

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	15 January 2019
USER MANUAL for Obtaining ARIS Digital Certificates Version 1.0	



Table of Contents

1	Intro	oduction	5
	1.1	Scope and Purpose	5
	1.2	Target audience	5
	1.3	Glossary	6
	1.4	Structure of the document	6
2	Step	os 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	ARI	S 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 <u>servicedesk@support.acer-remit.eu</u> 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 <u>https://documents.acer-remit.eu/category/remit-reporting-user-package/</u> 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*.



	APPLICATION FOR OBTAINING A USER DIGITAL CERTIFICATE
	FOR LEGAL ENTITIES
	LEGALENTITY
	Organization:
	Address:
Certificate holder's	City: Postal Code:
information	Country:
	CERTIFICATE HOLDER OR TECHNICAL REPRESENTATIVE
	Name:
	Surname:
	E-mail:
	LEGAL AND DATA PRIVACY STATEMENT
	Please read the documents (a) Subscriber agreement <u>https://repo.harica.ar/documents/SA-ToU_EN.adt</u> (b) Privacy Policy (section 9) the <u>PR</u>) <u>Declosure statement</u> <u>http://www.harica.ar/documents/PDS-EN.adt</u> (c) <u>Data Privacy Policy http://repo.harica.ar/documents/Data-Privacy-Statement-EN.pdf</u> (d) Certification Policy and Certification Practices Statement <u>http://www.harica.ar/documents/CPS-EN.pdf</u> 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 <u>https://documents.ace-remit.eu/astegon/remit-reportina- user-package/</u> , HARICA documentation about practices and policies is <u>here</u> <u>http://repo.harica.ar/procedures.php</u> .
	Place Date: Signature:

