Technical specifications

MONET+ Certificate Lifecycle Management

Manage the lifecycle of your organization’s digital certificates

Managing digital certificates is a demanding agenda for an organization, which It is mostly implemented by the manual activities of administrators.

Administrators of the organization manually manage their PKI infrastructure, record the results of their work (e.g. issuing certificates) in text or spreadsheet documents, and rely on the fact that in the future they will check the document in time and renew the certificate.

This approach not only leads to an inefficient use of employees’ time, but can even result in a critical outage of the part of the organization’s infrastructure that relies on on the use of digital certificates.

With MONET+ Certificate Lifecycle Management (CLM), the lifecycle of an organization’s technology certificates can be managed efficiently and securely. The CLM product family covers all **critical scenarios** (automated issuance of certificates using globally used protocols, checking of approved identification data)
in the certificate application, checking of supported cryptographic algorithms, etc.) as well as s**upporting processes** for certificate management (overviews of issued company certificates, notifications of issued certificates or certificates that are about to expire, automatic or manual revocation of certificates, etc.).

MONET+ Certificate Lifecycle Management **increases the stability and security of the organization** while saving human resources.

We place emphasis on:

- Delivery of a highly scalable system for managing the lifecycle of an organization’s certificates and their infrastructure
- Meeting the needs of smaller organizations as well as large companies that fall under the critical infrastructure of the state
- Automated and manual processes within the management of the organization’s PKI management
- Ensuring the security of the organization by enforcing the control of security compliance rules in the process of certificate management
- Ensuring the use of modern cryptographic algorithms in the certificate management process
- Disabling the issuance of a certificate to an unauthorized role or a certificate with unauthorized identification data of the requester

Centrally manage system settings

SYSTEM ROLE

- Global settings and management of system roles
- Assigning users/roles to predefined security profiles
- Ability to create your own security profiles
- The roles of the system are then tied to the scenarios of issuing certificates, so for each certificate it is possible to define who should be notified before its expiration (or when it is issued), who has the right to revoke the issued certificate, etc.

SECURITY FOR CERTIFICATE ISSUANCE

- Dynamic validation of the applicant’s supported identification data in the certificate application, including validation of supported algorithms and the length of the public key in the application
- Possibility to sign the certificate request with an authorization certificate before sending it to the CA (key support in HSM)
- Security settings can then be connected to any scenario - automated (ACME, EST, etc.), manual (Web Registration Authority)

BUILDING SCENARIOS FOR CERTIFICATE ISSUANCE

- A certificate issuance scenario in CLM is an entity that carries information about the sequence of actions that lead to the issuance of a certificate
- The scenario consists of components that define, for example, the address of the certification authority, the profile of the certification authority, the validation rules of the certificate request, etc.
- The CLM system allows you to dynamically build scenarios from pre-built components that can be reused in newly created scenarios
- Protocol interfaces (e.g. ACME, EST) are then connected to the resulting scenarios

The CLM system can be operated as:

- On-premise solution integrated into Active Directory domain using MS - IIS Web Server, MS SQL Server.
- On-premise solution running in containerized architecture (currently under development).
- Multitenant cloud solution, consumed as SaaS, with the possibility of integration with PKI organizations (planned in the next releases.

Interface for automated certificate lifecycle management

ACME

- implementation of a generic ACME server according to RFC 8555
- compatibility with the most frequently used ACME clients globally
- unique ACME External Account Binding concept - tailor-made for the concept of an internal ACME server for issuing certificates from an internal certification authority
- suitable for SSL certificates (Domain Validation certificates)

SCEP

- implementation of SCEP protocol according to RFC 8894
- suitable (not only) for certificates of network elements

