

R&S[®]ISEC

Instrument Security Service

User Manual



1179755602
Version 04

ROHDE & SCHWARZ
Make ideas real



This user manual applies to the R&S® ISEC service, **version 1.1.0** and later.

© 2025 Rohde & Schwarz

Muehldorfstr. 15, 81671 Muenchen, Germany

Phone: +49 89 41 29 - 0

Email: info@rohde-schwarz.com

Internet: www.rohde-schwarz.com

Subject to change – data without tolerance limits is not binding.

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG.

All other trademarks are the properties of their respective owners.

1179.7556.02 | Version 04 | R&S®ISEC

Throughout this manual, R&S® is indicated as R&S.

Contents

1	Welcome to the R&S ISEC service.....	5
1.1	Key features.....	5
1.2	Documentation overview.....	5
1.2.1	User manual (this manual).....	5
2	What's new.....	6
3	Concepts.....	7
3.1	R&S ISEC service overview.....	7
3.1.1	TLS authentication.....	8
3.1.2	Digital certificate enrollment.....	8
3.1.3	Certificate management protocols.....	9
4	Getting started.....	11
4.1	Configuring the R&S ISEC service.....	11
4.2	General work flow.....	12
4.3	Accessing, retrieving and handling data.....	13
5	Web user interface.....	15
5.1	Certificates.....	15
5.1.1	Certificates toolbar.....	15
5.1.2	Certificates/CA certificates tab fields.....	16
5.1.3	View a certificate.....	16
5.1.4	Edit a certificate.....	17
5.1.5	Delete a certificate.....	20
5.2	Certificate enrollment.....	21
5.2.1	Self-signed wizard.....	21
5.2.2	Import PFX/P12 wizard.....	26
5.2.3	ACME wizard.....	30
5.2.4	SCEP wizard.....	42
5.2.5	EST wizard.....	50
5.2.6	Manual export / import (CSR) wizard.....	60

5.3 Message log.....69

5.4 Expert settings..... 70

6 Contacting customer support.....72

1 Welcome to the R&S ISEC service

The R&S ISEC service is a web based application that allows you to create self-signed certificates and enroll public certificates from a certificate authority (CA). With R&S ISEC service, you can use different certificate management protocols to manage X.509 certificates efficiently. It uses HTTPS to browse the webpages of an Rohde & Schwarz instrument. The application is intended for system administrators who prepare an Rohde & Schwarz instrument for secure communication via LAN.

1.1 Key features

The R&S ISEC service provides the following features:

- Uses highly secure certificate management protocols to secure the message exchange
- Creates self-signed X.509 certificates
- Enrolls and updates X.509 digital certificates via SCEP and EST protocols
- Uploads digital certificates (including creation of certificate signing requests)
- Stores digital certificates in the file system or an operating system certificate store (Microsoft)
- Tracks the expiration of the currently active certificate
- Monitors the revocation of a digital certificate

1.2 Documentation overview

This section provides an overview of the R&S ISEC service user documentation.

1.2.1 User manual (this manual)

Describes the functionality of the R&S ISEC service and provides description of the web interface.

The manual is also available for download or for immediate display on the internet.

2 What's new

This documentation describes version version 1.1.0 and higher. Compared to version 1.0.5, it provides the following new features and changes:

- "ACME Account" settings added to the "ACME Account" page, see ["ACME Account"](#) on page 35.
- If an ACME CA offers profiles, a profile can be selected as ACME parameter, see [Section 5.2.3.5, "ACME account"](#), on page 34.

3 Concepts

The R&S ISEC service uses different cryptographic protocols to enable easier, scalable and secure certificate issuance. The certificates are usually generated by a trusted entity or certificate authority (CA), and can be validated using a Public Key Infrastructure (PKI).

3.1 R&S ISEC service overview

The R&S ISEC service is an operating system level service that takes care of the client-side certificate management. The ISEC service interface to the host PC is a private host interface and is only accessible from the host PC.

R&S ISEC service supports certificate-based TLS authentication. You can use a self-signed digital certificate and certificate authority (CA)-signed digital certificate in the R&S ISEC service for secure communication. The certificates are stored in the file system or an operating system certificate store (Microsoft).

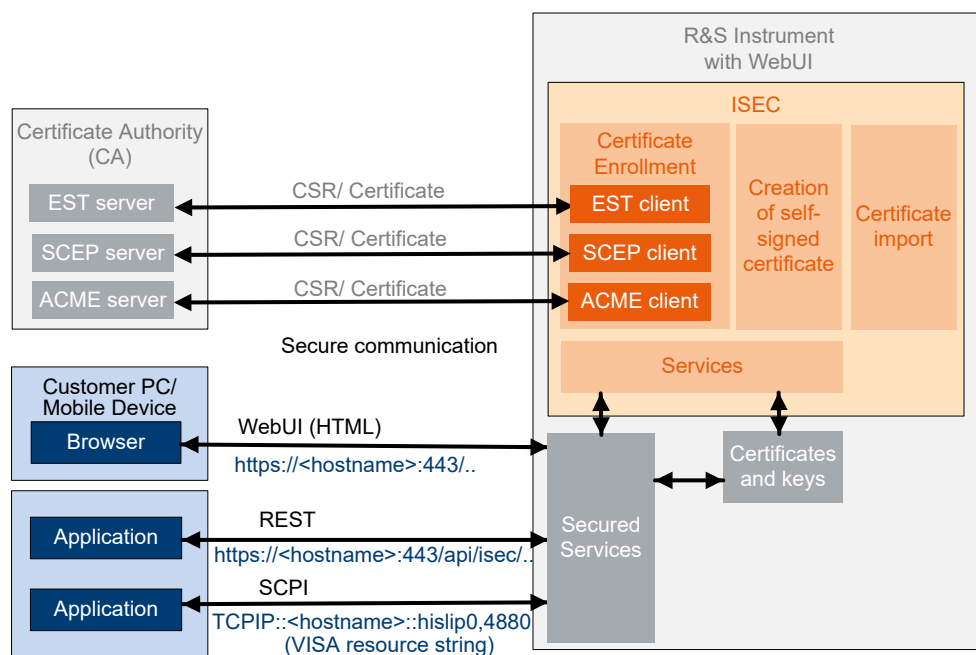


Figure 3-1: ISEC overview

If there is a self-signed certificate, R&S ISEC service creates an X.509 certificate on a Rohde & Schwarz instrument. A self-signed certificate is created by default as a fall-back. However, for CA-signed certificate, simple certificate enrollment protocol (SCEP) and enrollment over secure transport (EST) are two options used by the R&S ISEC service to enroll from the CA. The SCEP/EST server sits between R&S ISEC service and a certificate authority (CA). The SCEP/EST server receives a certificate signing request (CSR) from the R&S ISEC service and validates the request. It forwards this

request to the corresponding CA, gets the certificate issued, and finally provisions it to the Rohde & Schwarz instrument.



If you encounter any security issues with the R&S ISEC service or have suggestions to improve its security features, contact our product security team at productsecurity@rohde-schwarz.com.

3.1.1 TLS authentication

TLS (former SSL) is a communication protocol that provides authentication, encryption and integrity of the exchanged information. TLS uses digital X.509 certificates to bind a public key to a subject name and an internet/IP address. In public key encryption, a public key and a corresponding private key are generated for a subject. The data encrypted with the public key can be decrypted only with the corresponding private key. Similarly, the data encrypted with the private key can be decrypted only using the corresponding public key. The private key is a secret key. It must be stored in a safe key database and must never be published. Normally, only the owner can access the private key and use it to decrypt messages that are encrypted with the corresponding public key.

The R&S ISEC service generates key pairs and supports certificate creation (self-signed) or enrollment (SCEP, EST and manual) for these keys. R&S ISEC service takes care of the secret key (which never leaves the R&S ISEC service host system).

The R&S ISEC service supports the following two commonly used public key encryption algorithms:

- RSA: It is a public key cryptosystem widely used for secure data transmission.
- EC: Elliptic curve (NIST-P256, NIST-P384) is a second key type used for secure data exchange over an insecure channel.

3.1.2 Digital certificate enrollment

R&S ISEC service supports enrollment of both self-signed digital certificates and certificate authority (CA)-signed digital certificates.

A self-signed certificate is signed with its own private key and cannot be verified with a trusted source such as a certificate authority. This means that the self-signed certificate created by the R&S ISEC service is not trusted out-of-the-box and needs to be approved in the application (for example, browser).

A CA certificate enrollment involves submitting a certificate request to a trusted certification authority (CA), an entity that issues and manages digital certificate for use within the public key infrastructure (PKI). The request is made to the CA (using "Import/Export" Wizard) or automatically without manual interaction (using "SCEP"/"EST" Wizards). Many instruments can use SCEP and EST to automatically enroll and renew certificates from a well-known customer PKI. This reduces the overhead of a manual process to place CA-signed certificates on a fleet of Rohde & Schwarz instruments.



For better security, Rohde & Schwarz recommends you to connect your instruments to a corporate certificate authority.

3.1.3 Certificate management protocols

R&S ISEC service uses the following certificate management protocols to enroll and manage X.509 digital certificates:

3.1.3.1 Simple certificate enrollment protocol (SCEP)

SCEP is a certificate management protocol used by the R&S ISEC service to enroll digital certificates with a certificate authority using a secure and automated process. The SCEP certificate enrollment process involves the use of the "SCEP Wizard" in R&S ISEC service to enroll digital certificates with a certificate authority.

The certificate enrollment over SCEP protocol between a Rohde & Schwarz instrument and a certificate authority is done as follows:

1. R&S ISEC service initiates a mutual TLS-secured HTTP connection with the SCEP server and checks the server certificate to verify the legitimacy of the server.
2. R&S ISEC service generates a pair of public and private key using the configured algorithm.
3. R&S ISEC service creates a Certificate Signing Request to be sent to the CA. It includes the certificate profile, which contains the public key, necessary certificate information and a digital fingerprint, which the SCEP server can verify with the public key.
4. The SCEP server receives a newly created certificate from the CA as requested.
5. The R&S ISEC service user verifies/trusts the SCEP server by comparing the fingerprint of the SCEP server certificate with the reference fingerprint. The reference fingerprint must be obtained by out-of-band means, that is, via email from the server administrator or from the server website. The SCEP server uses the "Client Certificate" entry (if used) on the "SCEP CA" page to validate the Rohde & Schwarz instrument.
6. The R&S ISEC service user verifies/trusts the CA. It requests and verifies the chain of trust from the server, including any intermediate certificates that lie between the root and the SCEP CA, and stores the CA certificate chain.
7. ISEC stores the enrolled certificate on the Rohde & Schwarz instrument.

For information on how to create certificates using the SCEP wizard, refer to [Section 5.2.4, "SCEP wizard"](#), on page 42.

3.1.3.2 Enrollment over secure transport (EST)

EST protocol is another widely used protocol for certificate management. EST is considered to be more secure and efficient than SCEP. The EST certificate enrollment process is similar to the SCEP certificate enrollment process. However, the EST process involves the use of the "EST Wizard" in the R&S ISEC service to enroll digital certificates with a certificate authority.

For information on how to create certificates using the EST wizard, refer to [Section 5.2.5, "EST wizard"](#), on page 50.

3.1.3.3 Automatic certificate management environment (ACME)

ACME protocol is another communications protocol, similar to SCEP and EST, that enables automation of the issuance and renewal of certificates. This is a relatively new protocol and is widely used due to its easy configuration as compared to SCEP and EST. The ACME process involves the use of the "ACME Wizard" in the R&S ISEC service to enroll digital certificates with a certificate authority.

For information on how to create certificates using the ACME wizard, refer to [Section 5.2.3, "ACME wizard"](#), on page 30.

3.1.3.4 PFX

PFX, also known as a PKCS#12, is an archive file format that combines both the X.509 certificate and its associated private key into a single file. A PFX certificate is often password protected and stored in a single encryptable file with the extension `pfx` or `p12`.

The PFX/PKCS#12 file must satisfy the following conditions:

- The file must be encoded as `PEM` or `DER`.
- The file must be encrypted.
- The file must not be signed.
- The certificate chain must be included, if it is not already stored on the instrument.

For information on how to import certificate from a PKCS#12 file using R&S ISEC service, refer to [Section 5.2.2, "Import PFX/P12 wizard"](#), on page 26.

4 Getting started

This section describes the basic steps for operating the R&S ISEC service.

4.1 Configuring the R&S ISEC service

The R&S ISEC service is configured using the browser-based user interface.

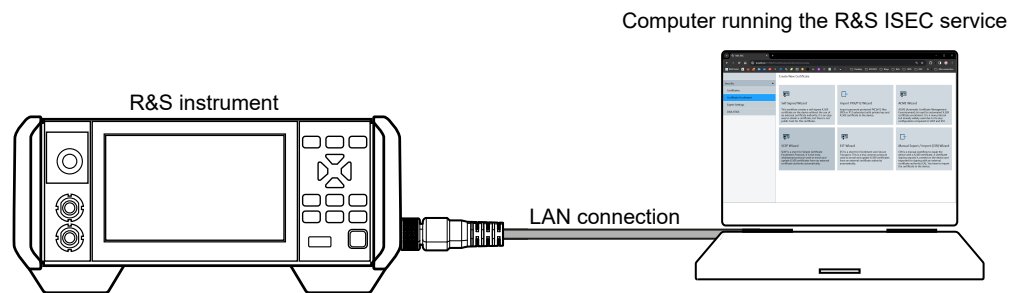


Figure 4-1: ISEC setup



A customer can access the R&S ISEC service using a browser from a PC or mobile device.

To start the R&S ISEC service:

1. Open the supported browser.
2. Enter the host name or IP address to connect to the instrument (*https://<host-name>:443/..*) where *443* is the secure port number.

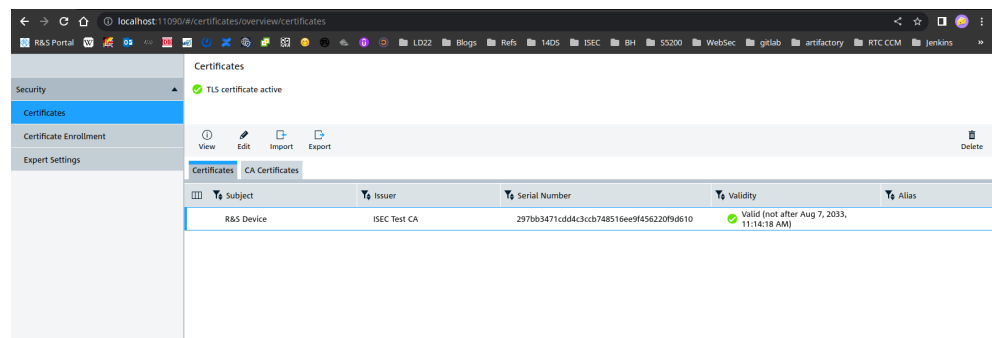


Figure 4-2: R&S ISEC service

The R&S ISEC service starts and the ISEC web interface appears.

SCEP - Simple Certificate Enrollment Protocol

Security

Certificates

Certificate Enrollment

Expert Settings

1 Subject Name

2 Attributes

3 SCEP CA

4 Verify CA

5 Enroll Certificate

Common Name: R&S NRX

Email Address: pki@customer.com

Organization: Customer Ltd.

Serial Number: 123456

Organization Unit: Power Department

Locality: Singapore

Country: SG

Figure 4-5: Step 1 of the enrollment wizard

Follow the instructions on the screen to execute the enrollment procedure. It contains several steps.

4. As the final step, click "Create"/"Enroll" to complete the certificate enrollment.

4.3 Accessing, retrieving and handling data

Depending on the origin and content, this description distinguishes between the following data types:

- Operational data
- Non-operational data

Operational data (data for intended use)

The R&S ISEC service stores all operational data in a single directory structure:

- Device certificates that are used by other services on the device, see [Section 5.1, "Certificates"](#), on page 15.
- Private keys of the device certificates.
- CA certificates that are used to validate the device certificates, see [Section 5.1.2, "Certificates/CA certificates tab fields"](#), on page 16.
- Certificate signing requests (CSR) used for the following:
 - ACME, see [Section 5.2.3, "ACME wizard"](#), on page 30.
 - SCEP, see [Section 5.2.4, "SCEP wizard"](#), on page 42.
 - EST, see [Section 5.2.5, "EST wizard"](#), on page 50.
 - Export/import workflow, see [Section 5.2.6, "Manual export / import \(CSR\) wizard"](#), on page 60.
- Certificate revocation lists (CRL), access via the REST interface: `https://<hostname>/api/isec/crl/<ca name>.pem`
- Configuration data required for operating the service.

The R&S ISEC service uses and creates this data because of its intended use and according to the settings and configuration you have made. Thus, this data makes up most of the data that the R&S ISEC service creates.

Non-operational data (usage data)

The R&S ISEC service maintains a record of its actions, especially the protocol workflows. The R&S ISEC service creates this data during and through its use. Such data is collected e.g. for troubleshooting, to help our customer support center find solutions quickly.

The R&S ISEC service generates this data continuously and in real-time, this data is saved on the product.

You can access the non-operational data as follows:

- Direct access in the web user interface, see [Section 5.3, "Message log"](#), on page 69.
- Download a file in text format using the REST API: `https://<hostname>/api/isec/v1/log`.

