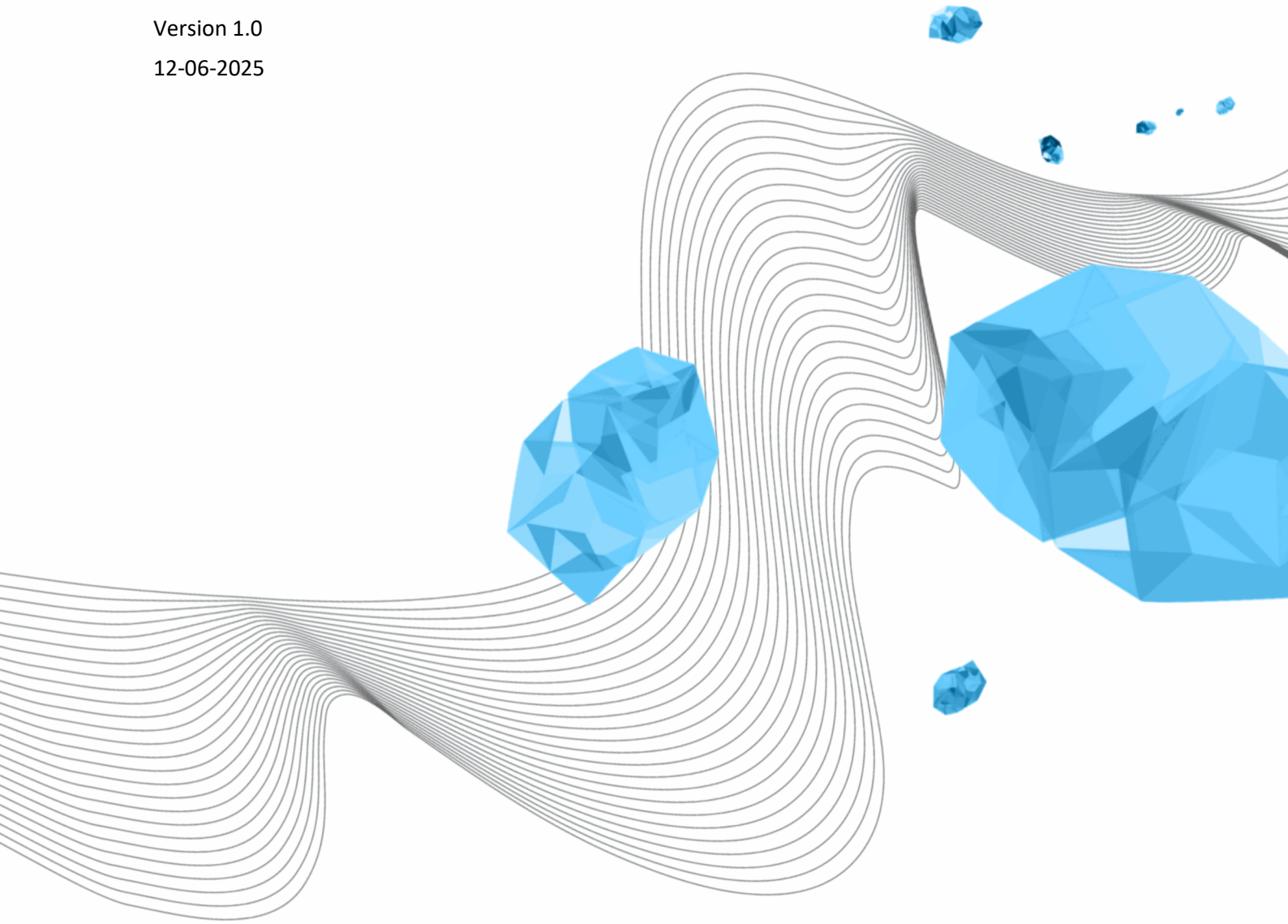
Status: Final
Date of adoption by LISA-MT: 10-06-2025
Revised:
Author: Peter Peters

GUIDELINES ON USING CERTIFICATES

Peter Peters

Version 1.0

12-06-2025



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Guidelines on Using Certificates

SUBJECT
Identification

PROJECT
[Project]

REFERENCE
LISA-0368

VERSION (STATUS)
1.0

DATE
12-06-2025

AUTHOR(S)
Peter Peters

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	REMARKS
0.1	1-2-2025	Peter Peters	Initial concept
0.2	11-2-2025	Peter Peters	Revocation added. Appendix I, HARICA processes added
0.3	1-4-2025	Peter Peters	Remarks processed Not all certificates are free.
0.4	14-5-2025	Peter Peters	Remarks Security team processed Updated according to the latest developments in processes and procedures. Changed terminology to be in line with the policy on cryptography.
1.0	12-6-2025	Peter Peters	Version adopted by LISA-MT Published version.

