

Modules - Certificates: Basics

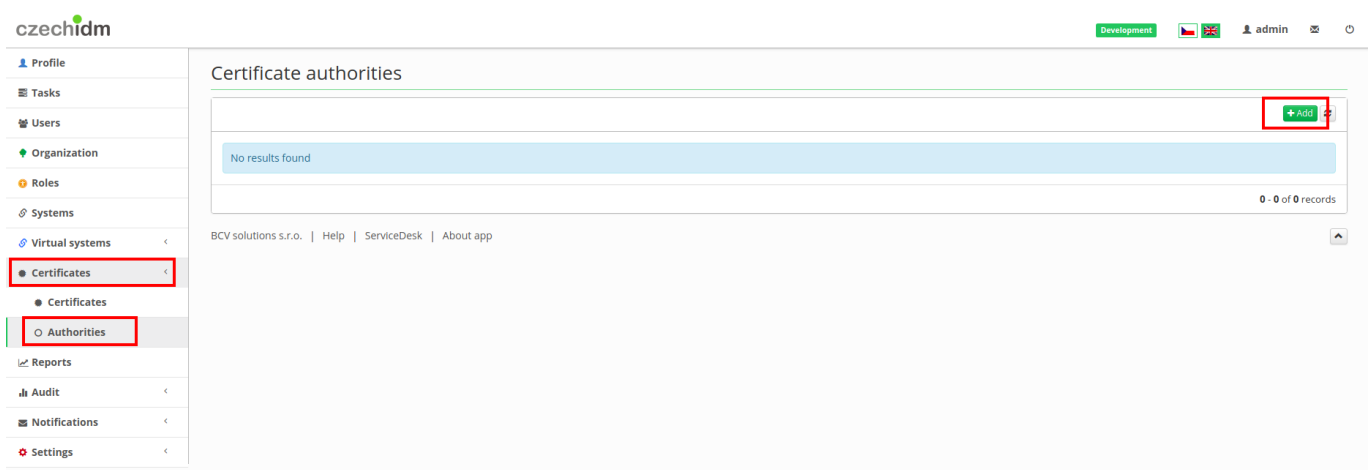
Certificate authority (crt) module was designed to handle various certificate authority implementations via specific drivers. Currently, there is one driver implemented - the CAW driver that handles the communication with CAW certificate authority (bundled in the module).

What do you need before you start

- You need to install **CzechIdM 7.7.0** (and higher).
- Modules imported via remote console through WinSCP (Windows) or SCP (Linux) into **/data/volumes/czechidm/modules/** :
 - idm-crt-api 3.x.x
 - idm-crt-impl 3.x.x
 - axis-1.x
 - jaxrpc-api-1.x
 - wsdl4j-1.6.x
- You need to be logged in as **admin**.
- You need to enable **Certificate** module.
- You need to install the **CAW** .

How to create an authority on Linux

By clicking on the left menu on **Certificates** and then on **Authorities** is shown a table with certificate authorities. Click on **Add** button and a popup window is shown.



Here you fill:

- **Code** - Label of certification authority
- **Driver** - We are using caw-driver. (There is only caw driver implemented for now.)
- **Path to the CAW distribution** and **Path to the certificate for that authority** - There is needed a path to CAW distribution and certificate for our new authority.
- **OU** - Fill organization unit, it is part of the certificate, it could be a specification of location or department.
- **Enable approving by workflow process** - It is an option if generating of certificates has to be

approved or not.

- **Approver roles** - Specified roles for approving generation of certificates. Users with these roles get tasks to be approved or not.

Then you click on **Save and continue** button and continue this tutorial with generating **certificate in GUI** or with **CSR file**.

Certificate authority detail

Code

Testing authority

Password policy for validation

validCrt

Password policy for generating

generateCrt

Driver

caw-driver

Identifier

test

Identifier of CA.

Supported certificate types (multi)

AUTHENTICATION

This CA supported this certificates types. Values have to be items from 'CertificateType' enumeration (AUTHENTICATION, SIGNING, ENCRYPTION)

Path to the CAW distribution

/home/john/java/caw2/caw

Path where is installed CAW distribution.

