MONET +

Životní cyklus klíčů a certifikátů

Jakub Kolařík

19. 11. 2025

Obsah

Digital Identity

solutions

Identity solutions

Workforce

Two-factor authentication, electronic signature and seal, secure employee identity and PKI systems for your organization.

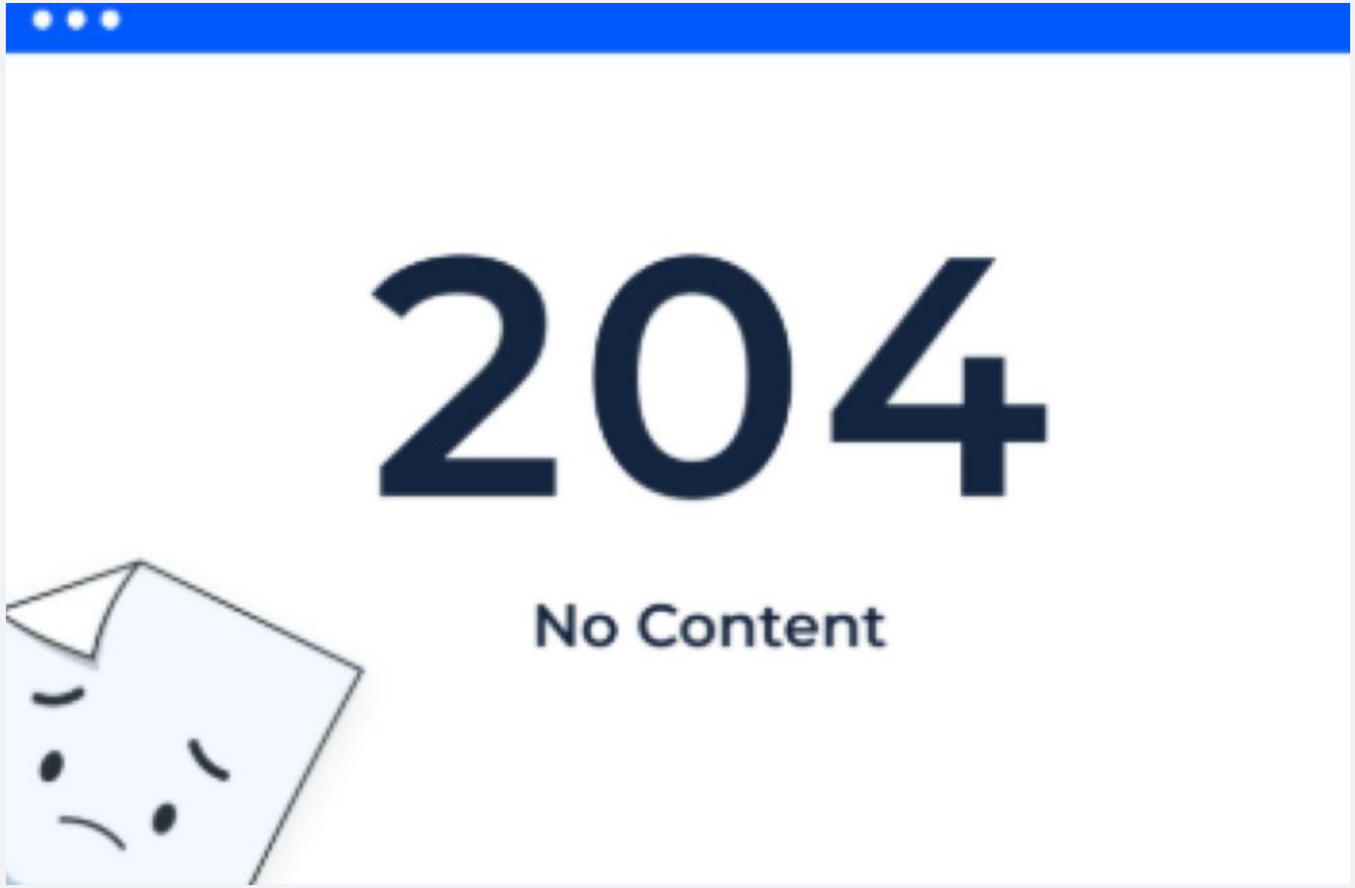
Customer

Solutions for strong customer authentication in your digital channels and applications.

Citizen

Electronic identification documents personalization systems, authentication and sensitive data security.

O tom to dnes nebude...




Digital Identity
Technical ID
MONET +

Certificate Lifecycle Management (CLM)
Key Management Server (KMIP protocol)

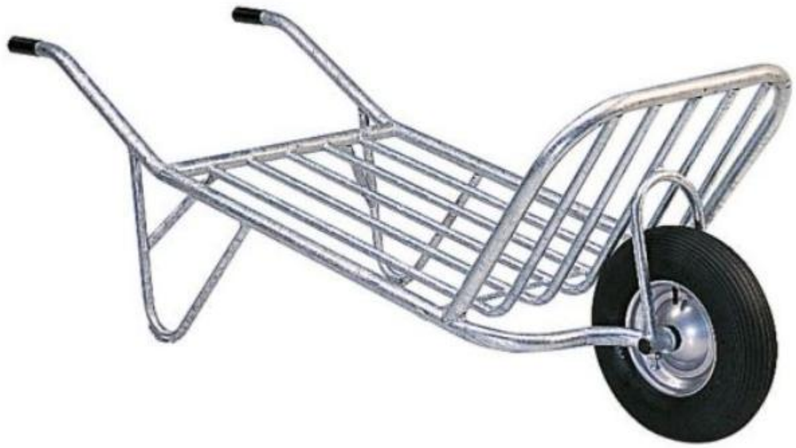
CLM

Certifikáty / PKI
Asymetrická kryptografie

KMS / KMIP

Symetrická kryptografie
Šifrování

Aktuální situace zákazníků

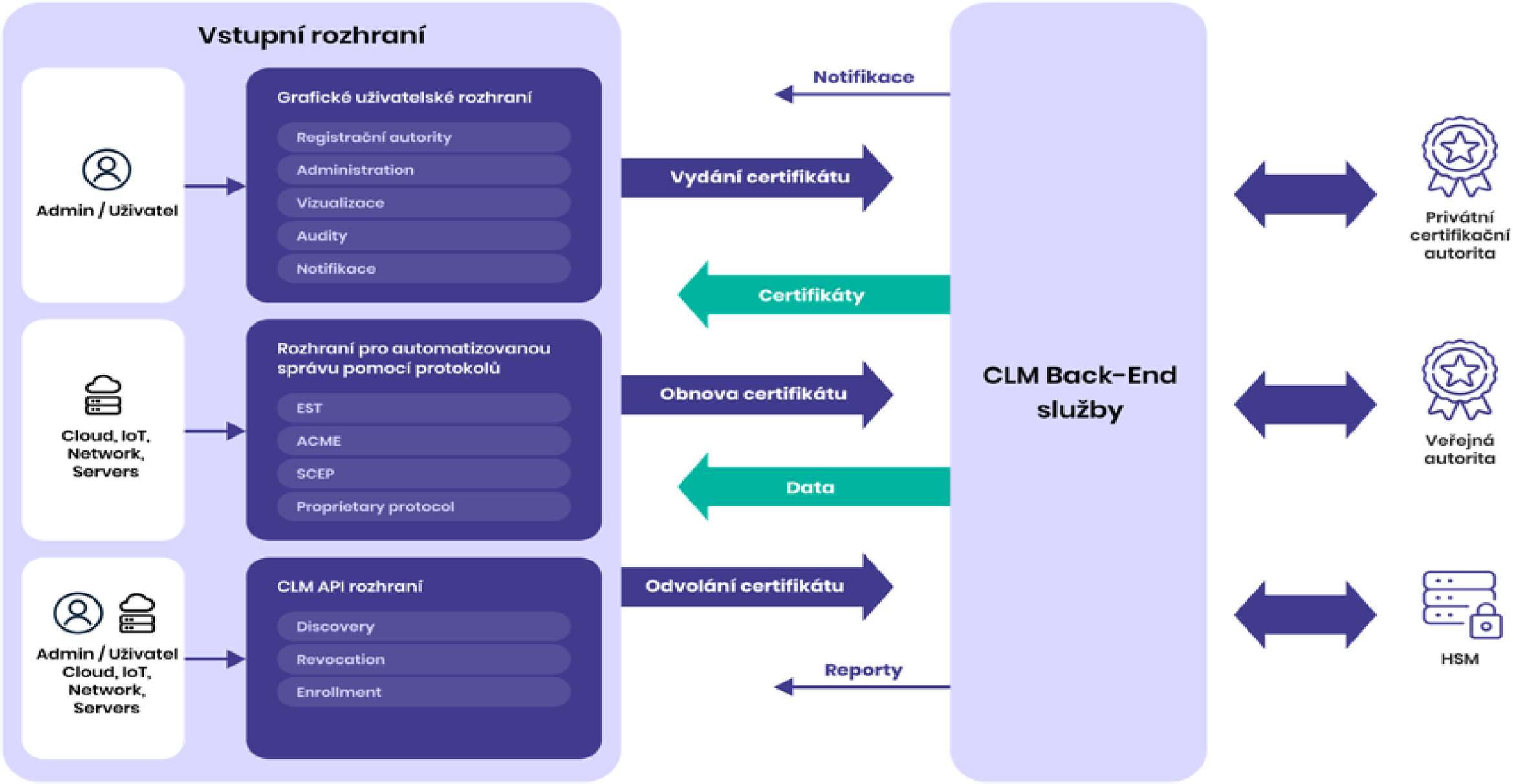


vs

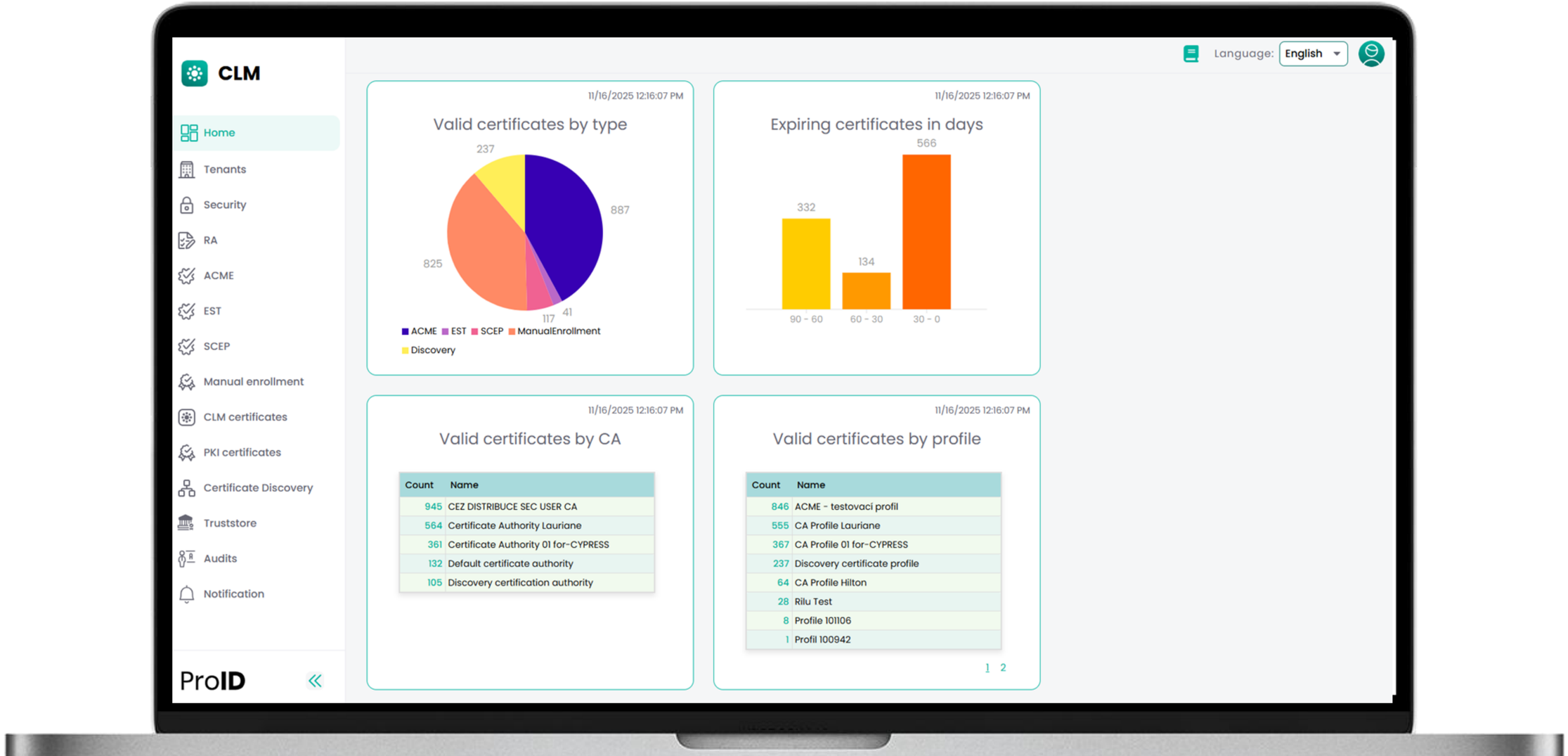
- Ruční evidence v excelových tabulkách
- Žádná automatizace
- Nepříliš velký důraz na bezpečnost - kdo může žádat o jaké certifikáty, resp. s jakými identifikačními daty žadatele