CONTENT

1 INTRODUCTION

This document accompanies the ***Policy on Cryptography***[1] established by LISA-MT on 10th June 2025.

These guidelines help implement certificates for personal use, on computer systems and for other purposes. This document also lists the allowed Certificate Authorities (CA) and how the University limits the use of other CAs.

A certificate is a digitally signed file that contains information about the identity of a website, organisation, piece of data or person. A trusted CA issues these certificates to verify the information provided.

Four kinds of certificates will be subject to these guidelines. Chapters 3 to 6 will present guidelines for each kind of certificate. Chapter 2 will provide some general guidelines.

1. Server certificates: These certificates have three main goals:
    a. **Authentication**: Verify the identity of the website[2] or organisation to which you're connecting.
    b. **Encryption**: Establish a secure connection between your device and the website.
    c. **Trust**: Establish trust with your users by ensuring an attacker does not spoof (fake) or impersonate your website.
2. Client certificates: Also, these certificates have three main goals:
    a. **Authentication**: Verify an individual's identity to access a secure system, network, or application.
    b. **Authorisation**: Grant access to specific resources, applications, or systems based on the individual's role, privileges, or clearance level.
    c. **Digital Signatures**: Allow individuals to sign email messages digitally[3]. Sometimes, client certificates can be used to sign digital content, but for that goal, other certificates (see items 3 and 4 below) are more often used.
3. Code signing certificates: These are used to digitally sign software code, ensuring its authenticity and integrity. The main goals of Code Signing Certificates are:
    a. **Authentication**: Verify that a trusted developer or organisation has created the software code.
    b. **Integrity**: Ensure that the software code has not been tampered with or modified since it was signed.
    c. **Authenticity**: Prove that the software code comes from a known and trusted source.
4. Document signing certificates: These certificates are closely related to Code signing certificates with respect to **Authentication** and **Integrity**. The third important goal of document signing, though, is **non-repudiation**. The signer of the document commits to the content of the document.

[1] https://www.utwente.nl/en/cyber-safety/cybersafety/legislation/policy-on-cryptography.pdf
[2] While the introduction mentions only websites, certificates can be used for other connections, too. Examples are connections between mail clients and servers. For clarity, we will assume websites in the remainder of this document. If something besides websites is meant, this will be clearly indicated.
[3] This relates to S/MIME email messages.

2 GENERAL GUIDELINES

2.1 CERTIFICATE AUTHORITIES

The University only allows a subset of existing Certificate Authorities (CAs) to issue certificates on the University's behalf.

For server certificates, only HARICA[4] and Let's Encrypt[5] are allowed to issue certificates.

For client certificates for email addresses @utwente.nl and @student.utwente.nl, only HARICA is allowed to issue certificates. The University does not allow using other email addresses in client certificates.

2.2 CAA RECORDS

CAA records[6] offer the University a way to show the world which CAs can issue certificates. See 2.1 for allowed CAs.

The University only allows *issue* and *issuemail* CAA records. An *issuewild* record is not permitted. The *issue* CAA record for all domains maintained by the University will include harica.org and letsencrypt.org. The *issuemail* CAA record for utwente.nl will only show an entry for HARICA. All other domains will show an *issuemail* CAA record prohibiting the issuance of a client certificate for that domain.

The CAA record will also show an entry for reporting invalid requests sent to other CAs. That CAA record will show that those reports should be sent to *scs-ra@utwente.nl*. This record will be present in all domains.

2.3 ISSUANCE OF CERTIFICATES

A certificate request should never be done from a public computer. This is implied in the ***Policy on Cryptography*** but is mentioned here for clarification.

2.4 REVOCATION

A certificate revocation indicates to the CA, and consequently, the whole world, that a certificate is no longer valid, irrespective of the validation period included in the certificate.

Typically, the task of revoking a certificate lies with the **Key Manager**[7]. Guidelines for revocation of each kind of certificate are included in the relevant chapters.

A **Key Custodian** can and will, in certain situations, start a revocation process independently:

- When informed by LISA Security Management that a server has been compromised and one or more private keys might have been accessed.
- When informed by LISA Security Management that a private key might have been compromised.

