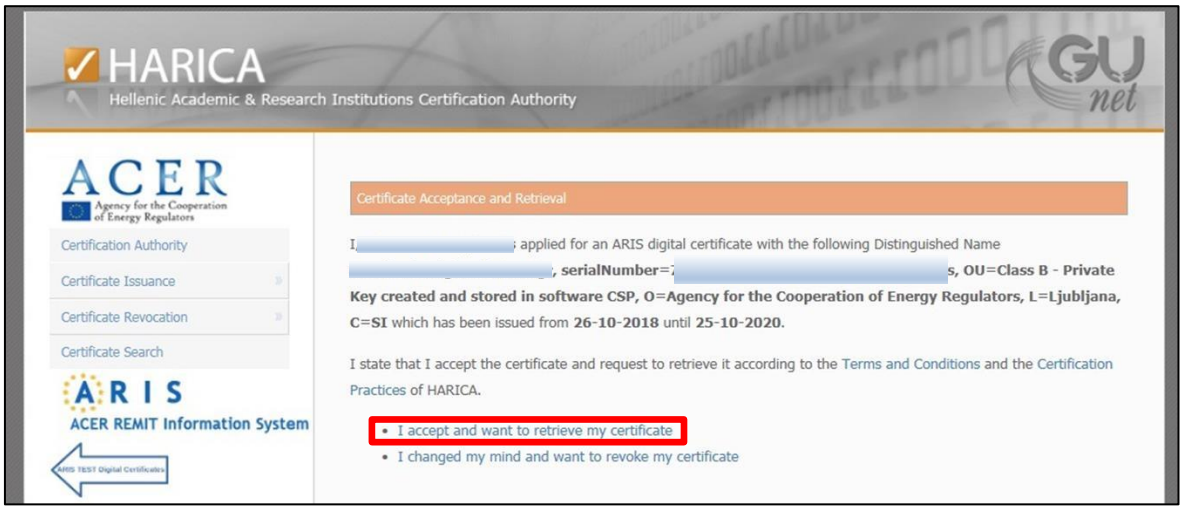


Figure 14: Accept and retrieve certificate

B. I changed my mind and want to revoke my certificate link (Figure 16) if you want to terminate the process and revoke your certificate.

Figure 15: Changed my mind and revocation option

If you select to revoke, you will be redirected to the **Request for revocation** page:

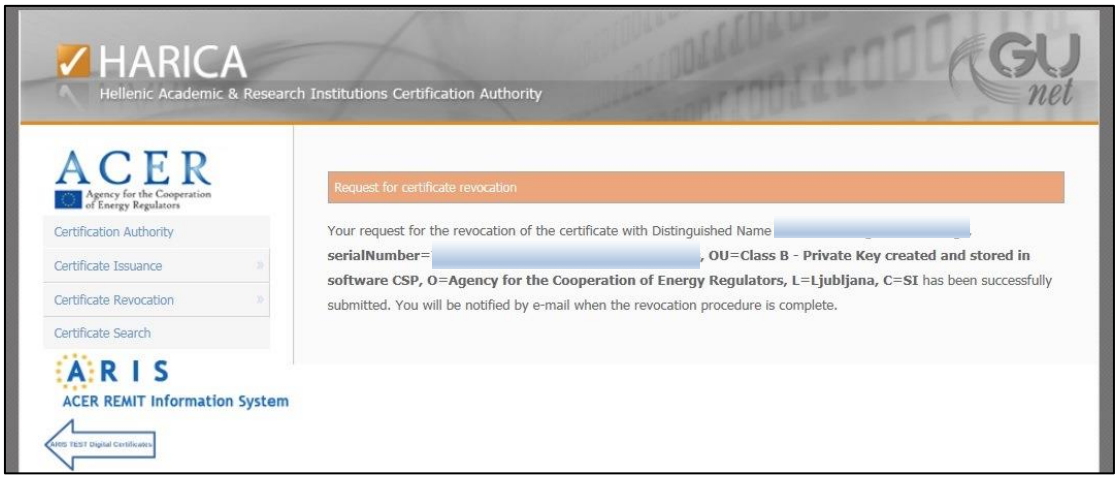


Figure 16: Changed my mind and revocation message

In addition, you will receive the email below:

The certificate revocation for the entity with Distinguished Name: , **serialNumber=** , **OU=Class B - Private Key created and stored in software CSP, O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI** and serial has been successfully completed.

Your certificate was revoked at: **26-10-2018 14:27:25** (Europe/Athens).

HARICA Public Key Infrastructure.

Figure 17: Changed my mind automatic email

Important notice:

If you are using Internet Explorer, the process will be finalised at this step. If you are using Microsoft Edge, Google Chrome or Mozilla, you will be directed to Step 3 before completing the process. You must unlock the certificate by providing the password you inserted in Step 5 of Section 2.1 of this manual.

Step 3. Enter the password you entered in Step 5 of Section 2.2 and click on **Unlock private key**.

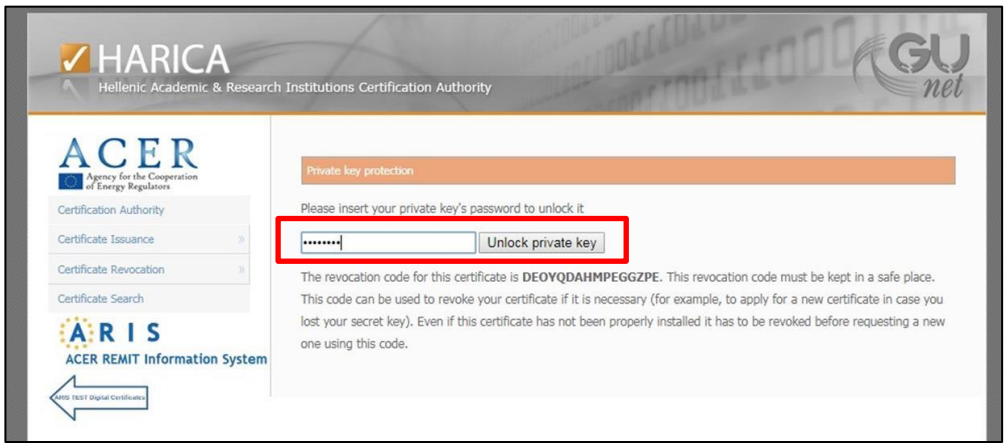


Figure 18: Unlock private key in Microsoft Edge, Mozilla Firefox and Google Chrome

Step 4. Click on **Download certificate & private key**.

Figure 19: Download certificate and private key

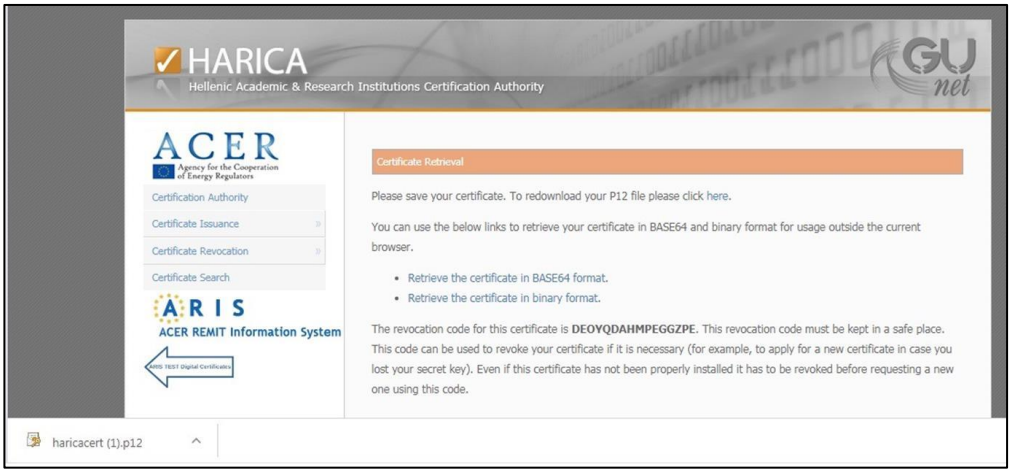


Figure 20: Retrieval of certificate in P12 file and additional options

There are two more options for downloading the public part of the certificate. You can choose to download it in the BASE64 format, or alternatively in a binary format if the certificate is intended to be used outside the current browser.

Step 5. After you retrieve your certificate, you will receive a confirmation email. Please save the email, since it contains important information, such as the revocation code of your certificate. The certificate is automatically saved in P12 file (this is the default) and imported into the browser (Internet explorer). For Mozilla Firefox, the necessary steps to import the certificate are presented in the following paragraphs (Section 2.6).

Dear Sir/Madam,

We would like to inform you that your ARIS digital certificate with the following Distinguished Name [redacted], **serialNumber=**[redacted], **OU=Class B - Private Key created and stored in software CSP, O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI** which was issued on **2018-10-26** (Europe/Athens) has been successfully retrieved.

The revocation code is **DEOYQDAHMPEGGZPE**.

Please keep this message for future reference.

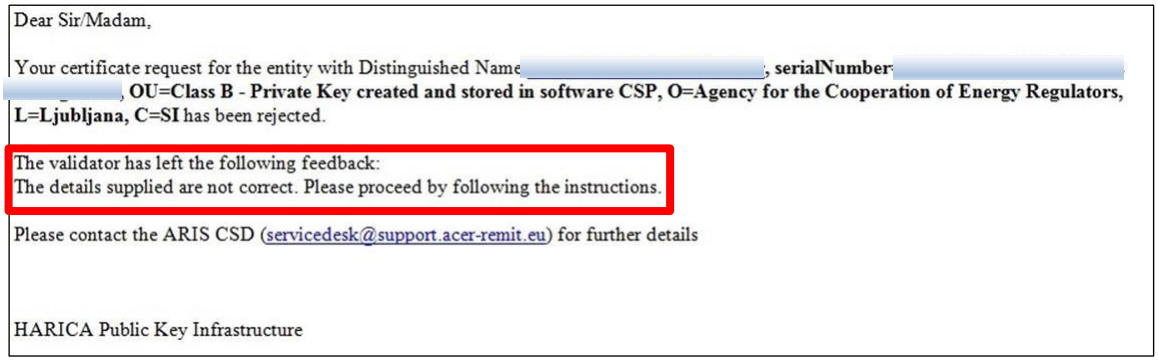
Please do not reply to this e-mail. In case of any questions please contact ARIS CSD (servicedesk@support.acer-remit.eu)

HARICA Public Key Infrastructure

Figure 21: Email on successful issuing of client digital certificate

2.4 Rejection message

In case ACER does not approve the issuing of a digital certificate for a user, the following email providing the reason for rejection of the request will be received by the end user.



Dear Sir/Madam,

Your certificate request for the entity with Distinguished Name [redacted], **serialNumber** [redacted], **OU=Class B - Private Key created and stored in software CSP, O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI** has been rejected.

The validator has left the following feedback:
The details supplied are not correct. Please proceed by following the instructions.