Path to the certificate for that authority

/home/john/java/caw2/ca/ca.crt

Country

CZ

Abbreviation for the country

Locality

Prague

ORG

BCV

Organization

OU

ExampleCA

Organization unit

State

Czech Republic

☒ Include certificate chain

☐ Enable approving by workflow process

Key of approving workflow process

crt-approve-request

Approver roles

Select or type to search ...

Every requests (generate, revoke, renew) for this CA have to be approve by approvers (with that roles).


☐ Inactive

Disabled authority cannot be used for generating new certificates.

Back

Save and continue

How to create an authority on Windows



On Windows, using diacritics in certificate/CSR DN's is currently not supported due to bug [#8317](#) in OpenSSL. This affects CRT module with CAW Windows driver. IdM



handles this by stripping diacritics from certain strings before passing them to the CAW. On Linux, diacritics works fine.

The process of creating an authority on Windows is similar to the one on Linux but you need to have [Git Bash](#) installed. When creating the authority on Windows, we select the win-caw-driver. Then we just need to fill out one extra field:

- **Path to Git Bash** - This path leads to the bash.exe file in git\bin.

An example of how we can configure the authority can be seen below:

Certificate authority detail

Code

test5

Password policy for validation

Password policy for validation

Password policy for generating

Password policy for generating

Driver

win-caw-driver

Identifier

test5

Identifier of CA.

Supported certificate types (multi)

AUTHENTICATION

This CA supported this certificates types. Values have to be Items from 'CertificateType' enumeration (AUTHENTICATION, SIGNING, ENCRYPTION)

Path to the CAW distribution

C:\caw\caw

Path to where the CAW distribution is installed, e. g., "/c/caw/caw"

Path to Git Bash

C:\Program Files\Git\bin\bash.exe

Path to the bash.exe file, e. g., "C:\Program Files\Git\bin\bash.exe"

Path to the certificate for that authority

C:\caw\ca\ca.crt

Path to the crt file, e. g., "C:\caw\ca\ca.crt"

Country

CZ

Abbreviation for the country

Locality

Prague

ORG

BCV

Organization

OU

Example1

Organization unit

State

Czech Republic

☒ Include certificate chain

☐ Enable approving by workflow process

Key of approving workflow process

Approver roles

Select or type to search ...

Every requests (generate, revoke, renew) for this CA have to be approve by approvers (with that roles).

☐ Inactive

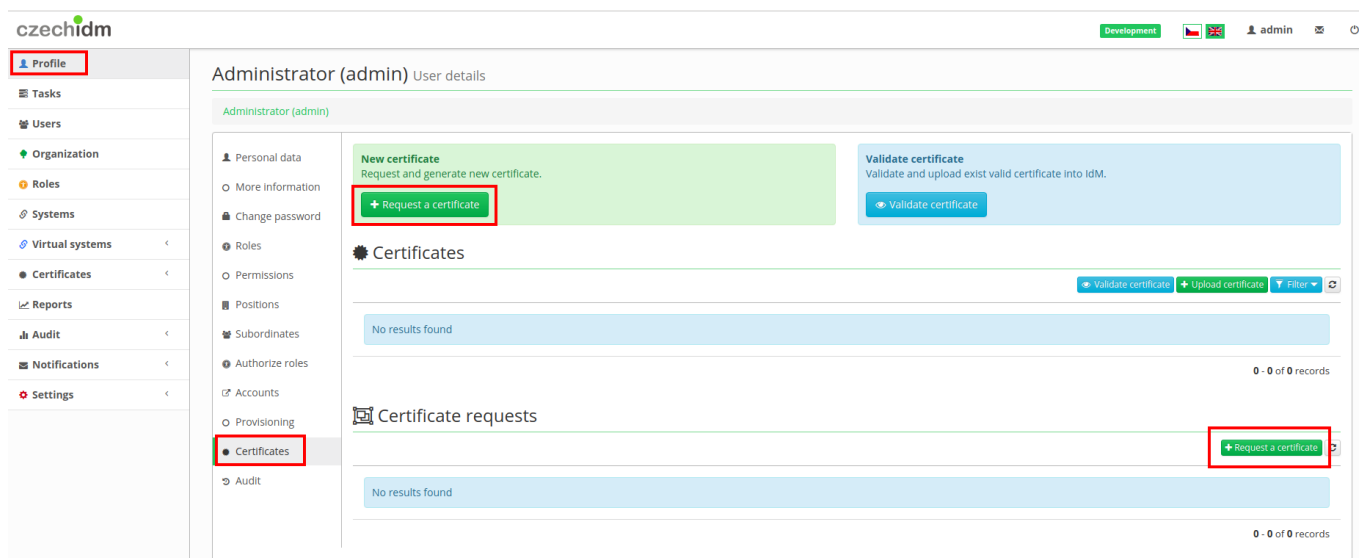
Disabled authority cannot be used for generating new certificates.

