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).

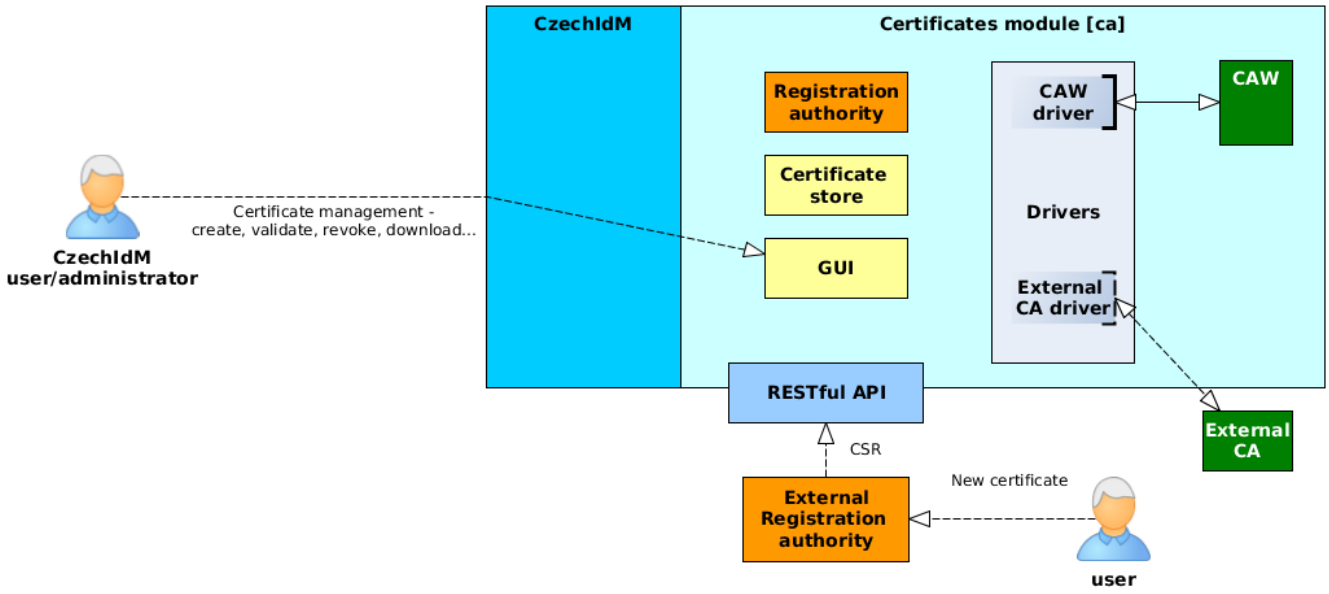
Operations with certificates

- **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.

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

Admin guide

- The CAW driver

Admin tutorials

- Modules - Certificates
- Modules - Approving certificate requests
- Modules - Scheduled tasks and notifications

Devel guide

- Certificate manager