Please contact the ARIS CSD (servicedesk@support.acer-remit.eu) for further details

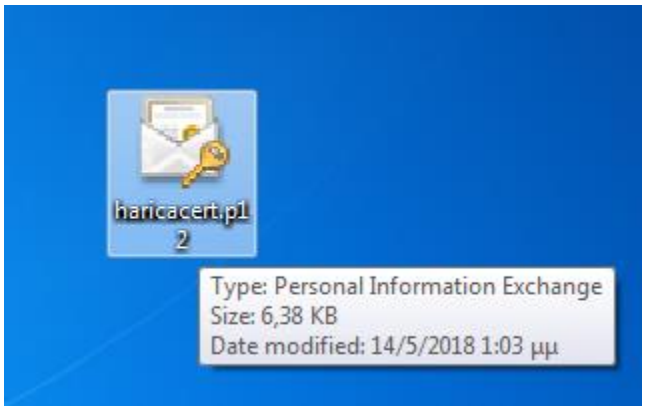
HARICA Public Key Infrastructure

2.5 Expiration message

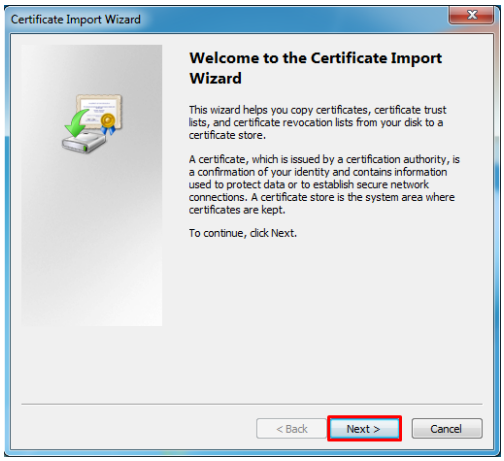
The ARIS digital certificate issued by CA HARICA is normally valid for a period of two years. Users will receive three expiration notices by email: the first one will be sent 30 days before the certificate expiration, the second one 15 days before the expiration, and the last one two days before the expiration.

2.6 Importing the certificate into the Windows certificate store

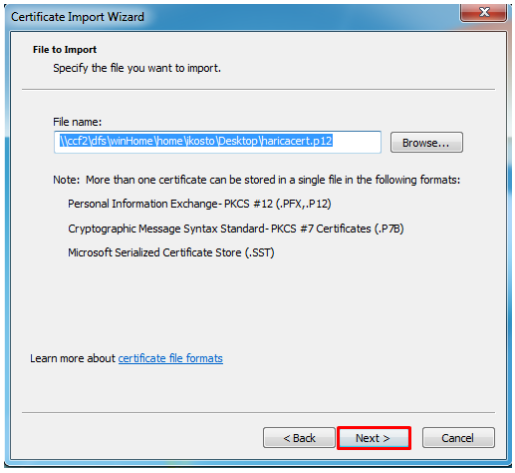
1. Double click the **haricacert.p12** to launch Certificate Import Wizard.



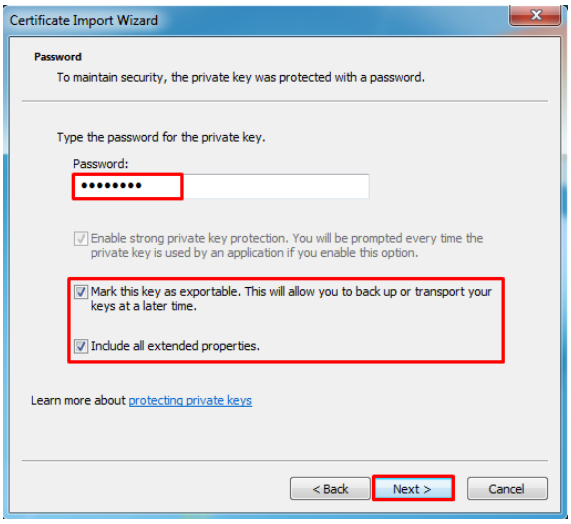
2. Choose **Next**.



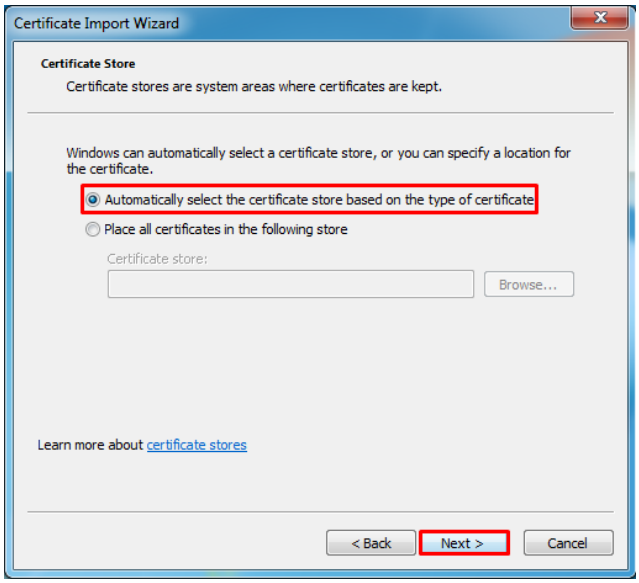
3. Choose **Next**.



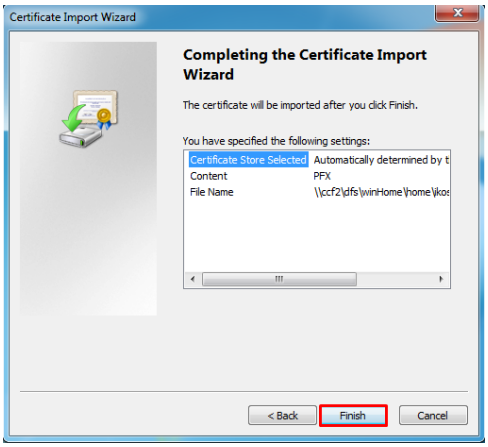
4. Enter the password you used to protect the private key when issuing your Certificate. Press **Next**.



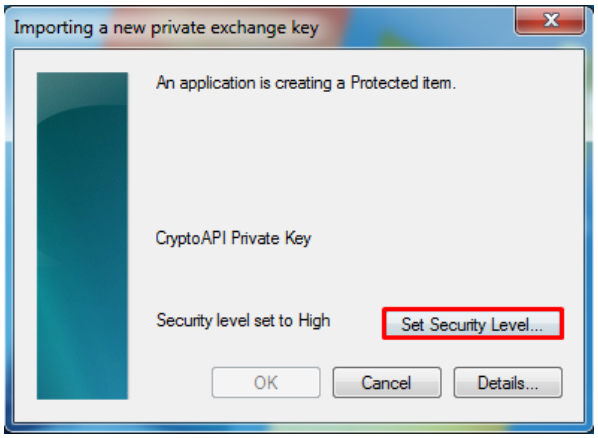
5. Choose **Next**.



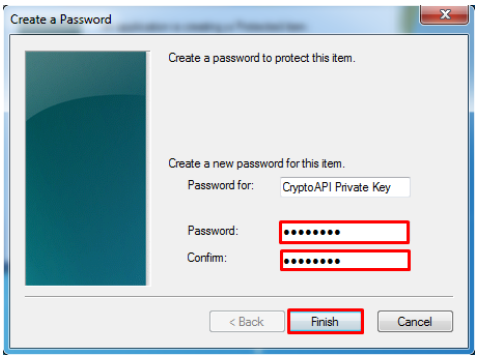
6. Choose **Finish**.



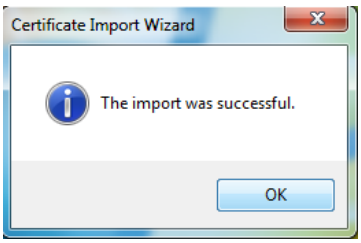
7. Press **Set Security Level**.



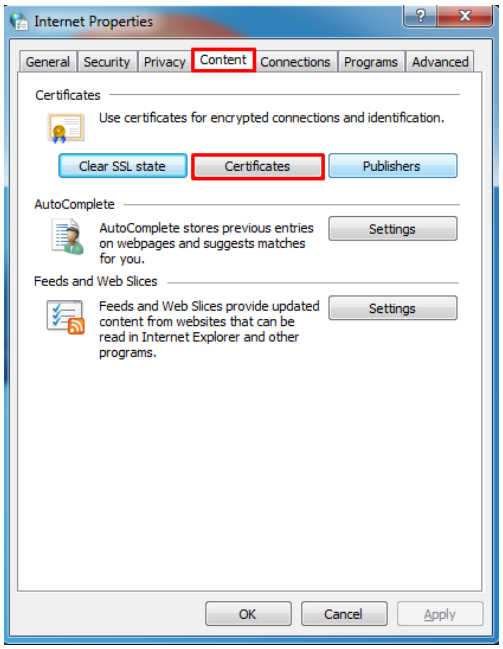
8. We recommend setting this level to 'High'. Set a **new** password to protect your certificate's private key. Press **Finish**.

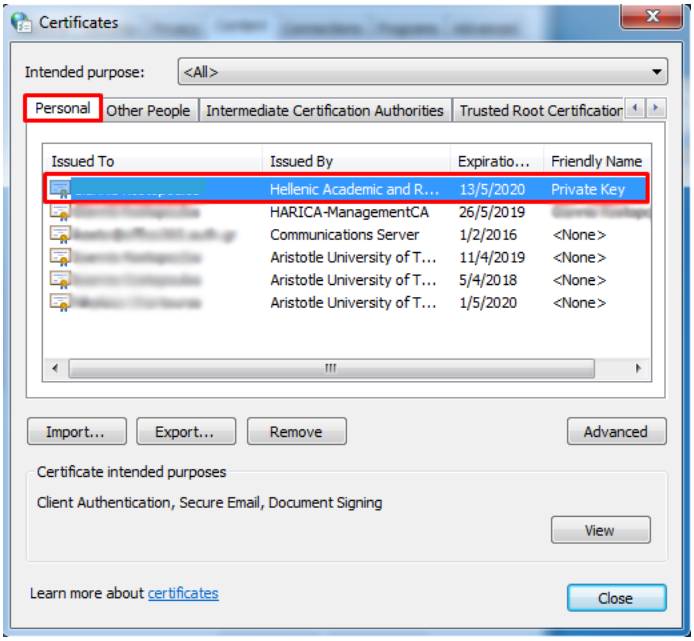


9. Choose **OK**.



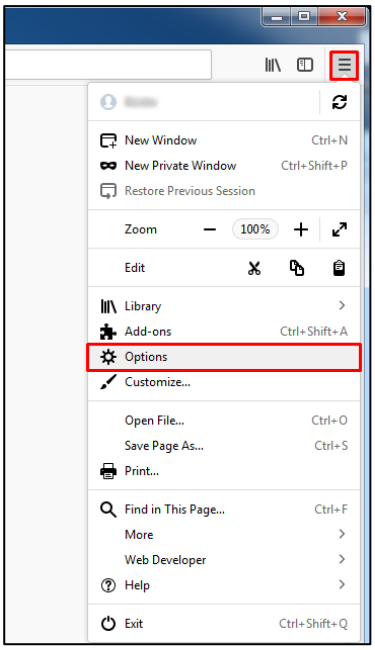
10. Your certificate with the private key is now added to the Windows certificate store.



