EVERTRUST

EverTrust Horizon documentation v2.7

User Guide

EVERTRUST

Table of Contents

1. Introduction

1.1. Description

Horizon is an EverTrust Certificate lifecycle management solution and is powered up by:

- Pekko
- BouncyCastle
- MongoDB
- Kamon
- Play! Framework
- Scala
- NGINX
- Vue.js
- Quasar

This document is specific to Horizon version **2.7**.

2. Request workflow

Each Request has the same lifecycle described by the following figure.

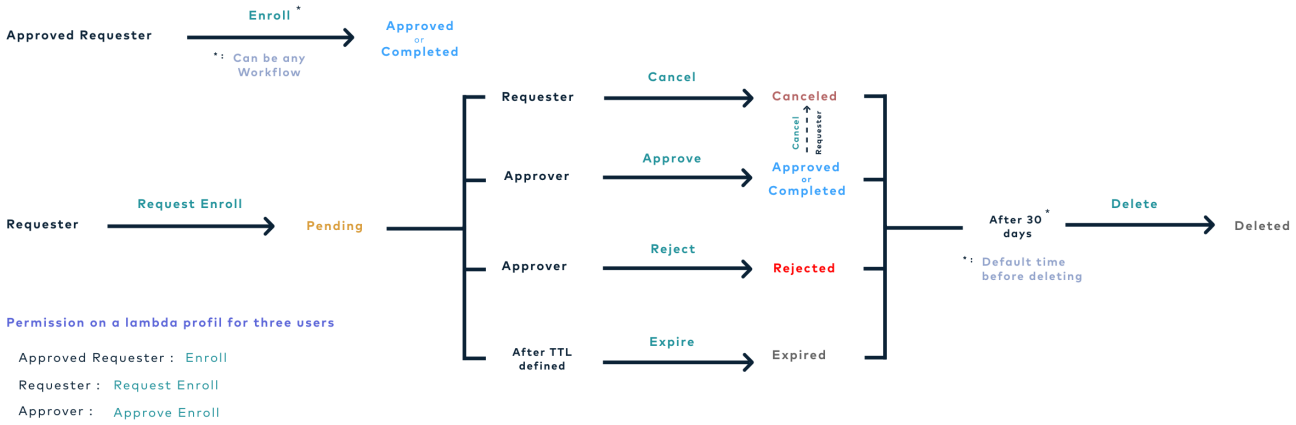

Figure 1. Request Workflow

2.1. Requester

A requester is someone who is granted the permission to request a certificate (enroll, renew, revoke, update, recover).

2.2. Approver

An approver is someone who is granted the permission to approve a request (enroll, renew, revoke, update, recover). An approver cannot approve its own request.

2.3. Owner

A request owner is someone who is designated as the benefactor for the request. It can view the request like the requester (in the `My requests` drawer), but unlike the requester, they can also access the certificate information (PKCS#12, challenge password).

The owner is computed according to the following rules:

- **enroll, update, migrate**: the owner is the one defined in the request template (ownership tab)
- **renew**: the owner of the request is the owner of the renewed certificate
- **recover**: the owner is the requester of the recover request
- **revoke**: no owner is associated with the request

Table 1. Owner vs Requester

User type	Can view the request	Can view the PKCS#12	Can view the challenge password
Requester	Yes	No	No
Owner	Yes	Yes	Yes

NOTE	Any user with the `Enroll API/ Renew API` permission can access the PKCS#12 or the challenge password for the workflow regardless of ownership status

2.4. How to enroll a certificate using the WebRA

1. Log in to Horizon registration authority Interface

2. Access Request Certificate from the drawer: **Request Certificate**

Profile tab

3. Fill in all the mandatory fields

- **Certificate profile***(string select)*:
  The certificate profile will be used in order to build the next step of the enrollment.