Back Save and continue

Other than the extra field Path to Git Bash, the process is the same as on Linux.

Generate certificate in GUI

In the left menu click on **Profile** and then on **Certificates**. There are 2 tables, in **Certificates** table are all certificates owned by the user and in the other table, there are requests of these certificates. Click on **Request certificate**.



Fill information in a popup window:

- **Certificate authority** - There can be more certificate authorities, so choose authority, which will issue the certificate.
- **Certificate type** - For which purpose certificate will be issued. **Signing** - for example signing some documents, **Authentication** - to grant access to a resource, network, application, etc. not based on a password, but rather on the certificate.
- **Generate certificate by** - It is a specification for whom certificate will be issued. Based on this information will be certificate generated.
- **Password** - Downloaded private key will be encrypted with this password. Because this is just tutorial we put a weak password, you should use more powerful one.

And click on **Submit a request** button.

New certificate request ×

Owner

Administrator (admin) ▼

Certificate authority

Main CA X ▼

Certificate authority for create (renew, revoke) certificate. Authority can support different certificate types.

Certificate type

Authentication ▼

Defines purpose of using the certificate.

Generate certificate by

Selected owner (identity) ▼

The certificate can be created by information stored in IdM on owner, or by a previously prepared CSR file.

Password

..... *

Re-enter password

..... *

Password will be used for creating certificate private key. Password will be needed after download, when key will be used.

Description

[Close](#)

[Save concept](#)

[Submit a request](#)

Now we have the valid certificate and we could download the certificate. **Certificate** button downloads public key and **Key** button downloads encrypted public and private key.

New certificate

Request and generate new certificate.

[+ Request a certificate](#)

Validate certificate

Validate and upload exist valid certificate into IdM.

[Validate certificate](#)

Certificates

										Validate certificate Upload certificate Filter ↺	
State	Type	Serial number	Subject	Publisher	Valid from	Valid till	Download	Archived	Actions	Id	
<input checked="" type="checkbox"/> Valid	Authentication	AAACCC0	Administrator	Main CA	07.02.2018 13:38:33	27.02.2020 13:38:33	Certificate Key	<input type="checkbox"/>	📄 🗑️	258ed8e	

1 - 1 of 1 records

Certificate requests

								+ Request a certificate ↺
State	Created	Type	Certificate type	Certificate	Certificate authority	Actions		Id
<input checked="" type="checkbox"/> Executed	07.02.2018 13:27:15	New certificate	Authentication	AAACCC0	Main CA			2a02ad2

1 - 1 of 1 records

For admin, there is another one important section in left menu **Certificates** and again in **Certificates**. This table shows all certificates. For version < 3.0.3 the key could be downloaded only by the owner of certificate, but from version 3.0.3, there is special permission for downloading key.



If the owner doesn't has this new permission, he won't be able to download it.