[4] Hellenic Academic and Research Institutions Certification Authority (HARICA); https://www.harica.gr/
[5] Let's Encrypt; https://letsencrypt.org/
[6] https://en.wikipedia.org/wiki/DNS_Certification_Authority_Authorization
[7] For terms used in these Guidelines, see the **Policy on Cryptography** if not otherwise referenced.

- In the case of a personal certificate, when a user is no longer an employee or a student at the University and has not revoked their certificate themselves.

3 GUIDELINES FOR SERVER CERTIFICATES

The University's guidelines are based on advice published by reputable organisations. If possible, we also use tests provided by some of these organisations to monitor adherence to the guidelines.

3.1 DUTCH STANDARDISATION GUIDELINES

As a public university, the University has to adhere to the guidelines of the Dutch Standardisation Forum[8]. Most important are the following guidelines:

- HTTPS: all web servers must use HTTPS for communication. If the server listens on the HTTP port, it should redirect to the HTTPS port. Non-web servers must use an equivalent protocol and show the same behaviour.
- TLS version: the protocol for encryption must be at least version TLS 1.2.
- HSTS: to prevent attackers from interfering with clients making a connection on the HTTP port, HSTS must be used with a max-age directive's value greater than 10368000.

3.2 CYPHER SUITES

SURF[9] and the Dutch NCSC[10] have published guidelines regarding cypher suites. They are used for different parts of the negotiation and encryption between parties. Both make a distinction between insufficient, sufficient and good algorithms. The University does not allow algorithms that are insufficient. Server administrators must have a plan in place to replace any insufficient algorithms. They might be considered insufficient next time a certificate is requested for that server. Good algorithms are always allowed.

Algorithm	**Good**	**Sufficient**	**Insufficient**
Certificate Verification	ECDSA, RSA		DSS, EXPORT-variants, PSK, Anon, NULL
Hash Function for Certificate Verification	SHA-512, SHA-384, SHA-256		SHA-1, MD5
Key Exchange	ECDHE	DHE	RSA, DH, ECDH, KRB5, NULL, PSK, SRP
Hash Function for Key Exchange	Support for SHA-256, SHA-384, SHA-512		No support for SHA-256, SHA-384, SHA-512
Bulk Encryption	AES-256-GCM, ChaCha20-Poly1305, AES-128-GCM	AES-256-CBC, AES-128-CBC	3DES-CBC, AES-256-CCM_8, AES-128-CCM_8, IDEA, DES, RC4, NULL

[8] https://www.forumstandaardisatie.nl/en/netherlands-standardisation-forum
[9] https://sec.surf.nl/wp-content/uploads/2024/01/Handreiking-TLS-v1.3.pdf
[10] https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2021/january/19/it-security-guidelines-for-transport-layer-security-2.1/IT+Security+Guidelines+for+Transport+Layer+Security+v2.1.pdf

Hash Function for Bulk Encryption and Random Number Generation	HMAC-SHA-512, HMAC-SHA-384, HMAC-SHA-256	HMAC-SHA-1	HMAC-MD5
RSA Key Length	3072 bits or more	2048 – 3071 bits	Less than 2048 bits
Elliptic curves	Secp384r1, secp256r1, curve 448, curve 25519		Secp224r1, others

3.3 TESTING

The **Key Manager** should test the configuration before requesting a certificate. Acceptable tests are SSL Labs[11] or internet.nl[12] (Dutch).

LISA uses a Certificate Transparency Monitor[13] tool to audit issued certificates for all the University's domains. LISA then uses SSL Labs to test for compliance. Each server should score at least an A[14]. If not, the **Key Manager** will be informed of that fact and asked to remedy the cause of the low score.

3.4 AUTOMATION

If possible, the Automatic Certificate Management Environment (ACME[15]) should be used.

ACME can be used for obtaining and managing TLS certificates from certificate authorities (CAs). It is designed to simplify the process of obtaining and renewing TLS certificates.

Here are some key features and benefits of the ACME protocol:

1. Automated Certificate Management: ACME allows for automated certificate issuance, renewal, and revocation, making it easier to manage TLS certificates.
2. Simplified Certificate Obtaining: The protocol provides a standardised way for organisations to obtain TLS certificates from CAs, eliminating the need for manual intervention.
3. Improved Security: ACME ensures that only authorized individuals or systems can request and obtain TLS certificates, reducing the risk of certificate abuse.
4. Reduced Administrative Burden: By automating many aspects of certificate management, ACME reduces the administrative burden on organisations, freeing up resources for more critical tasks.