- Automatizace (i když často formou interního skriptování)
- Velký focus managementu na úsporu času v této oblasti
- Důraz managementu na kvalitu v této oblasti
- Systém compliance pravidel

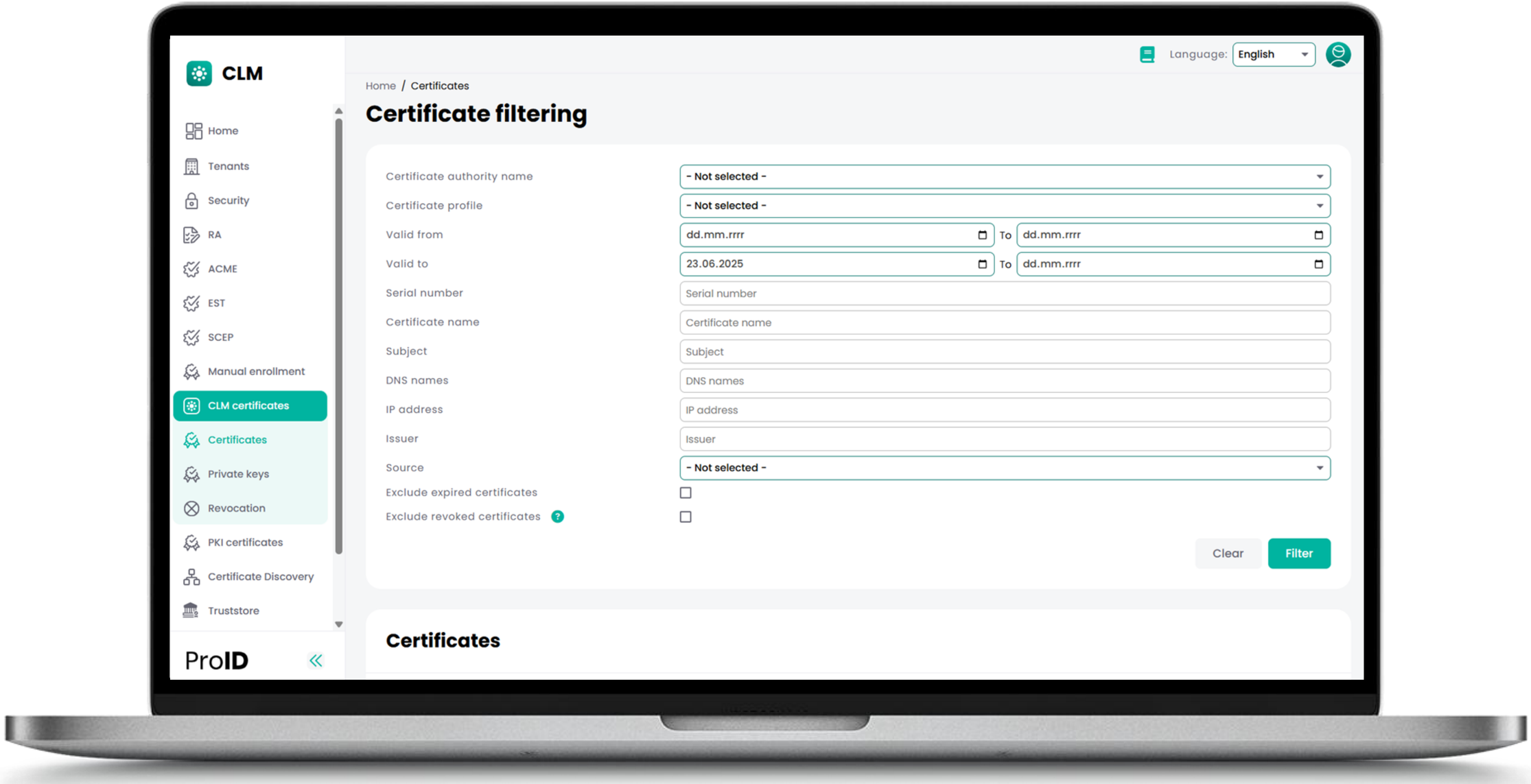
Certificate Lifecycle Management



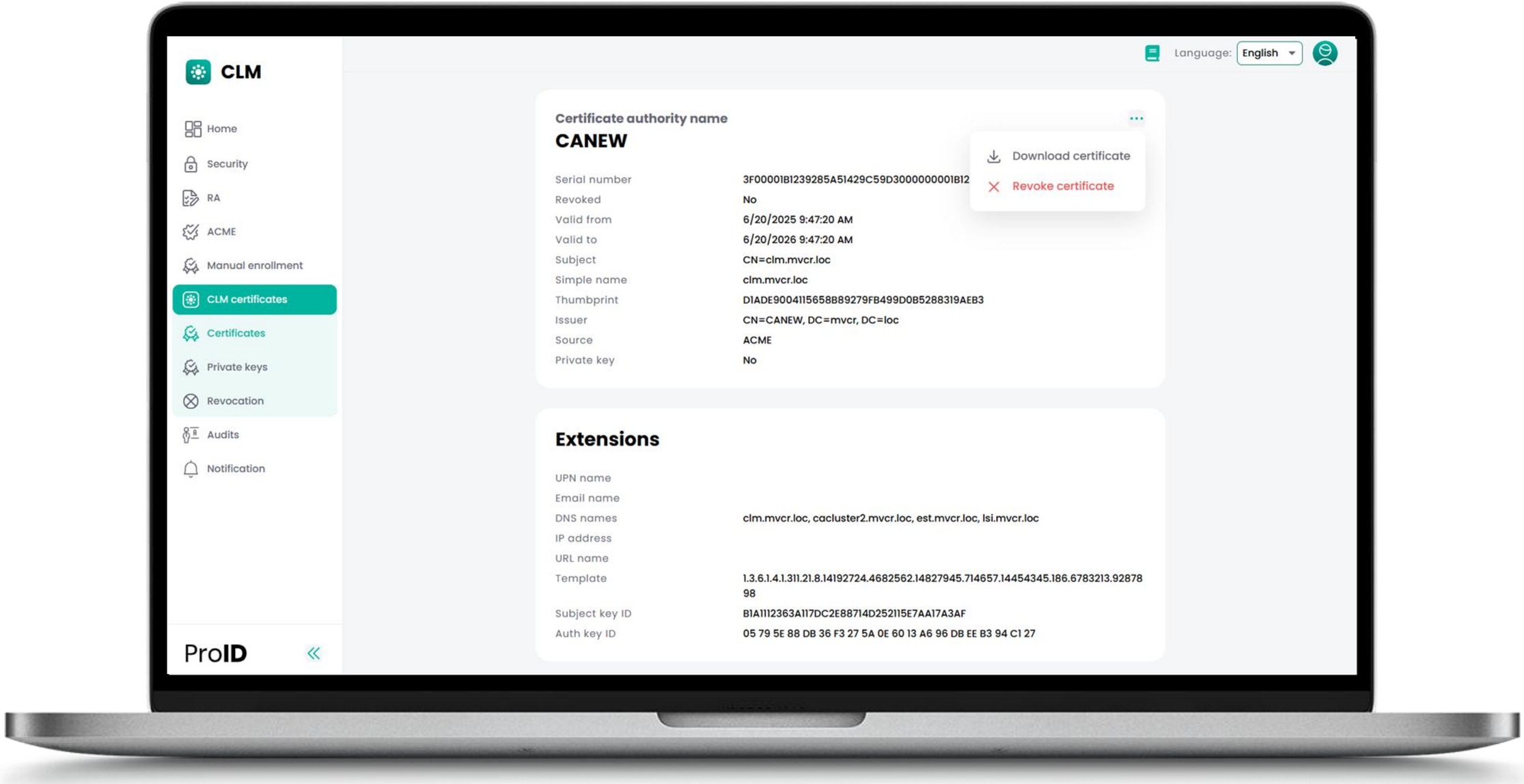
Visibility & Discovery



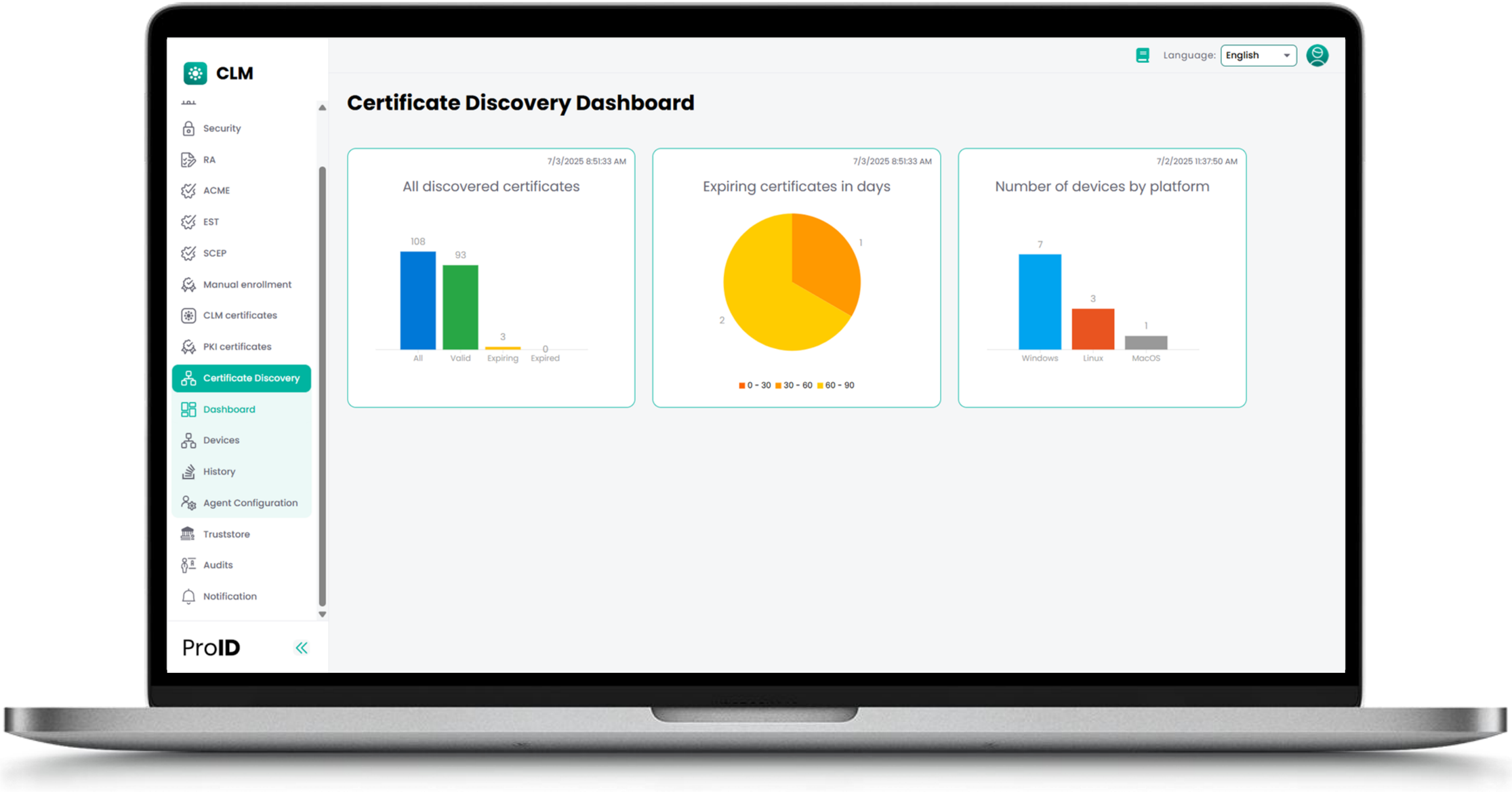
Visibility & Discovery



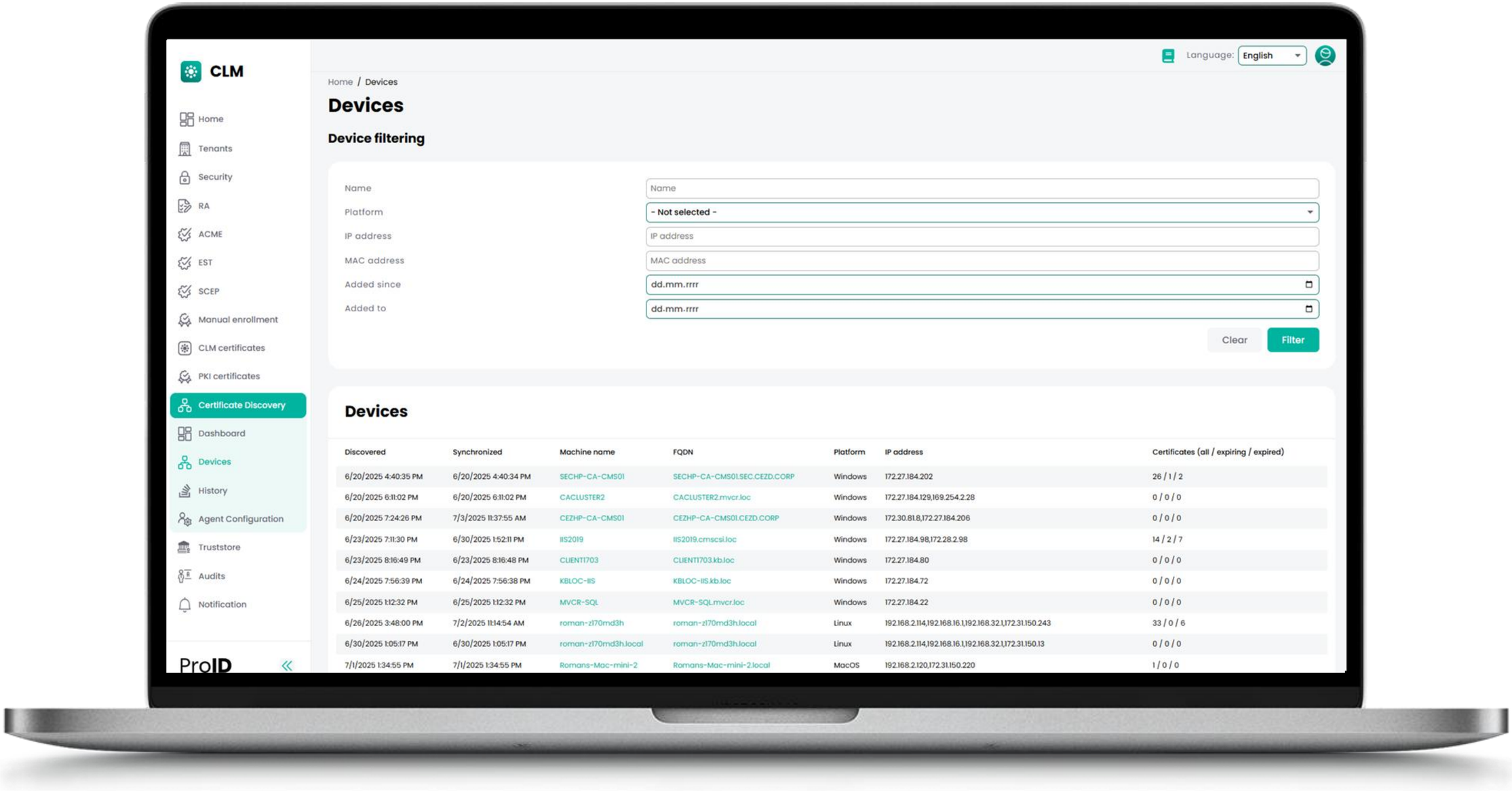
Visibility & Discovery



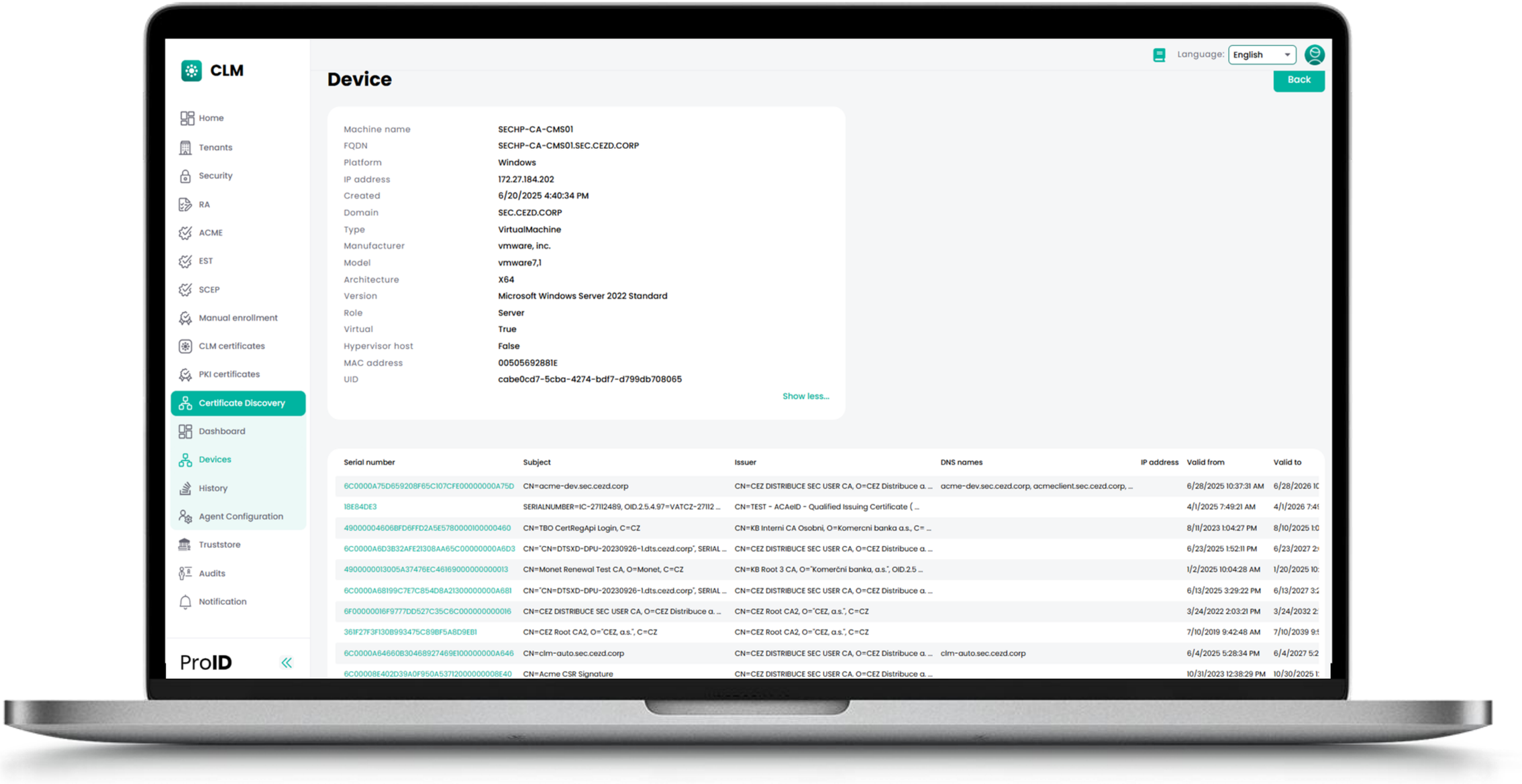
Discovery Across Environment



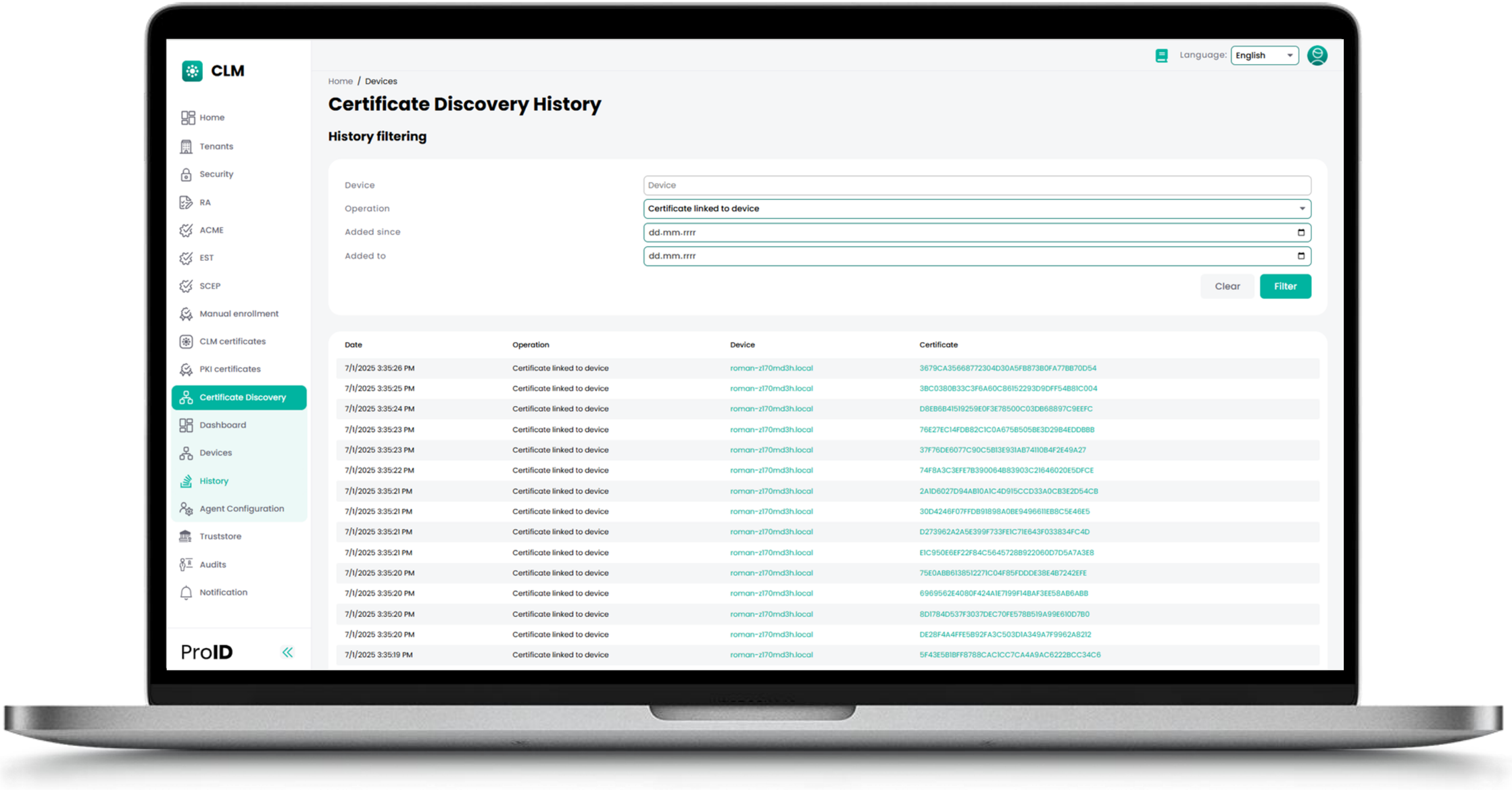
Discovery Across Environment



Discovery Across Environment



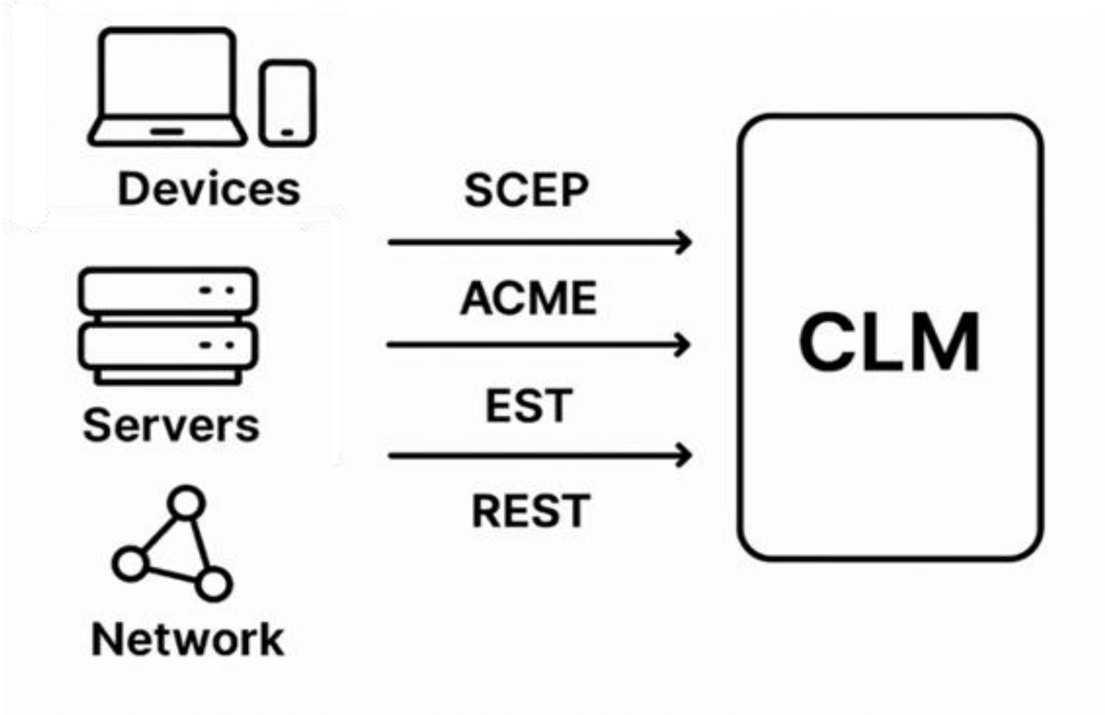
Discovery Across Environment



Full Lifecycle Automation

Support of standardized protocols:

- ACME (Automated Certificate Management Environment, RFC 8555
- SCEP (Simple Certificate Enrollment Protocol, RFC 8894
- EST (Enrollment over Secure Transport, RFC 7030



MONET+ ACME