The R&S ISEC generates the following data:

- User and authentication data
- Security and access control
- Network and communication data
- Diagnostic and troubleshooting data

The volume of the non-operational data depends on the usage of the product and typically amounts to about 3.5 MB.

5 Web user interface

The R&S ISEC service allows creation of self-signed digital certificates and interaction with the certificate authority (CA) through a set of wizards such as "Self-Signed Wizard", "SCEP Wizard", "EST Wizard" and "Import/Export".

This section provides a description of the web user interface including all operating elements and parameters.

- [Certificates](#)..... 15
- [Certificate enrollment](#)..... 21
- [Message log](#)..... 69
- [Expert settings](#)..... 70

5.1 Certificates

The "Certificates" page displays the list of Rohde & Schwarz instruments and CA certificates. If there are no certificates displayed, you need to create a self-signed certificate or enroll a CA certificate for displaying the certificate on this page.

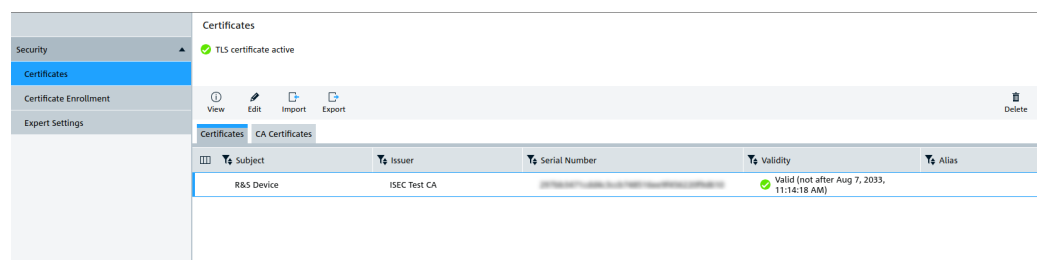


Figure 5-1: Certificates tab

5.1.1 Certificates toolbar

View

Opens the "View Certificate" page that displays the contents of the selected certificate.

Edit

Opens the "Edit Certificate" page that can be used to modify the alias of the selected certificate.

Import

Imports an X.509 certificate from your local drive into the application.

Export

Exports the currently selected certificate to the PEM format. This format can be viewed using a simple text editor.

Delete

Deletes the currently selected certificate.

5.1.2 Certificates/CA certificates tab fields

Certificates/CA Certificates tabs

The "Certificates" and "CA Certificates" tabs have a similar structure and consist of the same set of fields. These tabs display the properties of the available certificates in a table.

Subject ← Certificates/CA Certificates tabs

This field identifies the owner of the certificate.

A typical subject includes the following fields:

- Common Name
- Email Address
- Organization
- Serial Number
- Organization Unit
- Locality
- State or Province
- Country

Issuer ← Certificates/CA Certificates tabs

Displays the name of the source that provided the certificate.

Serial Number ← Certificates/CA Certificates tabs

Displays the unique serial number of the Rohde & Schwarz instrument.

Validity ← Certificates/CA Certificates tabs

Indicates if the certificate is still valid. Also, it displays the validity period (end date with time) of the certificate.

Alias ← Certificates/CA Certificates tabs

Displays a symbolic/human readable name that can be used as reference for the certificate. If multiple certificates are stored on an Rohde & Schwarz instrument, this name can be helpful to search for a specific certificate in the list.

5.1.3 View a certificate

To view the contents of a certificate:

1. Click the "Certificates" tab.
2. In the "Certificates" or "CA Certificates" table, select the certificate to view.
3. Click "View".

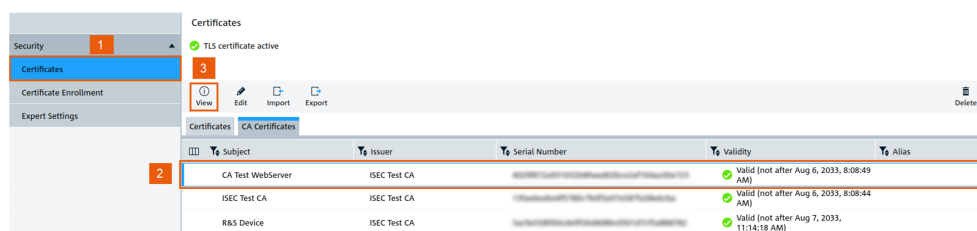


Figure 5-2: Certificates page - view a certificate

The "View Certificate" page appears. It displays the contents of the selected certificate.

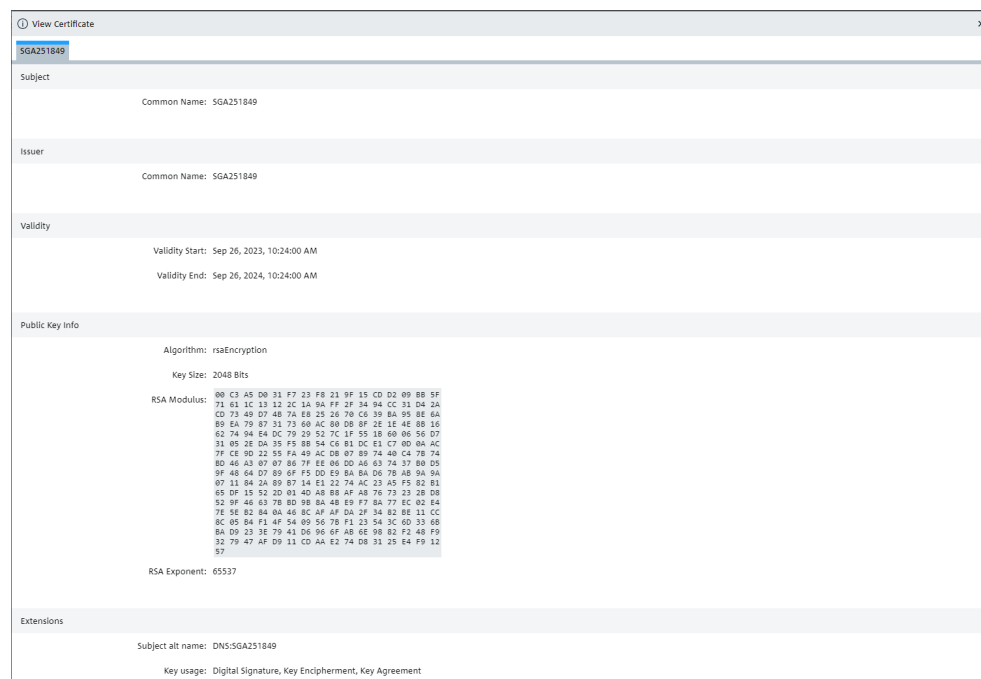


Figure 5-3: View certificate

5.1.4 Edit a certificate

R&S ISEC service allows you to change the alias of a certificate and remove the trust status.

To edit the alias of a certificate:

1. Click the "Certificates" tab.
2. In the "Certificates" or "CA Certificates" table, select the certificate to edit.
3. Click "Edit".

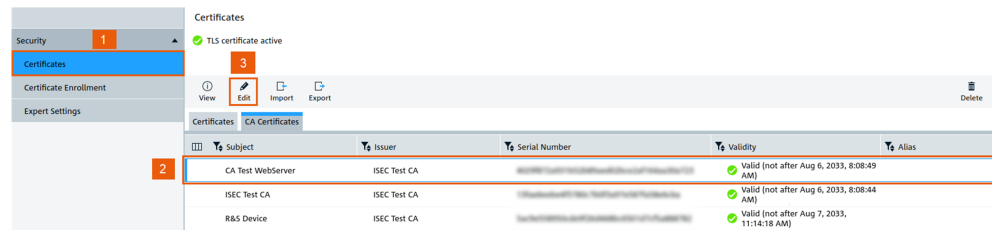


Figure 5-4: Certificates page - edit a certificate

The "Edit Certificate" page appears.

4. Modify the alias of the certificate.

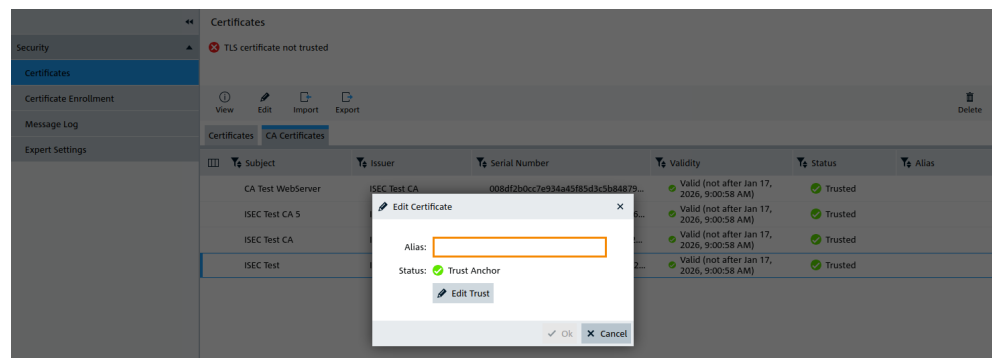


Figure 5-5: Change the alias

5. Click "Ok".

You can see the new alias for the certificate in the "Certificates" tab.

When obtaining a certificate from an external CA, R&S ISEC service also gets the CA certificate. Normally, it is not a single certificate but a chain of certificates. Certificate chains have a (usually self-signed) root certificate and one or more intermediate or issuing certificates. Certificate chains are only trusted if the root certificate is trusted and they are untrusted if the root certificate is not trusted. Therefore, it is sufficient to trust or untrust the root certificate. Then validity of the chain is then calculated by R&S ISEC service.

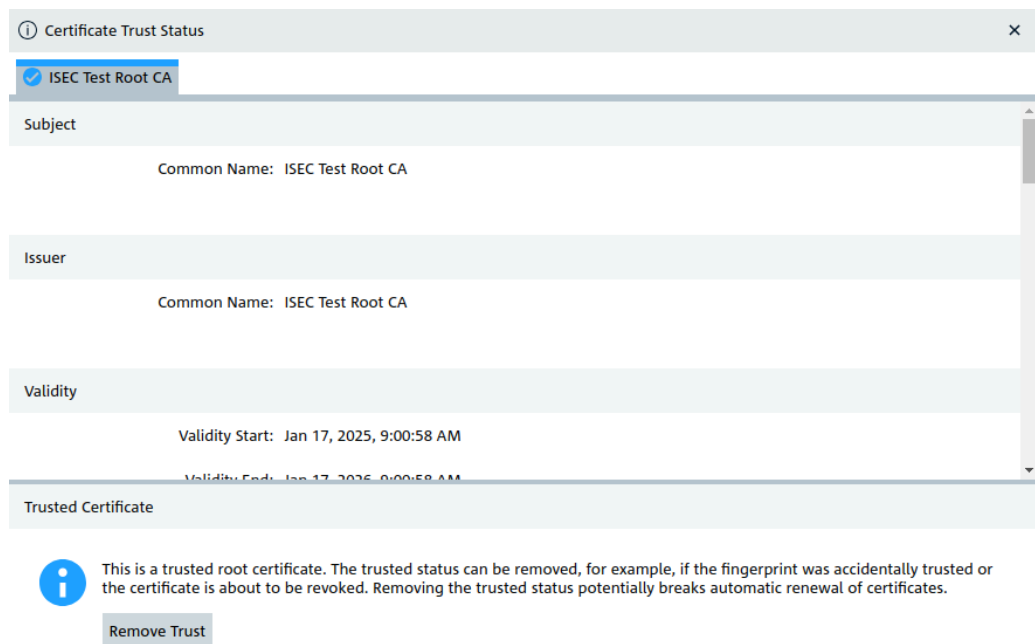


Figure 5-6: Certificate Trust Status page

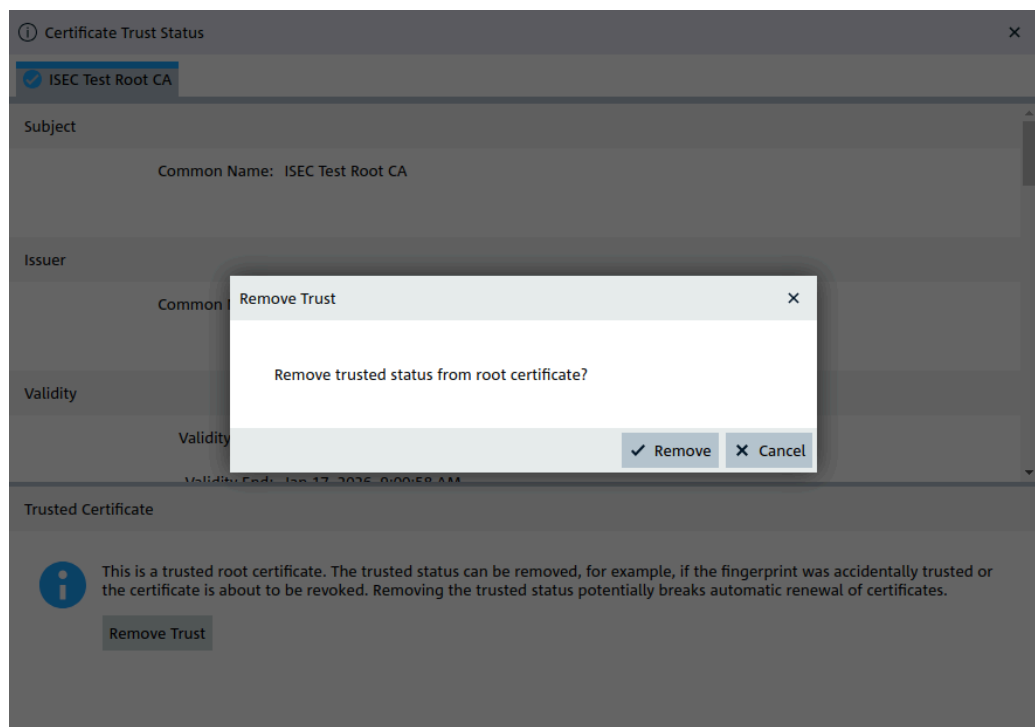


Figure 5-7: Remove Trust dialog

An untrusted certificate can be trusted anytime by clicking the "Trust Certificate" button. However, trust the certificate only if you have verified the SHA256 value.

① Certificate Trust Status

⚠ ISEC Test Root CA

Subject

Common Name: ISEC Test Root CA

Issuer

Common Name: ISEC Test Root CA

Validity

Validity Start: Jan 17, 2025, 9:00:58 AM

Validity End: Jan 17, 2036, 9:00:58 AM

Untrusted Certificate

⚠ The certificate chain of the connected Certificate Authority (CA) server is not trusted. Ask your IT department for the thumbprint (SHA-256 or SHA-1 hash value) of trusted CA certificates. By confirming the thumbprint of the CA certificates the device connection to the CA is secure on this device.

SHA-256: E8:89:27:32:7C:41:A6:09:7F:23:BB:A9:31:28:D1:63:BA:96:14:DE:56:4A:00:0F:B0:5C:24:15:1B:6D:6E:86

Trust Certificate

Figure 5-8: Untrusted certificate

5.1.5 Delete a certificate

To delete a certificate:

1. Click the "Certificates" tab.
2. In the "Certificates" or "CA Certificates" table, select the certificate you wish to delete.
3. Click "Delete".

Certificates

Security 1

⊕ TLS certificate active

Certificates

Certificate Enrollment

Expert Settings

View Edit Import Export

3 Delete

Subject	Issuer	Serial Number	Validity	Alias
CA Test WebServer	ISEC Test CA	...	Valid (not after Aug 6, 2033, 8:08:49 AM)	
ISEC Test CA	ISEC Test CA	...	Valid (not after Aug 6, 2033, 8:08:44 AM)	
R&S Device	ISEC Test CA	...	Valid (not after Aug 7, 2033, 11:14:18 AM)	

2

Figure 5-9: Certificates page - delete a certificate

The certificate is removed from the table and is not available in the application anymore.

5.2 Certificate enrollment

5.2.1 Self-signed wizard

The "Self-Signed Wizard" allows you to create and manage a self-signed certificate.

5.2.1.1 Subject name

The "Subject Name" page defines the general properties of a digital certificate such as the common name, email address.

Self-Signed

Security

Certificates

Certificate Enrollment

Expert Settings

DISA STIGS

1 Subject Name

2 Attributes

Common Name: R&S Device

E-Mail Address: name@customer.com

Organization: Customer Inc.

Serial Number: 123456

Organizational Unit: R&D

Location / City: Munich

State or Province: Bavaria

Country: DE

Next Cancel

Figure 5-10: Subject name page

Common Name

Provide a unique certificate name. The "Common Name" can be the name of an instrument, person, or other entity. It is the most specific level in the identification hierarchy. For example, *R&S Device*.

When using the ACME protocol, the "Common Name" must match to the DNS on the "Attributes" page ("[Add Device DNS Name to the Certificate](#)" on page 22).

Note: The "Common Name" is a required field. All other fields on the "Subject Name" page are optional but can be filled if a policy to show these fields in your certificates exists in a company.

Email Address

Specify the organization or your email address for the certificate. For example, *name@customer.com*.

Organization

Specify the company name for the certificate. For example, *Customer Inc.*

Serial Number

Specify the unique serial number of the Rohde & Schwarz instrument. For example, *123456*.

Organization Unit

Specify the name of the designated organization unit that the certificate is used for. For example, *R&D*.

Locality

Specify the name of your locality for the certificate. For example, *Munich*.