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



APPLI	CATION FOR OBTAINING A USER DIGITAL TRAT CERTIFICATE
	FOR LEGAL ENTITIES
LEGAL ENTITY	
Organization:	
Address:	
City:	Postal Code :
Country:	
TEET CERTIFICAT	
TEST CERTIFICAT	E HOLDER OK FECHNICAL REPRESENTATIVE
Name:	
Surname:	
9199000000 20 	
E-mail:	
LEGAL AND DATA	A PRIVACY STATEMENT
Please read the do	ocuments (a) Subscriber agreement <u>https://repo.ha.ica.gr/documents/SA-ToU_EN.pdf</u> (section 9) the P() Disclosure statement <u>http://www.harica.gr/documents/PDS-EN.adf</u>
(b) Privacy Policy	The second of the second of a second se
(b) Privacy Policy (c) <u>Data Privacy Po</u>	olicy <u>http://repo.harica.gr/documents/Data-Privacy-Statement-EN.pdf</u> (d) Certification
(b) Privacy Policy (c) <u>Data Privacy Policy</u> (c) <u>Data Privacy Policy</u> Policy and Certification to Data Retention	<u>blicy http://repo.harica.ar/documents/Data-Privacy-Statement-EN.pdf</u> (d) Certification ation Practices Statement <u>http://www.harica.ar/documents/CPS-EN.pdf</u> with reference Policy (section 5.5.2) Obligations for proper usage of certificates (e) (suggree of Digital
(b) Privacy Policy (c) <u>Data Privacy Policy</u> (c) <u>Data Privacy Policy</u> Policy and Certificato to Data Retention Certificates using	olicy http://repo.harica.ar/docum.ents/Data-Privacy-Statement-EN.pdf (d) Certification ation Practices Statement <u>http://www.harica.gr/docum.ents/CPS-EN.pdf</u> with reference Policy (section 5.5.2). Obligations for proper usage of certificates (e) Issuance of Digital HARICA Trusted Authority <u>https://documents.acer-remit.eu/categony/remit-reporting-</u>
(b) Privacy Policy ((c) <u>Data Privacy Policy</u> Policy and Certifica to Data Retention (Certificates using <u>user-package</u>).	olicy http://repo.harica.ar/docum.ents/Data-Privacy-Statement-EN.pdf (d) Certification ation Practices Statement <u>http://www.harica.ar/docum.ents/CPS-EN.pdf</u> with reference Policy (section 5.5.2). Obligations for proper usage of certificates (e) Issuance of Digital HARICA Trusted Authority <u>https://documents.acer-remit.eu/categon//remit-reporting-</u> HARICA documentation about practices and policies is <u>here</u> victorcedices abo
(b) Privacy Policy ((c) <u>Data Privacy Po</u> Policy and Certifice to Data Retention Certificates using <u>user-package</u> () <u>http://repo.harica.c</u>	olicy http://repo.harica.ar/docum.ents/Data-Privacy-Statement-EN.pdf (d) Certification ation Practices Statement <u>http://www.harica.ar/docum.ents/CPS-EN.pdf</u> with reference Policy (section 5.5.2). Obligations for proper usage of certificates (e) Issuance of Digital HARICA Trusted Authority <u>https://documents.acer-remit.eu/categony/remit-reporting-</u> HARICA documentation about practices and policies is <u>here</u> <u>w/procedures.php</u> .
(b) Privacy Policy () <u>Data Privacy Pelicy</u> Policy and Certifice to Data Retention I Certificates using <u>user-package</u> (. <u>http://repo.harica.c</u>	olicy http://repo.harica.ar/docum.ents/Data-Privacy-Statement-EN.pdf (d) Certification ation Practices Statement <u>http://www.harica.ar/docum.ents/CPS-EN.pdf</u> with reference Policy (section 5.5.2). Obligations for proper usage of certificates (e) Issuance of Digital HARICA Trusted Authority <u>https://documents.acer-remit.eu/categon/iremit-reporting-</u> HARICA documentation about practices and policies is <u>here</u> <u>ar/procedures.php</u> .
(b) Privacy Policy (c) <u>Data Privacy Policy</u> Policy and Certifics to Data Retention (Certificates using <u>user-package(</u>). <u>http://repo.harica.c</u>	olicy http://repo.harica.ar/docum.ents/Data-Privacy-Statement-EN.pdf (d) Certification ation Practices Statement <u>http://www.harica.ar/docum.ents/CPS-EN.pdf</u> with reference Policy (section 5.5.2). Obligations for proper usage of certificates (e) Issuance of Digital HARICA Trusted Authority <u>https://documents.acer-remit.eu/categony/remit-reporting-</u> HARICA documentation about practices and policies is <u>here</u> <u>pr/procedures.php</u> .
(b) Privacy Policy () <u>Data Privacy Policy and Certific</u> to Data Retention (Certificates using <u>user-package</u>). <u>http://repo.harica.c</u>	olicy http://repo.harica.ar/documents/Data-Privacy-Statement-EN.pdf (d) Certification ation Practices Statement <u>http://www.harica.ar/documents/CPS-EN.pdf</u> with reference Policy (section 5.5.2). Obligations for proper usage of certificates (e) Issuance of Digita I HARICA Trusted Authority <u>https://documents.acer-remit.eu/catedon//remit-reporting-</u> HARICA documentation about practices and policies is <u>here</u> <u>ar/procedures.php</u> .
(b) Privacy Policy (c) <u>Data Privacy Policy and Certifics</u> Policy and Certifics to Data Retention (Certificates using <u>user-package</u>). <u>http://repo.harica.c</u>	olicy http://repo.harica.ar/docum.ents/Data-Privacy-Statement-EN.pdf (d) Certification ation Practices Statement <u>http://www.harica.ar/docum.ents/CPS-EN.pdf</u> with reference Policy (section 5.5.2). Obligations for proper usage of certificates (e) Issuance of Digital HARICA Trusted Authority <u>https://documents.acer-remit.eu/cateaon/iremit-reporting-</u> HARICA documentation about practices and policies is <u>here</u> <u>ar/procedures.php</u> .
(b) Privacy Policy (c) <u>Data Privacy Policy</u> Policy and Certifics to Data Retention Certificates using <u>user-package</u> (: <u>http://repo.harica.c</u>	olicy http://repo.harica.ar/docum.ents/Data-Privacy-Statement-EN.pdf (d) Certification ation Practices Statement <u>http://www.harica.ar/docum.ents/CPS-EN.pdf</u> with reference Policy (section 5.5.2). Obligations for proper usage of certificates (e) Issuance of Digital HARICA Trusted Authority <u>https://documents.acer-remit.eu/catego.nv/remit-reporting-</u> HARICA documentation about practices and policies is <u>here</u> <u>tr/pracedures.php</u> .