Veřejné ACME CA:

- DNS / HTTP challenge, nebo:
- ACME External Account Binding + DNS / HTTP Challenge

MONET+ ACME:

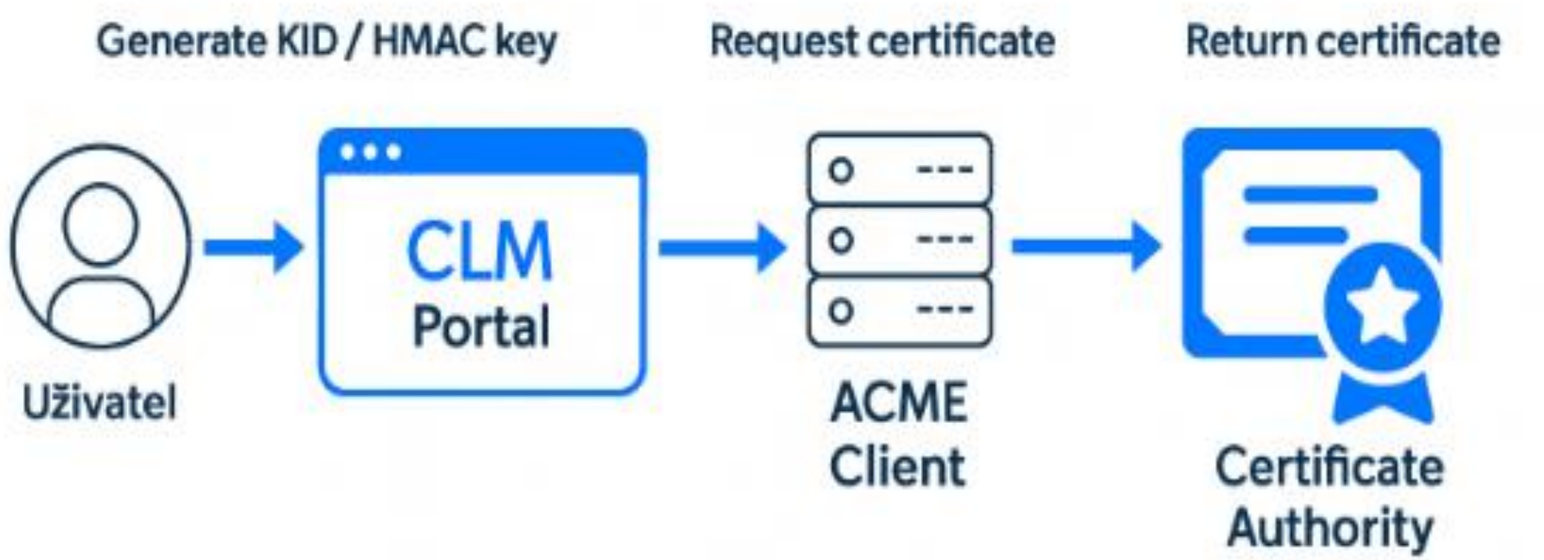
- ACME External Account Binding
  - Proč řešit ACME challenge v interním perimetru?
- MONET+ ACME flow:

🔐 Koncepce ACME EAB (External Account Binding) – stručné vysvětlení

ACME EAB je mechanismus, který umožňuje **ověřit, že ACME klient patří k určité organizaci nebo účtu**, ještě *před* tím, než si u CA založí ACME Account.

🟢 Jak to funguje v kostce:

1. **Server (CA / CLM)** vytvoří pro uživatele **KID** a **HMAC klíč**.
2. Uživatel tato dvě data vloží do ACME klienta.
3. ACME klient pomocí těchto hodnot vytvoří speciální podpis (JWS), kterým se **při zakládání ACME účtu prokáže**.
4. Server ověří podpis pomocí HMAC a pokud sedí, ví, že:
   - KID je správný,
   - uživatel má povolení ACME účet založit,
   - účet se správně "naváže" na příslušného tenant/uživatele.



ACME Clients Implementation