State or Province

Specify the state or province name for the certificate. For example, *Bavaria*.

Country

Specify the 2-letter country code of your country for the certificate. For example, *DE* (for *Germany*).

5.2.1.2 Attributes

The "Attributes" page is used to define other enrollment details of a certificate such as the validity period, DNS name, IP address of the instrument. For the self-signed certificates, specify the validity period.

The screenshot shows the 'Attributes' page for a 'Self-Signed' certificate. The page is divided into three steps: 1. Subject Name, 2. Attributes, and 3. Processing. The 'Attributes' step is active. The form includes the following fields and controls:

- Validity Start Date:
- Validity End Date:
- Add Device DNS Name to Certificate:
- Alternative DNS name:
- IP Addresses:
- Purpose: Server Authentication
- Key Algorithm: RSA4096_SHA256

At the bottom right, there are buttons for 'Previous', 'Create', and 'Cancel'.

Figure 5-11: Attributes page

Validity Start Date

Specify the beginning date that the certificate is valid for.

Note: Only applicable to the self-signed certificates.

Validity End Date

Specify the end date after which the certificate is no longer valid.

Note: Only applicable to the self-signed certificates.

Add Device DNS Name to the Certificate

Select this checkbox to include the DNS name of the instrument in the certificate.

Alternative DNS name

Enter a secondary DNS name (or host name), if any, for the certificate.

Note: This field is meant for the expert users only. The customers usually do not need to edit it.

IP Addresses

Enter the IP addresses of the Rohde & Schwarz instruments, if any.

Note: This field is meant for the expert users only. The customers usually do not need to edit it.

Purpose

Specifies the purpose for the certificate authentication. It is always *Server Authentication*. It is a certificate-based authentication, where the client initiates a TLS-secured HTTP session with the server (Rohde & Schwarz instrument) and validates the certificate offered by the server.

Key Algorithm

Select one of the available combinations of key algorithm, key size and hash function. These combinations are used to generate the key pair for the Rohde & Schwarz instrument.

- For RSA, the largest supported key size is 4096 bits.
- For Elliptic Curve, the largest supported key size is 384 bits.

The table below lists the different key algorithms supported by the R&S ISEC service.

Table 5-1: Key Algorithms

Algorithm	Type	Comment
RSA 2048 Bits	RSA	Default
RSA 3072 Bits	RSA	
RSA 4096 Bits	RSA	
NIST P-256	Elliptic Curve	NIST Standard
NIST P-384	Elliptic Curve	NIST Standard
ED25519	Elliptic Curve	

Note: Rohde & Schwarz recommends you to use the default option. If there are IT policies in place for higher security levels, you can choose one of the key algorithms that provide higher security (RSA 4096, NIST P-384).

5.2.1.3 Create a self-signed certificate

To create a self-signed certificate:

1. Click the "Certificate Enrollment" tab.
The "Create New Certificate" page appears.
2. On the "Create New Certificate" page, click "Self-Signed Wizard".

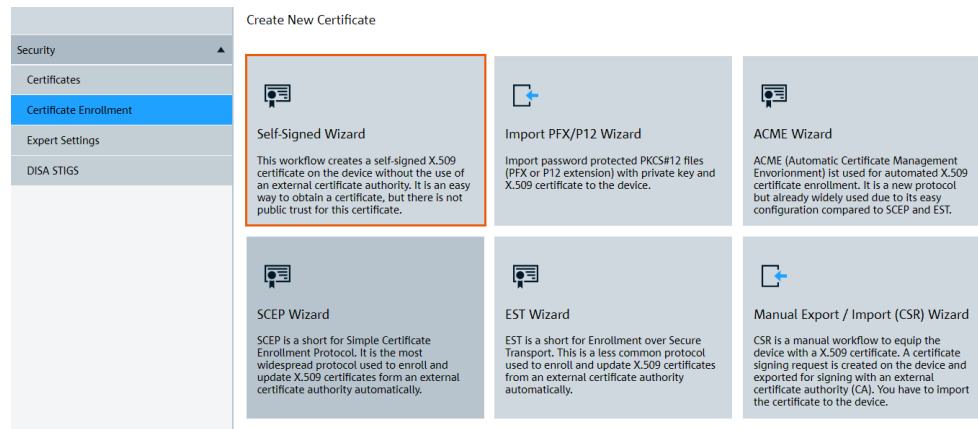


Figure 5-12: Self-signed wizard

- On the "Subject Name" page, enter the "Common Name" for the certificate.

Figure 5-13: Subject name page

Note: All the other fields are optional.

- Click "Next".
- On the "Attributes" page, specify the following:
 - Beginning and end date for the certificate
 - DNS settings for the instrument if you wish to add them to the certificate
 - Purpose of authentication
- Select one of the supported algorithms and key sizes from the "Key Algorithm" dropdown.
- Click "Create".

The screenshot shows the 'Self-Signed' certificate enrollment interface. On the left is a navigation menu with 'Certificate Enrollment' selected. The main area is titled 'Self-Signed' and has a progress bar with three steps: 1. Subject Name, 2. Attributes (current step), and 3. Processing. The 'Attributes' section includes:

- Validity Start Date: mm/dd/yyyy
- Validity End Date: mm/dd/yyyy
- Add Device DNS Name to Certificate:
- Alternative DNS name: +
- IP Addresses: +
- Purpose: Server Authentication
- Key Algorithm: RSA4096_SHA256

At the bottom right, there are buttons for 'Previous', 'Create', and 'Cancel'.

Figure 5-14: Attributes page

A status message "Certificate successfully received and installed" appears confirming that the self-signed certificate is successfully created.

The screenshot shows the 'Active Enrollment: Self-Signed' status page. The left navigation menu is the same as in Figure 5-14. The main area has tabs for 'Status' and 'Details', with 'Status' selected. It displays a green checkmark and the message "Certificate successfully received and installed". Below this, the following details are shown:

- Status: Enrolled
- Protocol: SelfSigned
- Subject: R&S NRX
- Issuer: R&S NRX

At the bottom right, there is a button labeled "Change Active Enrollment".

Figure 5-15: Status page

- Go to the "Details" page to view the enrolled certificate information.

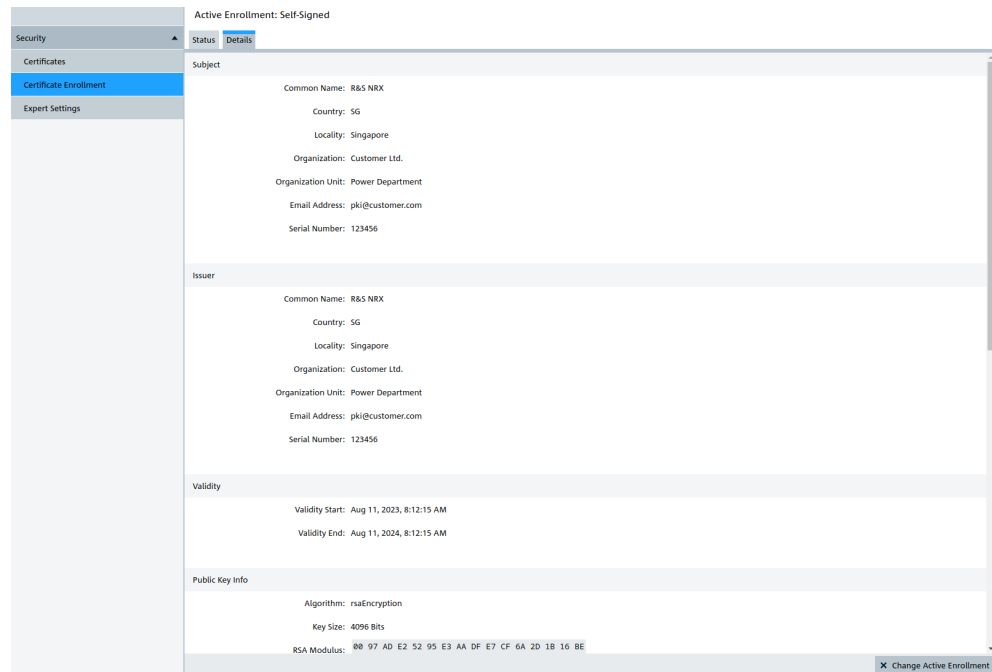


Figure 5-16: Details page

Note: You can view and manage all the certificates in the "Certificates" page.

- On the "Details" page, click "Change Active Enrollment" if you want to change the current enrollment information of the certificate.

5.2.2 Import PFX/P12 wizard

The "PFX/PKCS12 Wizard" allows you to import a certificate from a PKCS#12 file (`pfx` or `p12`) on your local drive.

The received certificate is installed by the R&S ISEC service on the Rohde & Schwarz instrument.

5.2.2.1 Import PFX/P12

The "Import PFX/P12" page allows you to select and import a digital certificate received from your CA to your instrument using the "Select File" button.

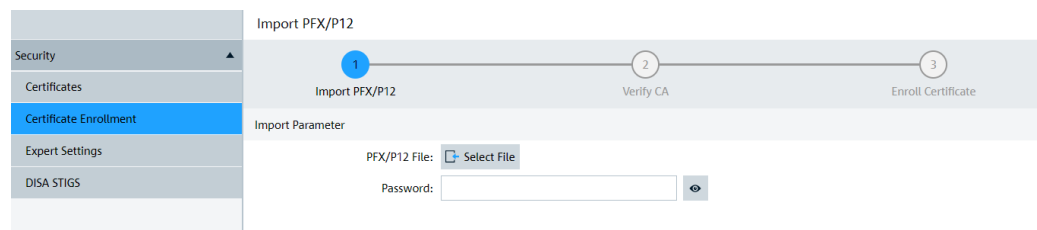


Figure 5-17: Import PFX/P12 page

PFX/P12 File

Browse for the `pfx` or `p12` file on your local drive using the "Select File" button.

Password

Specify the password for the PFX file.

5.2.2.2 Verify CA

The "Verify CA" page is used to confirm the authenticity of the received CA certificates. To ensure that the received CA certificate is authentic, you must compare the certificate fingerprint (SHA-256 or the less secure SHA-1) with the original fingerprint. Obtain the original fingerprint by out-of-band means such as through an email from the CA website.

The Rohde & Schwarz instrument does not receive a single CA certificate, but a certificate chain that can be used to verify the root certificate in this chain. The validity of the other certificates can be verified automatically by traversing the chain (if the chain is not broken). Once the CA information is verified, you can use the "Enroll" button to enroll the TLS certificate and store the signed certificate on the Rohde & Schwarz instrument. You can also use the "Import" button to import additional CA certificates, if necessary, from your local drive. The imported file can contain multiple PEM-encoded certificates or a single DER-encoded certificate.

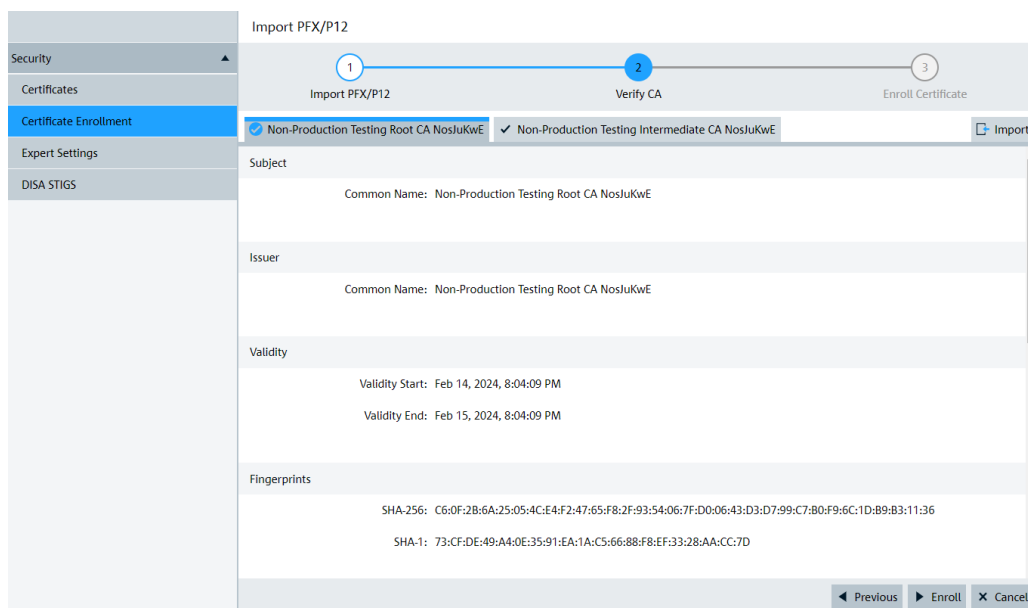


Figure 5-18: Verify CA page

5.2.2.3 Use import PFX/P12 wizard to enroll certificates

To create a CA-signed certificate using "Import PFX/P12 Wizard":

1. Click the "Certificate Enrollment" tab.

The "Create New Certificate" page appears.

2. On the "Create New Certificate" page, click "Import PFX/P12 Wizard".

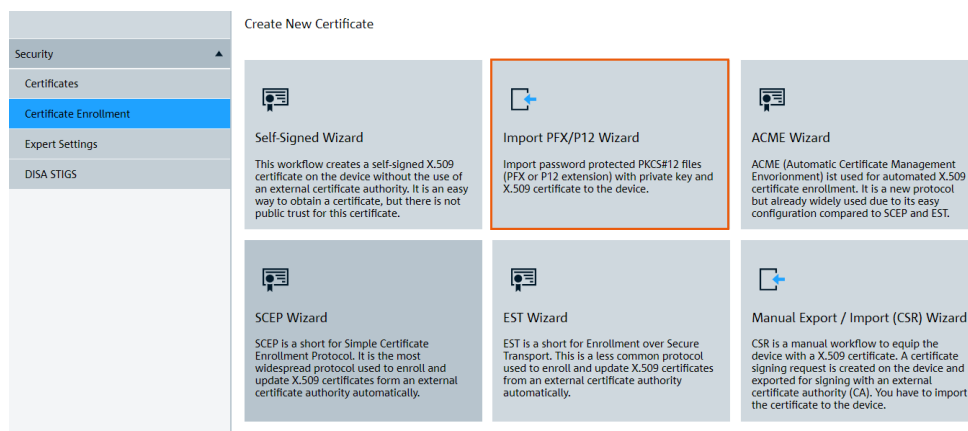


Figure 5-19: Import PFX/P12 wizard

3. On the "Import PFX/P12" page, click "Select File" to browse for the received `pfx` or `p12` file on your local drive. Select it.

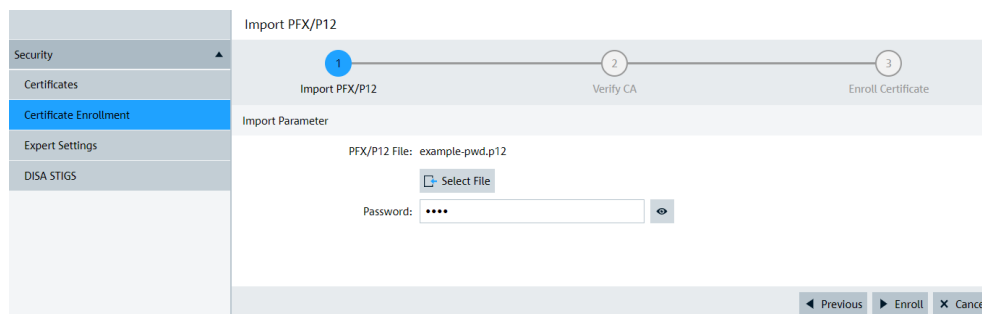


Figure 5-20: Import PFX/P12 page

4. Enter the password for the `pfx` or `p12` file.
5. Click "Next".
6. On the "Verify CA" page, verify if the digital fingerprint matches the known digital fingerprint of the trusted certificate authority.
7. Click "Trust Certificate" to confirm the authenticity of the certificate authority.

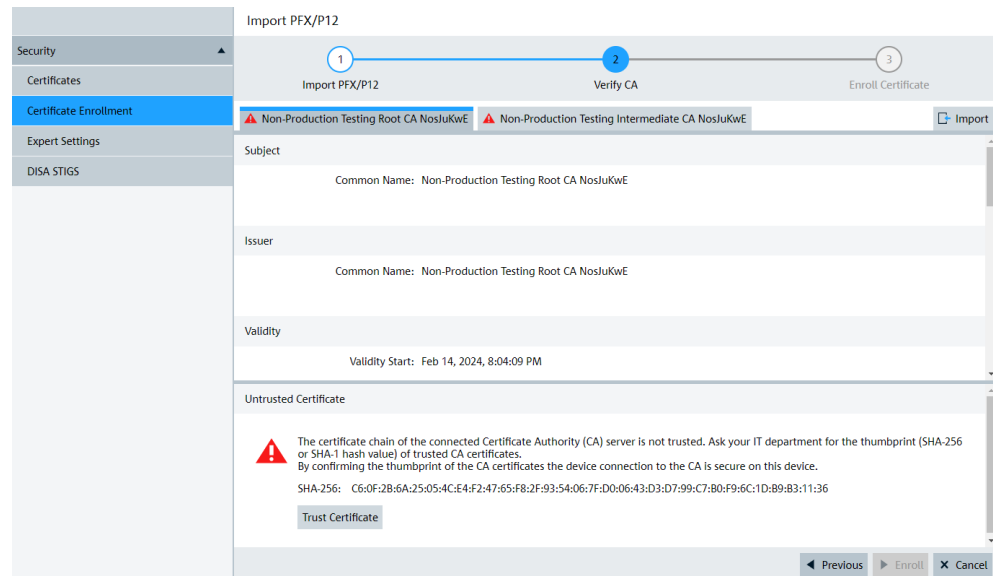


Figure 5-21: Verify CA page

8. Wait until a blue checkmark appears next to the tabs displaying the root certificate, intermediate certificate and instrument certificate names.