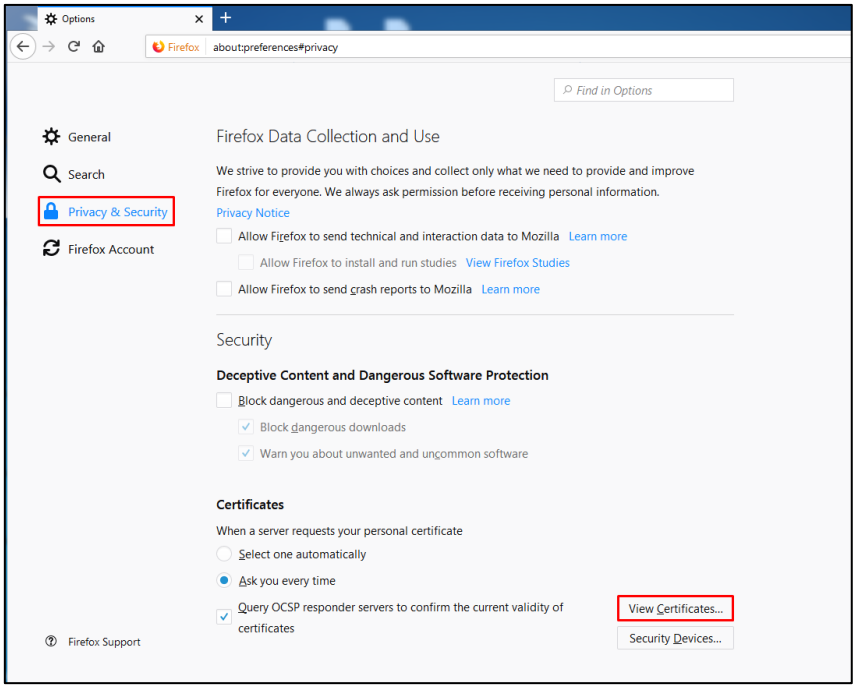


2.7 Importing the certificate into Mozilla Firefox

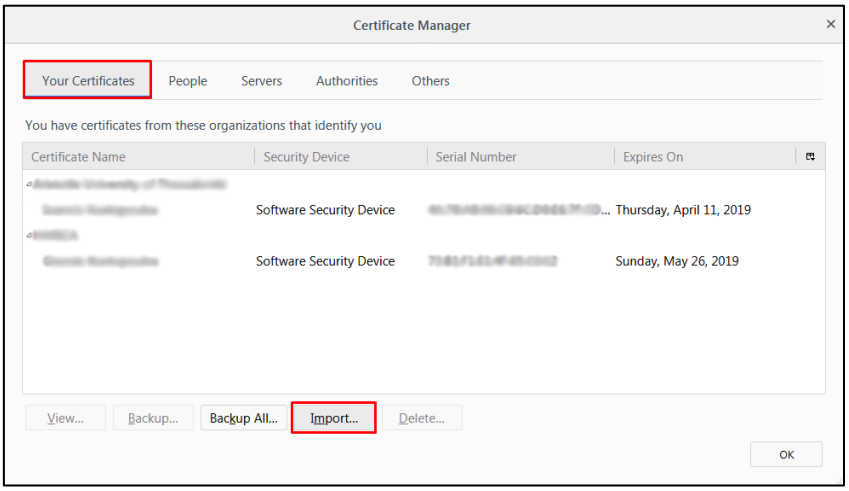
1. Open Firefox. Click on the icon with the three parallel horizontal lines and select **Options** from the drop-down list.



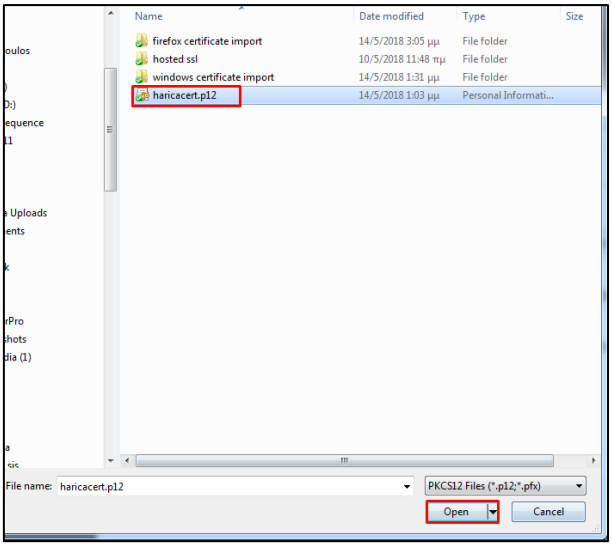
2. Choose **Privacy & Security** from the menu and scroll down to the Certificates section. Click on **View Certificates**.



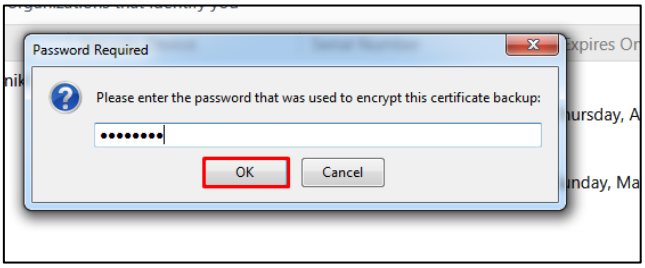
3. Click on the **Your Certificates** tab and press **Import**.



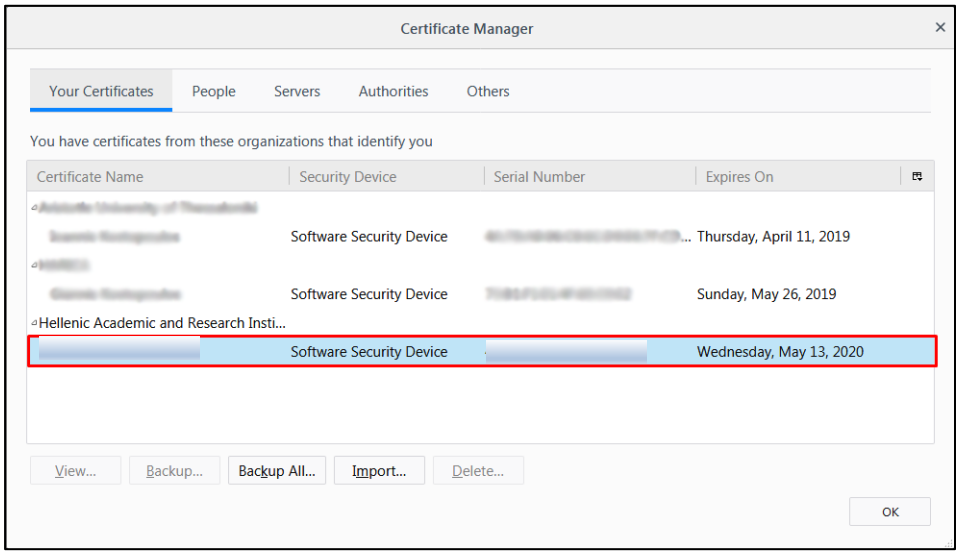
4. Browse and select the P12 file that contains your certificate with the private key. Press **Open**.



5. Enter the password you used to protect the private key when issuing your certificate. Press **OK**.

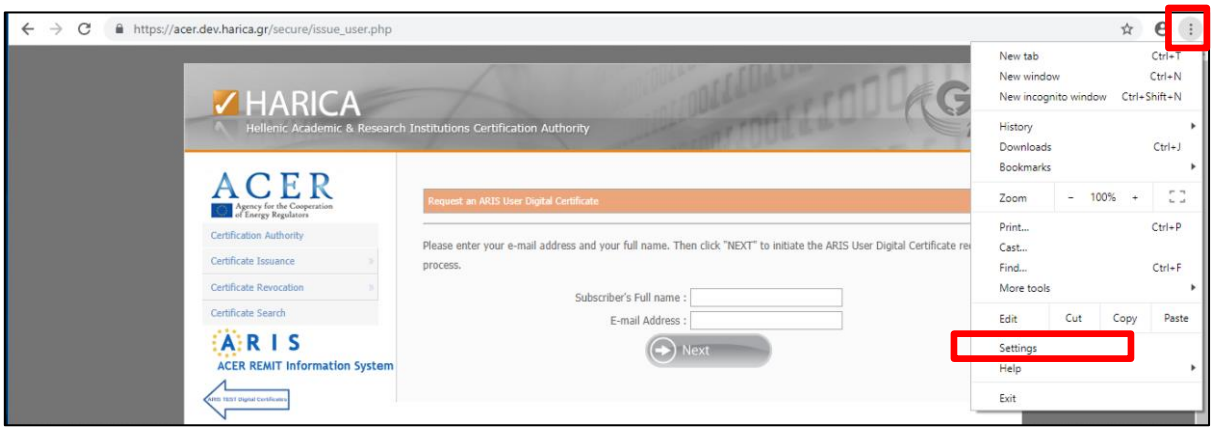


6. Your personal certificate with the private key is now added to the Firefox certificate store.

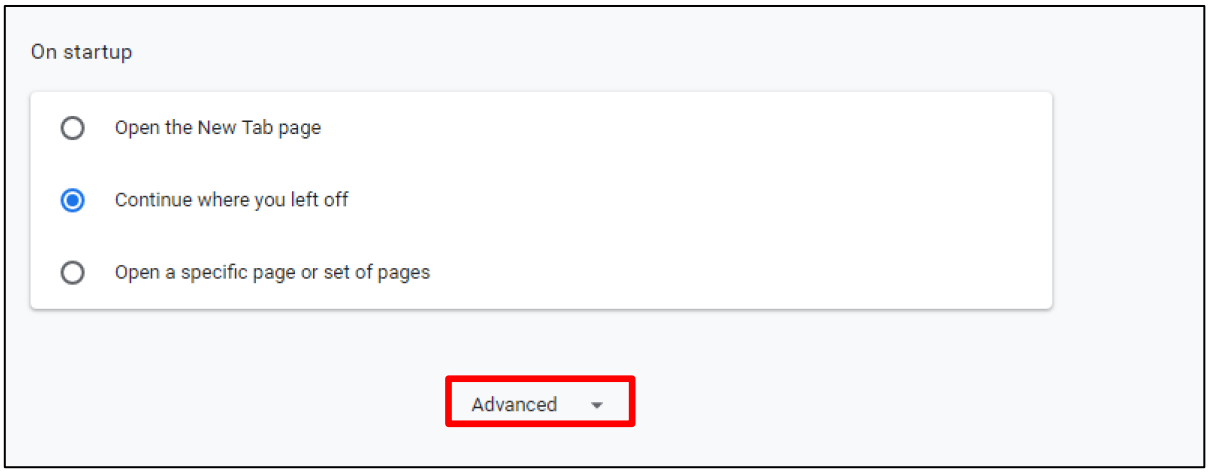


2.8 Importing the certificate into Chrome

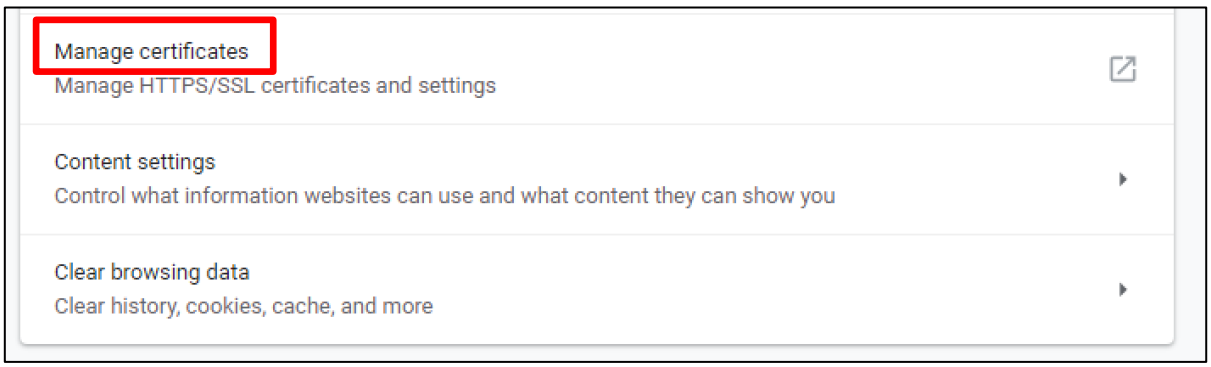
1. Open Chrome and click on the icon with the three vertical dots and select **Settings** from the drop-down list.