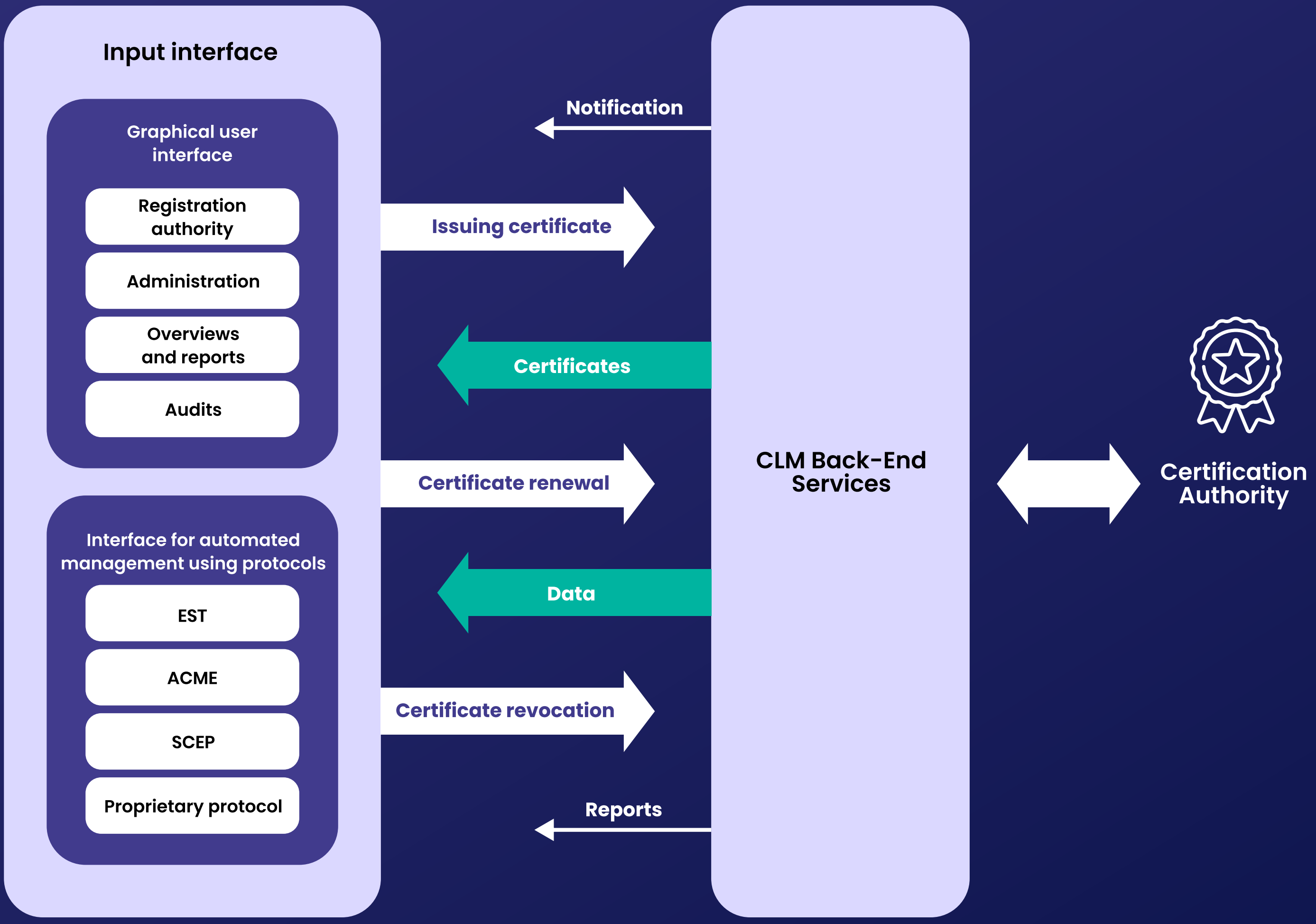
EST

- implementation of the EST protocol according to RFC 7030
- dynamic configuration of EST endpoint authorization rules (for authentication by client certificate or name/password)
- possibility to include the control of device serial numbers in the certificate request
- suitable (not only) for certificates of network elements

PROPRIETARY PROTOCOL

- With our development team, we are able to develop proprietary protocol support tailored to the customer's needs
- It can be used if the customer already uses devices or systems that have their own interface implemented on the PKI system

Solution architecture



User interface for manual issuance of certificates

WEB-BASED REGISTRATION AUTHORITY

- User interface for the possibility of servicing the issuance of a certificate according to a defined profile
- possibility of issuing a certificate according to a pre-created request, or with the possibility of generating keys and a request in the CLM system
- In a future release, RA will be able to be connected via ProID Web Bridge technology to the resources of the client's computer (e.g. smart card, operating system key/certificate store, HSM, etc.) - the key pair will be able to ignite directly in the client's HW resource

LICENSING

The MONET+ Certificate Lifecycle Management licensing model is based on licensing for a single functional module.

The function modules currently are:

Web-based Registration Authority | **ACME** | **SCEP** | **EST**

The license for a functional module includes an unlimited number of instances of the module.
This benefit can be used in the case of multiple customer environments, multiple domains, etc.

The Onboarding Certificate Lifecycle Management also includes a fixed license fee for the general functionalities of the system:

- Administrative functions of the system
- Certificate Overviews
- Notification function
- Revocation function

Selected

SKUPINA ČEZ

ČSSZ

KB

albert

eli

Are you interested in our solution?

Contact us.

info@proid.tech | **www.proid.tech**