← .:modules_reports | ^ .:start | Documentation ^ .:modules_rec | →

Modules - Certificates [crt]

certificate

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).

On Windows, using diacritics in certificate/CSR DNs 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.

Operations with certificates

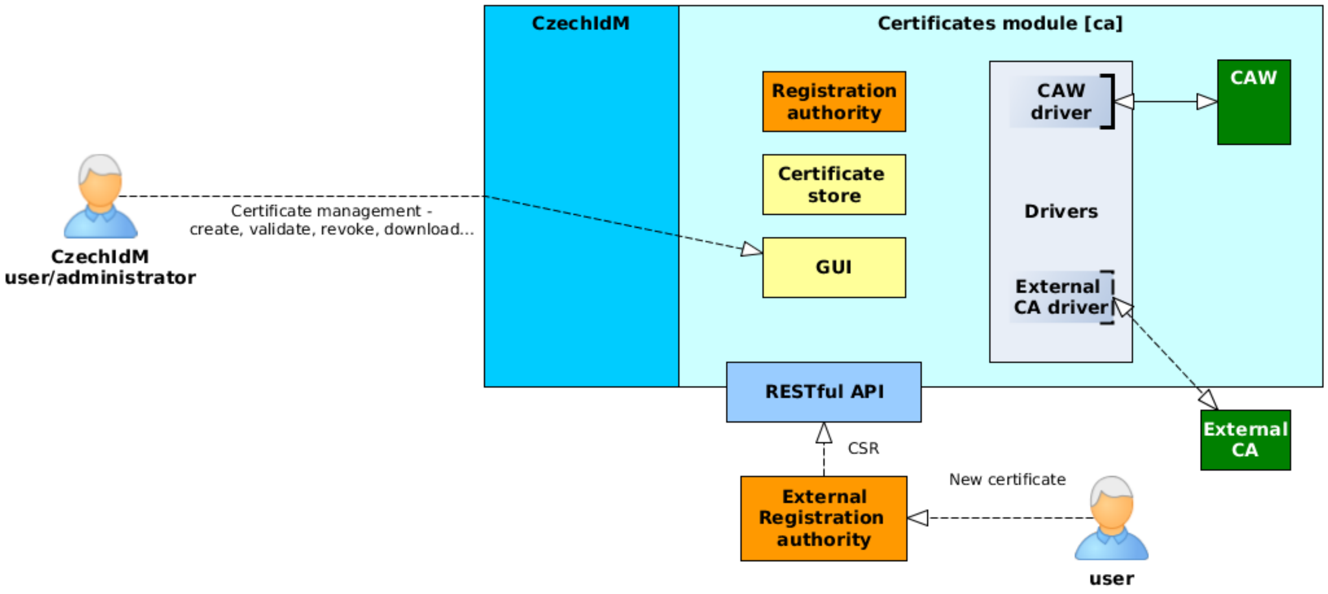
- **Generate** - Generate a new certificate. The user must select a certification authority, a certificate type (Authentication, Signing, Encryption), and a password. The password will be required to open a downloaded storage with a private key and a user certificate. The password will be stored in the confidential storage in IdM. If the certificate generation is complete, password will be removed from the IdM.
- **Generate by CSR** - Generate a certificate from an existing request (**Certificate Signing Request**). The user has a certificate request already generated in the CSR format. This request contains all the necessary information to generate. The user must only select authority and file with CSR request. In this case, it does not enter or store any password (the private part of the certificate already has the user with).
- **Renew** - Extending the validity of an existing certificate. Extensions can only be made on a valid certificate.
- **Revocate** - Certificate invalidation. For example, if the private part of the certificate is compromised, you must revoke the certificate to prevent further abuse.
- **Archive** - Certificate is archived ("soft delete"). Archived certificates cannot be renewed or revoked. They are still controlled for expiration (see long running tasks and notifications below).
- **Cancel request** - Certificate request can be canceled, when request is in concept state.
- **Download certificate** - Public certificate and private key (if exists) can be downloaded. Private key can be downloaded just by certificate owner.
- **Download secret** - Secret to any certificate can be downloaded by user with permissions CERTIFICATE_READ and CERTIFICATE_DOWNLODSECRET, it is meant to be used by external app signing documents on behalf of users

Architecture

Module consists of those basic parts:

- **GUI** - Users can manage their certificates or request a new one via standard CzechIdM web GUI

- **Registration authority** - When user requests for a certificate, the request is processed by appropriate driver.
- **Certificate store** - users' certificates are stored in CzechIdM for future download or e.g. provisioning (send to other managed system)
- **Drivers** - Driver implements mainly the communication mechanism between CzechIdM and CA (e.g. CAW or Microsoft CA). Currently CzechIdM provides the driver for CAW, others can be implemented on demand. If the request from registration authority does not contain CSR, driver creates it.
- **CAW** - Our CA implementation based on openssl.
- **RESTful API** - Standard communication API. Use it e.g. when users request for a new certificate via some external registration authority software.



Read more

[Info about versions]

Drivers

- The CAW driver
- The ADCS driver

Admin tutorials

- Modules - Certificates
- Modules - Approving certificate requests
- Modules - Scheduled tasks, notifications and automatic certificate renew, generating or revocation

Devel guide

- Certificate manager

Download secret

Secret to any certificate can be downloaded by user with permissions **CERTIFICATE_READ** and **CERTIFICATE_DOWNLOADSECRET**. Secret is encrypted by RSA **public key stored in** configuration item **idm.sec.crt.secret.pub**, length is arbitrary (2048 and more is recomended). Secret key is stored in external app and is used to decrypt secret. Key pair can be generated by these commands (you can change 2048 to 4096, 8192…)

```
openssl genrsa -out private.key 2048
openssl rsa -in private.key -outform PEM -pubout -out public.key
```

Public key to be stored in IdM configuration is in file public.key, save it without lines starting with —– and joined to one line (without spaces), private key to be used by external app for decrypting secret is in file private.key.

URL for secret download is **/api/v1/crt/certificates/{certificateId}/download-secret**, where certificateId is UUID of certificate in IdM, response is JSON with this structure:

```
{
  "certificate_id": "certificateId from URL",
  "secret": "Base64 encoded RSA encrypted certificate secret by public key
in idm.sec.crt.secret.pub"
}
```

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

Permanent link:
https://wiki.czechidm.com/devel/documentation/modules_crt

Last update: **2024/04/22 10:55**