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 <u>https://www.acer-remit.eu/certificates</u> 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 <u>https://pilot.test-acer-remit.eu/certificates</u> 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 <u>use the same internet browser</u> 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**.

HARICA Hellenic Academic & Research	Institutions Certification Author	ority
Certificate Issuance	Request an ARUS User Digital Cer Please enter your e-mail addres process.	tificate is and your full name. Then click "NEXT" to initiate the ARIS User Digital Certificate request Subscriber's Full name : Name Surname E-mail Address : email-id@domain.gr × Next
Ret	urn to starting page	

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



text:

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**.

HARICA Hellenic Academic & Resear	ch Institutions Certification Authority		
Certificate Issuance	Request an ARIS User Digital Certificate In order to proceed with the request for an ARIS User digital certificate please check your e-mail for a confirmation message from HARICA and follow the instructions. In case you have not received any email or you encounter an error, please contact the ARIS CSD (servicedesk at support.acer-remit.eu).		
Dear Sir/Madam, Please follow the link below in order to continue with your request. • <u>Request Confirmation Link</u> If you did not initiate the request for an ARIS User digital certificate please report this to the ARIS CSD (<u>servicedesk@support.acer-remit.eu</u>). Please do not reply to this e-mail. In case of any questions please contact the ARIS CSD (<u>servicedesk@support.acer-remit.eu</u>)			
HARICA Dublic V ou Infractoucture			

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: <u>https://documents.acerremit.eu/category/remit-reporting-user-package/</u>. 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

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. <u>IDs that do not display the full name in Latin will not be</u> <u>accepted and the request will be denied.</u>

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).



Below are the default ontions to request a certificate unless you are an expert user or received explicit instructions
please leave (1) and (2) selections to the default ones.
Cryptographic Service Provider (1):
Private Key extra protection (2): Message from webpage X
Please click 'Browse' to upload a scan (in 1 c and the filled in APPLICATION FOR OBTAIN resolution of at least 400x400px and must n
and the picture of the Applicant. IDs that do and the request will be denied.
Note: Uploading a valid photo 10 scan and a concept med roman mandatory in order to request a certificate. Identity+form upload: Browse Files uploaded: 0
 This option is usefull if you have installed special cryptographic software or hardware (eg smart cards or PKCS#11 eTokens).
(2) ATTENTION! By selecting "YES" your private key will be further protected and marked unexportable. This means you will not be able to transfer it to another computer <u>NOR</u> to another browser.
I accept the Terms of Use and Request the ARIS User Digital Certificate.

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).

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		
and the nicture of the Applicant. TDs that r Message from webpage X		
be denied. Note: Uploading a valid photo ID scan and Identity+form upload: Browse		
Files uploaded: 1 (1) This option is usefull if you have means the function of the function o		
I accept the Terms of Use and Request the ARIS User Digital Certificate.		

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).

Private key protection
Please insert the password to protect your private key. Please note that the password is required to obtain and use the certificate and should therefore be secured and not forgotten.
Please repeat the password:
Save private key

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**.



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).



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	, serialNumber
L=Ljubljana, C=SI has been rejected.	D=Agency for the Cooperation of Energy Regulators,
The validator has left the following feedback: The details supplied are not correct. Please proceed by following the instructions.	
Please contact the ARIS CSD (<u>servicedesk@support.acer-remit.eu</u>) for further deta	ails
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.