If decentralized enrollment is enabled for the profile:

Either:

- **CSR***(string)*:
  The CSR in PEM format
- **Import a CSR file***(file)*:
  The CSR file

If centralized enrollment is enabled for the profile:

- **Key type***(string select)*:
  The key type will be used for the private key generation

In case of the definition of a password policy:

- **Password***(string)*:
  The password will be used for the PKCS#12 encryption

CAUTION	You must comply with the configured password policy.

4. Click on Next button.

Data tab

5. Fill in all the mandatory fields:

- **Subject***(string)*:
  Fill the subject fields of the certificate
- **Subject Alternatives Names***(string)*:
  Fill the Subject Alternative Names of the certificate
- **Extensions***(string)*:

Fill the extensions of the certificate

TIP	In decentralized mode, CSR values will be used as default for the corresponding fields.

CAUTION	You must comply with the configured regular expression(s) that you can get with the ? icon.

6. Click on next button.

Labels tab

7. Fill in all the mandatory fields:

- **Labels***_(string)_:
  The labels will be used for permission, email and certificate search.

WARNING	You must comply with the configured regular expression(s) that you can get with the ? icon.

- **Requester comment** _(string)_:
  This comment appears:
  - to the approver when your request is in the pending status.
  - in the certificate info after the enrollment.

8. Click on next button.

Ownership tab

9. Fill in all the fields:

- **Owner** _(string input)_:
  Displayed if an owner policy is set. The owner of the certificate can search it, and request other actions on it (such as revoke, recover, ..).
- **Contact email address** _(string email format)_:
  Displayed if an email policy is set. An email can be sent each time the request status changes (see request lifecycle). This will also set the contact email of the certificate.
- **Team** _(string input)_:
  Displayed if a team policy is set. A team has the same rights as an owner on a certificate.

10. Click on next button.

Summary tab

If you own the enrolling permission

11. Click on enroll button
You can download the PKCS#12 after the enrollment if you are allowed to in the profile

If you own the request certificate permission

11. Click on request button
You have to wait until your request is approved, afterward you will be able to download the PKCS#12 if you are allowed to in the profile

2.5. How to request a certificate revocation

1. Log in to Horizon registration authority Interface

2. Access Either my certificates or Search certificates from the drawer: **My Certificates/Search Certificates**

3. Click on the Revoke icon 

CAUTION	The revoke icon appears only if you own the permission to revoke the certificate

Revocation Options tab

4. Fill in all the mandatory fields.

- **Revocation reason*** *(String select)*:
  The revocation reason that will appear on the CRL
- **Contact email address** *(string email format)*:
  Used if an email configuration is set. An email can be sent each time the request status changes (see request lifecycle)
- **Requester comment** *(String)*:
  This comment appears:
  - by the approver when your request is in the pending status
  - to the certificate info after the revocation

5. Click on Certificate tab

Certificate tab

6. Check the certificate's information

7. Click on Ownership tab

Ownership tab

8. Check the certificate's ownerhip information

If you have the revoke permission

9. Click on the revoke button
The certificate is now revoked.

9. Click on request button

You have to wait until your request is approved, afterward you will be able to see the certificate as revoked when you search for it

2.6. How to request a certificate update

1. Log in to Horizon Registration Authority Interface

2. Access request update from the drawer: **My certificates** or **Search certificates**

3. Click on request update button 

Labels tab

4. You can update in the labels section the labels

- **Label** *(string input)*:
  Enter a correct label

Ownership tab

5. You can update the ownership information

- **Owner** *(string input)*:
  Displayed if an owner policy is set. The owner of the certificate can search it, and request other actions on it (such as revoke, recover, ..).
- **Contact email address** *(string email format)*:
  Displayed if an email policy is set. An email can be sent each time the request status changes (see request lifecycle). This will also set the contact email of the certificate.
- **Team** *(string input)*:
  Displayed if a team policy is set. A team has the same rights as an owner on a certificate.