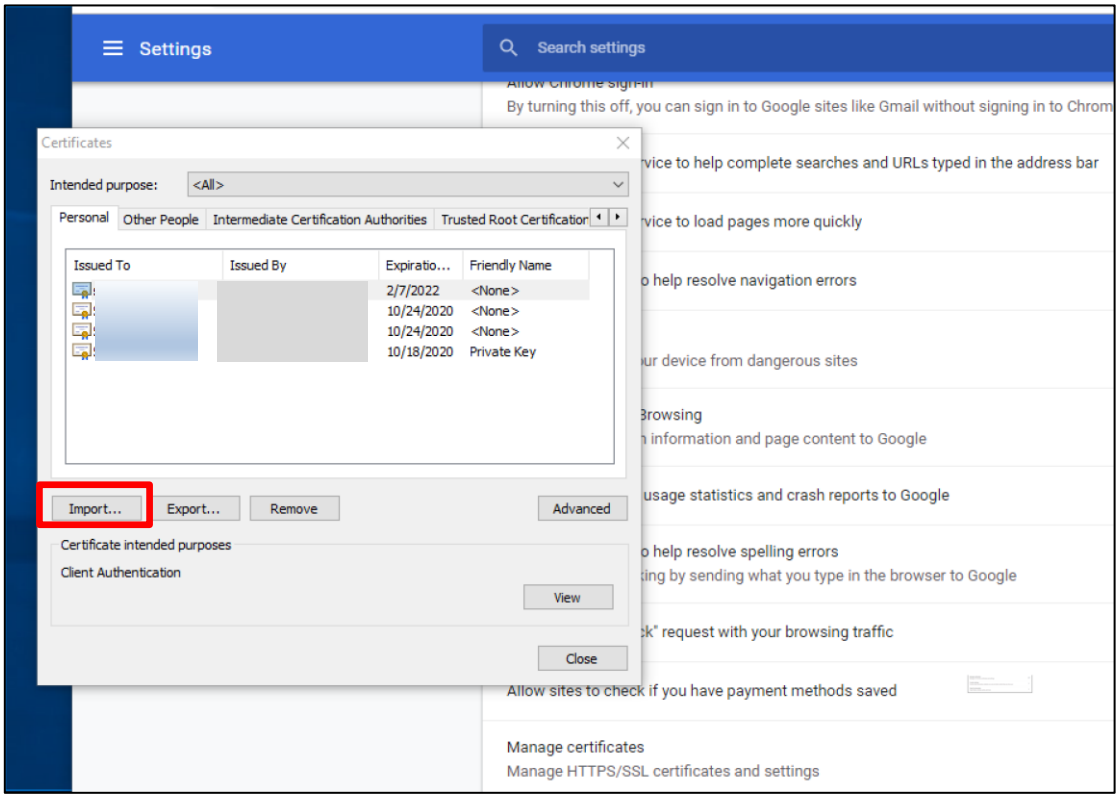
2. Scroll down and click on the **Advanced** option.



3. Scroll down and click on **Manage Certificates**.



4. Click on **Import**.



5. Follow the same process as described in '2.6 Import certificate in Windows certificate store', starting from Step 2.

2.9 Steps for a client certificate revocation

The following steps show how to revoke a client certificate. Start via:

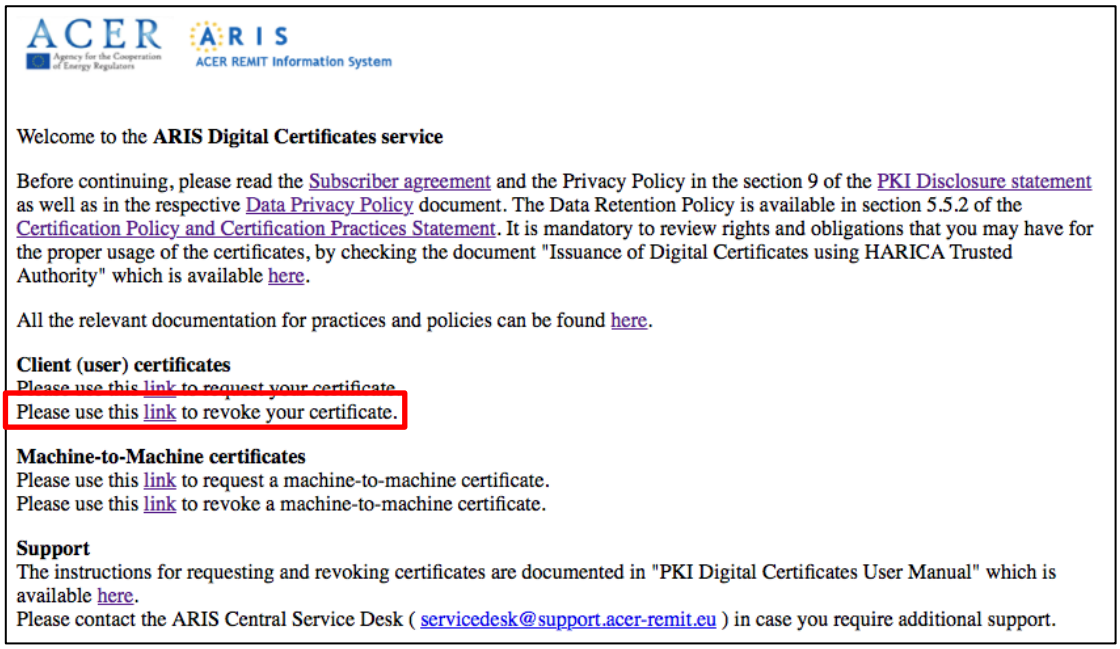
A. www.acer-remit.eu/certificates for the production environment, or

B. https://pilot.test-acer-remit.eu/certificates for the test environment

The revocation reasons can be one of the following:

- Certificate is no longer in use
- Certificate values are not valid
- Lost private key
- Exposed private key

Step 1 : Visit www.acer-remit.eu/certificates and select the link under the client (user) certificates tab.
For the test environment, use https://pilot.test-acer-remit.eu/certificates.


ACER Agency for the Cooperation of Energy Regulators
ARIS ACER REMIT Information System

Welcome to the **ARIS Digital Certificates service**

Before continuing, please read the Subscriber agreement and the Privacy Policy in the section 9 of the PKI Disclosure statement as well as in the respective Data Privacy Policy document. The Data Retention Policy is available in section 5.5.2 of the Certification Policy and Certification Practices Statement. It is mandatory to review rights and obligations that you may have for the proper usage of the certificates, by checking the document "Issuance of Digital Certificates using HARICA Trusted Authority" which is available here.

All the relevant documentation for practices and policies can be found here.

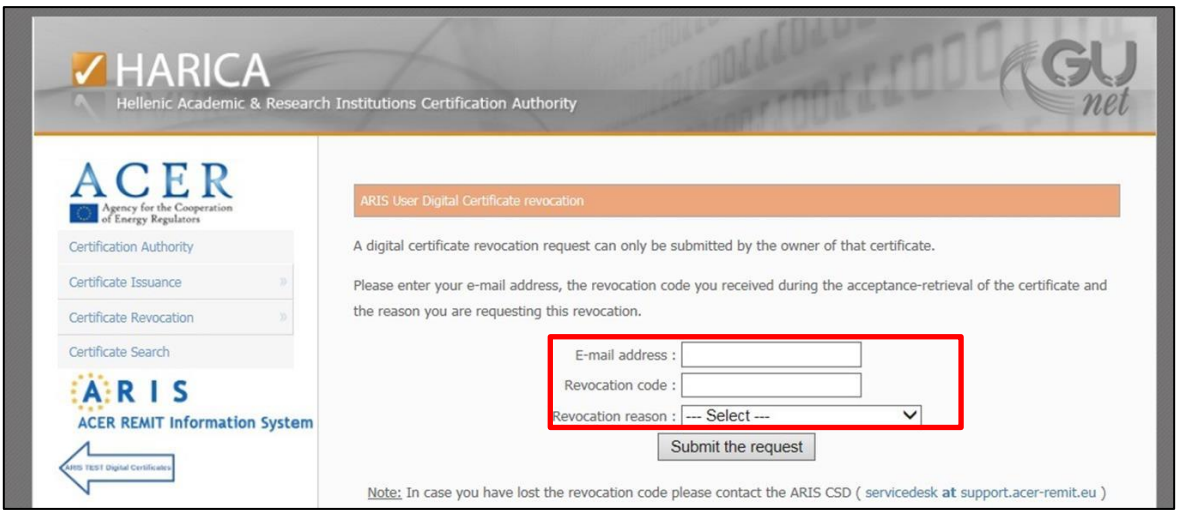
Client (user) certificates
Please use this link to request your certificate.
Please use this link to revoke your certificate.

Machine-to-Machine certificates
Please use this link to request a machine-to-machine certificate.
Please use this link to revoke a machine-to-machine certificate.

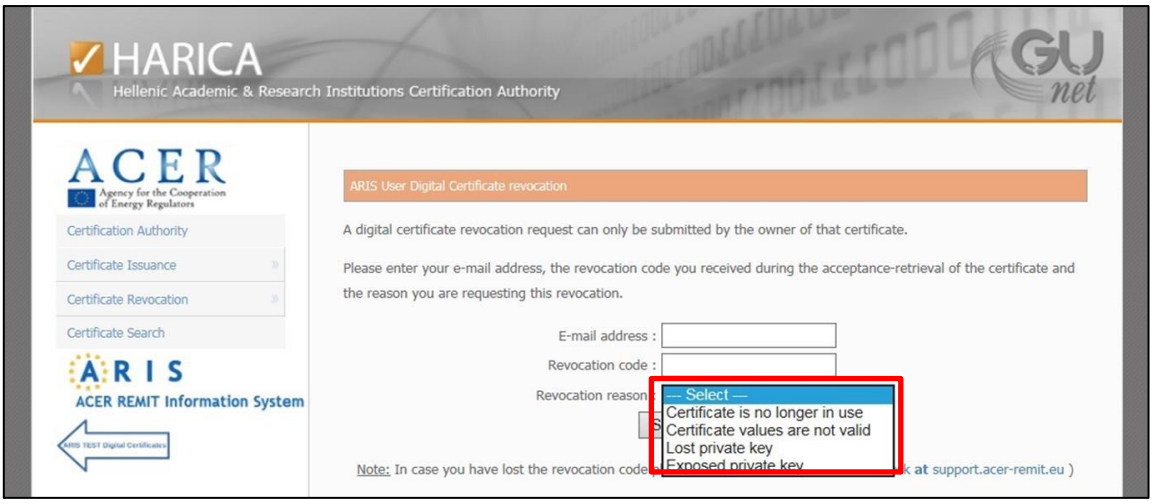
Support
The instructions for requesting and revoking certificates are documented in "PKI Digital Certificates User Manual" which is available here.
Please contact the ARIS Central Service Desk (servicedesk@support.acer-remit.eu) in case you require additional support.