Certificate Import Wizard	X
	Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust issued to a certificate revocation lists from your disk to a certificate strone. A certificate, which is issued by a certification authority, is used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, disk Next.
	<back next=""> Cancel</back>

3. Choose Next.

File to Import	
Specify the file you want to import.	
File name:	
\\ccf2\dfs\winHome\home\kosto\Desktop\haricacert.p1	Browse
Note: More than one certificate can be stored in a single	file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Ce	rtificates (.P7B)
Microsoft Serialized Certificate Store (.SST)	
earn more about certificate file formats	
earn more about <u>certificate file formats</u>	
earn more about <u>certificate file formats</u>	



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

Pass	vord					
	To maintain security, the private key was protected with a password.					
	Type the parsword for the private key					
	Password					
	••••••					
	\fbox Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.					
	☑ Mark this key as exportable. This will allow you to back up or transport your					
	kows at a later time					
	keys at a later time.					
	keys at a later time.					
	keys at a later time. Include all extended properties.					
Learr	keys at a later time. Include all extended properties. more about protecting private keys					
Learr	keys at a later time.					
Learr	keys at a later time.					

5. Choose Next.

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Output the select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse
Learn more about <u>certificate stores</u>
< Back Next > Cancel



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**.

Create a Password	and the second second	×
	Create a password to	protect this item.
	Create a new passw Password for:	ord for this item. CryptoAPI Private Key
	Password: Confirm:	•••••
	< Back	Finish Cancel



9. Choose OK.

Importing a new private exchange key	
An application is creating a Protected item.	
	Certificate Import Wizard
CyptoAPI Private Key	The import was successful.
Security level set to High Set Security Level	
OK Cancel Details	ОК

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

The Internet Properties	Certificates	×
General Security Privacy Content Connections Programs Advanced	Intended purpose: <a>l>	•
Use certificates for encrypted connections and identification.	Personal Other People Intermediate Certification Authorities Trusted Root C	Certification
Clear SSL state Certificates Publishers	Issued To Issued By Expiratio	Friendly Name
AutoComplete	Hellenic Academic and R 13/5/2020	Private Key
AutoComplete stores previous entries Settings	HARICA-ManagementCA 26/5/2019	Garris Tastapo
on webpages and suggests matches	Communications Server 1/2/2016	<none></none>
for you.	Aristotle University of T 11/4/2019	<none></none>
Feeds and Web Slices	Aristotle University of T 5/4/2018	<none></none>
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.	Aristotle University of T 1/5/2020	<none></none>
		4
	Import Export Remove	Advanced
	Certificate intended purposes	
	Client Authentication, Secure Email, Document Signing	
		View
OK Cancel Apply	Learn more about <u>certificates</u>	Close



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.

	x
lii\ 🗉	
0	e
Rew Window	Ctrl+N Shift+P
🗔 Restore Previous Session	
Zoom - 100% +	- 2 ⁷
Edit 🔏 🖒	Ê
III Library	>
Add-ons Ctrl+	Shift+A
Options	
Customize	
Open File	Ctrl+O
Save Page As	Ctrl+S
🖶 Print	
Q Find in This Page	Ctrl+F
More	>
Web Developer	>
⑦ Help	>
Ctrl+	Shift+Q

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.

			Certifica	te Manager		
Your Certificates	People	Servers	Authorities	Others		
ou have certificates fro	om these org	anizations th	at identify you			
Certificate Name		Securi	ty Device	Serial Number	Expires On	
Insenti Satigente MILA		Softwar	e Security Device	41/10/00103462440	Thursday, April 11, 2019	
Garatic Radiographic		Softwar	e Security Device	7181/1414945-0102	Sunday, May 26, 2019	
View			Terrent			
View Backi	Jp Bac	kup All	I <u>m</u> port	<u>D</u> elete		
						OK

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

	^	Name	~	Date modified	Туре	Size
		🐊 firefox certificate in	nport	14/5/2018 3:05	μμ File folder	
oulos		🐊 hosted ssl		10/5/2018 11:4	8 πμ File folder	
		🐊 windows certificate	import	14/5/2018 1:31	μμ File folder	
) D-1		laricacert.p12		14/5/2018 1:03	μμ Personal Informati	
equence						
11	E					
uploads						
ents						
k						
rPro						
Hia (1)						
uia (1)						
a						
sis	v 4					•
File name:	haricacert.p12			-	PKCS12 Files (*.p12;*.pfx)	-
					Open T Can	cel
					Can	

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.