6. You can also check the details information

Certificate tab

7. You can also check the certificate information

8. Once you have made changes you can request the update by clicking on the update button

2.7. How to request a certificate duplication

A Duplication is a simplification of the enroll process. When choosing the duplication on a certificate, a new certificate enrollment request is created with the information from the previous certificate. Certificate data and metadata are still editable, as opposed to a renewal.

1. Log in to Horizon Registration Authority Interface

2. Access request duplication from the drawer: **My certificates** or **Search certificates**

3. Click on request duplication button 

Profile tab

4. Fill in all the mandatory fields

- **Key type*** *(string)*:
  The key type will be used for the private key generation

In case of the definition of a password policy:

- **Password***_(string)_:
  The password will be used for the PKCS#12 encryption

5. Go to enroll (same as duplicate) and follow all the steps

2.8. How to request a certificate renewal

A certificate renewal will enroll a certificate strictly identical to the previous one. No edition of certificate data or metadata can take place.

1. Log in to Horizon Registration Authority Interface

2. Access request renew from the drawer: **My certificates** or **Search certificates**

3. Click on request renew button 

Renew options tab

4. Fill in all the fields

- **Key type*** *(string)*:
  *Enabled on **centralized** enrollment:* The key type will be used for the private key generation.
- **Password***_(string)_:
  *Enabled on **centralized** enrollment with **manual** password policy:* The password will be used for the PKCS#12 encryption.
- **CSR*** *(string)*:
  *Enabled on **decentralized** enrollment:* The CSR, defining the public key of the enrolled certificate.
- **Comment** *(string)*:
  This comment appears:
  - to the approver when your request is in the pending status.
  - in the certificate info after the enrollment.

Certificate tab

5. You can also check the certificate information

Ownership tab

6. You can also check the certificate ownership information

7. Renew. You will obtain a strictly identical certificate to the one used for renewal, except for the key.

2.9. How to request a certificate recovery

1. Log in to Horizon Registration Authority Interface

2. Access request recover from the drawer: **My certificates** or **Search certificates**

3. Click on request recover button 

Recover Options tab

4. Fill in the information you want to add.

- **Contact_Email** *(string email format)*:
  Used if an email configuration is set. An email can be sent every time the request status change (see request lifecycle).
- **Recover comment** *(string inpuy)*:
  This comment appears:
  - to the approver when your request is in the pending status.
  - in the certificate info after the enrollment.

Certificate tab

5. You can also check the certificate information

Ownership tab

6. You can also check the certificate ownership information

7. Once you have checked and added the information you wanted you can request the recover by clicking on the recover button

8. You will be able to see and copy the password and download the certificate PKCS#12

3. How to Request a SCEP challenge

This section details how you can get a SCEP Challenge.

1. Log in to Horizon Registration Authority Interface

2. Access Request a SCEP Challenge from the drawer:  **Request a SCEP Challenge**

CAUTION	You must have the permission to request a SCEP challenge on at least one SCEP profile.

3.1. Profile tab

1. Select the SCEP profile

2. Click on next button

3.2. Metadata tab

1. Fill in all the mandatory fields:

- Labels(string):
  The labels are used for permission, email and request search.
- Contact email address(string email format):
  Used if an email configuration is set. An email can be sent each time the request status changes (see request lifecycle).
- Requester comment(string):
  This comment appears:
  - to the approver when your request is in the pending status
  - in the certificate information after the enrollment

2. Click on next button

3.3. Summary

If you own the enrolling permission on the SCEP profile:

1. Click on the Retrieve challenge button

If you own the request permission on the SCEP profile:

1. Click on request button

CAUTION	You have to wait that your request is approved by an operator and its status is 'completed', in order to use your SCEP challenge

2. click on View Request 

You now have access to your SCEP challenge

NOTE

In order to enroll using SCEP you will need at least a challenge and the SCEP endpoint:

- https://<horizon_url>/scep/<profile>/pkiclient.exe

In case you use the NDES emulation, the enrollment and challenge URLs will be respectively: - https://<horizon_url>/certsrv/<profile>/mscep - https://<horizon_url>/certsrv/<profile>/mscep_admin

TIP

You can cancel your request at any time, as long as the request status is pending, by clicking on 

4. How to Request an EST challenge

This section details how you can get an EST Challenge.