https://letsencrypt.org/docs/client-options/

Bash

- GetSSL (bash, also automates certs on remote hosts via ssh)
- acme.sh (Compatible to bash, dash and sh)
- dehydrated (Compatible to bash and zsh)
- ght-acme.sh (batch update of http-01 and dns-01 challenges is available)
- bacme (simple yet complete scripting of certificate generation)

C

- OpenBSD acme-client
- uacme
- acme-client-portable
- Apache httpd Support via the module mod_md.
- mod_md Separate, more frequent releases of the Apache module.
- CycloneACME (client implementation of ACME dedicated to microcontrollers)

C++

- acme-lw
- esp32-acme-client allows IoT devices to get certificates

Clojure

- certificaat

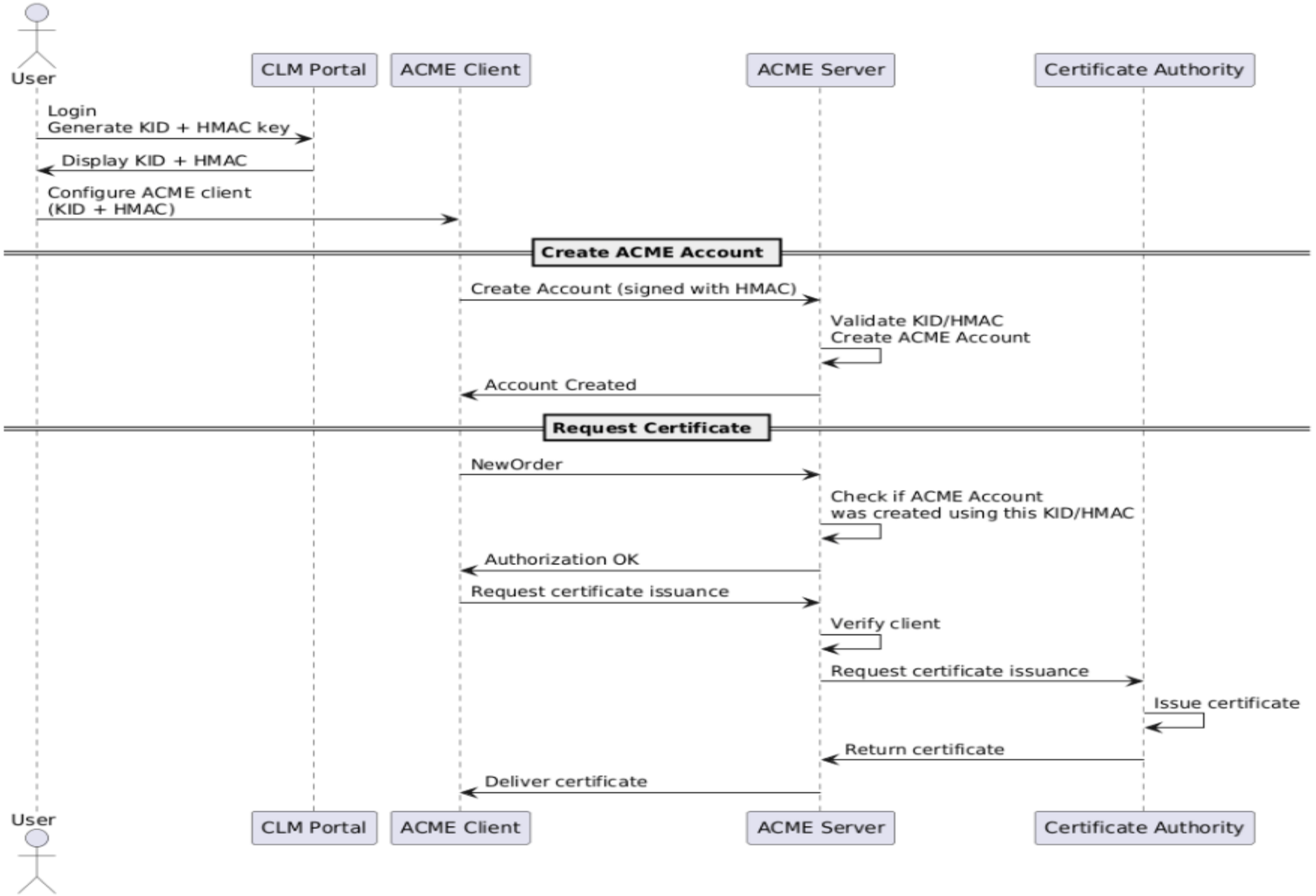
Configuration management tools

- Ansible acme_certificate module
- Ansible collection: acme (ACME V2 integration with acme_certificate module. Supports multiple providers for challenges)
- Pulumi ACME Provider
- Terraform ACME Provider