		Certificat	te Manager		
Your Certificates	People	Servers Authorities	Others		
You have certificates fr	om these orga	anizations that identify you			
Certificate Name		Security Device	Serial Number	Expires On	EQ.
	1	Software Security Device	41,75,48,48,05,61,0465,77	Thursday, April 11, 2019	
^a Hellenic Academic an	d Research In	Software Security Device sti	718171014100000	Sunday, May 26, 2019	
		Software Security Device		Wednesday, May 13, 2020	
View Back	up Bac	kup All Import)elete	Ok	<



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.

 Open the New Tab page Continue where you left off 	Open the New Tab page
O Continue where you left off	
	O Continue where you left off
O Open a specific page or set of pages	Open a specific page or set of pages

3. Scroll down and click on Manage Certificates.

Manage certificates Manage HTTPS/SSL certificates and settings	Z
Content settings Control what information websites can use and what content they can show you	Þ
Clear browsing data Clear history, cookies, cache, and more	•



4. Click on Import.

≡ Settings	Q Search setting	gs
	By turning this off,	, you can sign in to Google sites like Gmail without signing in to Chron
Certificates Intended purpose: <a>All>	×	vice to help complete searches and URLs typed in the address bar
Personal Other People Intermediate Certification Authorities Truste	ed Root Certification	vice to load pages more quickly
Issued To Issued By Expiratio F	riendly Name <none></none>	o help resolve navigation errors
10/24/2020 10/24/2020 10/24/2020 10/18/2020	<none> <none> Private Key</none></none>	ur device from dangerous sites
		3rowsing n information and page content to Google
Import Export Remove	Advanced	usage statistics and crash reports to Google
Certificate intended purposes Client Authentication	View	o help resolve spelling errors ting by sending what you type in the browser to Google
	Close	:k" request with your browsing traffic
	Allow sites to chee	ck if you have payment methods saved
	Manage certificate Manage HTTPS/S	es SL certificates and settings

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. <u>www.acer-remit.eu/certificates</u> for the production environment, or
- B. <u>https://pilot.test-acer-remit.eu/certificates</u> 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 <u>www.acer-remit.eu/certificates</u> and select the link under the client (user) certificates tab. For the test environment, use https://pilot.test-acer-remit.eu/certificates.



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.

HARICA Hellenic Academic & Research	Institutions Certification Authority
Certificate Issuance Certificate Action Certificate Search Certificate Search Certificate Search	ARIS User Digital Certificate revocation A digital certificate revocation request can only be submitted by the owner of that certificate. Please enter your e-mail address, the revocation code you received during the acceptance-retrieval of the certificate and the reason you are requesting this revocation. E-mail address : Revocation code : Revocation code : Submit the request

Select the revocation reason as depicted below:

HARICA Hellenic Academic & Research	Institutions Certification Authority
Certificate Revocation	ARIS User Digital Certificate revocation A digital certificate revocation request can only be submitted by the owner of that certificate. Please enter your e-mail address, the revocation code you received during the acceptance-retrieval of the certificate and the reason you are requesting this revocation.
ACER REMIT Information System	E-mail address : Revocation code : Revocation reason Certificate is no longer in use Certificate values are not valid Lost private key Note: In case you have lost the revocation code a Exposed nrivate key K at support.acer-remit.eu)



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).



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.

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. <u>www.acer-remit.eu/certificates</u> for the production environment, or
- B. <u>https://pilot.test-acer-remit.eu/certificates</u> 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 <u>www.acer-remit.eu/certificates</u> (or <u>https://pilot.test-acer-remit.eu/certificates</u> 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 <u>servicedesk@support.acer-remit.eu</u>.





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.