1. Log in to Horizon Registration Authority Interface

2. Access Request an EST Challenge from the drawer:  **Request an EST Challenge**

CAUTION	You must have the permission to request an EST challenge on at least one EST profile.

4.1. Profile tab

1. Select the EST profile.

2. Click on next button.

4.2. Metadata tab

1. Fill in all the mandatory fields:

- Labels(string):
  The labels are used for permission, email and request search.
- Contact email address(string email format):
  Used if an email notification is set. An email can be sent each time the request status changes (see request lifecycle).
- Requester comment(string):
  This comment appears:
  - to the approver when your request is in the pending status
  - in the certificate information after the enrollment

2. Click on next button

4.3. Summary

If you own the enrolling permission on the EST profile:

1. Click on the Retrieve challenge button

If you own the "request" permission on the EST profile:

1. Click on request button

CAUTION	You have to wait that your request is approved by an operator and its status is 'completed', in order to use your EST challenge

2. click on View Request 

You now have access to your EST challenge

TIP	You can cancel your request at any time, as long as the request status is pending, by clicking on 

4.4. How to enroll using EST

This section details how to enroll using the Horizon Client (`horizon-cli`). It is also possible to use another EST client implementation, as long as it complies with RFC 7030.

4.4.1. Prerequisites

You need the `horizon-cli` tools

4.4.2. Enroll with Horizon Client

1. Set the horizon root endpoint

```
export ``ENDPOINT``=https://<horizon_url>
```

NOTE	The `endpoint` can instead be set in `horizon-cli` configuration file

2. Enroll with `horizon-cli`

```
horizon-cli est --enroll <your_challenge> --profile <est_profile> --key
<link_to_the_privatekey> --cn <certificate_cn> --cert <name_of_the_output_certificate>
```

CAUTION	If the enrollment succeeds, the challenge is no longer usable, as it is a one-time password.

5. Operator

An Operator is someone who owns the permission to approve or deny a request.

5.1. Manage Request

This section details how to manage a request (view, approve, deny).

1. Log in to Horizon Registration Authority Interface

2. Access Manages requests from the drawer: **Manage requests**

5.1.1. How to view a request

3. Click on view request button

4. Check all the information from the request

5. At the end you can either approve or deny the request

5.1.2. How to approve a request

3. Click on approve request button and approve the request

CAUTION	If the certificate has mandatory metadata you will need to fill it in before approving the request, otherwise you will get an error.

5.1.3. How to deny a request

3. Click on deny request button and deny the request

5.2. Search Request

Here is the section where you can search easily find all information regarding the request.

5.2.1. How to do a simple request search

1. Log in to Horizon Registration Authority Interface

2. Access request search from the drawer: **My request** or **Request dashboard**

3. Fill in the information you want to look at:

- **Search in request DNs** *(string input)*:
  Enter the Certificate DNs you are looking for in a request
- **Search in IDs** *(string input)*:
  Enter the IDs you are looking for in a request
- **Search in Requester** *(string input)*:
  Enter the Requester you are looking for in a request
- **Search in Protocols** *(string input)*:
  Select the Protocols you are looking for in a request
- **Include status** *(string select multiple)*:
  Select the status you are looking for in a request
- **Include workflow** *(string select)*:
  Select if the workflow you are looking in a request
- **Include expired requests** *(string select)*:
  Select if the request you are looking is expired

4. Click on the filter button

You can reset the search by clicking on reset button

5.3. Search Certificate

Here is the section where you can search easily find all information regarding the certificate.