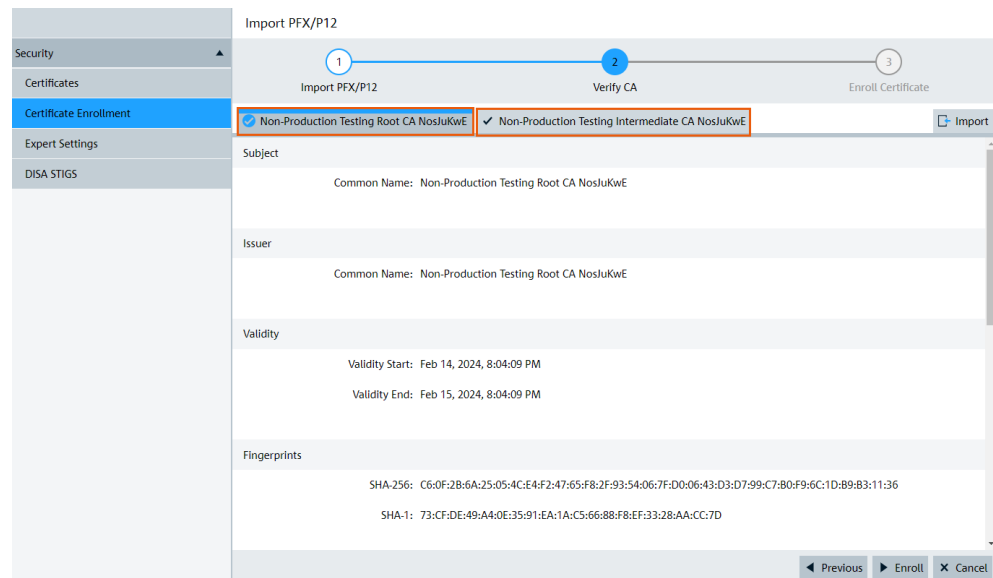


Figure 5-22: Verify CA page - establish certificate trust chain

The blue checkmarks confirm that a certificate trust chain has been established with the CA server.

Note: If a red warning symbol appears on one of the above tabs, Rohde & Schwarz recommends you to verify if the validation process is complete. If the validation process is complete and the warning symbol does not disappear, you can check if the certificate information is correct. Then restart the enrollment process.

9. Click "Enroll".

A status message "Certificate successfully received and installed" appears confirming that the certificate is successfully installed on the Rohde & Schwarz instrument.

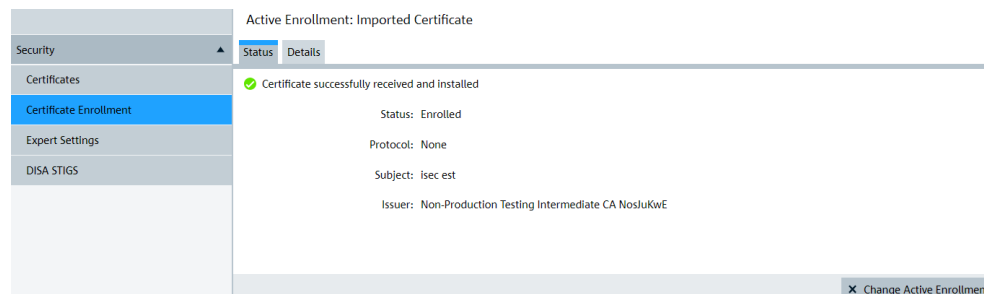


Figure 5-23: Status page

10. Go to the "Details" page to view the enrolled certificate information.

Note: You can view and manage all the certificates in the "Certificates" page.

11. On the "Details" page, click "Change Active Enrollment" if you want to change the current enrollment information of the certificate.

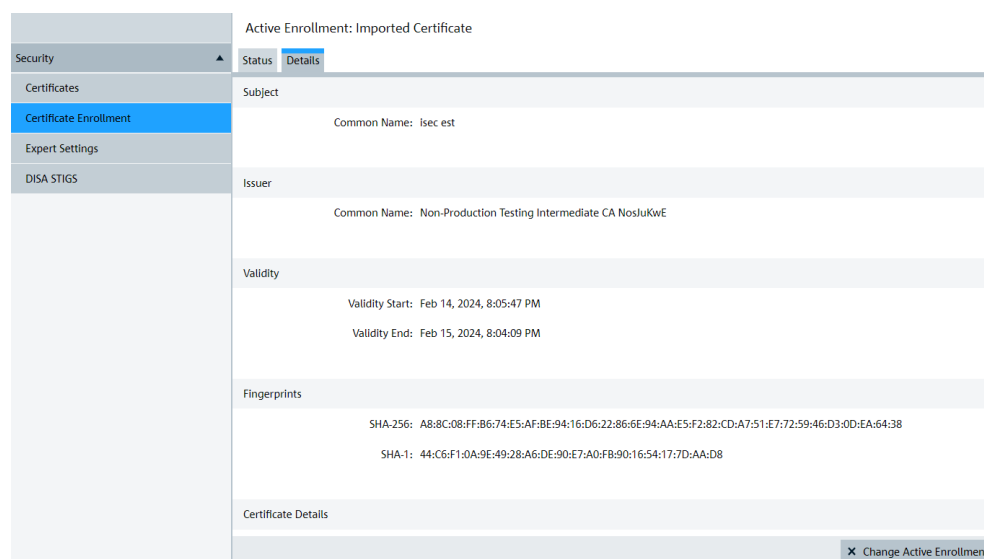


Figure 5-24: Details page

5.2.3 ACME wizard

The "ACME Wizard" supports automatic enrollment of certificates with the ACME Server over the Automatic Certificate Management Environment (ACME) protocol. The certificates are enrolled automatically by submitting a certificate enrollment request to the ACME certificate authority using the R&S ISEC service.

The "ACME Wizard" allows you to enroll and manage ACME certificates automatically.

5.2.3.1 Subject name

The "Subject Name" page defines the general properties of a digital certificate such as the common name, email address.

Self-Signed

Security

Certificates

Certificate Enrollment

Expert Settings

DISA STIGS

1 Subject Name

2 Attributes

Common Name: R&S Device

E-Mail Address: name@customer.com

Organization: Customer Inc.

Serial Number: 123456

Organizational Unit: R&D

Location / City: Munich

State or Province: Bavaria

Country: DE

Next Cancel

Figure 5-25: Subject name page

Common Name

Provide a unique certificate name. The "Common Name" can be the name of an instrument, person, or other entity. It is the most specific level in the identification hierarchy. For example, *R&S Device*.

When using the ACME protocol, the "Common Name" must match to the DNS on the "Attributes" page ("[Add Device DNS Name to the Certificate](#)" on page 22).

Note: The "Common Name" is a required field. All other fields on the "Subject Name" page are optional but can be filled if a policy to show these fields in your certificates exists in a company.

Email Address

Specify the organization or your email address for the certificate. For example, *name@customer.com*.

Organization

Specify the company name for the certificate. For example, *Customer Inc.*

Serial Number

Specify the unique serial number of the Rohde & Schwarz instrument. For example, *123456*.

Organization Unit

Specify the name of the designated organization unit that the certificate is used for. For example, *R&D*.

Locality

Specify the name of your locality for the certificate. For example, *Munich*.

State or Province

Specify the state or province name for the certificate. For example, *Bavaria*.

Country

Specify the 2-letter country code of your country for the certificate. For example, *DE* (for *Germany*).

5.2.3.2 Attributes

The "Attributes" page is used to define other enrollment details of a certificate such as the DNS name, IP address of the instrument.

The screenshot shows the 'Attributes' page in the R&S ISEC web user interface. The page is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with the following items: Security, Certificates, Certificate Enrollment (highlighted), Expert Settings, and DISA STIGS. The main content area has a progress bar at the top with two steps: 'Subject Name' (1) and 'Attributes' (2). Below the progress bar, there are several fields and controls: 'Add Device DNS Name to Certificate' (checked checkbox), 'Alternative DNS name' (plus sign), 'IP Addresses' (plus sign), 'Purpose: Server Authentication' (dropdown menu), and 'Key Algorithm: RSA2048_SHA256' (dropdown menu). At the bottom right of the page, there are three buttons: 'Previous', 'Next', and 'Cancel'.

Figure 5-26: Attributes page

Add Device DNS Name to the Certificate

Select this checkbox to include the DNS name of the instrument in the certificate.

Alternative DNS name

Enter a secondary DNS name (or host name), if any, for the certificate.

Note: This field is meant for the expert users only. The customers usually do not need to edit it.

IP Addresses

Enter the IP addresses of the Rohde & Schwarz instruments, if any.

Note: This field is meant for the expert users only. The customers usually do not need to edit it.

Purpose

Specifies the purpose for the certificate authentication. It is always *Server Authentication*. It is a certificate-based authentication, where the the client initiates a TLS-secured HTTP session with the server (Rohde & Schwarz instrument) and validates the certificate offered by the server.

Key Algorithm

Select one of the available combinations of key algorithm, key size and hash function. These combinations are used to generate the key pair for the Rohde & Schwarz instrument.

- For RSA, the largest supported key size is 4096 bits.
- For Elliptic Curve, the largest supported key size is 384 bits.

The table below lists the different key algorithms supported by the R&S ISEC service.

Table 5-2: Key Algorithms

Algorithm	Type	Comment
RSA 2048 Bits	RSA	Default
RSA 3072 Bits	RSA	
RSA 4096 Bits	RSA	
NIST P-256	Elliptic Curve	NIST Standard
NIST P-384	Elliptic Curve	NIST Standard
ED25519	Elliptic Curve	

Note: Rohde & Schwarz recommends you to use the default option. If there are IT policies in place for higher security levels, you can choose one of the key algorithms that provide higher security (RSA 4096, NIST P-384).

5.2.3.3 ACME CA

The "ACME CA" page is used to set up the basic connection properties of the ACME CA server. The properties are used to authenticate and securely connect to the ACME CA server. This page allows you to define the ACME properties such as ACME CA server address, port number and ACME directory.

Figure 5-27: ACME CA page

Server Address

Specify the host name of the ACME CA. For example, *pki.mycompany.local*.

Port

Indicates the TCP port number used for communication with the ACME CA server. This port is normally standard HTTP port number 443.

Note: R&S ISEC service uses "Server Address", "Directory" and "Port" fields to define the request URL. For example, `https://<Server Address>:<Port>/<Directory>`

Directory

Specify the ACME CA directory URL that contains the ACME configuration metadata.

Note: Ask your system administrator for the correct URL path.

Disable Proxy Settings

Select this checkbox to disable the HTTP proxy settings.

5.2.3.4 Trust ACME server

The "Trust ACME Server" page is used to confirm the authenticity of the received CA certificates. To ensure that the received CA certificate is authentic, you must compare the certificate fingerprint (SHA-256 or the less secure SHA-1) with the original fingerprint. Obtain the original fingerprint by out-of-band means such as through an email from the CA website.

The Rohde & Schwarz instrument does not receive a single CA certificate, but a certificate chain that can be used to verify the root certificate in this chain. The validity of the other certificates can be verified automatically by traversing the chain (if the chain is not broken).

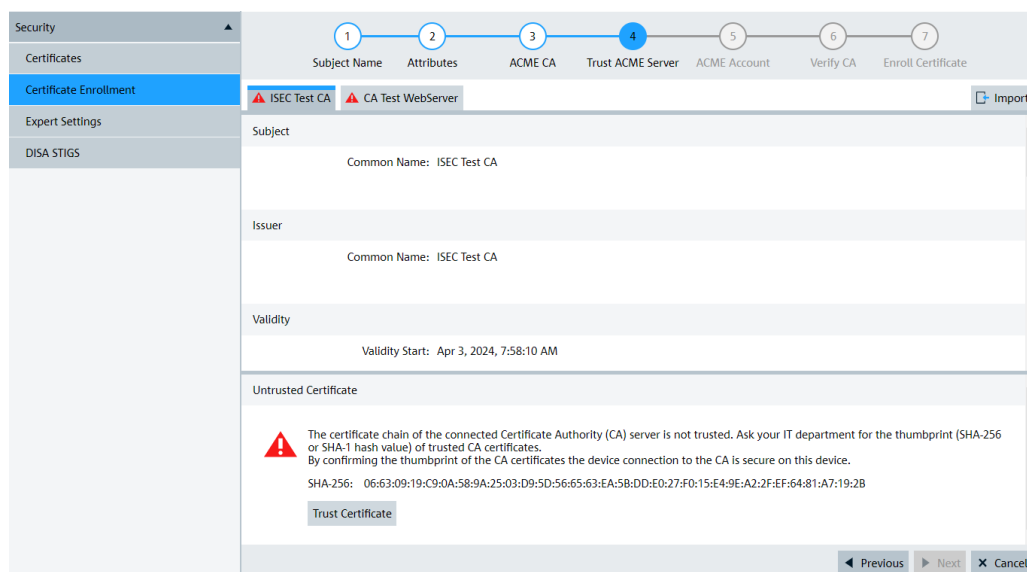


Figure 5-28: Trust ACME server page

5.2.3.5 ACME account

The "ACME Account" page is used to set up your ACME account to bind it to the ACME CA. These properties are crucial for securely linking your ACME account to the CA and play a vital role in automating certificate issuance and renewal. Once the CA information is verified and ACME account is linked to the ACME CA, you can use the "Enroll" button to enroll the TLS certificate.

Figure 5-29: ACME account page

ACME Parameter

Specify the ACME account information.

- "Email" It is an optional field. Specify the email address used for communication by the ACME CA. The ACME CA sends a notification to this email address in case a certificate is expired or revoked.
- "Profile" Certificate profiles have been announced in early 2025. If an ACME CA offers profiles, these can be selected to enroll certificates with different sets of attributes.

External Account Binding

Indicates whether the ACME CA server requires external account binding. To link the ACME account with the CA, you can enter EAB credentials such as Key ID and a hash-based message authentication code (HMAC). This information is provided by the ACME CA server by out-of-band methods— such as the CA's support portal, email, or a dedicated API – which are not specified by the ACME protocol itself.

- "Key ID" A unique identifier associated with your ACME account.
- "HMAC" A unique Base64-encoded value used for authentication.

Terms of Service

If shown, click the link to navigate to the given website and accept the terms of service.

Note: Continuing with the ACME wizard is considered as acceptance of the terms of service.

Website

Displays the URL of the ACME CA website. This information is for your reference only.

ACME Account

Provides information about the current ACME account and offers management options.

"ACME Account established"	Indicates whether an ACME account was created by a previous enrollment.
"ACME Account Key Rollover"	Triggers the creation of a new key pair for your existing ACME account. This is recommended if you suspect a key compromise or as a proactive security measure.
"Delete ACME Account"	Deletes the existing ACME account. This can also be used to force the creation of a new account, which can be helpful if you are experiencing persistent issues with the current account. This is typically not necessary.
"ACME ARI Renewal Info Status"	Displays information regarding the CA's recommended certificate renewal schedule, utilizing Automated Renewal Information (ARI) if supported.

5.2.3.6 Verify CA

The "Verify CA" page is used to verify the PKI certificates. It is also used to enroll and store the signed certificates on the Rohde & Schwarz instrument. You can also use the "Import" button to import additional CA certificates, if necessary, from your local drive. The imported file can contain multiple PEM-encoded certificates or a single DER-encoded certificate.

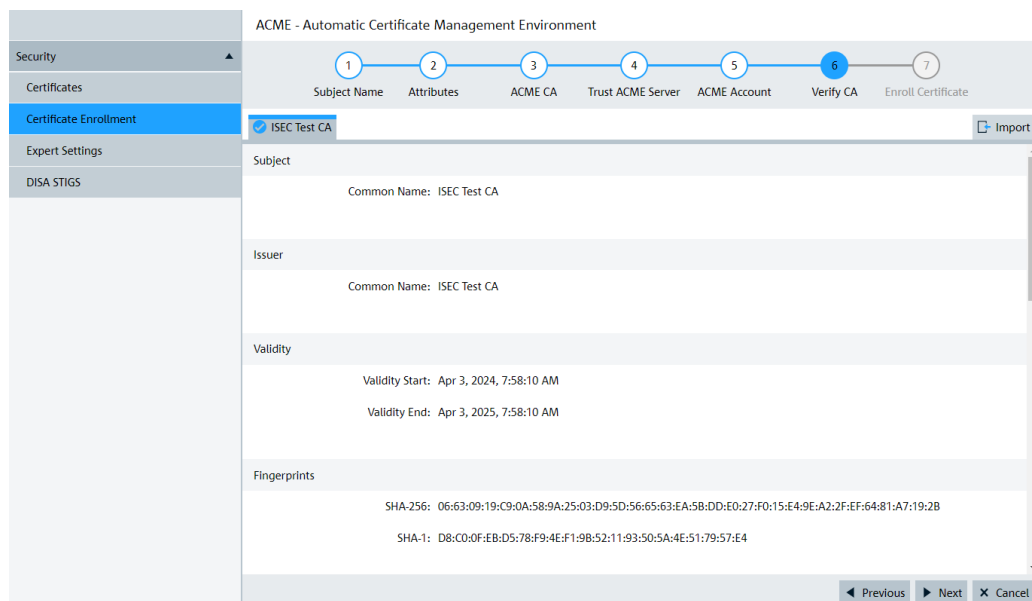


Figure 5-30: Verify CA page

5.2.3.7 Enroll ACME certificates

To enroll an ACME certificate:

1. Click the "Certificate Enrollment" tab.

The "Create New Certificate" page appears.