Especially benefit number 4 will become more critical in the next few years. Currently, certificates have a lifetime of just over one year. This will be reduced in the next couple of years.[16]

[11] https://www.ssllabs.com/ssltest/
[12] https://internet.nl/test-site/
[13] https://sslmate.com/certspotter/
[14] Currently, students and student associations are exempt from this requirement.
[15] https://en.wikipedia.org/wiki/Automatic_Certificate_Management_Environment
[16] As of March 15, 2026, the maximum lifetime for a TLS certificate will be 200 days. As of March 15, 2027, the maximum lifetime for a TLS certificate will be 100 days. As of March 15, 2029, the maximum lifetime for a TLS certificate will be 47 days.

3.5 REVOCATION

A **Key Manager** should revoke a certificate when:

- a system or application is decommissioned;
- a new certificate is issued for the same CN and SAN;
- a new certificate is issued for the same CN but a different SAN;
- and any other situation where a certificate is no longer used.

For how to revoke a server certificate, see the Appendix (chapter 8.4).

4 GUIDELINES FOR CLIENT CERTIFICATES

Client certificates are personal. They will contain the name and email address of the person making the request. Like any other credential, certificates are not allowed to be shared.

Client certificates should not be requested from a public or shared computer.

Client certificates should not be installed in browsers or email clients shared by multiple people.

When installing a certificate in an application, a strong password should be used to access the certificate.

If certificates are stored outside the applications they are used in, that storage should also be secured with a strong password. This can be either a Hardware Security Module (HSM)[17] or dedicated vault software[18].

The user, or a representative, should revoke a client certificate according to the **Policy on Cryptography**. For how to revoke a client certificate, see the Appendix (chapter 8.6).

[17] https://en.wikipedia.org/wiki/Hardware_security_module

[18] Some password managers support the secure storage of files. In these cases, these managers are considered dedicated vault software.

5 GUIDELINES FOR CODE SIGNING CERTIFICATES

Remark: This chapter is still a work in progress.

Code signing certificate private keys must be generated and stored in a cryptographic module that meets at least FIPS 140-2 Level 3, FIPS 140-3 Level 3, or Common Criteria Protection EAL 4+[19].

Private keys used for other certificates shall never be used for code signing. Revocation of such a certificate does not impact the code being signed.

Include a timestamp with every signed artefact. This ensures the certificate's validity is tied to a specific date and time, even if the CA revokes the certificate later.

For each use of the certificate, it should be checked for validity (not expired, not revoked).

All components (e.g., executables, libraries, scripts) shall be signed if the software is signed. Unsigned components can be vectors for malicious activity.

Include version information in the signing process to differentiate between different versions of the same code.

Automate the code signing process as part of your build and deployment workflows. Ensure that automated processes are secure and do not expose private keys to unauthorized systems or personnel.

Keep detailed logs of all code signing activities, including who signed the code and when. Regularly audit these logs to detect any unauthorized or suspicious activity. Keep detailed logs of all systems requiring (parts of) code to be signed.

Always test the code signing process in a development environment before deploying it to production. Verify that signatures are applied correctly and that they remain intact after distribution. Use different private keys for development, testing and production.

[19] https://cabforum.org/uploads/Baseline-Requirements-for-the-Issuance-and-Management-of-Code-Signing.v3.9.pdf

6 GUIDELINES FOR DOCUMENT SIGNING CERTIFICATES

Remark: This chapter is still a work in progress.

For as far as relevant, the guidelines for document signing certificates will be identical to the guidelines in chapter 5.

7 REVIEW OF THESE GUIDELINES

These guidelines will be reviewed every year. The following review will be in mid-2026. There may be grounds for an interim evaluation. If that evaluation gives cause to do so, these guidelines will be adjusted sooner.

The review will be conducted in cooperation with the Product Focus Group for Certificate Services.

The CISO of the University of Twente is responsible for these guidelines.

LISA-MT determines these guidelines. In cases not provided for in this regulation, LISA-MT decides with the CISO.

8 APPENDIX I: HARICA PROCESSES

This appendix will help users of the HAIRCA interface adhere to the ***Policy on Cryptography*** and these guidelines. It contains information about the interface, how to log onto the website and fill in the forms correctly.