5.3.1. How to do a simple certificate search

1. Log in to Horizon Registration Authority Interface

2. Access certificate search from the drawer: **My certificates** or **Search certificates** or **Certificates dashboard**

3. Fill in the information you want to look at:

- **Search in DNs** *(string input)*:
  Enter the DNs you are looking for in a certificate
- **Search in SANs** *(string input)*:
  Enter the SANs you are looking for in a certificate
- **Search in serials** *(string input)*:
  Enter the serials you are looking for in a certificate
- **Search in issuer DNs** *(string input)*:
  Enter the issuer DNs you are looking for in a certificate
- **Expiration date start** *(string input)*:
  Enter the expiration date start you are looking for in a certificate
- **Expiration end start** *(string input)*:
  Enter the expiration end start you are looking for in a certificate
- **Search in profiles** *(string input)*:
  Enter the profile you are looking for in a certificate
- **Search in modules** *(string select multiple)*:
  Select the module you are looking for in a certificate
- **Search in Discovery campaigns** *(string input)*:
  Enter the discovery campaigns you are looking for in a certificate
- **Include status** *(string select multiple)*:
  Select the status you are looking for in a certificate
- **Include signed** *(string select)*:
  Select if the certificate you are looking is Self-Signed or Not Self-Signed or all
- **Include discovery** *(string select)*:
  Select if the certificate you are looking is Discovered trusted or Discovered not trusted

4. Click on the search button

You can reset the search by clicking on reset button or try the expert mode by clicking on expert mode button

5.3.2. How to do an expert certificate search

1. Log in to Horizon Registration Authority Interface

2. Access certification search from the drawer: **My certificates** or **Search certificate** or **Certificate dashboard**

3. Enter your research line.

To do so you will need to click on the input field. A list appears and you will be able to choose between all selector, then condition, then field, and you can add an operator to refine the search.

- **Element*** *(string input)*:
  Enter the element you are looking for in a certificate
- **Condition*** *(string input)*:
  Enter the condition you are looking for in a certificate for this element
- **Field*** *(string input)*:
  Enter the name of the element
- **Operation*** *(string input)*:
  Choose an operator if you want to refine your search

Certificate Search Structure

- <element> <condition> <"name"> (<operator> [<element> <condition> <"name">])

Table 2. Table element

Name	Type	Description
`dn`	*string*	Distinguished name
`san`	*string*	Subject Alternative name
`serial`	*string*	Certificate serial number
`issuer`	*string*	Issuer distinguished name
`status`	*string*	Certificate status
`module`	*string*	Certificate module
`profile`	*string*	Certificate profile
`valid.until`	*date*	Certificate 'not after' date
`valid.from`	*date*	Certificate 'not before' date
`keytype`	*string*	Certificate key type
`signingalgorithm`	*string*	Certificate signing algorithm
`owner`	*string*	Certificate owner
`holderid`	*string*	Certificate holder ID
`metadata.contact_email`	*string*	Contact email
`metadata.pki_connector`	*string*	PKI Connector

Name	Type	Description
`label.`	*string*	Label
`discoveryinfo.campaign`	*string*	Discovery campaign
`discoverydata.ip`	*string*	Discovery IP
`discoverydata.hostnames`	*string*	Discovery Hostnames
`discoverydata.tls.port`	*int*	Discovery TLS port
`discoverydata.tls.version`	*string*	Discovery TLS version
`discoverydata.operatingsystems`	*string*	Discovery TLS version
`discoverydata.sources`	*string*	Discovery TLS version
`thirdparty.id`	*string*	Third-Party ID
`thirdparty.connector`	*string*	Third-Party connector
`thirdparty.fingerprint`	*string*	Third-Party fingerprint

Table 3. Table condition combination

Name	Description
contains	Field contains the specified value (case insensitive)
not contains	Criteria does not contain
equals	Criteria exactly equals to
not equals	Criteria exactly not equals
in	Criteria exactly in the following array
not in	Criteria exactly not in the following array
within	Criteria contain in the following array
not within	Criteria contain not in the following array