You need to set permission:

- CrtCertificate - DOWNLOADKEY
- CrtAuthority - DOWNLOADKEY

You can use BaseEvaluator so the user can download all keys. Or if you use for example UUID evaluator for CrtAuthority, then user will be able to download keys only for certificates from this specific authority.

Generate certificate by CSR

In the left menu click on **Profile** and then on **Certificates**. There are 2 tables, in **Certificates** table are all certificates owned by the user and in the other table, there are requests of certificates. Click on **Request certificate**.

Fill information in a popup window:

- **Certificate authority** - There can be more certificate authorities, so choose authority, which will issue the certificate.
- **Certificate type** - For which purpose certificate will be issued. **Signing** - for example signing some documents, **Authentication** - to grant access to a resource, network, application, etc. not based on a password, but rather on the certificate.
- **Generate certificate by** - Fill option **Selected CSR file** and drag CSR file to the marked field right below.

And then click on **Submit a request** button.

Certificate request detail

Owner

Administrator (admin)

Type

New certificate

Request for create, renew, revoke certificate.

Certificate authority

Main CA

Certificate authority for create (renew, revoke) certificate. Authority can support different certificate types.

Certificate type

Authentication

Defines purpose of using the certificate.

Náhled CSR souboru (www_tutorial_com.csr)

Attribute	Value
cn	www.tutorial.com
ou	IT
organization	BCV
locale	Prague
state	Czech Republic
country	CZ
fingerprint	5B:F0:09:8B:64:46:76:6A:3D:37:C2:06:A9:DF:71:E5:14:F5:B4:F8
signature_type	1.2.840.113549.1.1.11

State

Concept

Result

Created

Close

Submit a request

Now we have two certificates and as you can see in the picture below, the private part of certificate generated with CSR file cannot be downloaded. It is because CzechIdM does not have a private part. Users have it with CSR file, so if you lose it you will probably have to generate a new certificate.

Certificates

Validate certificate + Upload certificate Filter										
State	Type	Serial number	Subject	Publisher	Valid from	Valid till	Download	Archived	Actions	Id
<input checked="" type="checkbox"/> Valid	Authentication	AAACCC0	www.tutorial.cz	Main CA	08.02.2018 08:31:31	28.02.2020 08:31:31	Certificate	<input type="checkbox"/>	Renew Revoke	dd7f3c7
<input checked="" type="checkbox"/> Valid	Authentication	AAACCC0	Administrator	Main CA	07.02.2018 13:38:33	27.02.2020 13:38:33	Certificate Key	<input type="checkbox"/>	Renew Revoke	258ed8e

1 - 2 of 2 records

Upload certificate

Certificate generated by third-party authority can be uploaded to CzechIdM (or synchronized from target system). In the left menu **Profile** and then in **Certificates** menu, you can upload certificate by clicking on an **Upload certificate** button.

The screenshot shows the CzechIdM Administrator interface. On the left, the 'Profile' menu item is highlighted. The main content area shows the 'Administrator (admin)' user details. Under the 'Certificates' section, there is a table of certificates. The 'Upload certificate' button is highlighted with a red box.

And then just drag certificate file to marked box in a popup window.

If we want to allow a user to upload a certificate, we set authorization policies as follows:

- Permission to read, create and download one's own identity certificates: Certificates (CrtCertificate) | Read, Create | SelfCertificateEvaluator

Renew and revoke certificate

For users:

It is on the same page as generating a certificate. By clicking on **Profile** in the left menu and then on **Certificates**. And as you can see in the picture below, in column **Action** there are two buttons. Green one is for **renew** a certificate, it prolongs the validity of a certificate. The red one revokes a certificate (e.g. certificate was compromised), the certificate will stay in certificates section, but it will not be valid.