Figure 22: Starting page link to the revocation process of client digital certificate

Step 2 : Enter your email address and the revocation code, as well the reason for revoking the certificate.



Select the revocation reason as depicted below:



You can find your revocation code in the email containing information about the client certificate retrieval (see below). In case you cannot find the email or you lost the revocation code, please contact the ARIS Central Service Desk (ARIS CSD).

Dear Sir/Madam,

We would like to inform you that your ARIS digital certificate with the following Distinguished Name **serialNumber=[redacted], OU=Class B - Private Key created and stored in software CSP, O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI** which was issued on **2018-10-26** (Europe/Athens) has been successfully retrieved.

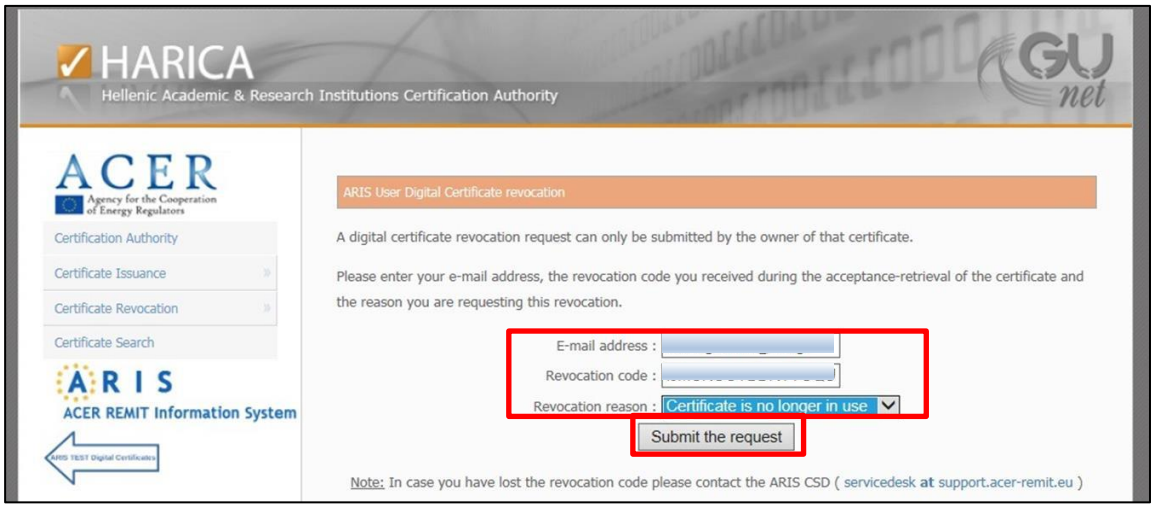
The revocation code is **HJMUKGGYBDRYTGQU**.

Please keep this message for future reference.

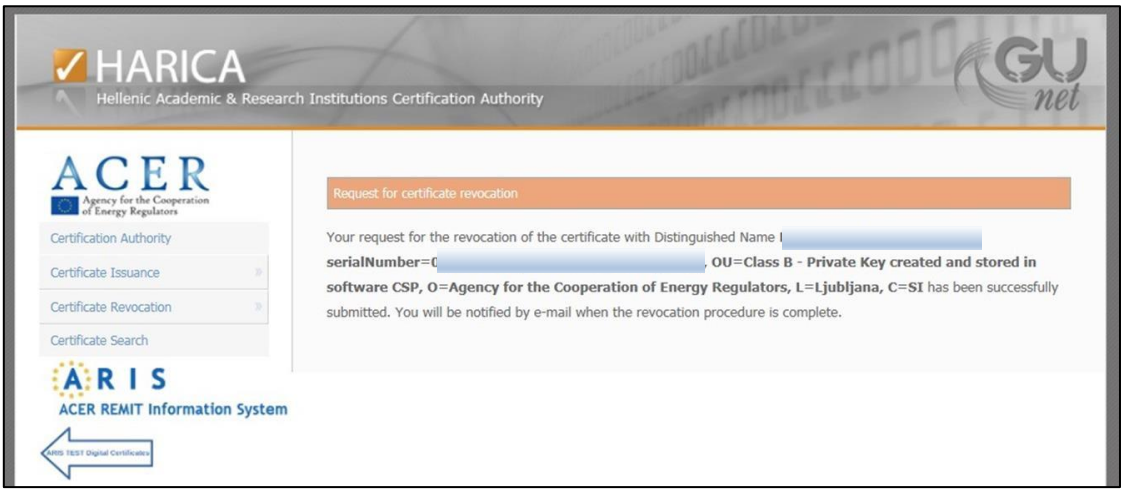
Please do not reply to this e-mail. In case of any questions please contact ARIS CSD (servicedesk@support.acer-remit.eu)

HARICA Public Key Infrastructure

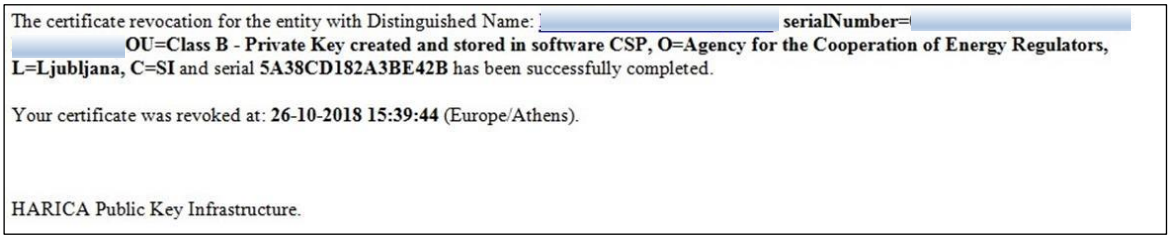
If you have the revocation code, please provide the information on the revocation home page and click on **Submit the request**.



Step 3 : You will then receive the following information.



Step 4 : You will receive an email informing you of the details of your action and that your revocation has been completed.



The certificate revocation for the entity with Distinguished Name: [redacted] **serialNumber=**[redacted] **OU=Class B - Private Key created and stored in software CSP, O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI** and serial **5A38CD182A3BE42B** has been successfully completed.

Your certificate was revoked at: **26-10-2018 15:39:44** (Europe/Athens).

HARICA Public Key Infrastructure.

Your client (user) certificate is now revoked. No further actions are needed.

3 ARIS machine-to-machine certificate request

The following steps show how to request a machine-to-machine certificate. Start via:

A. www.acer-remit.eu/certificates for the production environment, or

B. https://pilot.test-acer-remit.eu/certificates for the test environment

3.1 Steps for machine-to-machine certificate request

Important notice:

The basic prerequisite for requesting a machine-to-machine certificate for ARIS is to have an already valid HARICA ARIS client (user) digital certificate imported in your browser.

ONLY FOR TEST CERTIFICATES: In order for the client computer to consider the test certificates as trusted, the test root CA certificate has to be manually installed as a 'Trusted Root Certification Authority' certificate. The test root CA certificate can be obtained from this link:

https://www.dev.harica.gr/certs/StagingHaricaRootCA2015.der

Please note that on some computers specific user privileges may be required to install the test root CA certificate.

Step 1 : Visit www.acer-remit.eu/certificates (or https://pilot.test-acer-remit.eu/certificates for the test environment) and select the link under the client (user) certificates tab.

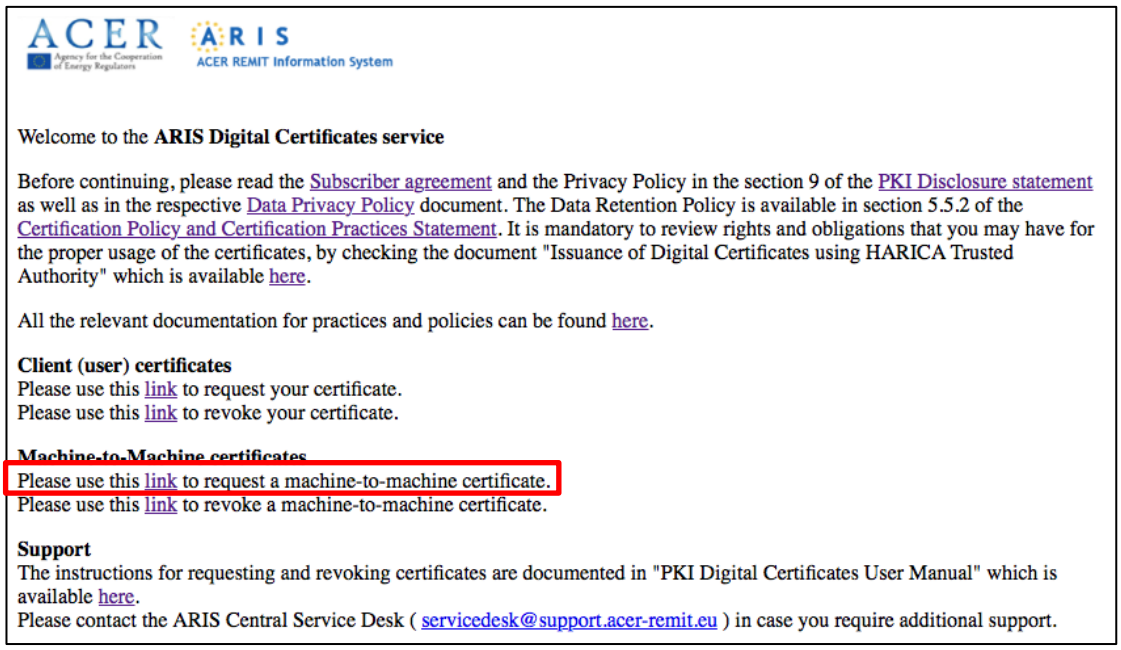


Figure 23: Starting page and machine-to-machine selection

Step 2 : Please enter a Certificate Name (FQDN) for your machine-to-machine ARIS digital certificate below.

For validation purposes, the name needs to be unique and has to be in the form of ***yourmachinename.yourorganisationname.yourcountrydomain***

The field ***yourcountrydomain*** is the standard two-letter country domain (e.g. .si for Slovenia).

Note that this name is only used for naming the requested certificate – no configuration of this name has to be done on your machine.

Then, press **Next** in order to authenticate with your client certificate and initiate the machine-to-machine certificate request.

The domain *yourorganisationname.yourcountrydomain* should be the whitelisted domain for your organisation.

If, for any reason, your domain is not authorised, this authorisation can be done by opening a ticket via servicedesk@support.acer-remit.eu.