Table 4. Table operation combination

Name	Description
and	Evaluate a AND logical operation on two criteria or set of criteria
or	Evaluate a OR logical operation on two criteria or set of criteria

Name	Contains	Not contains	Equals	Not equals	In	Not in	Within	Not within
dn	✓	✓	✓	✓	✓	✓	✓	✓
san	✓	✓	✓	✓	✓	✓	✓	✓
serial	✓	✓	✓	✓	✓	✓	✓	✓
issuer	✓	✓	✓	✓	✓	✓	✓	✓
status	✓	✓	✓	✓	✓	✓	✓	✓
module	✓	✓	✓	✓	✓	✓	✓	✓
profile	✓	✓	✓	✓	✓	✓	✓	✓
valid.until	✗	✗	✓	✗	✗	✗	✗	✗
valid.from	✗	✗	✓	✗	✗	✗	✗	✗
keytype	✓	✓	✓	✓	✓	✓	✓	✓
signingalgorithm	✓	✓	✓	✓	✓	✓	✓	✓
owner	✓	✓	✓	✓	✓	✓	✓	✓
holderid	✓	✓	✓	✓	✓	✓	✓	✓
metadata.contact_email	✓	✓	✓	✓	✓	✓	✓	✓
metadata.pki_connector	✓	✓	✓	✓	✓	✓	✓	✓
label.	✓	✓	✓	✓	✓	✓	✓	✓
discoveryinfo.campaign	✓	✓	✓	✓	✓	✓	✓	✓
discoverydata.ip	✓	✓	✓	✓	✓	✓	✓	✓
discoverydata.hostnames	✓	✓	✓	✓	✓	✓	✓	✓
discoverydata.tls.port	✗	✗	✓	✓	✓	✓	✗	✗
discoverydata.tls.version	✓	✓	✓	✓	✓	✓	✓	✓
discoverydata.operatingsystems	✓	✓	✓	✓	✓	✓	✓	✓

Name	Contains	Not contains	Equals	Not equals	In	Not in	Within	Not within
discoverydata.sources	✓	✓	✓	✓	✓	✓	✓	✓
thirdparty.id	✓	✓	✓	✓	✓	✓	✓	✓
thirdparty.connector	✓	✓	✓	✓	✓	✓	✓	✓
thirdparty.fingerprint	✓	✓	✓	✓	✓	✓	✓	✓

Name (part 2)	Is	Before	After	Exists
dn	✗	✗	✗	✗
san	✗	✗	✗	✗
serial	✗	✗	✗	✗
issuer	✗	✗	✗	✗
status	✗	✗	✗	✗
module	✗	✗	✗	✗
profile	✗	✗	✗	✗
valid.until	✗	✓	✓	✗
valid.from	✗	✓	✓	✗
keytype	✗	✗	✗	✗
signingalgorithm	✗	✗	✗	✗
owner	✗	✗	✗	✗
holderid	✗	✗	✗	✗
metadata.contact_email	✗	✗	✗	✓
metadata.pki_connector	✗	✗	✗	✓
label.	✗	✗	✗	✓

discoveryinfo.campaign	⊗	⊗	⊗	⊗
discoverydata.ip	⊗	⊗	⊗	⊗
discoverydata.hostnames	⊗	⊗	⊗	⊗
discoverydata.tls.port	⊗	⊗	⊗	⊗
discoverydata.tls.version	⊗	⊗	⊗	⊗
discoverydata.operatingsystems	⊗	⊗	⊗	⊗
discoverydata.sources	⊗	⊗	⊗	⊗
thirdparty.id	⊗	⊗	⊗	⊗
thirdparty.connector	⊗	⊗	⊗	⊗
thirdparty.fingerprint	⊗	⊗	⊗	⊗

4. Click on the search button