- On the "Create New Certificate" page, click "ACME Wizard".

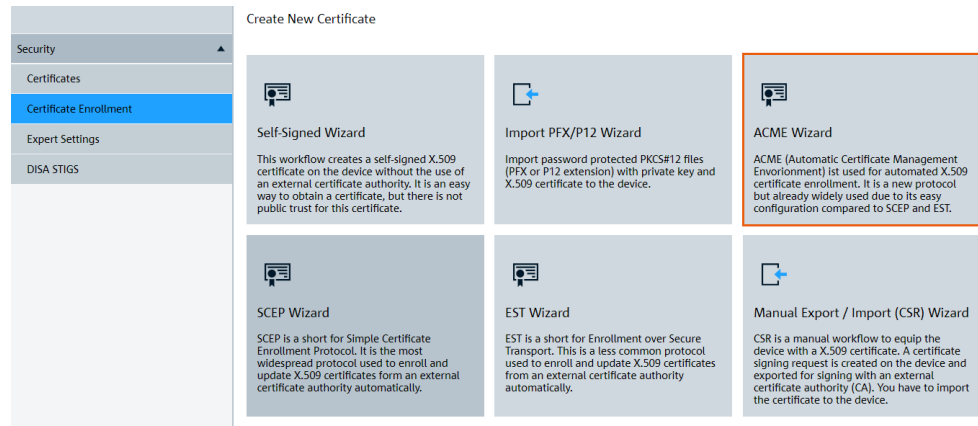


Figure 5-31: ACME wizard

- On the "Subject Name" page, enter the "Common Name" for the certificate.

The screenshot shows the 'ACME - Automatic Certificate Management Environment' wizard. A progress bar at the top indicates seven steps: 1. Subject Name (active), 2. Attributes, 3. ACME CA, 4. Trust ACME Server, 5. ACME Account, 6. Verify CA, and 7. Enroll Certificate. The 'Subject Name' step contains the following form fields:

- Common Name: R&S Device
- E-Mail Address: name@customer.com
- Organization: Customer Inc.
- Serial Number: 123456
- Organizational Unit: R&D
- Location / City: Munich
- State or Province: Bavaria
- Country: DE

At the bottom right, there are 'Next' and 'Cancel' buttons.

Figure 5-32: Subject name page

Note: All the other fields are optional.

- Click "Next".
- On the "Attributes" page, specify the DNS settings for the instrument if you wish to add them to the certificate.
- Select one of the supported algorithms and key sizes from the "Key Algorithm" dropdown.

Figure 5-33: Attributes page

7. Click "Next".
8. On the "ACME CA" page, specify the following:
 - Host name of the ACME CA server
 - URL of the ACME CA directory
 - Port number used for communication and authentication with ACME CA server

Figure 5-34: ACME CA page

Note: Select "Disable Proxy Settings" to disable the proxy settings in case they are enabled for your instrument.

9. Click "Request CA Settings".
10. On the "Trust ACME Server" page, verify if the digital fingerprint matches the known digital fingerprint of the trusted ACME CA.
11. Click "Trust Certificate" to confirm the authenticity of the certificate. Trust the certificate chain of the certificate authority.

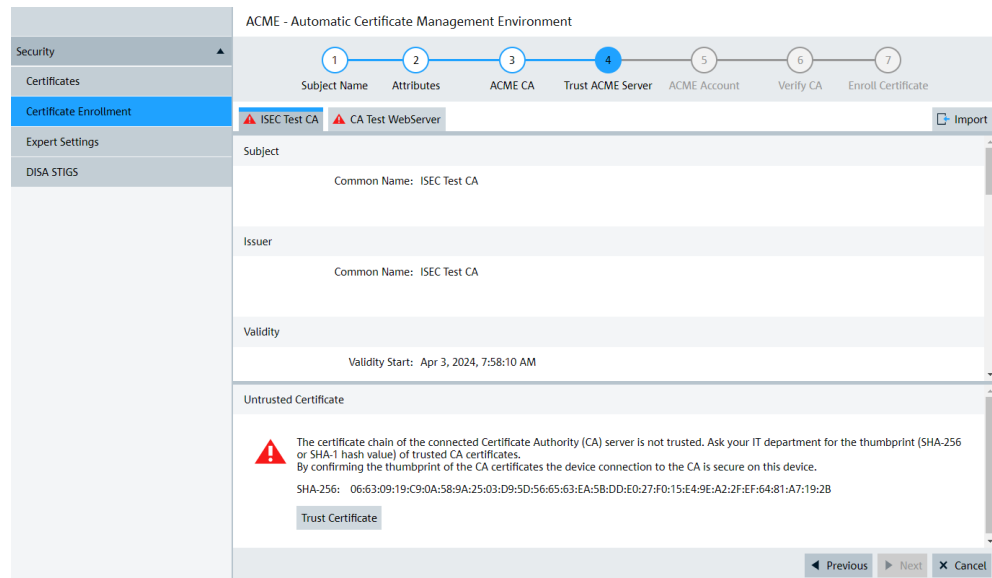


Figure 5-35: Trust ACME server page

- Wait until a blue checkmark appears next to the tabs displaying the root certificate, intermediate certificate and instrument certificate names.

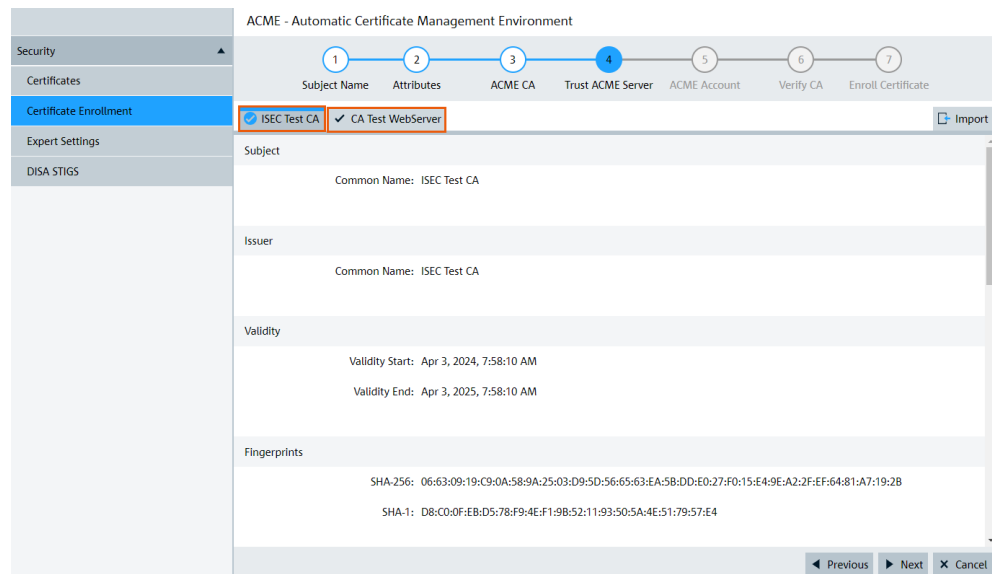


Figure 5-36: Trust ACME server page - Establish certificate trust chain

The blue checkmarks confirm that a certificate trust chain has been established with the ACME CA server.

Note: If a red warning symbol appears on one of the above tabs, Rohde & Schwarz recommends you to verify if the validation process is complete. If the validation process is complete and the warning symbol does not disappear, you can check if the certificate information is correct. Restart the enrollment process.

13. Click "Next".

14. On the "ACME Account" page, specify the following:

- Email Address used for communication with ACME CA
- EAB credentials if the ACME CA requires external account binding

Figure 5-37: ACME account page

15. Click "Terms of Service" to accept the terms and conditions.

16. Click "Enroll".

17. On the "Verify CA" page, verify if the displayed ACME certificate information is correct.

Figure 5-38: Verify CA page

18. Click "Next".

A status message "Certificate successfully received and installed" appears confirming that the ACME certificate is successfully installed on the Rohde & Schwarz instrument.

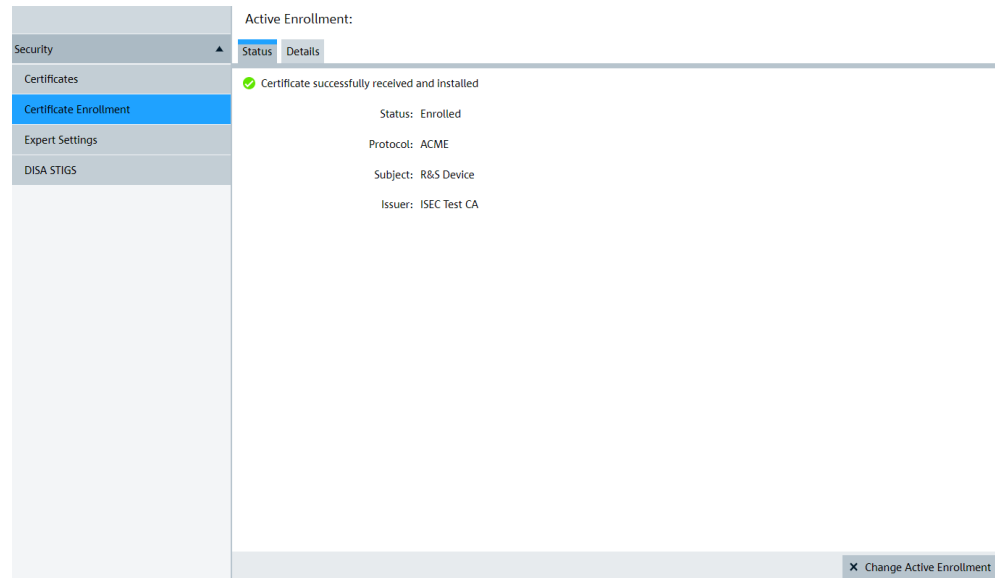


Figure 5-39: Status page

19. Go to the "Details" page to view the enrolled certificate information.

Note: You can view and manage all the certificates in the "Certificates" page.

20. On the "Details" page, click "Change Active Enrollment" if you want to change the current enrollment information of the certificate.

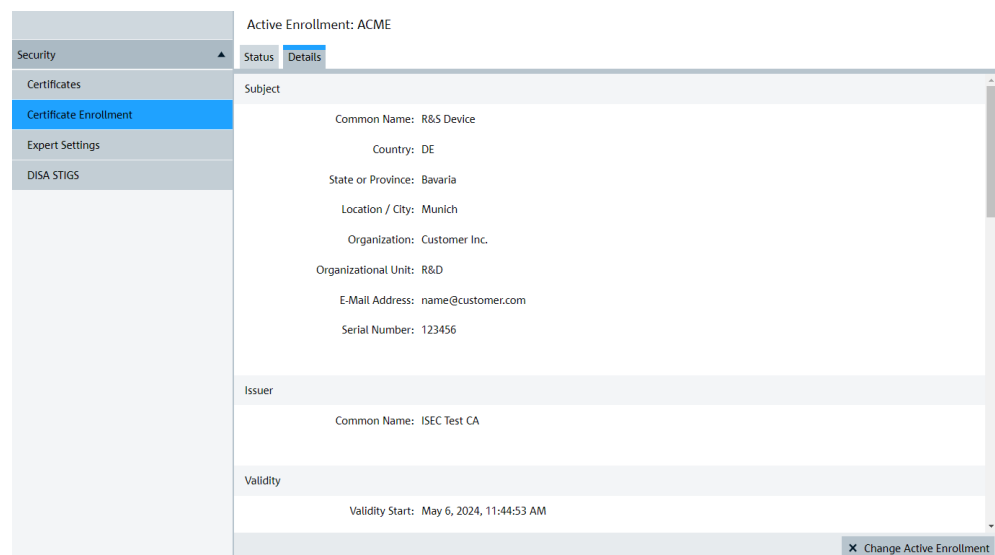


Figure 5-40: Details page

5.2.4 SCEP wizard

The "SCEP Wizard" supports automatic enrollment of certificates with the SCEP Server over the Simple Certificate Enrollment Protocol (SCEP) protocol. The certificates are enrolled automatically by submitting a certificate enrollment request to the SCEP certificate authority using the R&S ISEC service.

The "SCEP Wizard" allows you to enroll and manage SCEP certificates automatically.

5.2.4.1 Subject name

The "Subject Name" page defines the general properties of a digital certificate such as the common name, email address.

Self-Signed

Security

Certificates

Certificate Enrollment

Expert Settings

DISA STIGS

1 Subject Name

2 Attributes

Common Name: R&S Device

E-Mail Address: name@customer.com

Organization: Customer Inc.

Serial Number: 123456

Organizational Unit: R&D

Location / City: Munich

State or Province: Bavaria

Country: DE

Next Cancel

Figure 5-41: Subject name page

Common Name

Provide a unique certificate name. The "Common Name" can be the name of an instrument, person, or other entity. It is the most specific level in the identification hierarchy. For example, *R&S Device*.

When using the ACME protocol, the "Common Name" must match to the DNS on the "Attributes" page ("[Add Device DNS Name to the Certificate](#)" on page 22).

Note: The "Common Name" is a required field. All other fields on the "Subject Name" page are optional but can be filled if a policy to show these fields in your certificates exists in a company.

Email Address

Specify the organization or your email address for the certificate. For example, *name@customer.com*.

Organization

Specify the company name for the certificate. For example, *Customer Inc.*

Serial Number

Specify the unique serial number of the Rohde & Schwarz instrument. For example, *123456*.

Organization Unit

Specify the name of the designated organization unit that the certificate is used for. For example, *R&D*.

Locality

Specify the name of your locality for the certificate. For example, *Munich*.

State or Province

Specify the state or province name for the certificate. For example, *Bavaria*.

Country

Specify the 2-letter country code of your country for the certificate. For example, *DE* (for *Germany*).

5.2.4.2 Attributes

The "Attributes" page is used to define other enrollment details of a certificate such as the DNS name, IP address of the instrument.

Figure 5-42: Attributes page

Add Device DNS Name to the Certificate

Select this checkbox to include the DNS name of the instrument in the certificate.

Alternative DNS name

Enter a secondary DNS name (or host name), if any, for the certificate.

Note: This field is meant for the expert users only. The customers usually do not need to edit it.

IP Addresses

Enter the IP addresses of the Rohde & Schwarz instruments, if any.

Note: This field is meant for the expert users only. The customers usually do not need to edit it.

Purpose

Specifies the purpose for the certificate authentication. It is always *Server Authentication*. It is a certificate-based authentication, where the client initiates a TLS-secured HTTP session with the server (Rohde & Schwarz instrument) and validates the certificate offered by the server.

Key Algorithm

Select one of the available combinations of key algorithm, key size and hash function. These combinations are used to generate the key pair for the Rohde & Schwarz instrument.

- For RSA, the largest supported key size is 4096 bits.
- For Elliptic Curve, the largest supported key size is 384 bits.

The table below lists the different key algorithms supported by the R&S ISEC service.

Table 5-3: Key Algorithms

Algorithm	Type	Comment
RSA 2048 Bits	RSA	Default
RSA 3072 Bits	RSA	
RSA 4096 Bits	RSA	
NIST P-256	Elliptic Curve	NIST Standard
NIST P-384	Elliptic Curve	NIST Standard
ED25519	Elliptic Curve	

Note: Rohde & Schwarz recommends you to use the default option. If there are IT policies in place for higher security levels, you can choose one of the key algorithms that provide higher security (RSA 4096, NIST P-384).

5.2.4.3 SCEP CA

The "SCEP CA" page is used to set up the basic connection properties of the SCEP CA server. The properties are used to authenticate and securely connect to the SCEP CA server. This page allows you to define the SCEP properties such as SCEP CA server address, URL path, port number and challenge password.

Figure 5-43: SCEP CA page

Server Address

Specify the host name of the SCEP CA. For example, *pki.mycompany.local*.

URL Path

Specify the URL path of the SCEP CA.

Note: Ask your system administrator for the correct URL path.

Port

Indicates the TCP port number used for communication with the SCEP CA server. This port is normally standard HTTP port number 80.

Note: R&S ISEC service uses "Server Address", "URL Path" and "Port" fields to define the request URL. For example, *https://<Server Address>:<Port>/<URL Path>*

Challenge

Sets a challenge password used in the Certificate Signing Request. This password is verified by the SCEP CA to authorize SCEP requests.

Note: Ask your system administrator for the configured password.

Disable Proxy Settings

Select this checkbox to disable the HTTP proxy settings.

5.2.4.4 Verify CA

The "Verify CA" page is used to confirm the authenticity of the received CA certificates. To ensure that the received CA certificate is authentic, you must compare the certificate fingerprint (SHA-256 or the less secure SHA-1) with the original fingerprint. Obtain the original fingerprint by out-of-band means such as through an email from the CA website.