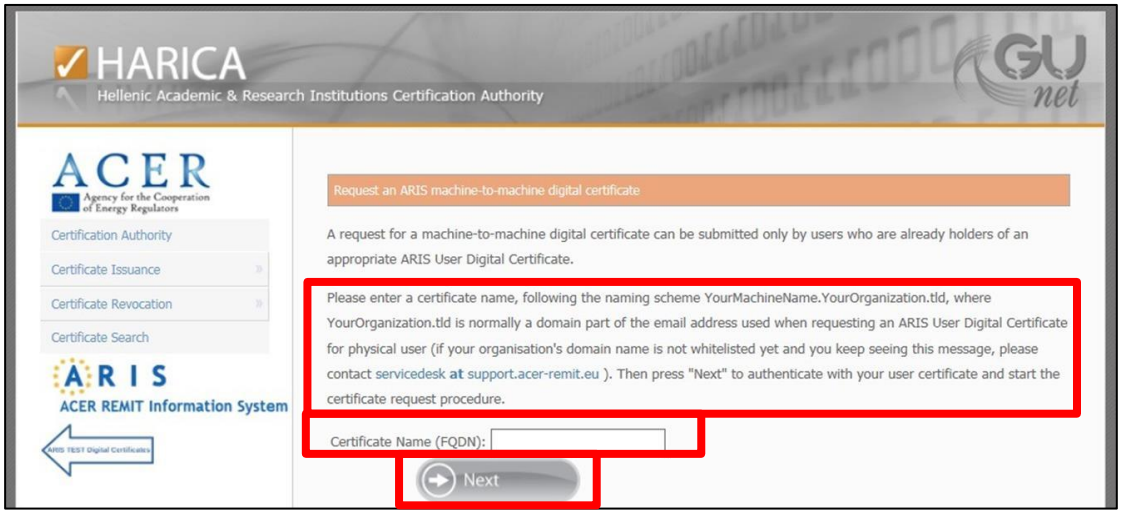
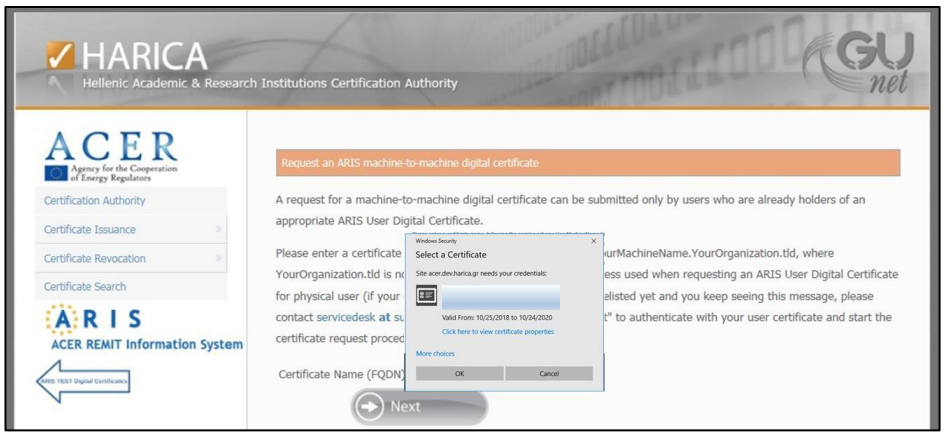


Figure 24: Initial page in order to insert the details for the machine (Certificate Name)

Step 3 : Select your certificate for ARIS in order to authenticate and press **OK**.



Step 4 : Then select **Generate new CSR** in order to create a new private key and a Code Signing Request for your machine-to-machine-certificate.

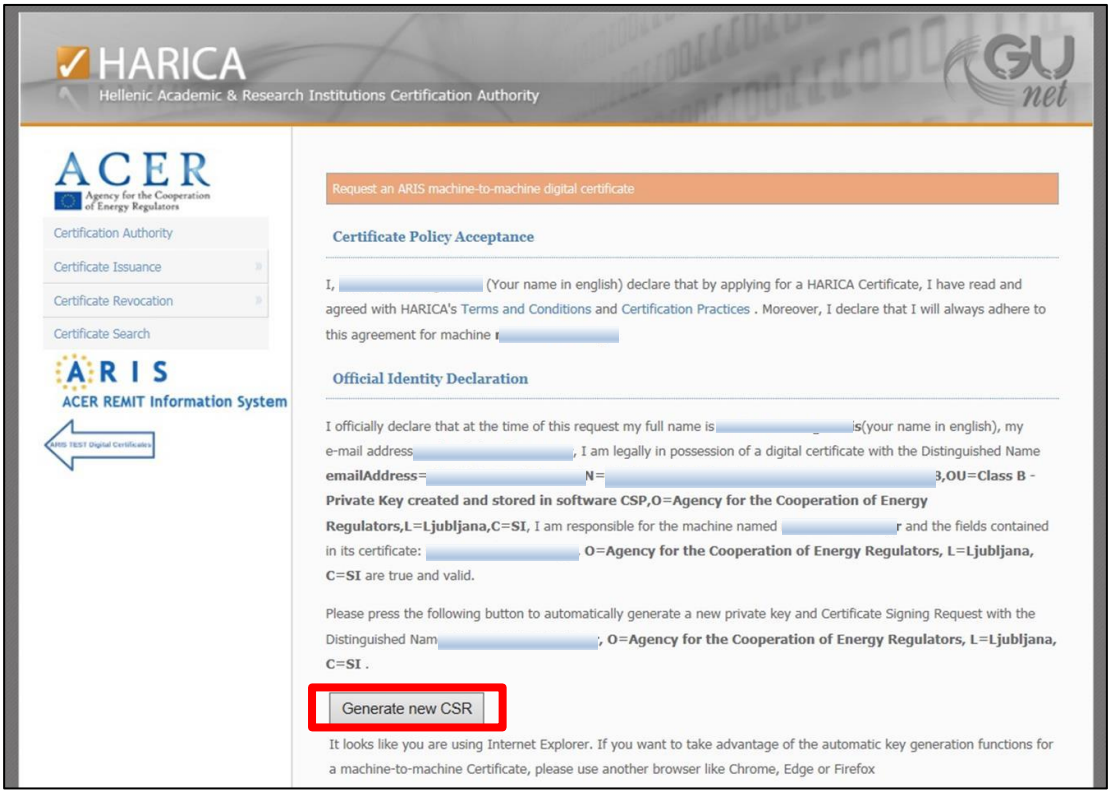


Figure 25: Generate CSR selection

Step 5 : The next step is to **export** a **private key** and insert a password to protect it.

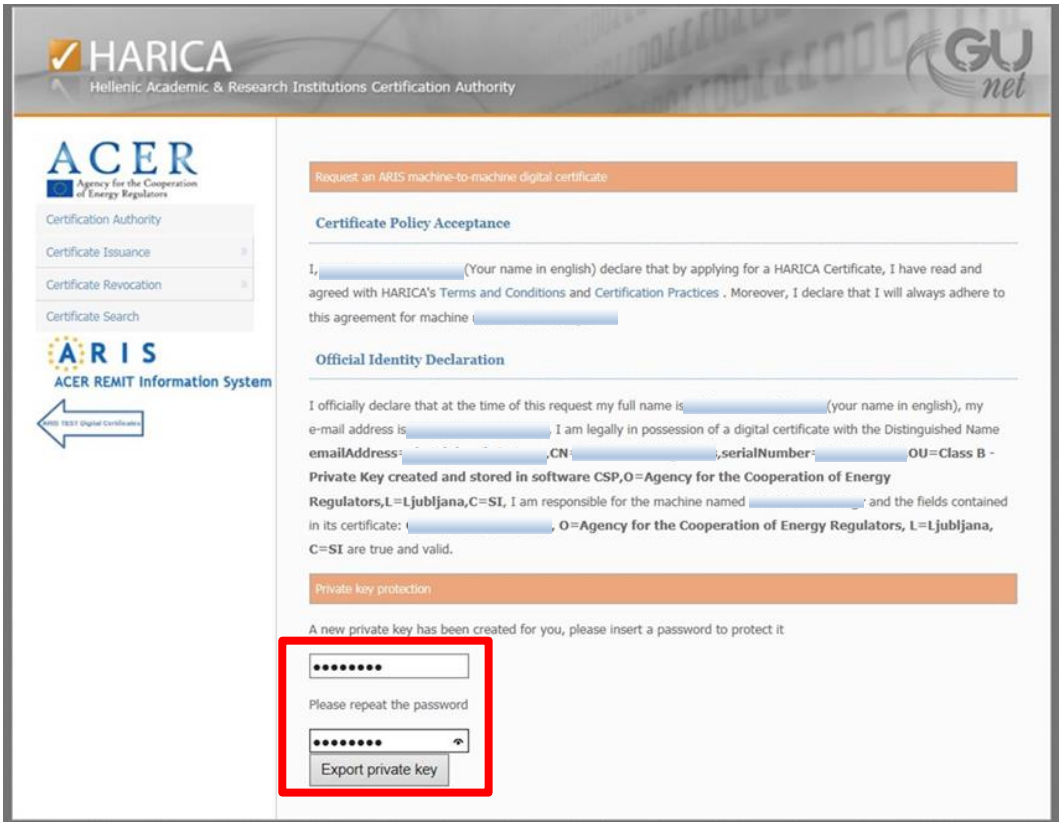


Figure 26: Export private key and password insertion for protecting the private key

After saving your private key, continue by selecting **I have saved my private key and I won't forget the password**.

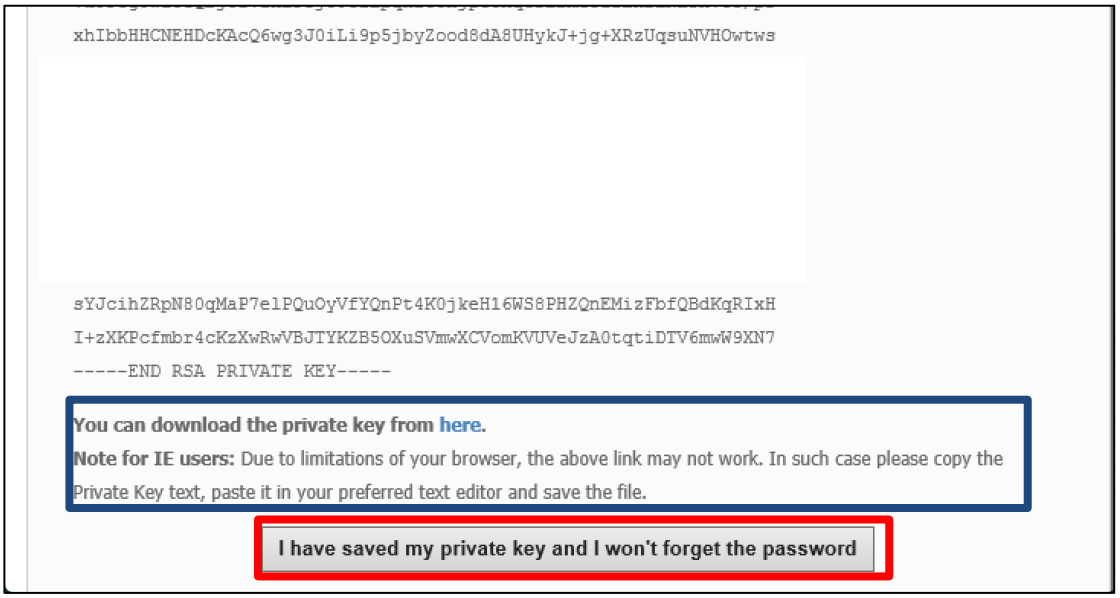


Figure 27: Save the private key

Note for IE users: If you are using Internet Explorer, the link '**You can download the private key from here**' does not work (this is a known issue of this browser).