> Not all certificates available through HARICA are free. If you select one with a fee attached, you must pay for the certificate by Credit Card. You will not be able to claim this expense at the University.

8.1 ACME

The easiest way to request server certificates is by using ACME. Currently, this is not possible in a secure way. When HARICA offers ACME EAB[20], this chapter will be updated.

8.2 LOGGING IN

Requesting, revoking, and other HARICA interactions must be done through their Certificate Management interface. It can be reached at https://cm.harica.gr/.

HARICA offers authentication through SURFconext. You can use the Academic Login button and continue logging into the University's SSO system.[21]

You will be presented with your personal dashboard. It will show the issued certificates and offer options for your certificate management tasks.

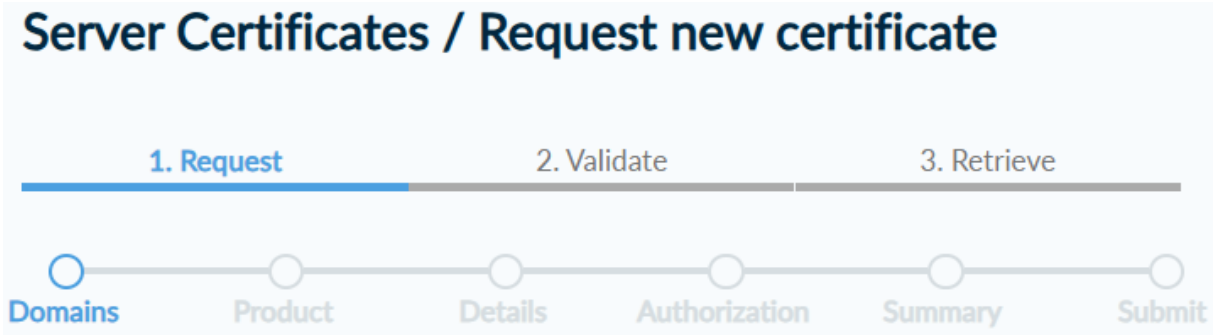
8.3 SERVER CERTIFICATE REQUESTS

Select **Server** in the menu on the left.

Follow the steps in the process.

[20] External Account Binding, where an organization uses different ACME accounts controlled by external accounts.

[21] If assigned specific roles in the Certificate Management interface, you might be presented with a question for a second factor.



How to proceed with a request will be described in the following paragraphs (8.3.1 to 8.3.5).

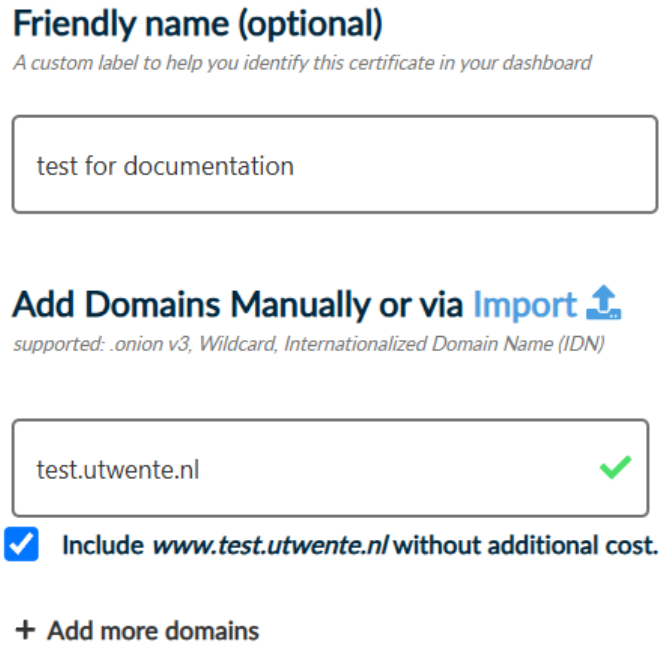
After the request, you will receive an email telling you your request is pending until it is validated by a **Key Custodian**. Validation can take up to five workdays. You may receive more messages with feedback from the **Key Custodian**. Take care of those messages because they might impede validation if you do not.

Finally, your request will be validated, and you will receive a message telling your certificate is ready. Log in again to download your certificate (see 8.3.6).

8.3.1 DOMAINS

Fill in the form.

- *Friendly name* can be anything that might help you recognise the certificate later. It does not need to be the computer's name (CN).
- *Add Domains Manually* has to contain the CN. If you have SANs, you can use *+ Add more domains* to add them individually.
- If you have a list of domains, you can use *Import* to add them via a CSV file.