D

- acme-lw-d

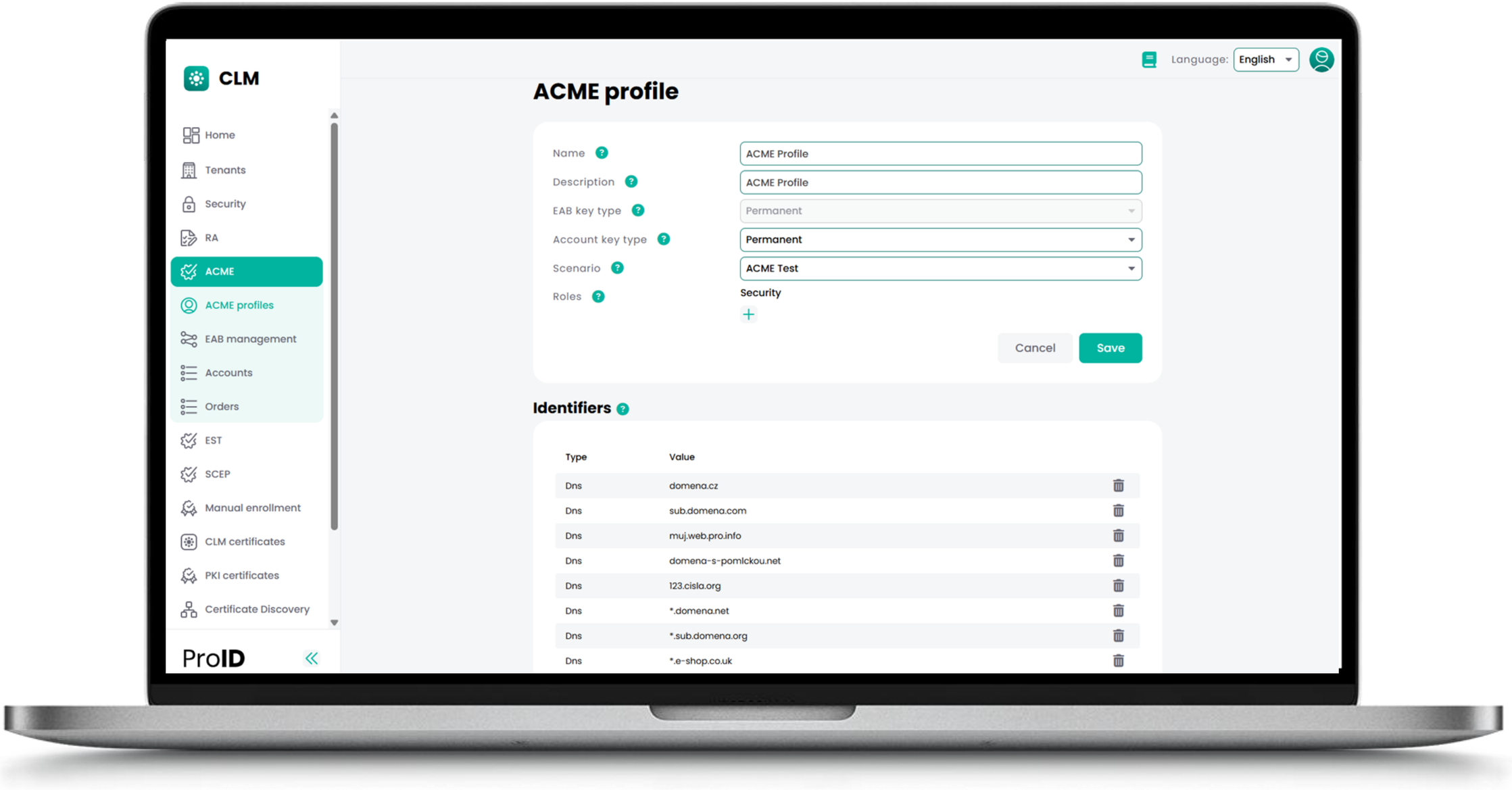
MONET+ ACME


User
CLM Portal
ACME Client
ACME Server
Certificate Authority
Login
Generate KID + HMAC key
Display KID + HMAC
Configure ACME client
(KID + HMAC)
Create ACME Account
Create Account (signed with HMAC)
Validate KID/HMAC
Create ACME Account
Account Created
Request Certificate
NewOrder
Check if ACME Account
was created using this KID/HMAC
Authorization OK
Request certificate issuance
Verify client
Request certificate issuance
Issue certificate
Return certificate
Deliver certificate
User
CLM Portal
ACME Client
ACME Server
Certificate Authority

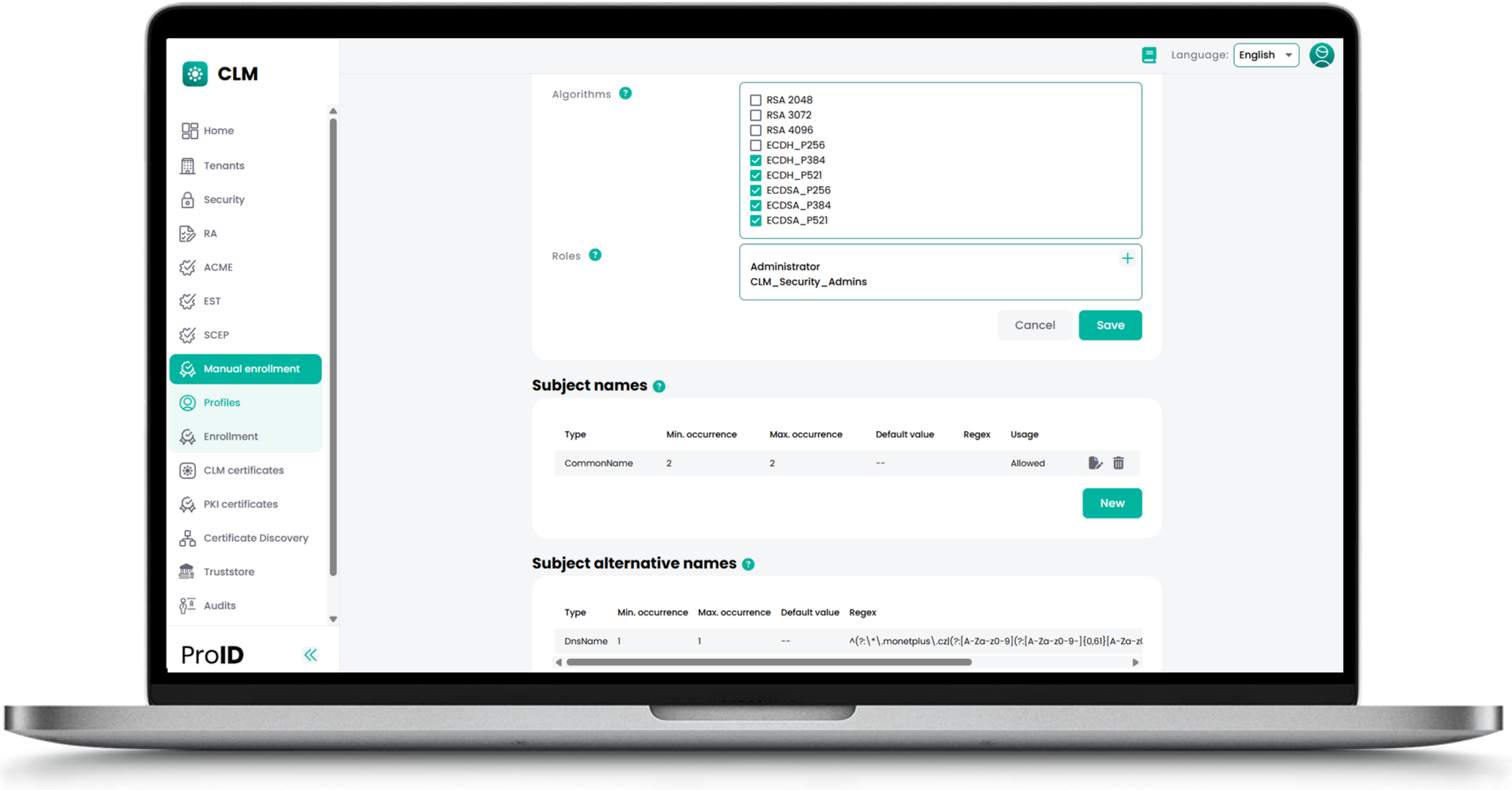
CLM jako ACME klient

- **Vydávání certifikátů z Let’s Encrypt (či jiných veřejných ACME CA)**
- CLM jako ACME client
- Certifikát s klíčem může být dále importován do koncových systémů
  - Např. odeslán na F5, viz další slides
- Případně možné použít v jakémkoliv stávajícím scénáři CLM, i jako ACME CA proxy, komunikace na CLM ACME Server, následné vydání certifikátu z veřejné CA

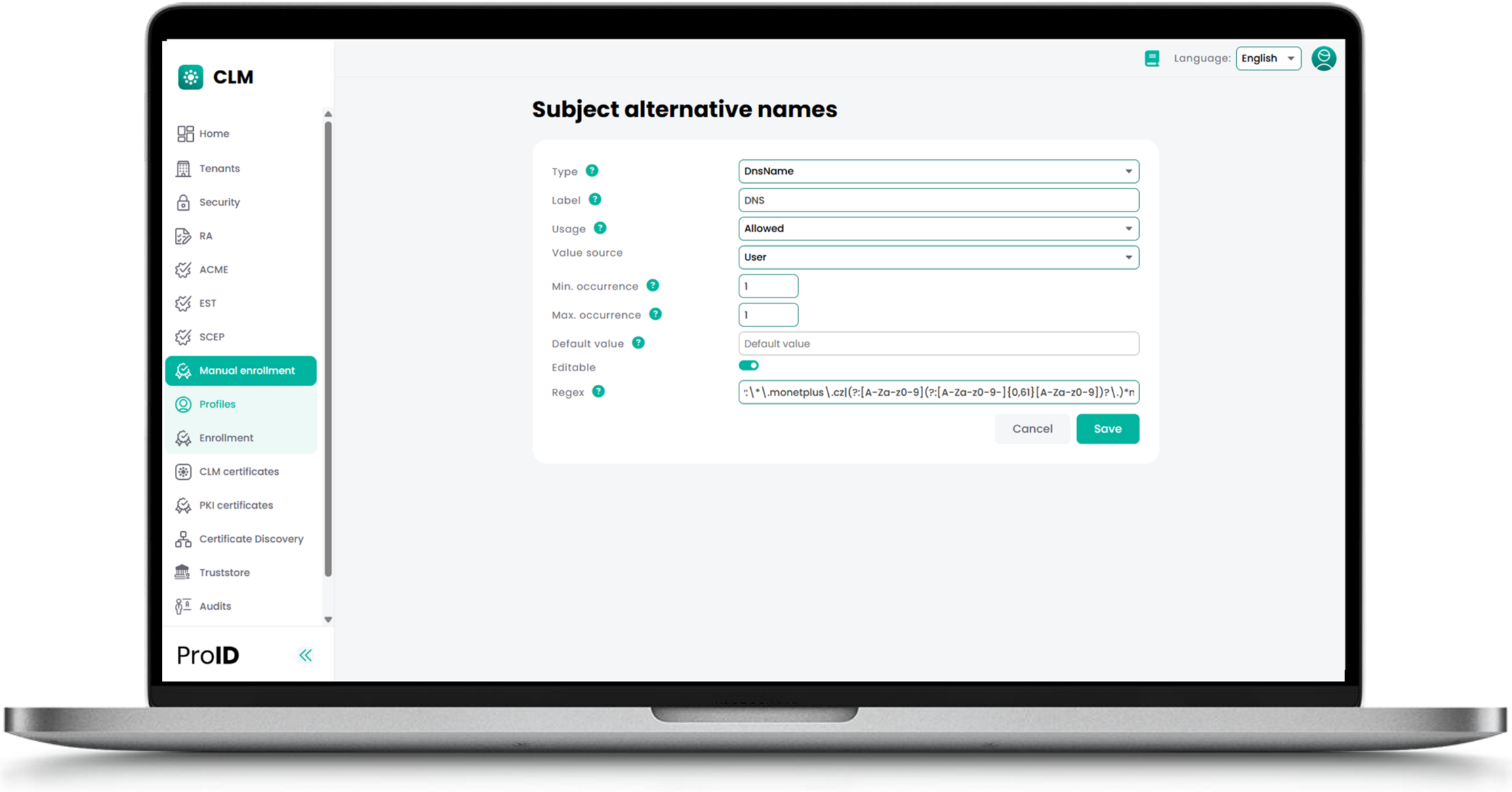
ACME DNS Identifiers



CSR Validation



CSR Validation



MONET+ EST / SCEP

Síťové a další prvky:

- 30 000+ prvků spravovaných CLM MONET+
- např. kritická infrastruktura státu

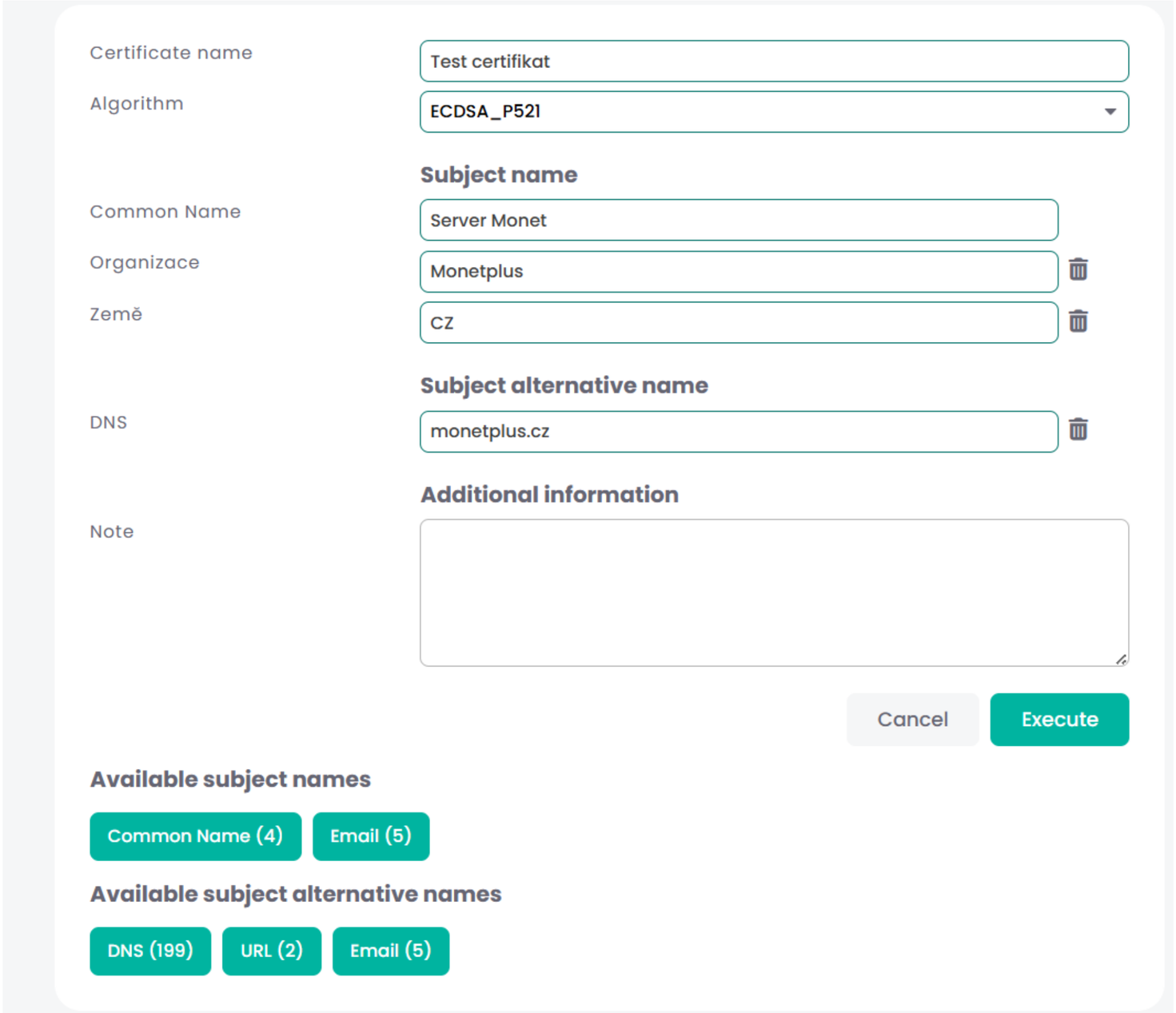
Manuální vydání certifikátu

Generování klíčů v CLM

- následně stažení certifikátu a klíče
  - PFX, PEM, JKS

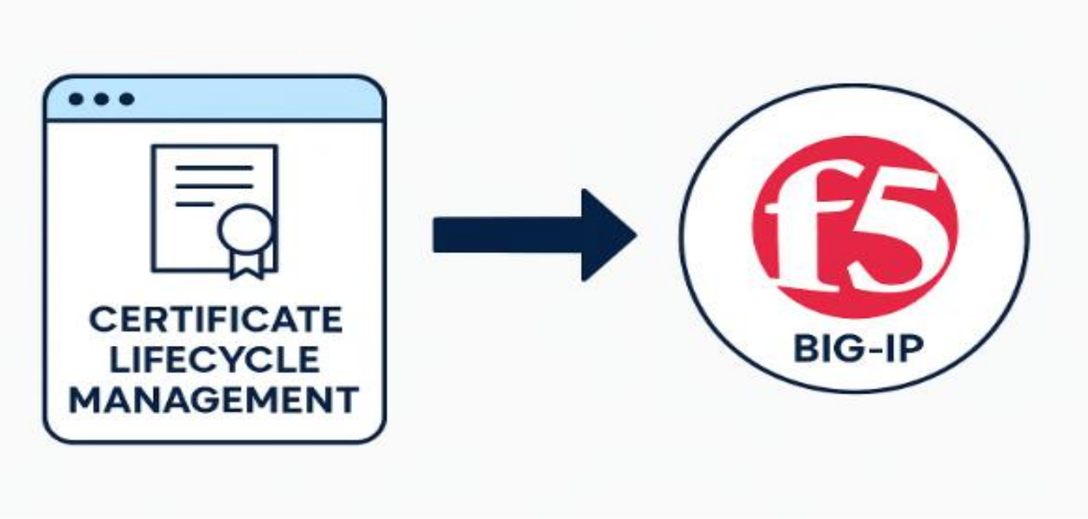
Importem vytvořené žádosti o certifikát

Interní CA i veřejná CA (ACME CA)



F5 management

- **Automatizovaná správa certifikátů F5**
- Zavedení / přehled F5 prvků
- Prvotní vydání certifikátu
- Automatizovaná obnova certifikátů
- Přes management rozhraní F5



F5 management

Step 1: Upload the SSL Certificate

First, we need to upload the SSL certificate file to the BIG-IP system.

```
curl -i -sk -u admin:your-password -X POST \
-H "Content-Type: application/octet-stream" \
-H "Content-Range: 0-1253/1254" \
--data-binary "@test.crt" \
https://<BIG-IP-ADDRESS>:8443/mgmt/shared/file-transfer/uploads/mycert.crt
```

Step 2: Upload the Private Key

Similarly, upload the private key file:

```
curl -i -sk -u admin:your-password -X POST \
-H "Content-Type: application/octet-stream" \
-H "Content-Range: 0-1253/1254" \
--data-binary "@test.key" \
https://<BIG-IP-ADDRESS>:8443/mgmt/shared/file-transfer/uploads/mycert.key
```

Step 3: Install the SSL Certificate

Once uploaded, install the certificate on the BIG-IP system:

```
curl -sk -u admin:your-password -H "Content-Type: application/json" -X POST
-d '{"command":"install","name":"mycert","from-local-file":"/var/config/res
https://<BIG-IP-ADDRESS>:8443/mgmt/tm/sys/crypto/cert
```

Step 4: Install the Private Key

Next, install the private key:

```
curl -sk -u admin:your-password -H "Content-Type: application/json" -X POST
-d '{"command":"install","name":"mycert","from-local-file":"/var/config/res
https://<BIG-IP-ADDRESS>:8443/mgmt/tm/sys/crypto/key
```

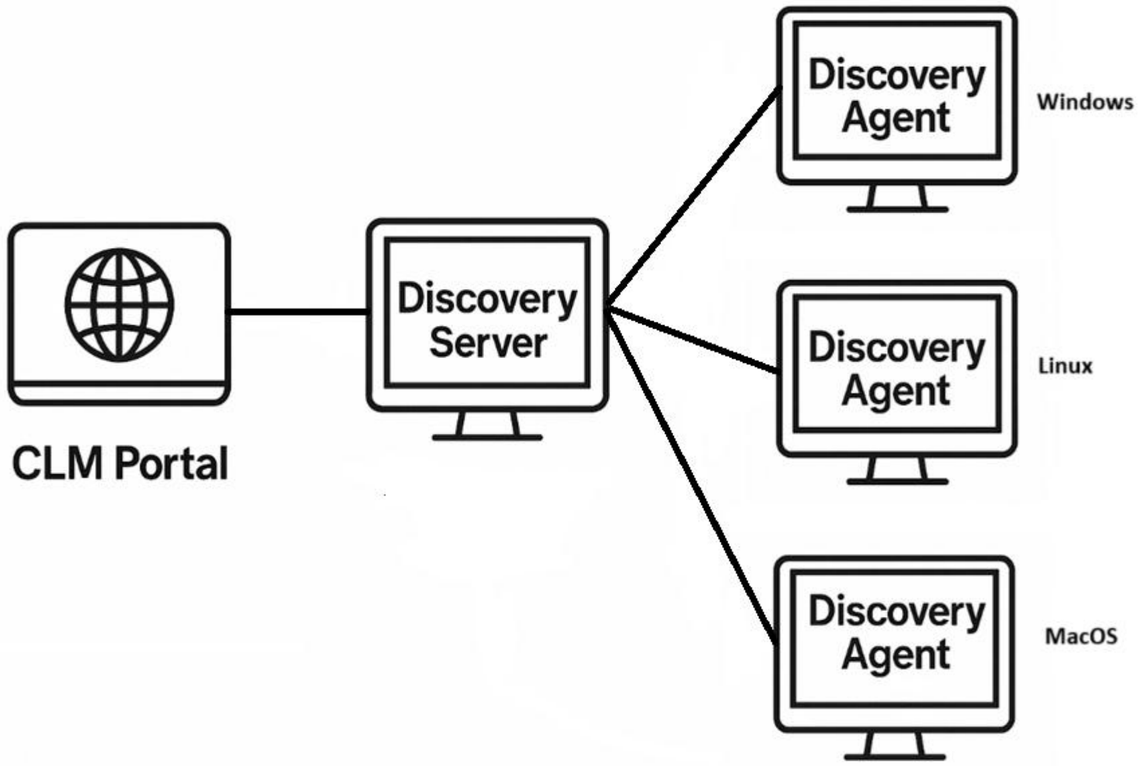
Step 5: Update the SSL Profile

Finally, bind the new certificate and key to an existing clientssl profile:

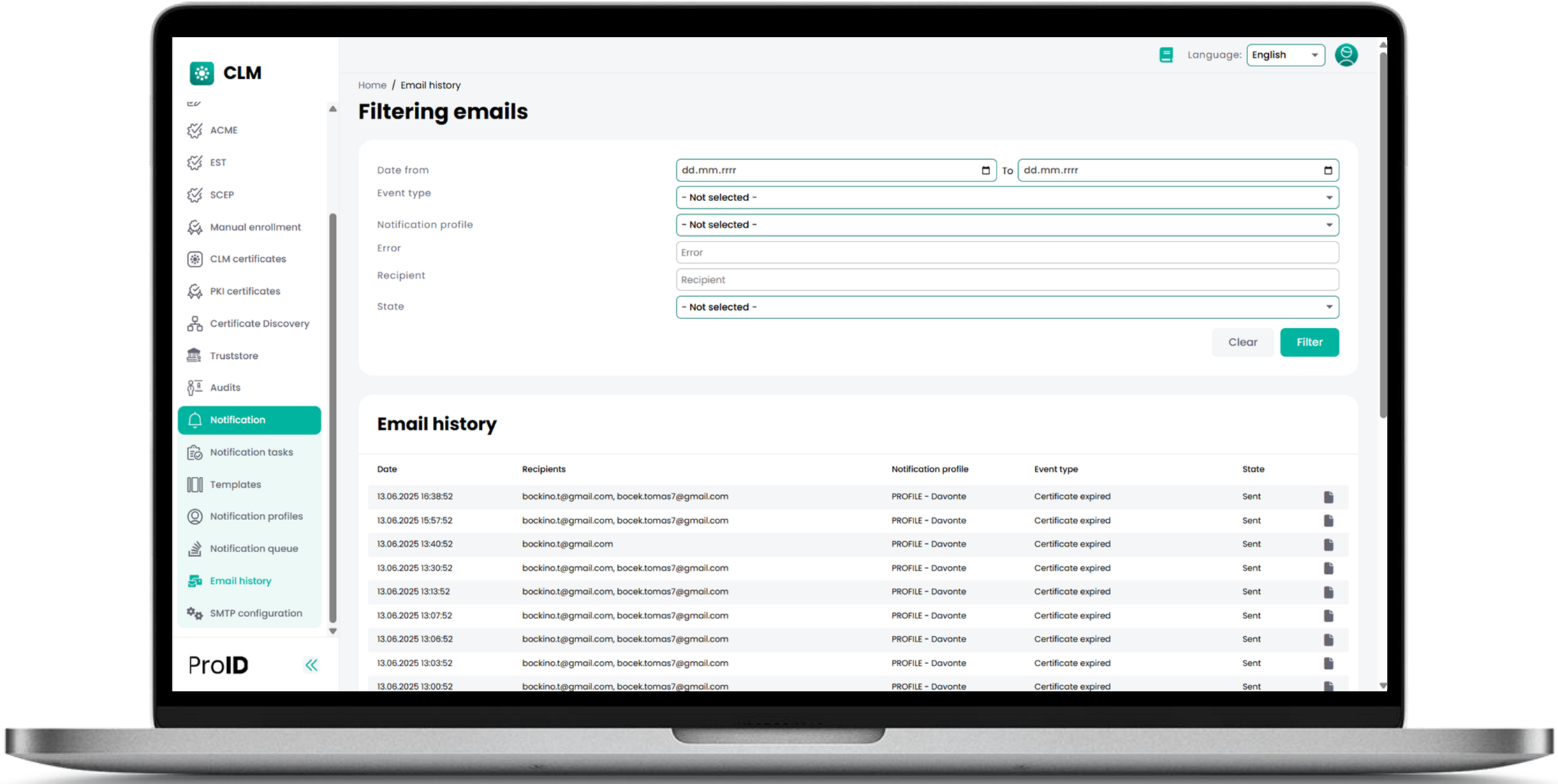
```
curl -sk -u admin:your-password \
  -X PATCH \
  https://<BIG-IP-ADDRESS>:8443/mgmt/tm/ltm/profile/client-ssl/clientssl_te
  -H "Content-Type: application/json" \
  -d '{
    "cert": "/Common/mycert",
    "key": "/Common/mycert"
  }'
```

CLM protokol pro automatizaci vydávání certifikátů

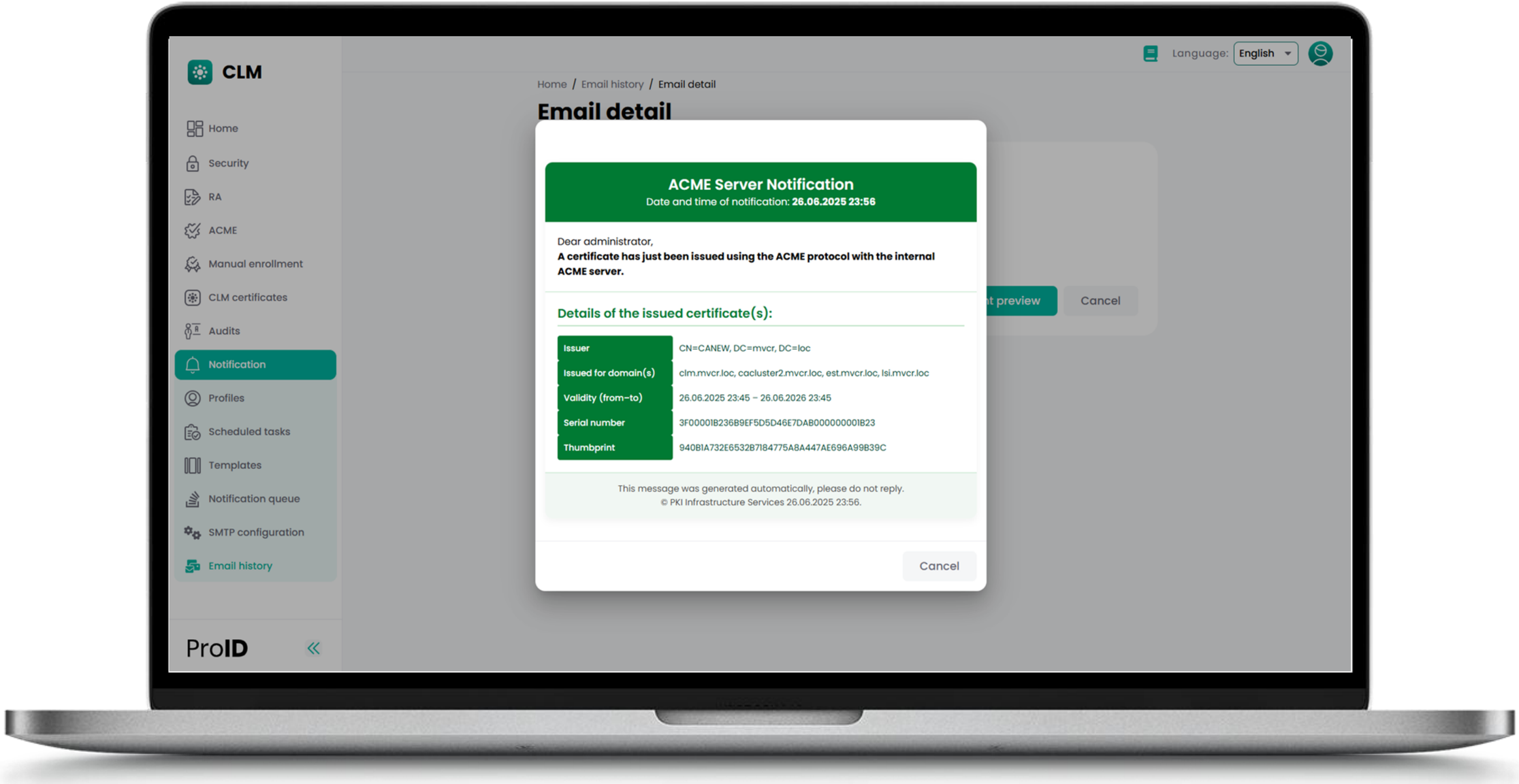
- **Využití discovery agentů pro vydávání certifikátů**
- CLM discovery agenti mohou sloužit jako agenti pro vydávání certifikátů
- Vlastní automatizační protokol
- Velký potenciál
- Feature s obrovskou přidanou hodnotou
  - Neumí seriozně řešit ani globální konkurence