To manually save the private key, please copy the text between the lines
-----BEGIN RSA PRIVATE KEY-----
and
-----END RSA PRIVATE KEY-----
(including the first and last row) and paste it into a text document and then save it as the machine-to-machine certificate's private key.

Figure 28: Save the private key (workaround for IE)

Step 6 : You have to upload a filled out form for requesting a machine-to-machine certificate. The form is available here: https://documents.acer-remit.eu/category/remit-reporting-user-package/
Please refer to Section 2.1 of this document for information on how to fill out the form. Please make sure you enter the **Certificate Name (FQDN)** according to the instructions in Step 2 of Section 3.1.

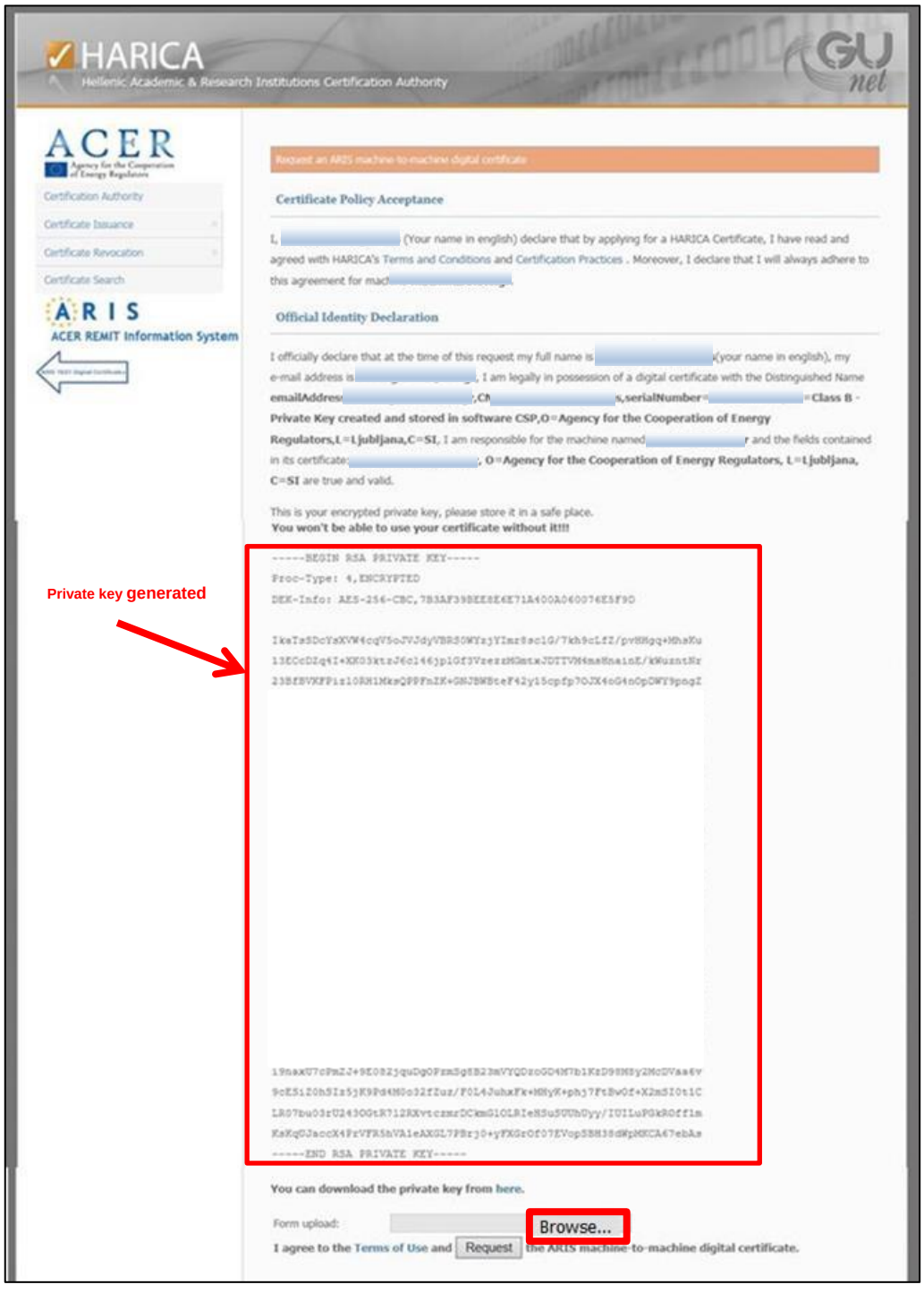


Figure 29: Form upload for machine-to-machine

Step 7 : After uploading the necessary form, click on **Request.**

Figure 30: Request for machine-to-machine certificate

Step 8 : The next screen informs you that the request has been successfully submitted and is under validation.

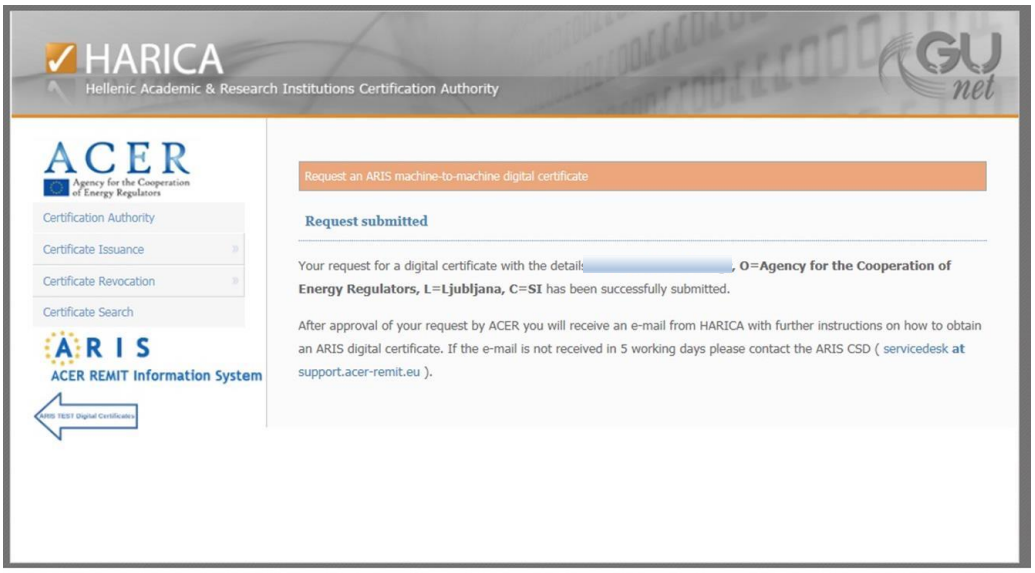


Figure 31: Request submitted information screen

In case a user tries to upload a file that does not fulfill the requirements (regarding resolution or size), the following error message will appear. You are kindly requested to start over the machine-to-machine certificate request process.

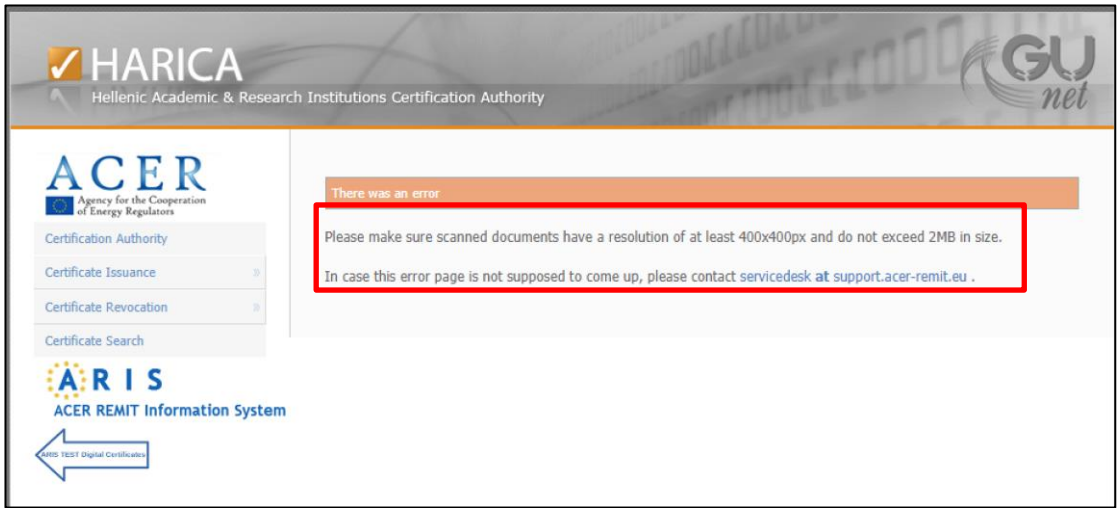
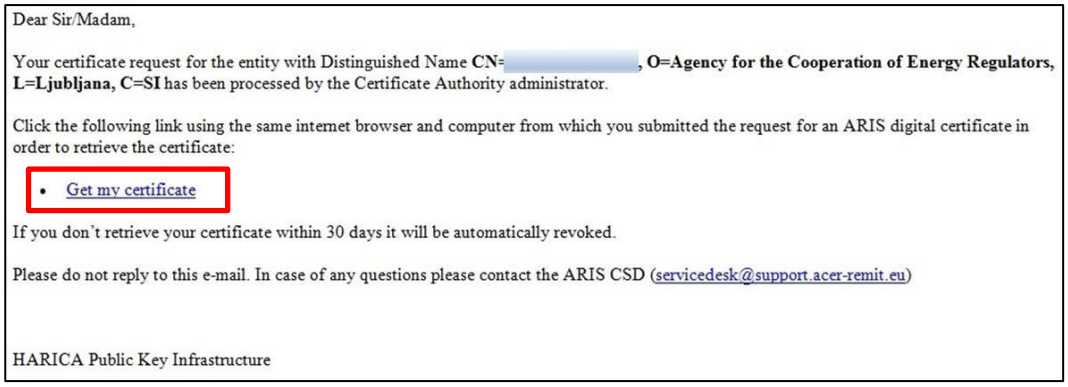


Figure 32: Error message when uploading a file not aligned with requirements

Step 9 : Once the certificate application is submitted successfully, you will have to wait for ACER to check and approve your request.

3.2 Steps for a machine-to-machine certificate retrieval

Step 1. After the approval of your request, you will receive an email to proceed with the certificate acceptance. Select **Get my certificate**.



Dear Sir/Madam,

Your certificate request for the entity with Distinguished Name **CN=[redacted], O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI** has been processed by the Certificate Authority administrator.

Click the following link using the same internet browser and computer from which you submitted the request for an ARIS digital certificate in order to retrieve the certificate:

- Get my certificate

If you don't retrieve your certificate within 30 days it will be automatically revoked.