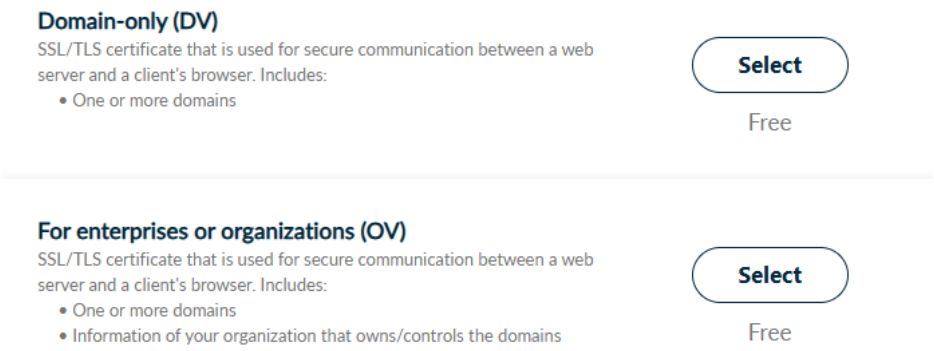


The first domain added or in the imported list will be used as the CN. All domains will be in the SAN parameter of the certificate.

Remember, all Domains added must exist when a certificate is requested, e.g., they must be resolvable.

8.3.2 PRODUCT

Preferably, use OV certificates. These will be linked to the University[22].



In the following paragraphs, a request for an OV certificate will be presumed.

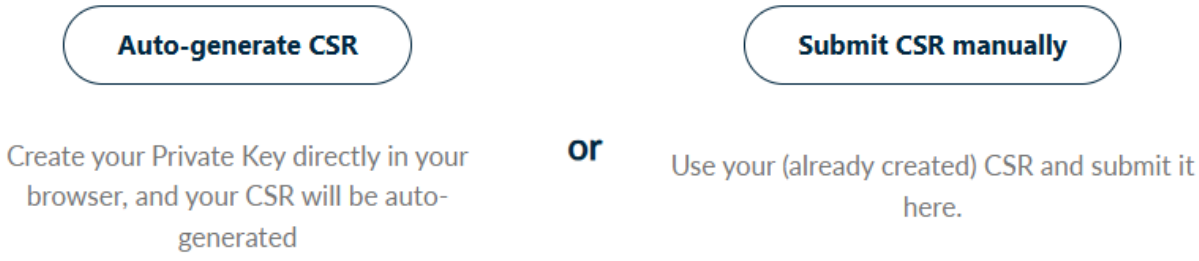
8.3.3 DETAILS

HARICA will show the Organisation Information that will be added to the certificate, no matter what information is in the CSR.

8.3.4 AUTHORIZATION

Verify the information and confirm your agreement with the terms mentioned.

8.3.5 SUBMIT



Preferably, you already have generated a CSR, so you have to *Submit CSR manually*. Then, you can paste your CSR and *Submit* the request.

After you submit the request, you will be returned to the dashboard. You will notice the request is pending. It can take up to five workdays for it to be validated.

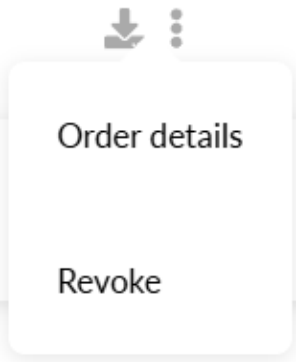
8.3.6 DOWNLOAD

You can download the certificate and install it on your system.

[22] If you request a certificate for a website you don't want to be related to the University, you can select a Domain-only certificate.

8.4 SERVER CERTIFICATE REVOCATION

As mentioned in paragraph 3.5 a **Key Manager** has to revoke a certificate under some conditions. This paragraph will show the steps necessary.



On your dashboard, you will find the certificates you requested. Click the three vertical bullets and select **Revoke**.

On the next page, you will find information about the certificate revocation. Make sure to specify the correct reason.