The Rohde & Schwarz instrument does not receive a single CA certificate, but a certificate chain that can be used to verify the root certificate in this chain. The validity of the other certificates can be verified automatically by traversing the chain (if the chain is

not broken). Once the CA information is verified, you can use the "Enroll" button to enroll the TLS certificate and store the signed certificate on the Rohde & Schwarz instrument. You can also use the "Import" button to import additional CA certificates, if necessary, from your local drive. The imported file can contain multiple PEM-encoded certificates or a single DER-encoded certificate.

Figure 5-44: Verify CA page

5.2.4.5 Enroll SCEP certificates

To enroll a SCEP certificate:

1. Click the "Certificate Enrollment" tab.
The "Create New Certificate" page appears.
2. On the "Create New Certificate" page, click "SCEP Wizard".

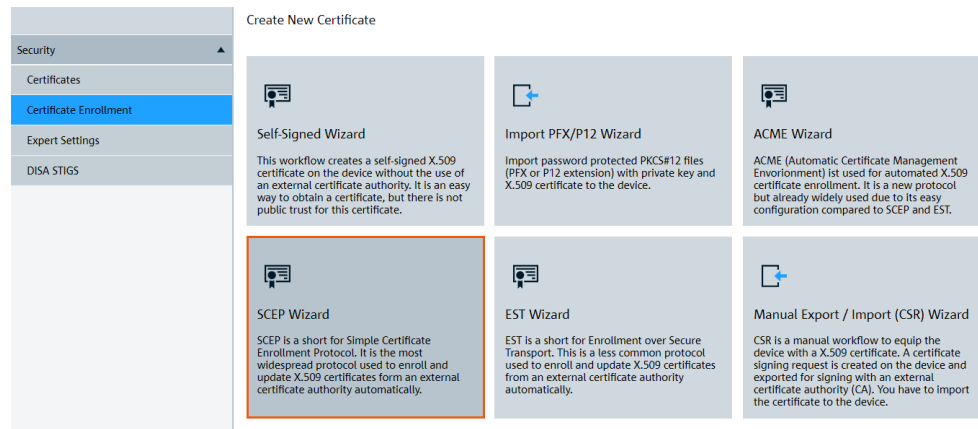


Figure 5-45: SCEP wizard

- On the "Subject Name" page, enter the "Common Name" for the certificate.

Figure 5-46: Subject name page

Note: All the other fields are optional.

- Click "Next".
- On the "Attributes" page, specify the DNS settings for the instrument if you wish to add them to the certificate.
- Select one of the supported algorithms and key sizes from the "Key Algorithm" dropdown.

Figure 5-47: Attributes page

7. Click "Next".
8. On the "SCEP CA" page, specify the following:
 - Host name and URL of the SCEP CA server
 - Port number and challenge password used for communication and authentication with the SCEP CA server

Figure 5-48: SCEP CA page

Note: Select "Disable Proxy Settings" to disable the proxy settings in case they are enabled for your instrument.

9. Click "Request CA Settings".
10. On the "Verify CA" page, verify if the digital fingerprint matches the known digital fingerprint of the trusted SCEP certificate authority.
11. Click "Trust Certificate" to confirm the authenticity of the certificate authority.

Figure 5-49: Verify CA page

- Wait until a blue checkmark appears next to the tabs displaying the root certificate, intermediate certificate and instrument certificate names.

Figure 5-50: Verify CA page - establish certificate trust chain

The blue checkmarks confirm that a certificate trust chain has been established with the SCEP CA server.

Note: If a red warning symbol appears on one of the above tabs, Rohde & Schwarz recommends you to verify if the validation process is complete. If the validation process is complete and the warning symbol does not disappear, you can check if the certificate information is correct. Restart the enrollment process.

13. Click "Enroll".

A status message "Certificate successfully received and installed" appears confirming that the SCEP certificate is successfully installed on the Rohde & Schwarz instrument.

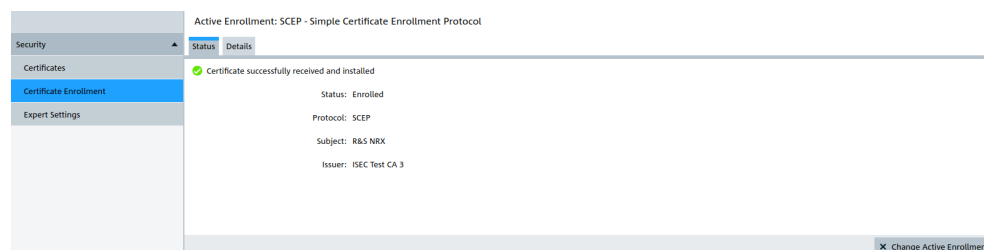


Figure 5-51: Status page

14. Go to the "Details" page to view the enrolled certificate information.

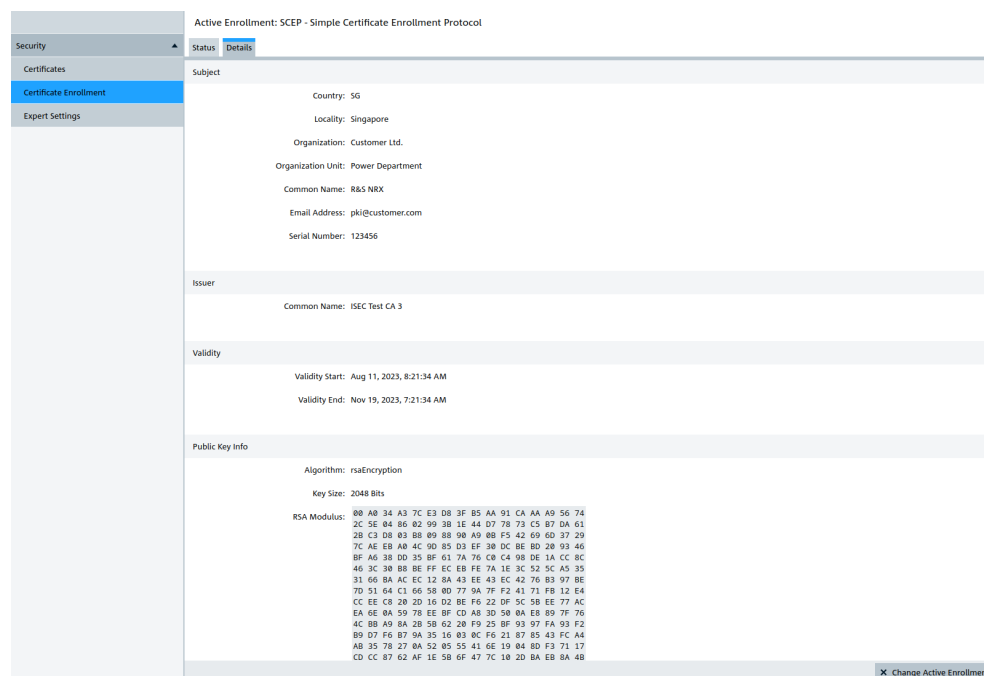


Figure 5-52: Details page

Note: You can view and manage all the certificates in the "Certificates" page.

15. On the "Details" page, click "Change Active Enrollment" if you want to change the current enrollment information of the certificate.

5.2.5 EST wizard

The "EST Wizard" supports automatic enrollment of certificates with the EST Server over the Enrollment over Secure Transport (EST) protocol. The certificates are enrolled

automatically by submitting a certificate enrollment request to the EST certificate authority using the R&S ISEC service.

The "EST Wizard" allows you to enroll and manage EST certificates automatically.

5.2.5.1 Subject name

The "Subject Name" page defines the general properties of a digital certificate such as the common name, email address.

The screenshot shows the 'Subject Name' page in the R&S ISEC web user interface. The page is titled 'Self-Signed' and features a progress bar with two steps: 'Subject Name' (step 1) and 'Attributes' (step 2). The 'Subject Name' step is active. The form contains several input fields: Common Name (R&S Device), E-Mail Address (name@customer.com), Organization (Customer Inc.), Serial Number (123456), Organizational Unit (R&D), Location / City (Munich), State or Province (Bavaria), and Country (DE). A 'Next' button and a 'Cancel' button are visible at the bottom right.

Figure 5-53: Subject name page

Common Name

Provide a unique certificate name. The "Common Name" can be the name of an instrument, person, or other entity. It is the most specific level in the identification hierarchy. For example, *R&S Device*.

When using the ACME protocol, the "Common Name" must match to the DNS on the "Attributes" page ("[Add Device DNS Name to the Certificate](#)" on page 22).

Note: The "Common Name" is a required field. All other fields on the "Subject Name" page are optional but can be filled if a policy to show these fields in your certificates exists in a company.

Email Address

Specify the organization or your email address for the certificate. For example, *name@customer.com*.

Organization

Specify the company name for the certificate. For example, *Customer Inc.*

Serial Number

Specify the unique serial number of the Rohde & Schwarz instrument. For example, *123456*.

Organization Unit

Specify the name of the designated organization unit that the certificate is used for. For example, *R&D*.

Locality

Specify the name of your locality for the certificate. For example, *Munich*.

State or Province

Specify the state or province name for the certificate. For example, *Bavaria*.

Country

Specify the 2-letter country code of your country for the certificate. For example, *DE* (for *Germany*).

5.2.5.2 Attributes

The "Attributes" page is used to define other enrollment details of a certificate such as the DNS name, IP address of the instrument.

Figure 5-54: Attributes page

Add Device DNS Name to the Certificate

Select this checkbox to include the DNS name of the instrument in the certificate.

Alternative DNS name

Enter a secondary DNS name (or host name), if any, for the certificate.

Note: This field is meant for the expert users only. The customers usually do not need to edit it.

IP Addresses

Enter the IP addresses of the Rohde & Schwarz instruments, if any.

Note: This field is meant for the expert users only. The customers usually do not need to edit it.

Purpose

Specifies the purpose for the certificate authentication. It is always *Server Authentication*. It is a certificate-based authentication, where the client initiates a TLS-secured HTTP session with the server (Rohde & Schwarz instrument) and validates the certificate offered by the server.

Key Algorithm

Select one of the available combinations of key algorithm, key size and hash function. These combinations are used to generate the key pair for the Rohde & Schwarz instrument.

- For RSA, the largest supported key size is 4096 bits.
- For Elliptic Curve, the largest supported key size is 384 bits.

The table below lists the different key algorithms supported by the R&S ISEC service.

Table 5-4: Key Algorithms

Algorithm	Type	Comment
RSA 2048 Bits	RSA	Default
RSA 3072 Bits	RSA	
RSA 4096 Bits	RSA	
NIST P-256	Elliptic Curve	NIST Standard
NIST P-384	Elliptic Curve	NIST Standard
ED25519	Elliptic Curve	

Note: Rohde & Schwarz recommends you to use the default option. If there are IT policies in place for higher security levels, you can choose one of the key algorithms that provide higher security (RSA 4096, NIST P-384).

5.2.5.3 EST CA

The "EST CA" page is used to set up the basic connection properties of the EST CA server. The properties are used to authenticate and securely connect to the EST CA server. This page allows you to define the EST properties such as EST CA server address, CA name, port number, user name, password and client certificate.

Figure 5-55: EST CA page

Server Address

Specify the URL path of the EST CA. For example, *https://estserver.domain.org*.

Note: Ask your system administrator for the correct URL path.

Port

Indicates the TCP port number used for communication with the EST CA server. The default port is 443.

CA Name

Specify the host name of the EST CA. For example, *pki.mycompany.local*.

Note: R&S ISEC service uses "Server Address", "Port" and "CA Name" fields to define the request URL. For example, *https://<Server Address>:<Port>/<CA Name>*

User Name

Sets a username for the EST client. For example, *estuser*.

Password

Sets a password for the EST client. The password must always be unique.

Note: If you create a connection entry that requires an EST certificate for authentication, enter the certificate username and password each time you initiate a connection first time. The password is not stored on the instrument. For certificate renewal, the previous password is not required anymore for authentication. Renewal uses the previously issued certificate for authentication.

Client Certificate

Select an existing instrument certificate, if any, for the EST server to recognize the Rohde & Schwarz instrument.

Disable Proxy Settings

Select this checkbox to disable the specified EST HTTP proxy settings.

Trust OS Certificate Store

Select this checkbox to allow the R&S ISEC service to use root certificates from the certificate store of the operating system on the instrument. This feature is an advanced feature for exceptional cases and usually optional.

5.2.5.4 Trust EST server

The "Trust EST Server" page is used to confirm the authenticity of the received CA certificates. To ensure that the received CA certificate is authentic, you must compare the certificate fingerprint (SHA-256 or the less secure SHA-1) with the original fingerprint. Obtain the original fingerprint by out-of-band means such as through an email from the CA website.

The Rohde & Schwarz instrument does not receive a single CA certificate, but a certificate chain that can be used to verify the root certificate in this chain. The validity of the other certificates can be verified automatically by traversing the chain (if the chain is not broken).

Figure 5-56: Trust EST server page

5.2.5.5 Verify CA

The "Verify CA" page is used to verify the PKI certificates. It is also used to enroll and store the signed certificates on the Rohde & Schwarz instrument. Once the CA information is verified, you can use the "Enroll" button to enroll the TLS certificate and store the signed certificate on the Rohde & Schwarz instrument. You can also use the "Import" button to import additional CA certificates, if necessary, from your local drive. The imported file can contain multiple PEM-encoded certificates or a single DER-encoded certificate.

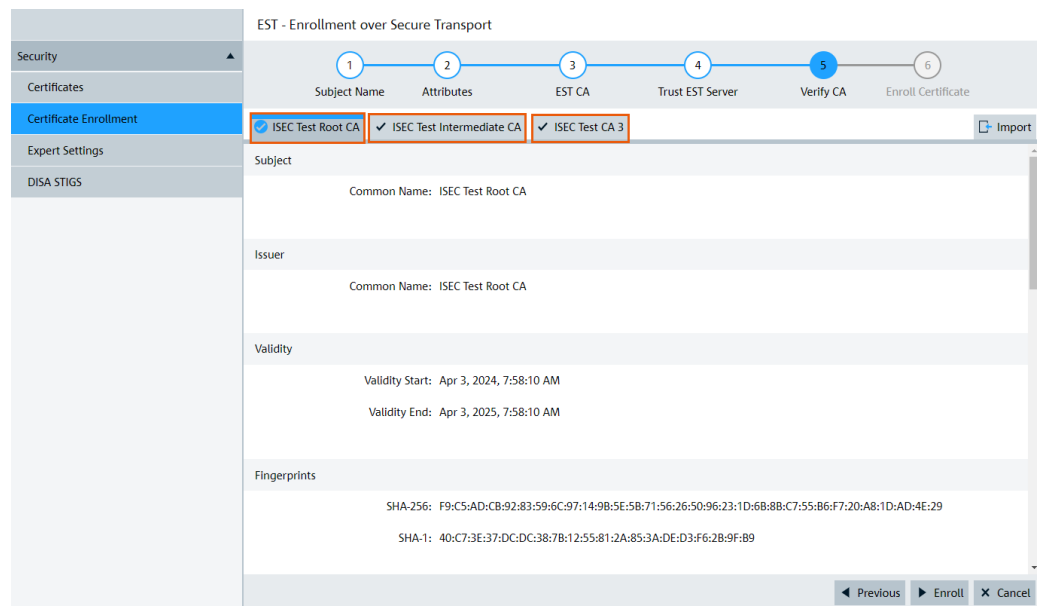


Figure 5-57: Verify CA page

5.2.5.6 Enroll EST certificates

To enroll an EST certificate:

1. Click the "Certificate Enrollment" tab.
The "Create New Certificate" page appears.
2. On the "Create New Certificate" page, click "EST Wizard".

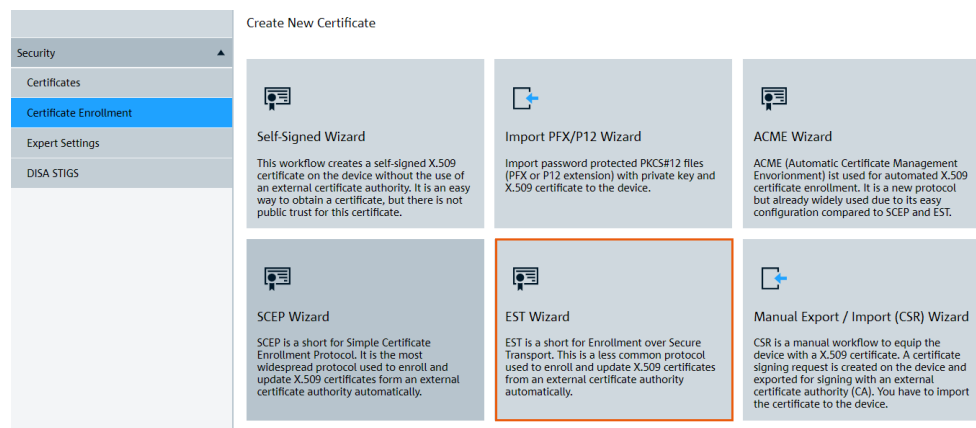


Figure 5-58: EST wizard

3. On the "Subject Name" page, enter the "Common Name" for the certificate.

Figure 5-59: Subject name page

Note: All the other fields are optional.

4. Click "Next".
5. On the "Attributes" page, specify the DNS settings for the instrument if you wish to add them to the certificate.
6. Select one of the supported algorithms and key sizes from the "Key Algorithm" dropdown.