HARICA	Institutions Certification A	authority	GU
ACER Agency for the Cooperation of Energy Regulators	Request an ARIS machine-b	o-machine digital certificate	
Certification Authority	A request for a machine-to	-machine digital certificate can be	e submitted only by users who are already holders of an
Certificate Issuance	appropriate ARIS User Dig	ital Certificate.	and farming
Cartificate Revocation	Please enter a certificate	Windows Security Select a Certificate	× urMachineName.YourOrganization.tld, where
	YourOrganization.tld is no	Site acer.dev.harica.gr needs your credentials:	ess used when requesting an ARIS User Digital Certificate
Certificate Search	for physical user (if your	22	elisted yet and you keep seeing this message, please
A R I S ACER REMIT Information System	contact servicedesk at su certificate request proced	Valid From: 10/25/2018 to 10/24/2020 Click here to view certificate properties More choices	t" to authenticate with your user certificate and start the
CHRIST Digital Continues	Certificate Name (FQDN)	OK Gancel	

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.









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

HARICA Hellenic Academic & Research	Institutions Certification Authority	GU
Approxy for the Cooperation of Energy Replaces	Request an ARIS machine-to-machine digital certificate Certificate Policy Acceptance	
Certificate Issuance	I, (Your name in english) declare that by applying for a HARICA Certific agreed with HARICA's Terms and Conditions and Certification Practices . Moreover, I declare the this agreement for machine . Official Identity Declaration	ate, I have read and at I will always adhere to
ACER REMIT Information System	I officially declare that at the time of this request my full name is (your e-mail address is I am legally in possession of a digital certificate with emailAddress: CN: serialNumber: Private Key created and stored in software CSP,0=Agency for the Cooperation of EmRegulators,L=Ljubljana,C=SI, I am responsible for the machine named I in its certificate: (C), O=Agency for the Cooperation of Energy Regu	hame in english), my the Distinguished Name OU=Class B - ergy r and the fields contained lators, L=Ljubljana,
	A new private key has been created for you, please insert a password to protect it Please repeat the password Export private key	

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



<u>Note for IE users</u>: 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: <u>https://documents.acer-remit.eu/category/remit-reporting-user-package/</u>

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.**

You can download the private key from	here.
Form upload: I agree to the Terms of Use and Requ	Browse he ARIS machine-to-machine digital certificate.

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.

Certificate Issuance 2 Certificate Issuance 2 Certificate Revocation 2 Certificate Revocation 2 Certificate Search 3	The Carety for the Cooperation Cartification Authority Cartificate Issuance Cartificate Revocation Cartificate Search Cartificate Search <th>Certificate Issuance Certificate Revocation Certificate Search Certificate Search Certificate Search After A</th> <th>Request submitted vur request for a digital certificate with the details our request</th>	Certificate Issuance Certificate Revocation Certificate Search Certificate Search Certificate Search After A	Request submitted vur request for a digital certificate with the details our request
Certificate Issuance Certificate Issuance Certificate Issuance Certificate Revocation Certificate Revocation Certificate Search	Certificate Issuance Percentificate Issuance Certificate Issuance Pour request for a digital certificate with the details O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI has been successfully submitted. Certificate Search After approval of your request by ACER you will receive an e-mail from HARICA with further instructions on how to obtain an ARIS digital certificate. If the e-mail is not received in 5 working days please contact the ARIS CSD (servicedesk at support.acer-remit.eu).	Certificate Issuance Certificate Revocation Certificate Revocation Certificate Search Certificate Search After Af	Request submitted our request for a digital certificate with the detail: , O=Agency for the Cooperation of nergy Regulators, L=Ljubljana, C=SI has been successfully submitted.
Certificate Issuance Your request for a digital certificate with the details O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI has been successfully submitted. Certificate Search After approval of your request by ACER you will receive an e-mail from HARICA with further instructions on how to obtain an ARIS digital certificate. If the e-mail is not received in 5 working days please contact the ARIS CSD (servicedesk at support.acer-remit.eu).	Certificate Issuance Certificate Issuance Certificate Revocation Certificate Search Certificate Search	Certificate Issuance Your Certificate Revocation Energy Certificate Search After ARIS an A	our request for a digital certificate with the details, O=Agency for the Cooperation of nergy Regulators, L=Ljubljana, C=SI has been successfully submitted.
Certificate Revocation Your request for a digital certificate with the details O=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI has been successfully submitted. Certificate Search After approval of your request by ACER you will receive an e-mail from HARICA with further instructions on how to obtain an ARIS digital certificate. If the e-mail is not received in 5 working days please contact the ARIS CSD (servicedesk at support.acer-remit.eu). That Deput certificate .	Certificate Revocation Your request for a digital certificate with the details , 0=Agency for the Cooperation of Energy Regulators, L=Ljubljana, C=SI has been successfully submitted. Certificate Search After approval of your request by ACER you will receive an e-mail from HARICA with further instructions on how to obtain an ARIS digital certificate. If the e-mail is not received in 5 working days please contact the ARIS CSD (servicedesk at support.acer-remit.eu).	Certificate Revocation Energy Certificate Search After After an A	our request for a digital certificate with the details, O=Agency for the Cooperation of nergy Regulators, L=Ljubljana, C=SI has been successfully submitted.
Certificate Search Certificate Search After approval of your request by ACER you will receive an e-mail from HARICA with further instructions on how to obtain an ARIS digital certificate. If the e-mail is not received in 5 working days please contact the ARIS CSD (servicedesk at support.acer-remit.eu).	Certificate Search Certificate Search After approval of your request by ACER you will receive an e-mail from HARICA with further instructions on how to obtain an ARIS digital certificate. If the e-mail is not received in 5 working days please contact the ARIS CSD (servicedesk at support.acer-remit.eu).	Certificate Search After A R I S an A	nergy regulators, c-cjubijana, c-oz nas been successibiliy submitted.
After approval of your request by ACER you will receive an e-mail from HARICA with further instructions on how to obtain an ARIS digital certificate. If the e-mail is not received in 5 working days please contact the ARIS CSD (servicedesk at support.acer-remit.eu).	After approval of your request by ACER you will receive an e-mail from HARICA with further instructions on how to obtain an ARIS digital certificate. If the e-mail is not received in 5 working days please contact the ARIS CSD (servicedesk at support.acer-remit.eu).	After an A	
		ACER REMIT Information System Supp	ter approval of your request by ACER you will receive an e-mail from HARICA with further instructions on how to obtain ARIS digital certificate. If the e-mail is not received in 5 working days please contact the ARIS CSD (servicedesk at apport.acer-remit.eu).