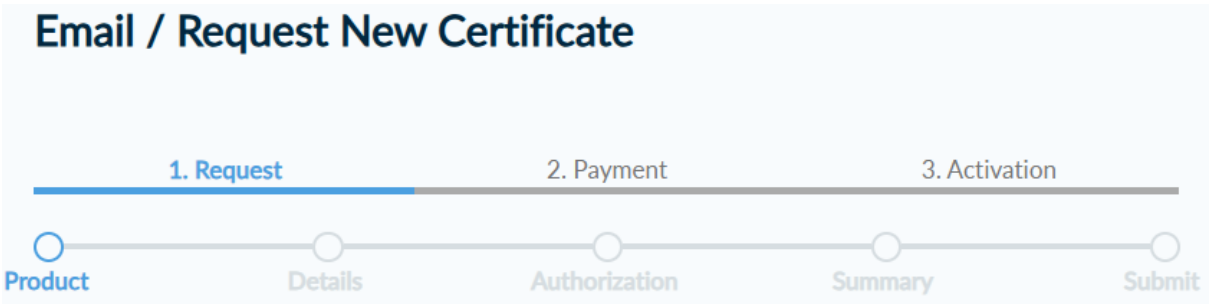
1. **Certificate's subject information has changed**. Use this reason when the Common Name or SAN has changed, and a new certificate with the changed information has been issued[23].
2. **Subscriber no longer controls**… This is when a domain part of the certificate SAN is transferred to another organisation.
3. **Unspecified reason**. This reason is not allowed to be used.
4. **Private key is compromised**. This reason is used when there is proof that the private key of a certificate is compromised. Also, report this incident to CERT-UT[24].
5. **Domain name or Full Name**… There are currently no situations where this is to be expected.
6. **Website or email address is no longer in use**. This reason should be used when a website is decommissioned.
7. **Private key is exposed**. This is similar to bullet 4 above, but there is no proof that the private key is compromised. This is the case when the system where the key is stored is compromised. Also, report this incident to CERT-UT.
8. **Existing certificate has been replaced**. Use this when a new certificate with the same information has been issued. This is similar to bullet 1.

If asked for, provide more details about the reason in the field below reason and click *Revoke*. The certificate will show as Revoked in your dashboard, and you will receive an email with information about the revocation.

8.5 CLIENT CERTIFICATE REQUEST

Select **Email** in the menu on the left.

Follow the steps in the process.



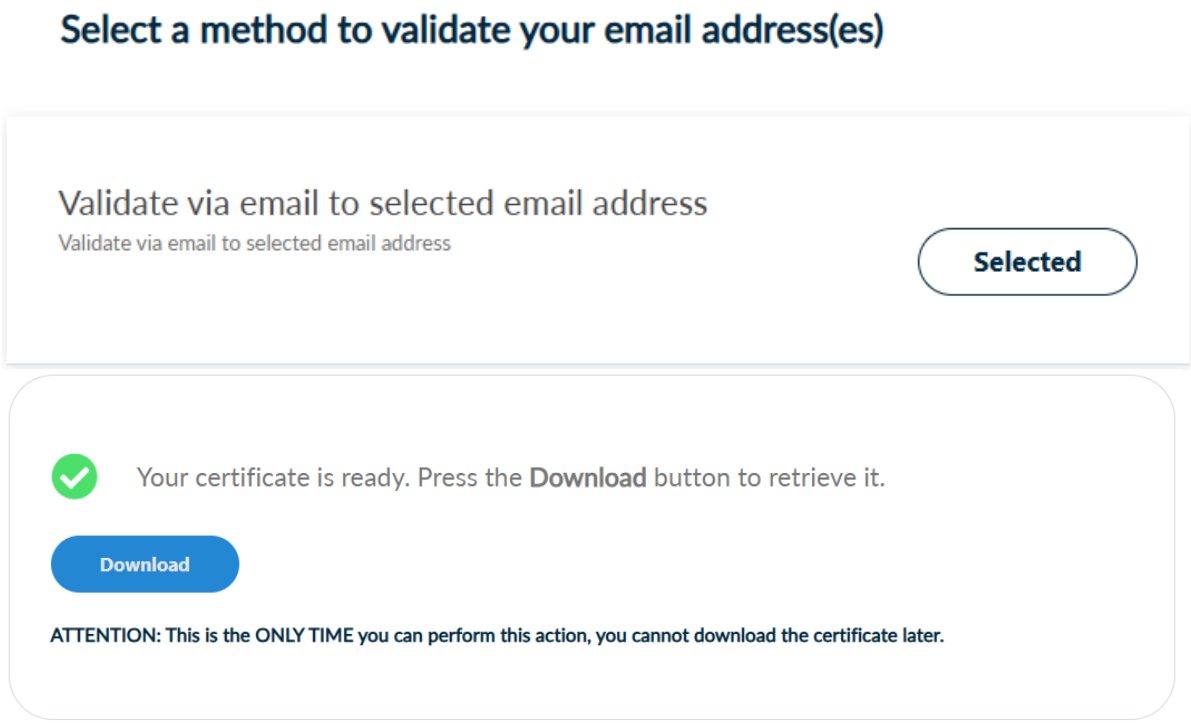
[23] Be sure to request and install the new certificate before revoking the old one. Once revoked the certificate will be invalid and users will not be able to connect to your server.
[24] cert@utwente.nl, 053 489 13 13