Figure 5-60: Attributes page

7. Click "Next".
8. On the "EST CA" page, specify the following:
 - Host name of the EST CA server
 - Name of the EST CA
 - User name, password and port number used for communication and authentication with EST CA server
9. In the "Client Certificate" dropdown, select an existing instrument certificate, if any, for the EST CA server to recognize the instrument.

Figure 5-61: EST CA page

Note: Select "Disable Proxy Settings" to disable the proxy settings in case they are enabled for your instrument.

10. Click "Request CA Settings".
11. On the "Trust EST Server" page, verify if the digital fingerprint matches the known digital fingerprint of the trusted EST certificate authority.
12. Click "Trust Certificate" to confirm the authenticity of the certificate. Trust the certificate chain of the certificate authority.

Figure 5-62: Trust EST server page

13. Click "Next".
14. Wait until a blue checkmark appears next to the tabs displaying the root certificate, intermediate certificate and instrument certificate names.

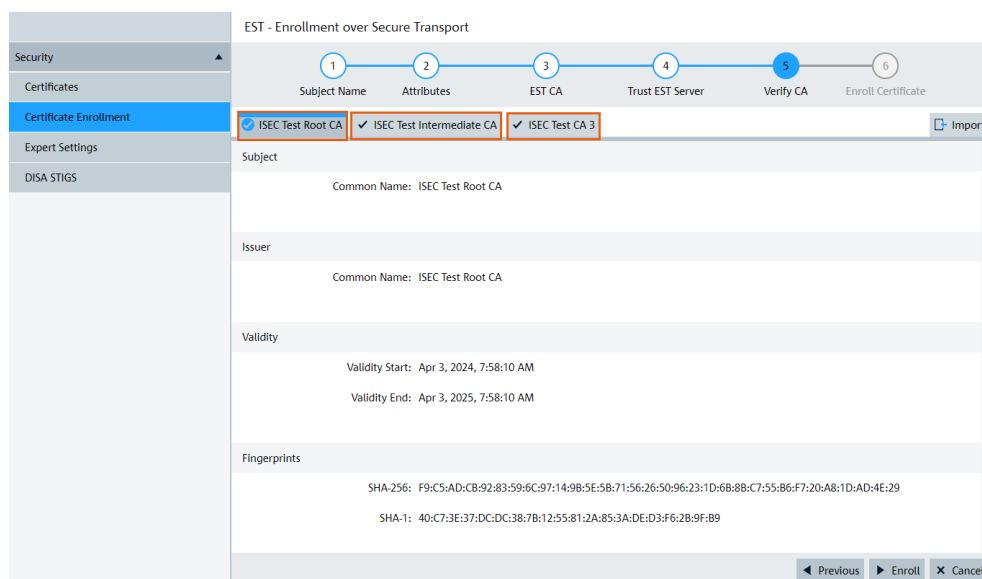


Figure 5-63: Verify CA page - establish certificate trust chain

The blue checkmarks confirm that a certificate trust chain has been established with the EST CA server.

Note: If a red warning symbol appears on one of the above tabs, Rohde & Schwarz recommends you to verify if the validation process is complete. If the validation process is complete and the warning symbol does not disappear, you can check if the certificate information is correct. Restart the enrollment process.

15. Click "Enroll".

A status message "Certificate successfully received and installed" appears confirming that the EST certificate is successfully installed on the Rohde & Schwarz instrument.

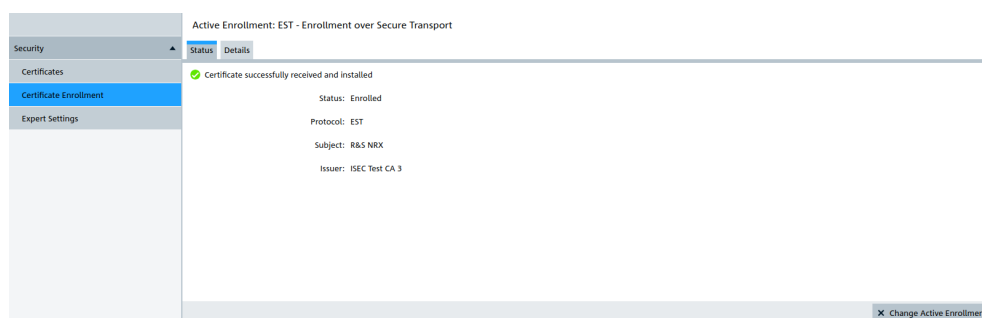


Figure 5-64: Status page

16. Go to the "Details" page to view the enrolled certificate information.

Active Enrollment: EST - Enrollment over Secure Transport

Security

Certificates

Certificate Enrollment

Expert Settings

DISA STIGS

Status Details

Subject

Country: SG

Locality: Singapore

Organization: Customer Ltd.

Organization Unit: Power Department

Common Name: R&S NRX

Email Address: pk@customers.com

Serial Number: 123456

Issuer

Common Name: ISEC Test CA 3

Validity

Validity Start: Aug 7, 2023, 8:08:44 AM

Validity End: Aug 6, 2033, 8:08:44 AM

Public Key Info

Algorithm: rsaEncryption

Key Size: 3072 Bits

RSA Modulus: 8B FA 85 6C 3B D8 CB 88 66 B8 F2 B6 6D 81 A9 DC
 4C F9 82 62 78 EE 22 75 3F 5E 12 07 3F E9 B8 C4
 EA E7 C2 AC DF 2A 48 CD 29 AB DA 0A F2 2A 27 28
 9E 36 C5 95 27 52 CE 8F A9 56 EF E2 E8 11 84 A0
 72 FE 43 38 6A EF F7 C3 56 28 25 5A 25 02 B8 82
 AB C5 9E 18 9F 28 4E 83 D1 A1 81 56 1E FC 8F 00
 5F B3 81 A8 38 5C F7 86 11 F7 D3 27 E4 81 41 24
 34 79 81 08 BF 55 03 8D 91 FA 7A 77 9C F5 9A 56
 7B 9A CC 85 25 C4 36 E1 6E 98 55 A4 D2 88 B9 71
 65 F4 EA 40 7C 2A 32 F7 CB 45 94 F5 18 68 57 A1
 B8 8C 43 E7 6C 66 C3 8D 4A 85 8F 39 CA 88 27 28
 DB 84 9A 31 D1 B7 26 16 C5 21 3C 37 14 98 86 CD
 29 BE 08 83 85 AC 01 AC 87 F2 08 88 8A A5 26
 CC FE 2E 97 FE 88 12 17 99 2A 53 84 A7 11 B8 34
 26 34 42 95 E3 14 E8 4F 3F 61 27 B8 48 88 78 BF
 94 8D 9F F3 48 FC 1E 8F AC 24 E2 2A 93 13 4E 2F
 7C 88 F4 84 5A FF F9 FF 4C FF 44 0C 2F 2A 84 C8

Figure 5-65: Details page

Note: You can view and manage all the certificates in the "Certificates" page.

- On the "Details" page, click "Change Active Enrollment" if you want to change the current enrollment information of the certificate.

5.2.6 Manual export / import (CSR) wizard

The "Manual Export / Import (CSR) Wizard" allows you to create and download a certificate signing request (CSR) to your local drive. You can use the CSR to request a certificate from a certificate authority. The received certificate can then be uploaded and imported by the R&S ISEC service.

5.2.6.1 Subject name

The "Subject Name" page defines the general properties of a digital certificate such as the common name, email address.

Self-Signed

Security

Certificates

Certificate Enrollment

Expert Settings

DISA STIGS

1 Subject Name

2 Attributes

Common Name: R&S Device

E-Mail Address: name@customer.com

Organization: Customer Inc.

Serial Number: 123456

Organizational Unit: R&D

Location / City: Munich

State or Province: Bavaria

Country: DE

Next Cancel

Figure 5-66: Subject name page

Common Name

Provide a unique certificate name. The "Common Name" can be the name of an instrument, person, or other entity. It is the most specific level in the identification hierarchy. For example, *R&S Device*.

When using the ACME protocol, the "Common Name" must match to the DNS on the "Attributes" page ("[Add Device DNS Name to the Certificate](#)" on page 22).

Note: The "Common Name" is a required field. All other fields on the "Subject Name" page are optional but can be filled if a policy to show these fields in your certificates exists in a company.

Email Address

Specify the organization or your email address for the certificate. For example, *name@customer.com*.

Organization

Specify the company name for the certificate. For example, *Customer Inc.*

Serial Number

Specify the unique serial number of the Rohde & Schwarz instrument. For example, *123456*.

Organization Unit

Specify the name of the designated organization unit that the certificate is used for. For example, *R&D*.

Locality

Specify the name of your locality for the certificate. For example, *Munich*.

State or Province

Specify the state or province name for the certificate. For example, *Bavaria*.

Country

Specify the 2-letter country code of your country for the certificate. For example, *DE* (for *Germany*).

5.2.6.2 Attributes

The "Attributes" page is used to define other enrollment details of a certificate such as the DNS name, IP address of the instrument.

Figure 5-67: Attributes page

Add Device DNS Name to the Certificate

Select this checkbox to include the DNS name of the instrument in the certificate.

Alternative DNS name

Enter a secondary DNS name (or host name), if any, for the certificate.

Note: This field is meant for the expert users only. The customers usually do not need to edit it.

IP Addresses

Enter the IP addresses of the Rohde & Schwarz instruments, if any.

Note: This field is meant for the expert users only. The customers usually do not need to edit it.

Purpose

Specifies the purpose for the certificate authentication. It is always *Server Authentication*. It is a certificate-based authentication, where the client initiates a TLS-secured HTTP session with the server (Rohde & Schwarz instrument) and validates the certificate offered by the server.

Key Algorithm

Select one of the available combinations of key algorithm, key size and hash function. These combinations are used to generate the key pair for the Rohde & Schwarz instrument.

- For RSA, the largest supported key size is 4096 bits.

- For Elliptic Curve, the largest supported key size is 384 bits.

The table below lists the different key algorithms supported by the R&S ISEC service.

Table 5-5: Key Algorithms

Algorithm	Type	Comment
RSA 2048 Bits	RSA	Default
RSA 3072 Bits	RSA	
RSA 4096 Bits	RSA	
NIST P-256	Elliptic Curve	NIST Standard
NIST P-384	Elliptic Curve	NIST Standard
ED25519	Elliptic Curve	

Note: Rohde & Schwarz recommends you to use the default option. If there are IT policies in place for higher security levels, you can choose one of the key algorithms that provide higher security (RSA 4096, NIST P-384).

5.2.6.3 Export CSR

The "Export CSR" page allows you to generate and download a certificate signing request (CSR) using the "Export" button. The CSR is created in a PEM format and can be viewed using a simple text editor.

You can use the R&S ISEC service to generate a CSR for your instrument and send it to the respective certificate authority to order a certificate. It contains the common name, domain name and public key of the instrument. The certificate authority uses the data from the CSR to build and issue a digital certificate.



The certificate must always include the certificate chain of the CA.

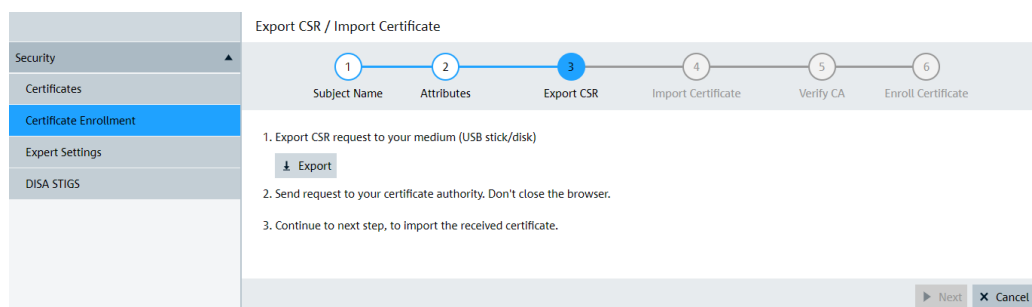


Figure 5-68: Export CSR page

5.2.6.4 Import certificate

When you receive a TLS certificate from your certificate authority, you need to import and install it on your instrument. The "Import Certificate" page allows you to import a

digital certificate received from your certificate authority to your instrument using the "Import" button.

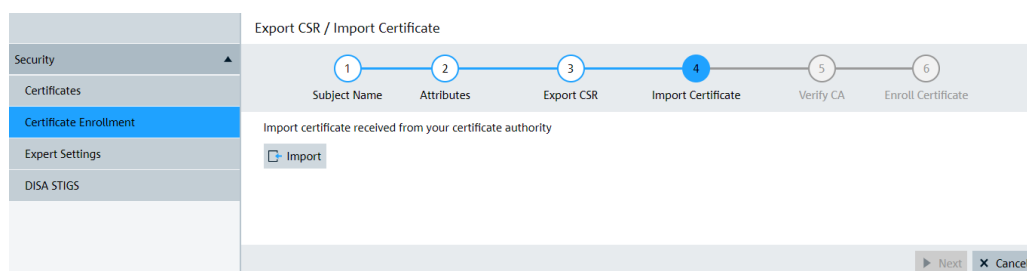


Figure 5-69: Import certificate page

5.2.6.5 Verify CA

The "Verify CA" page is used to confirm the authenticity of the received CA certificates. To ensure that the received CA certificate is authentic, you must compare the certificate fingerprint (SHA-256 or the less secure SHA-1) with the original fingerprint. Obtain the original fingerprint by out-of-band means such as through an email from the CA website.

The Rohde & Schwarz instrument does not receive a single CA certificate, but a certificate chain that can be used to verify the root certificate in this chain. The validity of the other certificates can be verified automatically by traversing the chain (if the chain is not broken). Once the CA information is verified, you can use the "Enroll" button to enroll the TLS certificate and store the signed certificate on the Rohde & Schwarz instrument. You can also use the "Import" button to import additional CA certificates, if necessary, from your local drive. The imported file can contain multiple PEM-encoded certificates or a single DER-encoded certificate.

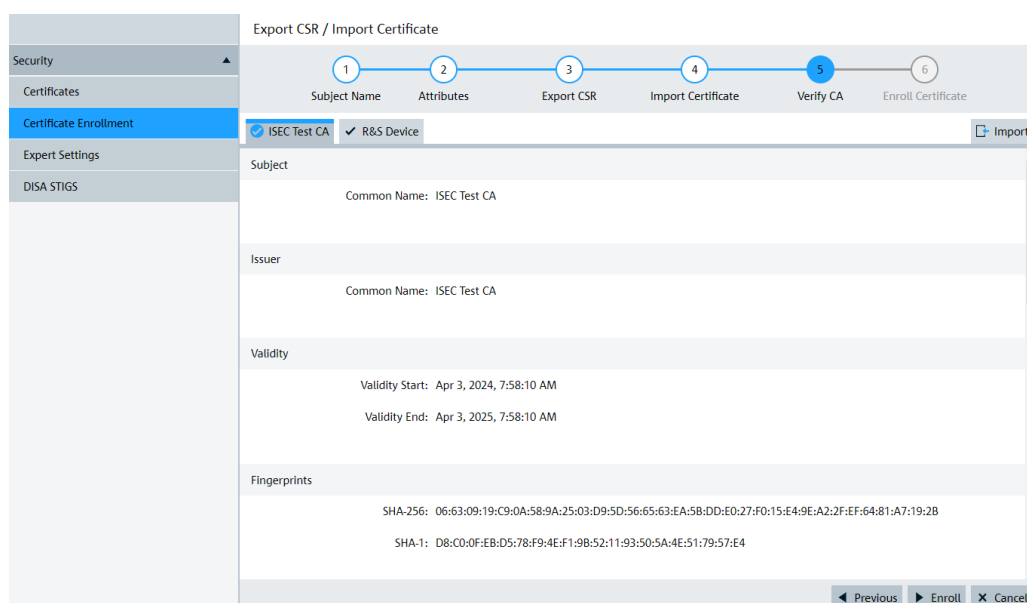


Figure 5-70: Verify CA page

5.2.6.6 Use manual export / import (CSR) wizard to enroll certificates

To create a CA-signed certificate using "Manual Export / Import (CSR) Wizard":

1. Click the "Certificate Enrollment" tab.

The "Create New Certificate" page appears.