Please do not reply to this e-mail. In case of any questions please contact the ARIS CSD (servicedesk@support.acer-remit.eu)

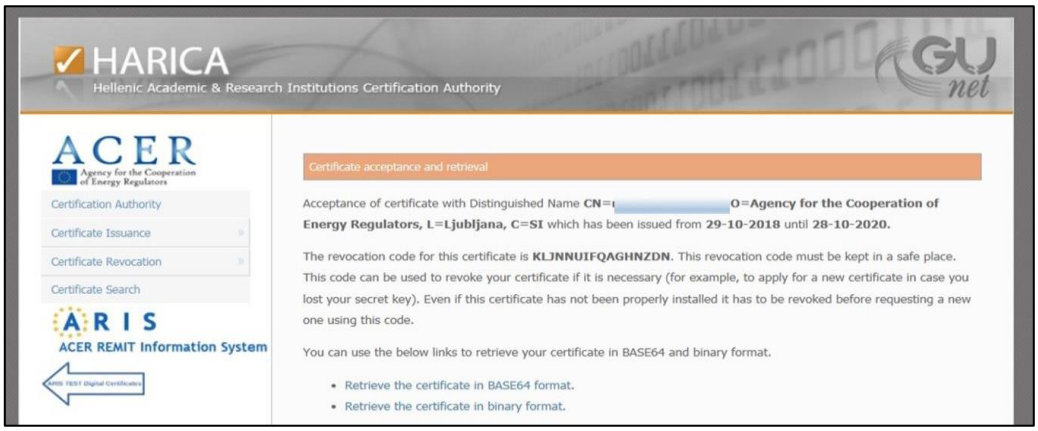
HARICA Public Key Infrastructure

Figure 33: Get my certificate e-mail confirmation

Step 2. Select **I accept and want to retrieve my certificate.**

Figure 34: Certificate retrieval

In case you have changed your mind and do not want to obtain a certificate, please follow Step 2B in Section 2.3 for requesting a client certificate.



Step 3. The following email will be received by the end user. The process is completed.

Dear Sir/Madam,

We would like to inform you that your ARIS digital certificate with the following Distinguished Name **CN=[redacted] O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI** which was issued on **2018-10-29** (Europe/Athens) has been successfully retrieved.

The revocation code is **KLJNNUIFQAGHNZDN**.

Please keep this message for future reference.

Please do not reply to this e-mail. In case of any questions please contact ARIS CSD (servicedesk@support.acer-remit.eu)

HARICA Public Key Infrastructure

Figure 35: Confirmation email for machine-to-machine certificate

3.3 Steps for a machine-to-machine certificate revocation

The following steps show how to revoke a machine-to-machine certificate. Start via:

A. www.acer-remit.eu/certificates for the production environment, or

B. https://pilot.test-acer-remit.eu/certificates for the test environment

The revocation reasons can be one of the following:

- Certificate is no longer in use
- Certificate values are not valid
- Lost private key
- Exposed private key

Step 1 : Visit www.acer-remit.eu/certificates (or https://pilot.test-acer-remit.eu/certificates for the test environment) and select the link under the machine-to-machine certificates tab**.**

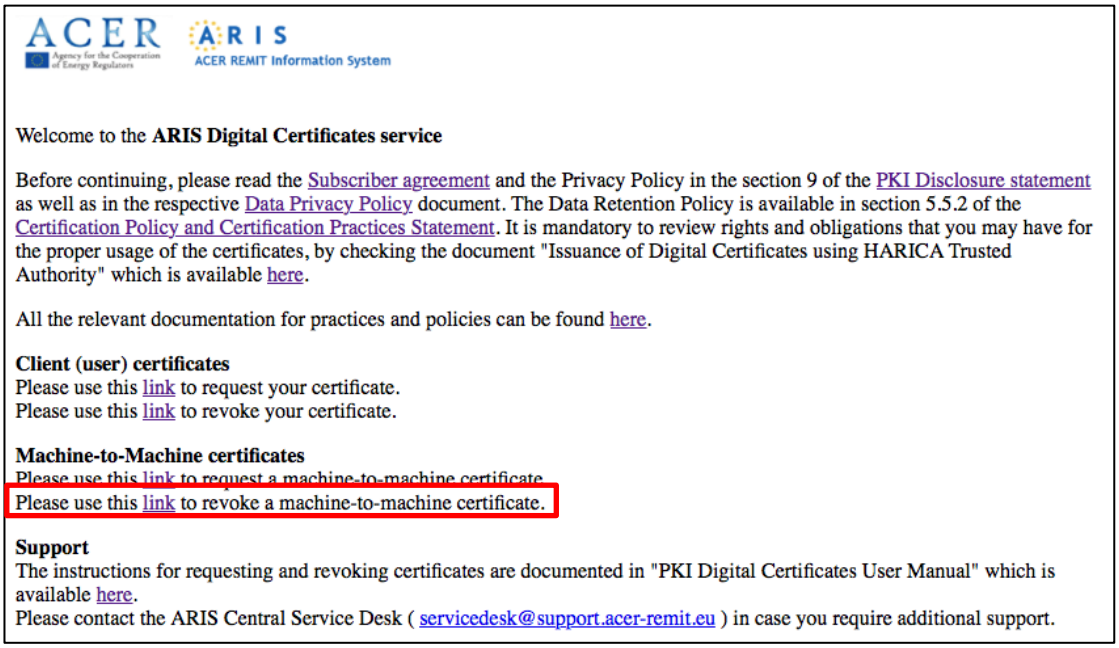


Figure 36: Starting page for machine-to-machine revocation

Step 2 : Insert the required details and select a revocation reason**.** After selecting all the options and providing the requested data, name, code and reason, click on **Submit the request**.

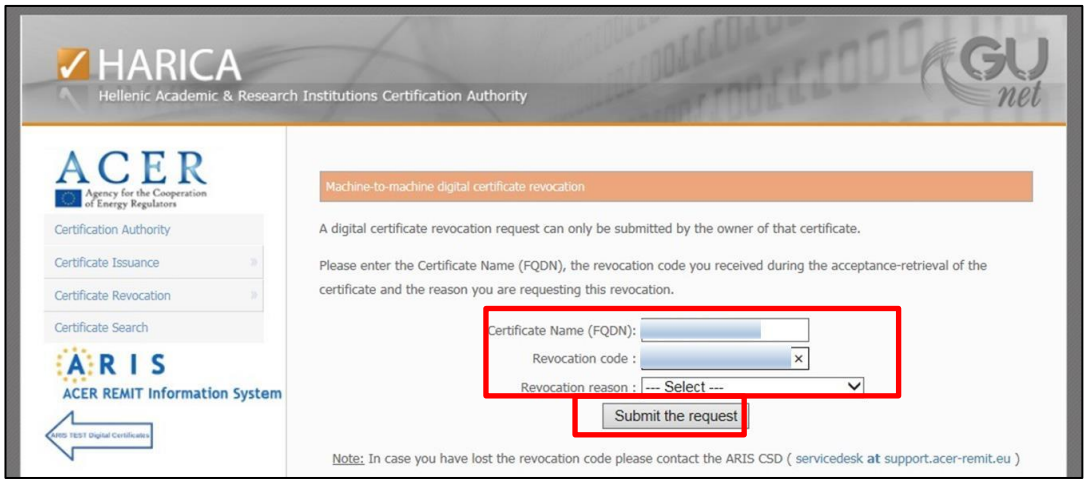
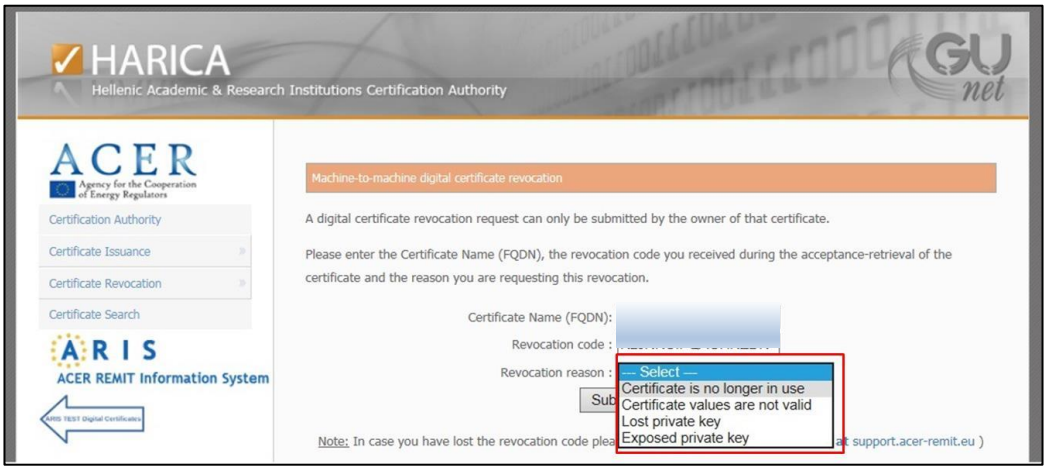
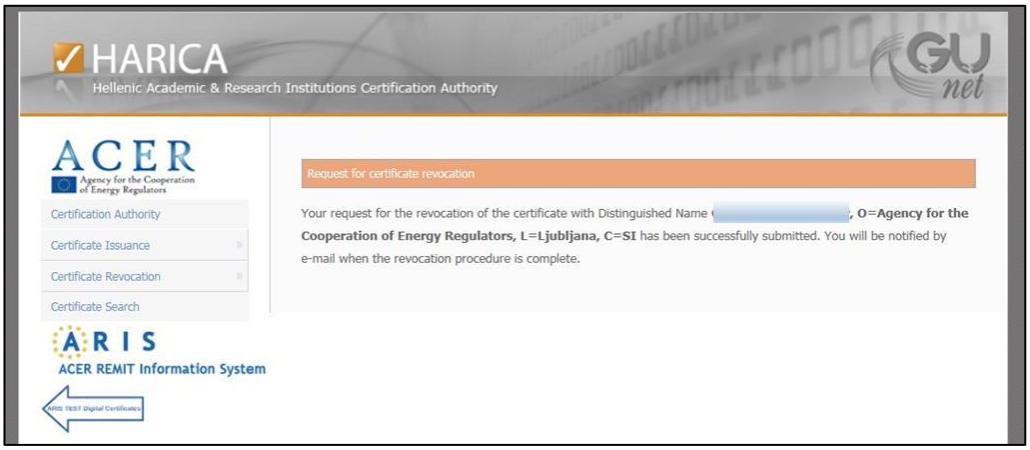


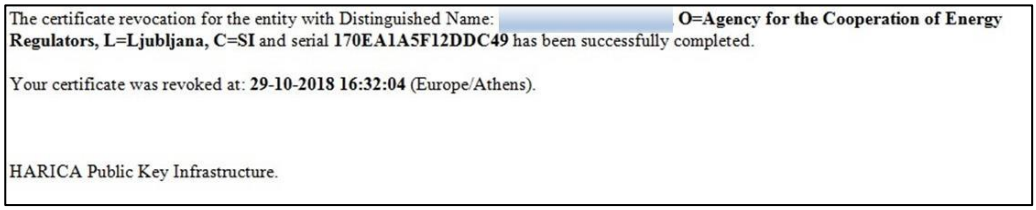
Figure 37: Revocation details



Step 3 : You will get the following information page.



Step 4 : You will receive the following email containing all the information about the revocation.



The certificate revocation for the entity with Distinguished Name: [redacted] **O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI** and serial **170EA1A5F12DDC49** has been successfully completed.

Your certificate was revoked at: **29-10-2018 16:32:04** (Europe/Athens).

HARICA Public Key Infrastructure.

Your machine-to-machine certificate is now revoked. No further actions are needed.