8.5.1 PRODUCT

The only products currently available for users at the University are **Email-only** and **For enterprises and Organizations**. Select either one, depending on your preferences. Your email address will be filled in based on the information provided by the university when you log in. Click **Next**.

8.5.2 AUTHORIZATION

Validation is always done by email.



8.5.3 SUMMARY

On the next page, you will be able to review the information. Verify the information and confirm your agreement with the terms mentioned.

8.5.4 ENROLL

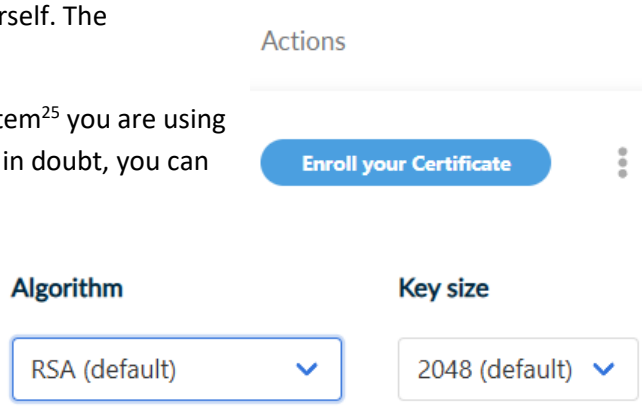
You can get your certificate by clicking **Enrolling your Certificate**.

You will be taken to a new page to choose between automatically generating a Certificate Signing Request (CSR) or using one you generated yourself. The University advises having the CSR generated.

The Algorithm and Key Size depend on the system[25] you are using it with. The defaults are usually correct. When in doubt, you can request an RSA and an ECDSA certificate.

Set a passphrase[26]. You need to remember it to be able to use the certificate later.

Click **Enroll Certificate**.



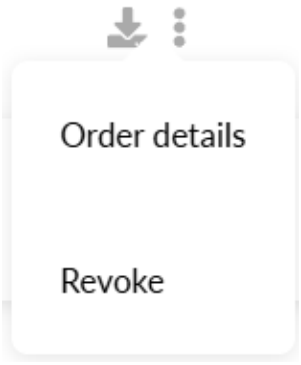
[25] For S/MIME email encryption you can only use RSA. You can still use your ECDSA certificate to authenticate towards website that support certificate authentication.

[26] The University advises to use a Password manager application to generate and store the passphrase.

Next, you can download and start using the certificate.

8.6 CLIENT CERTIFICATE REVOCATION

As mentioned in chapter 4 the user has to revoke their certificate(s) under some conditions. This paragraph will show the steps necessary.



On your dashboard, you will find the certificates you requested. Click the three vertical bullets and select **Revoke**.

On the next page, you will find information about the certificate revocation. Make sure to specify the correct reason.

1. **Certificate has been used to sign Suspect Code**.
2. **Certificate's subject information has changed**. Your email address has changed, and the one in the certificate is no longer valid.
3. **Subscriber no longer controls**…
4. **Unspecified reason**. This reason is not allowed to be used.
5. **Private key is compromised**. This reason is used when there is proof that the private key of a certificate is compromised. Also, report this incident to CERT-UT[27].
6. **Domain name or Full Name**… There are currently no situations where this is to be expected.
7. **Website or email address is no longer in use**. This reason should be used when a user has left the University. This is different from the reason in bullet 2
8. **Private key is exposed**. This is similar to bullet 5 above, but there is no proof that the private key is compromised. This is the case when the system where the key is stored is compromised. Also, report this incident to CERT-UT.
9. **Existing certificate has been replaced**. Use this when a new certificate with the same information has been issued.

If asked for, provide more details about the reason in the field below reason and click *Revoke*. The certificate will show as Revoked in your dashboard, and you will receive an email with information about the revocation.

[27] cert@utwente.nl, 053 489 13 13