2. On the "Create New Certificate" page, click "Manual Export / Import (CSR) Wizard".

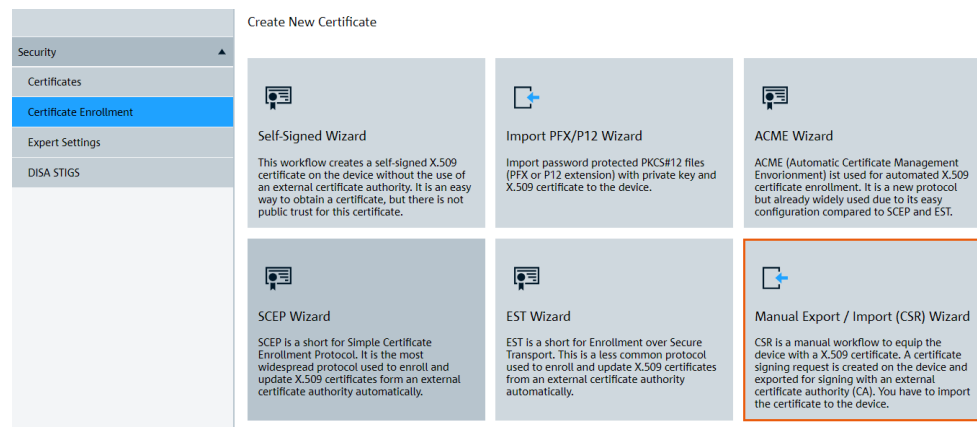


Figure 5-71: Manual export / import (CSR) wizard

3. On the "Subject Name" page, enter the "Common Name" for the certificate.

The screenshot shows the 'Export CSR / Import Certificate' page with a progress bar at the top indicating six steps: 1. Subject Name, 2. Attributes, 3. Export CSR, 4. Import Certificate, 5. Verify CA, and 6. Enroll Certificate. The 'Subject Name' step is currently active. The form contains the following fields:

- Common Name: R&S Device
- E-Mail Address: name@customer.com
- Organization: Customer Inc.
- Serial Number: 123456
- Organizational Unit: R&D
- Location / City: Munich
- State or Province: Bavaria
- Country: DE

At the bottom right, there are 'Next' and 'Cancel' buttons.

Figure 5-72: Subject name page

Note: All the other fields are optional.

4. Click "Next".
5. On the "Attributes" page, specify the DNS settings for the instrument if you wish to add them to the certificate.
6. Select one of the supported algorithms and key sizes from the "Key Algorithm" dropdown.

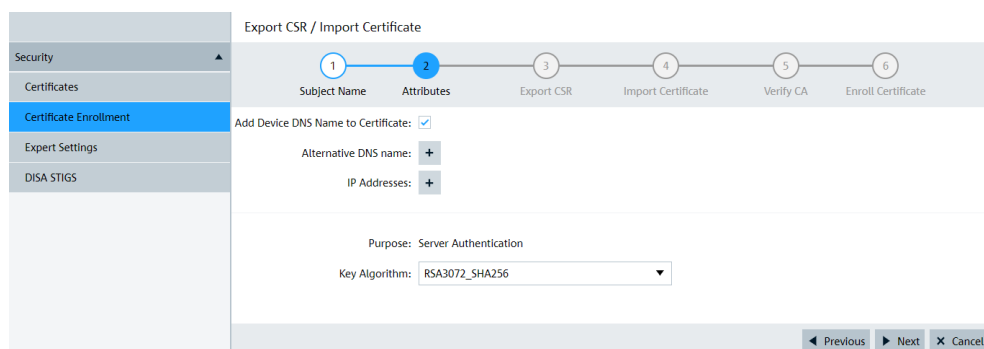


Figure 5-73: Attributes page

7. Click "Next".
8. On the "Export CSR" page, click "Export" to download the PEM Certificate Signing Request file to your local drive.

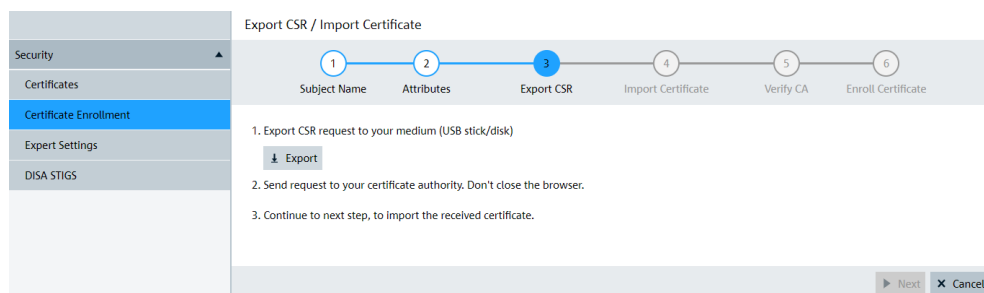


Figure 5-74: Export CSR page

9. Send the PEM request file to the certificate authority to create the necessary CA certificate.
10. Once you receive the CA signed certificate, click "Next".
11. On the "Import Certificate" page, click "Import" to browse for the received certificate on your local drive. Select it.

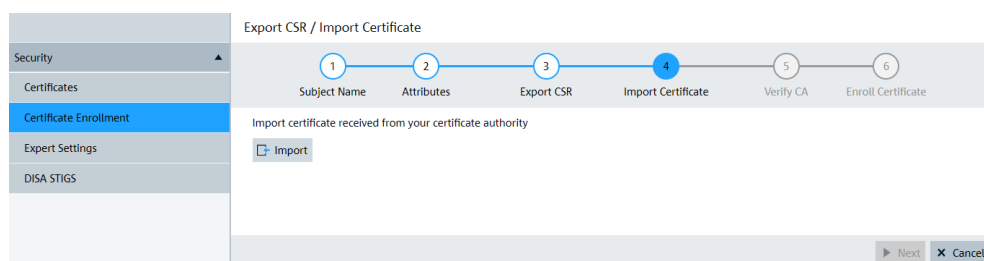


Figure 5-75: Import certificate page

A status message "Certificate was imported successfully" appears confirming that the certificate is successfully uploaded.

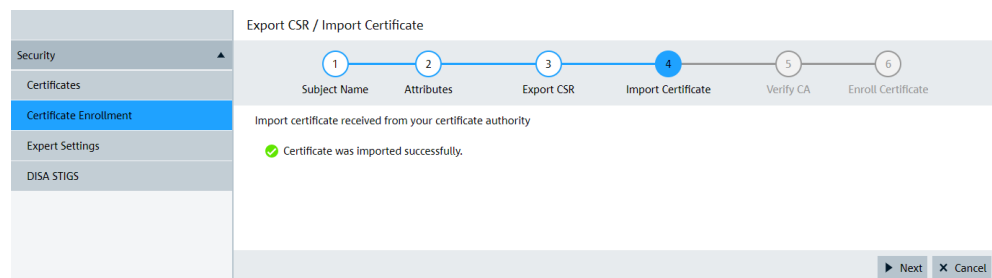


Figure 5-76: Import certificate page - certificate

12. Click "Next".
13. On the "Verify CA" page, verify if the digital fingerprint matches the known digital fingerprint of the trusted CA.
14. Click "Trust Certificate" to confirm the authenticity of the certificate authority.

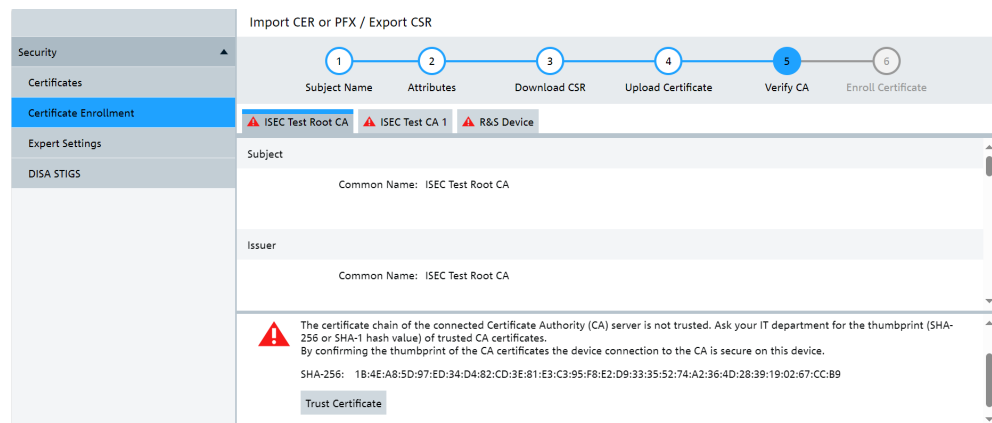


Figure 5-77: Verify CA page

15. Wait until a blue checkmark appears next to the tabs displaying the root certificate, intermediate certificate and instrument certificate names.

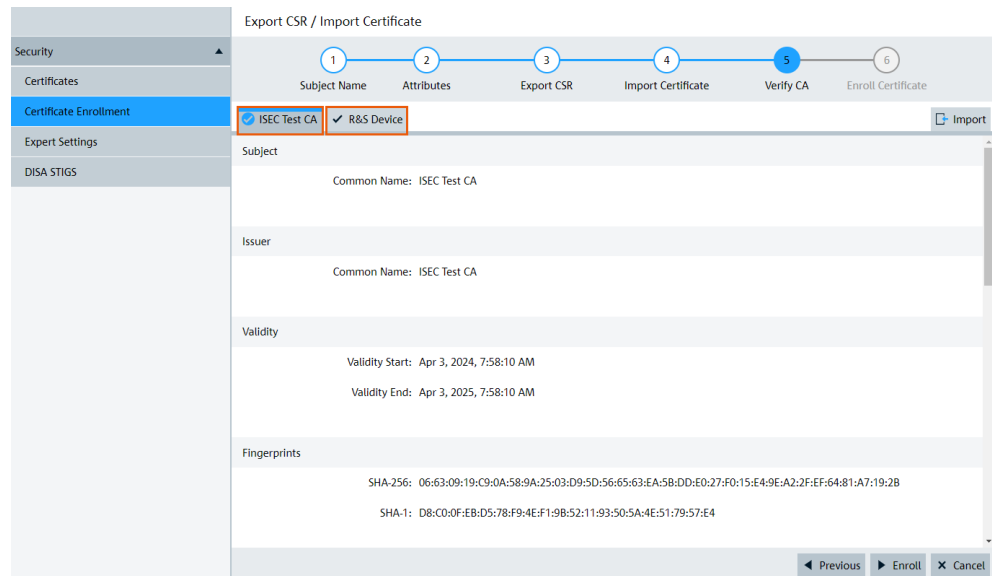


Figure 5-78: Verify CA page - establish certificate trust chain

The blue checkmarks confirm that a certificate trust chain has been established with the CA server.

Note: If a red warning symbol appears on one of the above tabs, Rohde & Schwarz recommends you to verify if the validation process is complete. If the validation process is complete and the warning symbol does not disappear, you can check if the certificate information is correct. Restart the enrollment process.

16. Click "Enroll".

A status message "Certificate successfully received and installed" appears confirming that the certificate is successfully installed on the Rohde & Schwarz instrument.

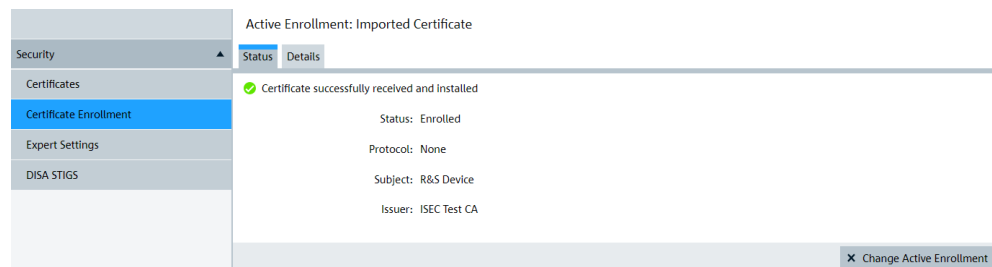


Figure 5-79: Status page

17. Go to the "Details" page to view the enrolled certificate information.

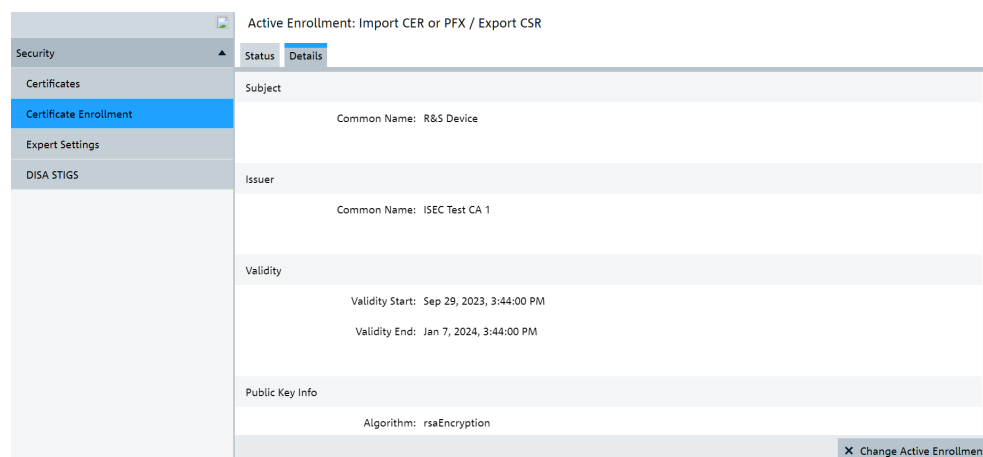


Figure 5-80: Details page

Note: You can view and manage all the certificates in the "Certificates" page.

- On the "Details" page, click "Change Active Enrollment" if you want to change the current enrollment information of the certificate.

5.3 Message log

All changes in certificates status are recorded in a message log. The message log can be viewed in the Web user interface by navigating to "Message Log" in the menu bar. The view does not refresh itself. You can request the current message log by clicking the "Update" button in the top menu bar.

Severity	Timestamp	Message	Details	Span
INFO	2025-01-17T13:29:37.276218Z	Certificate deleted (lx005876.rsint.net)	✓	host event
INFO	2025-01-17T13:29:37.737209Z	Reliability status of certificate 'lx005876.rsint.net' changed to NotReliable	—	
INFO	2025-01-17T13:29:37.737262Z	Reliability status of certificate 'lx005876.rsint.net' changed to Reliable	—	
INFO	2025-01-17T13:29:37.738068Z	Fallback to self-signed certificate.	—	
INFO	2025-01-17T13:29:37.738128Z	New certificate (lx005876.rsint.net)	✓	host event

Figure 5-81: Message log page

The column headers in the table can be used to sort and filter message lines. The "Span" column gives the context in which the message was generated. It is possible to filter the context for a more clearly arranged view.

The log entries carry details. Display the details by selecting the entry and clicking "Details" in the top menu bar.

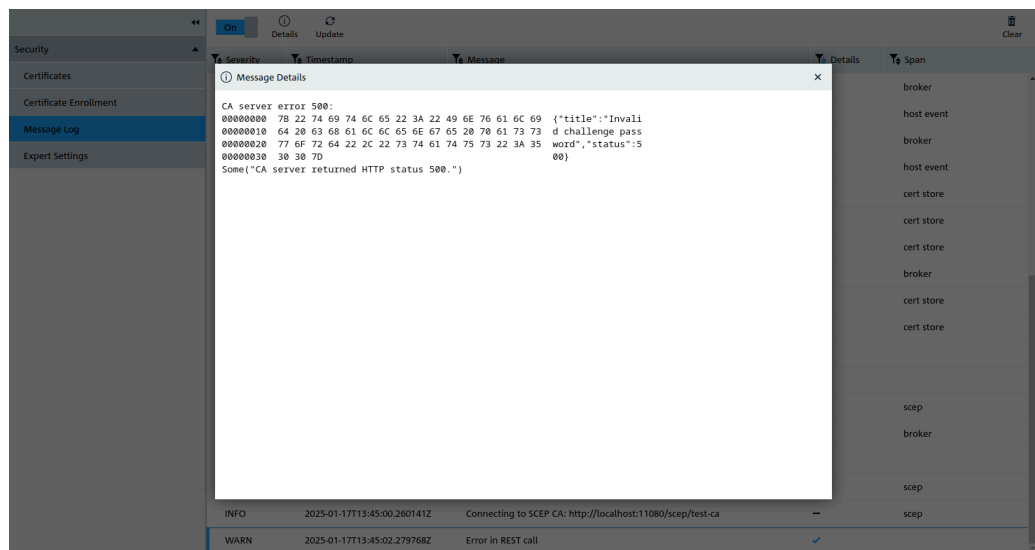


Figure 5-82: Message details page

5.4 Expert settings

The "Expert Settings" page is used to define the administrative settings of the R&S ISEC service such as renewal threshold, expiration warning threshold and CRL cron settings. It contains the following fields:

Figure 5-83: Expert settings page

Renewal Threshold

Specify the time interval (in ISO 8601 duration format) before the instrument requests renewal of the certificate. The default time is 2 weeks. For example, specifying *P4W* represents a period of 4 weeks. In this case, the R&S ISEC service requests for the renewal of the certificate after every 4 weeks.

Expiration Warning Threshold

Specify the time interval (in ISO 8601 duration format) before the application sends a warning message for the renewal of the certificate. For example, specifying *P2W* represents a period of two weeks, *PT10H* represents a period of 10 hours.

CRL Cron

Specify a time period (in cron syntax) to enable a cron job. The cron job triggers a periodic revocation check based on the specified value. The revocation check compares the currently used certificate with the certificate revocation list (CRL). The CRL is located on a server accessible for all communication participants; it is located on an external server outside the Rohde & Schwarz instrument especially for CA certificates.

Create a self-signed fallback certificate for

Select this checkbox if you want the R&S ISEC service to replace a CA certificate (once it is expired) for a particular instrument with a self-signed certificate automatically. You can also select this checkbox to create and enroll a self-signed certificate automatically.

6 Contacting customer support

Technical support – where and when you need it

For quick, expert help with any Rohde & Schwarz product, contact our customer support center. A team of highly qualified engineers provides support and works with you to find a solution to your query on any aspect of the operation, programming or applications of Rohde & Schwarz products.

Contact information

Contact our customer support center at www.rohde-schwarz.com/support, or follow this QR code:



Figure 6-1: QR code to the Rohde & Schwarz support page