Administrator (admin) User details

Administrator (admin) User details

New certificate
Request and generate new certificate.
[+ Request a certificate](#)

Validate certificate
Validate and upload exist valid certificate into IDM.
[Validate certificate](#)

Certificates

[Validate certificate](#) [+ Upload certificate](#) [Filter](#)

State	Type	Serial number	Subject	Publisher	Valid from	Valid till	Download	Archived	Actions	Id
Valid	Authentication	AAACCC0	Administrator	Main CA	07.02.2018 13:38:33	27.02.2020 13:38:33	Certificate Key	<input type="checkbox"/>	Renew Revoke	258ed8e

1 - 1 of 1 records

Certificate requests

[+ Request a certificate](#)

State	Created	Type	Certificate type	Certificate	Certificate authority	Actions	Id
Executed	07.02.2018 13:27:15	New certificate	Authentication	AAACCC0	Main CA		2a02ad2

1 - 1 of 1 records

For admin:

There is agenda in left menu **Certificates** → **Certificates** (picture below), where are all certificates and admin can revoke or renew certificates even of other user's.

czechidm

Development admin

Certificates

[Validate certificate](#) [+ Upload certificate](#) [Filter](#)

Serial number: Owner:

State: Type: Certificate authority: Archived: No

[Cancel filter](#) [Filter](#)

State	Type	Serial number	Owner	Subject	Publisher	Valid from	Valid till	Download	Archived	Actions	Id
Valid	Authentication	AAACCC0	Administrator (admin)	www.tutorial.cz	Main CA	08.02.2018 08:31:31	28.02.2020 08:31:31	Certificate	<input type="checkbox"/>	Renew Revoke	dd7f3c7
Revoked	Signing	AAACCC0	Jack Approver (crtapp)	Jack Approver	Main CA	07.02.2018 13:45:32	27.02.2020 13:45:32	Certificate	<input type="checkbox"/>		ac28ac3
Valid	Authentication	AAACCC0	Administrator (admin)	Administrator	Main CA	07.02.2018 13:38:33	27.02.2020 13:38:33	Certificate Key	<input type="checkbox"/>	Renew Revoke	258ed8e

1 - 3 of 3 records

BCV solutions s.r.o. | [Help](#) | [ServiceDesk](#) | [About app](#)



When a certificate expires, it no longer can be renewed. But in **Settings** and in **Task scheduler** process can be created, which sends a notification with a warning, when certificates will expire in few days. Or you can find help in [warning notification](#) tutorial.



To allow using this agenda, users have to have this permissions:

- CrtRequest - Read, Create, Update
- CrtCertificate - Read, Create
- CrtAuthority - autocomplete, SETTOCRTREQUEST
- IdmIdentity - SETTOCRTREQUEST

You can create new role, [add this permissions to the role](#) and assign this role to users.

Congratulations, if you are reading this, you successfully completed this tutorial.

Permissions

For CRT exists two special permissions for validating and requesting certificate by CSR request:

- Validate CRS request,
- Upload CSR request.

These permission must be set to user before they want upload or validate CSR request. Basic requesting via frontend form works with permission create/update.

Configuration

Configuration option that allow create password as another user. For example: admin requesting new certificate for user.

```
# If value is true admin can set new password, this password will be sent to
user in notification.
# If set to false admin will not able set password to request. The password
for certificate will be generated by password policy.
idm.pub.crt.configuration.passCreate.enabled=true
#
# Default status for all identity certificates that will be revoked after
identity will be disabled.
idm.sec.crt.configuration.identityDisabledRevocationReason=UNSPECIFIED
#
# Default status for all identity certificates that will be revoked after
identity will be deleted.
idm.sec.crt.configuration.identityDeletedRevocationReason=UNSPECIFIED
```

There is a processor which start provisioning for user when a new certificate is created for them. This processor is disabled by default and can be enabled, find the "certificate-provisioning-processor".

Revocation status list

- UNSPECIFIED
- KEY_COMPROMISE
- CA_COMPROMISE
- AFFILIATION_CHANGED
- SUPERSEDED
- CESSATION_OF_OPERATION
- CERTIFICATE_HOLD

From:

<https://wiki.czechidm.com/> - **IdStory Identity Manager**

Permanent link:

https://wiki.czechidm.com/tutorial/adm/modules_crt

Last update: **2025/06/18 08:29**