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.







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**.



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.



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. <u>www.acer-remit.eu/certificates</u> for the production environment, or
- B. <u>https://pilot.test-acer-remit.eu/certificates</u> 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 <u>www.acer-remit.eu/certificates</u> (or <u>https://pilot.test-acer-remit.eu/certificates</u> 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.

HARICA Hellenic Academic & Research	Institutions Certification Authority
Certificate Issuance	Machine-to-machine digital certificate revocation A digital certificate revocation request can only be submitted by the owner of that certificate. Please enter the Certificate Name (FQDN), the revocation code you received during the acceptance-retrieval of the certificate and the reason you are requesting this revocation. Certificate Name (FQDN): Revocation code : Revocation code : Certificate number of the certificate revocation code revocation requesting the code revocation request in the revocation code revocation request revocation request revocation code revocation request revocation request revocation revocation request revocation request revocation revoca
THE TEST Digital Certificates	Submit the request Note: In case you have lost the revocation code please contact the ARIS CSD (servicedesk at support.acer-remit.eu)

Figure 37: Revocation details

HARICA Hellenic Academic & Research	Institutions Certification Authority
Acer Remit Information System	Machine-to-machine digital certificate revocation A digital certificate revocation request can only be submitted by the owner of that certificate. Please enter the Certificate Name (FQDN), the revocation code you received during the acceptance-retrieval of the certificate and the reason you are requesting this revocation. Certificate Name (FQDN): Revocation reason: Select - Certificate values are not valid Lost private key Exposed private key Exposed private key Exposed private key



A C E R	Request for certificate revocation	
Certification Authority	Your request for the revocation of the certificate with Distinguished Name	, O=Agency for the
Certificate Issuance	Cooperation of Energy Regulators, L=Ljubljana, C=SI has been successfully sub	omitted. You will be notified by
Certificate Revocation	e-mail when the revocation procedure is complete.	
Certificate Search		



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

The certificate revocation for the entity with Distinguished Name: 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.