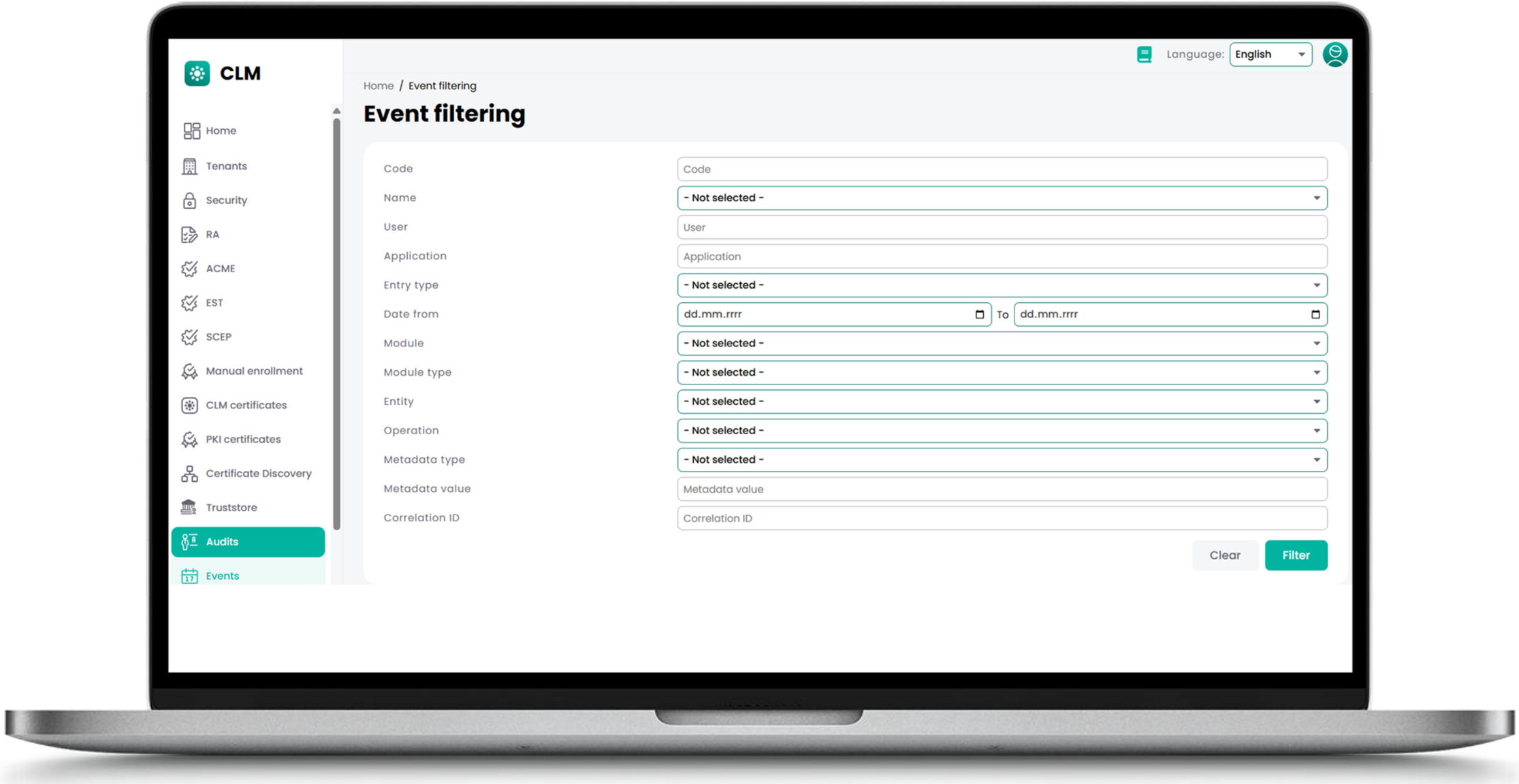
Notifikace


CLM
ACME
EST
SCEP
Manual enrollment
CLM certificates
PKI certificates
Certificate Discovery
Truststore
Audits
Notification
Notification tasks
Templates
Notification profiles
Notification queue
Email history
SMTP configuration
ProID
Language: English
Home / Email history
Filtering emails
Date from
dd.mm.rrrr
To
dd.mm.rrrr
Event type
- Not selected -
Notification profile
- Not selected -
Error
Recipient
State
- Not selected -
Clear
Filter
Email history
Date
Recipients
Notification profile
Event type
State
13.06.2025 16:38:52 bockino.t@gmail.com, bocek.tomas7@gmail.com PROFILE - Davonte Certificate expired Sent
13.06.2025 15:57:52 bockino.t@gmail.com, bocek.tomas7@gmail.com PROFILE - Davonte Certificate expired Sent
13.06.2025 13:40:52 bockino.t@gmail.com PROFILE - Davonte Certificate expired Sent
13.06.2025 13:30:52 bockino.t@gmail.com, bocek.tomas7@gmail.com PROFILE - Davonte Certificate expired Sent
13.06.2025 13:13:52 bockino.t@gmail.com, bocek.tomas7@gmail.com PROFILE - Davonte Certificate expired Sent
13.06.2025 13:07:52 bockino.t@gmail.com, bocek.tomas7@gmail.com PROFILE - Davonte Certificate expired Sent
13.06.2025 13:06:52 bockino.t@gmail.com, bocek.tomas7@gmail.com PROFILE - Davonte Certificate expired Sent
13.06.2025 13:03:52 bockino.t@gmail.com, bocek.tomas7@gmail.com PROFILE - Davonte Certificate expired Sent
13.06.2025 13:00:52 bockino.t@gmail.com, bocek.tomas7@gmail.com PROFILE - Davonte Certificate expired Sent

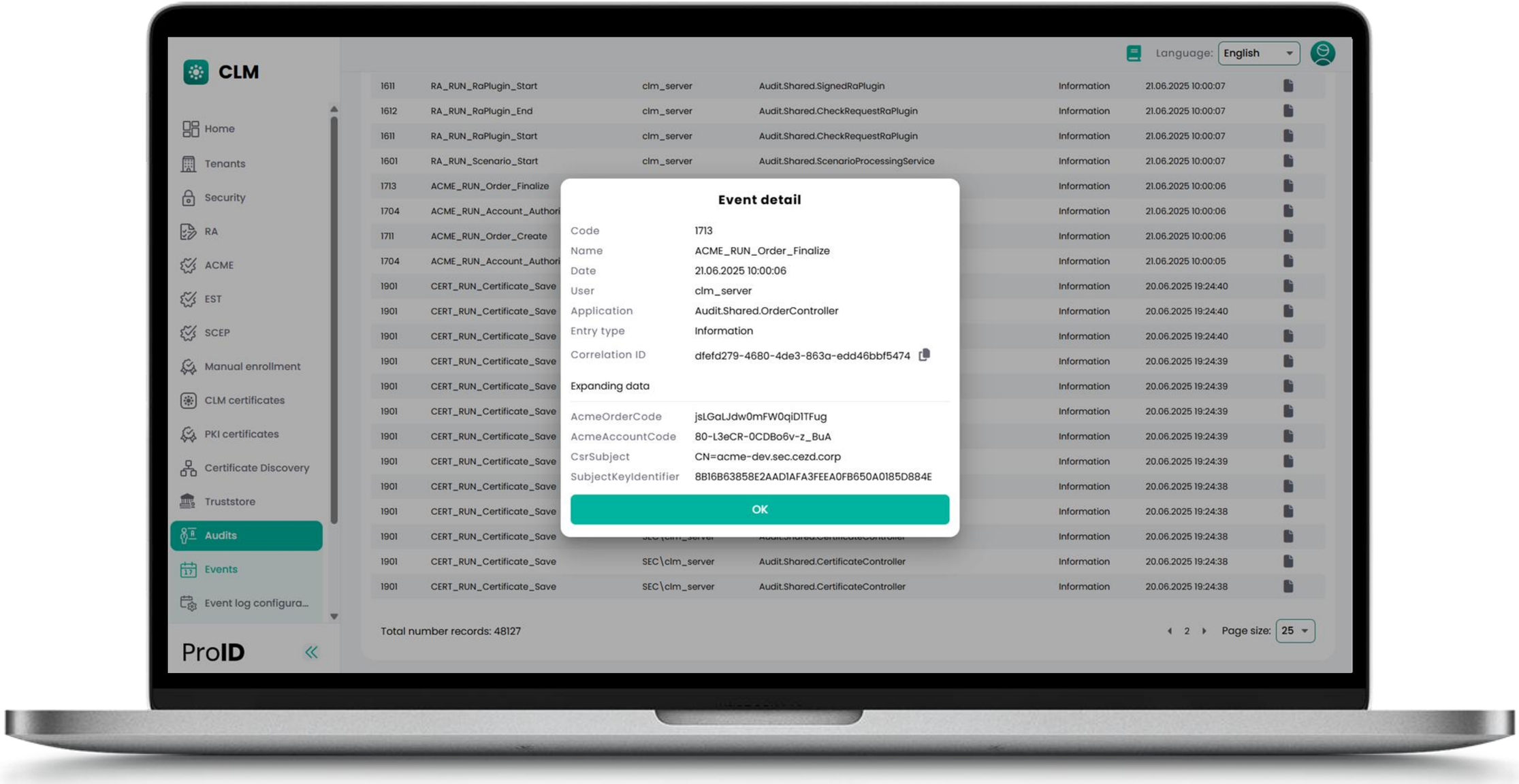
Notifikace


CLM
Language: English
Home / Email history / Email detail
Email detail
Home
Security
RA
ACME
Manual enrollment
CLM certificates
Audits
Notification
Profiles
Scheduled tasks
Templates
Notification queue
SMTP configuration
Email history
ProID
t preview
Cancel
ACME Server Notification
Date and time of notification: 26.06.2025 23:56
Dear administrator,
A certificate has just been issued using the ACME protocol with the internal ACME server.
Details of the issued certificate(s):
Issuer
CN=CANEW, DC=mvcr, DC=loc
Issued for domain(s)
clm.mvcr.loc, cacluster2.mvcr.loc, est.mvcr.loc, lsi.mvcr.loc
Validity (from–to)
26.06.2025 23:45 – 26.06.2026 23:45
Serial number
3F00001B236B9EF5D5D46E7DAB000000001B23
Thumbprint
940B1A732E6532B7184775A8A447AE696A99B39C
This message was generated automatically, please do not reply.
© PKI Infrastructure Services 26.06.2025 23:56.
Cancel

Audit


CLM
Language: English
Home / Event filtering
Event filtering
Home
Tenants
Security
RA
ACME
EST
SCEP
Manual enrollment
CLM certificates
PKI certificates
Certificate Discovery
Truststore
Audits
Events
Code
Name
User
Application
Entry type
Date from
To
Module
Module type
Entity
Operation
Metadata type
Metadata value
Correlation ID
- Not selected -
dd.mm.rrrr
Clear
Filter

Audit


CLM
Language: English
Home
Tenants
Security
RA
ACME
EST
SCEP
Manual enrollment
CLM certificates
PKI certificates
Certificate Discovery
Truststore
Audits
Events
Event log configura...
ProID
1611 RA_RUN_RaPlugin_Start clm_server Audit.Shared.SignedRaPlugin Information 21.06.2025 10:00:07
1612 RA_RUN_RaPlugin_End clm_server Audit.Shared.CheckRequestRaPlugin Information 21.06.2025 10:00:07
1611 RA_RUN_RaPlugin_Start clm_server Audit.Shared.CheckRequestRaPlugin Information 21.06.2025 10:00:07
1601 RA_RUN_Scenario_Start clm_server Audit.Shared.ScenarioProcessingService Information 21.06.2025 10:00:07
1713 ACME_RUN_Order_Finalize Information 21.06.2025 10:00:06
1704 ACME_RUN_Account_Authori Information 21.06.2025 10:00:06
1711 ACME_RUN_Order_Create Information 21.06.2025 10:00:06
1704 ACME_RUN_Account_Authori Information 21.06.2025 10:00:05
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:40
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:40
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:40
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:39
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:39
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:39
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:39
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:39
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:38
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:38
1901 CERT_RUN_Certificate_Save Information 20.06.2025 19:24:38
1901 CERT_RUN_Certificate_Save SEC\clm_server Audit.Shared.CertificateController Information 20.06.2025 19:24:38
1901 CERT_RUN_Certificate_Save SEC\clm_server Audit.Shared.CertificateController Information 20.06.2025 19:24:38
Event detail
Code 1713
Name ACME_RUN_Order_Finalize
Date 21.06.2025 10:00:06
User clm_server
Application Audit.Shared.OrderController
Entry type Information
Correlation ID dfefd279-4680-4de3-863a-edd46bbf5474
Expanding data
AcmeOrderCode jsLGaLJdw0mFW0qiD1TFug
AcmeAccountCode 80-L3eCR-0CDBo6v-z_BuA
CsrSubject CN=acme-dev.sec.cezd.corp
SubjectKeyIdentifier 8B16B63858E2AAD1AFA3FEEA0FB650A0185D884E
OK
Total number records: 48127
2
Page size: 25

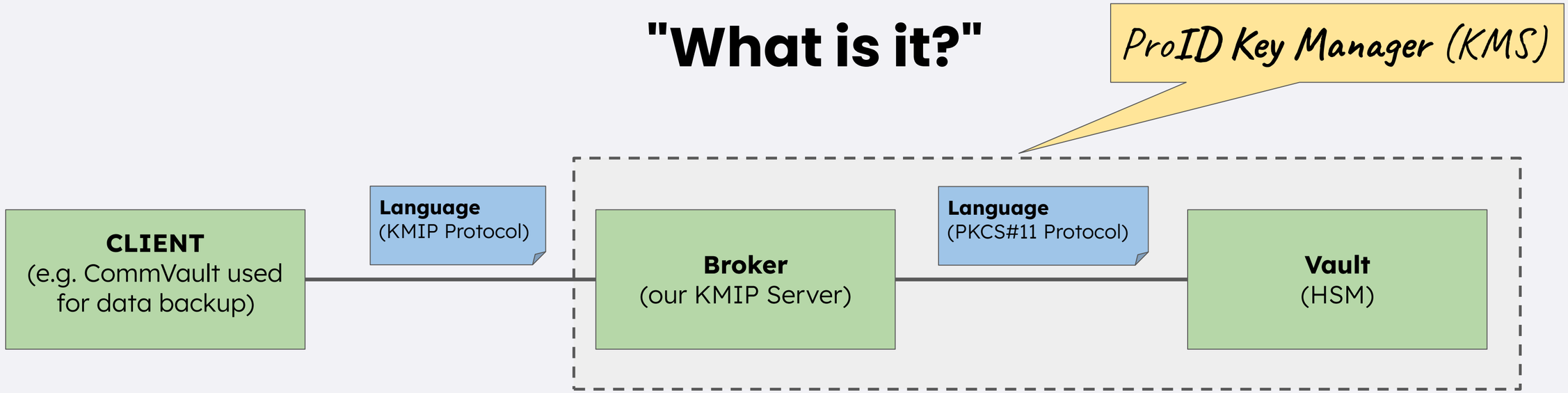
Key Management Server (KMIP protocol)

KMS / KMIP

Symetrická kryptografie
Šifrování

- zálohy
- VMWare
- DBs
- atp.

"What is it?"



Broker (KMIP Server)

Manages the entire lifecycle of all keys (creation, policy, destruction) and acts as the secure intermediary between applications and the HSM Vault.

Vault (HSM)

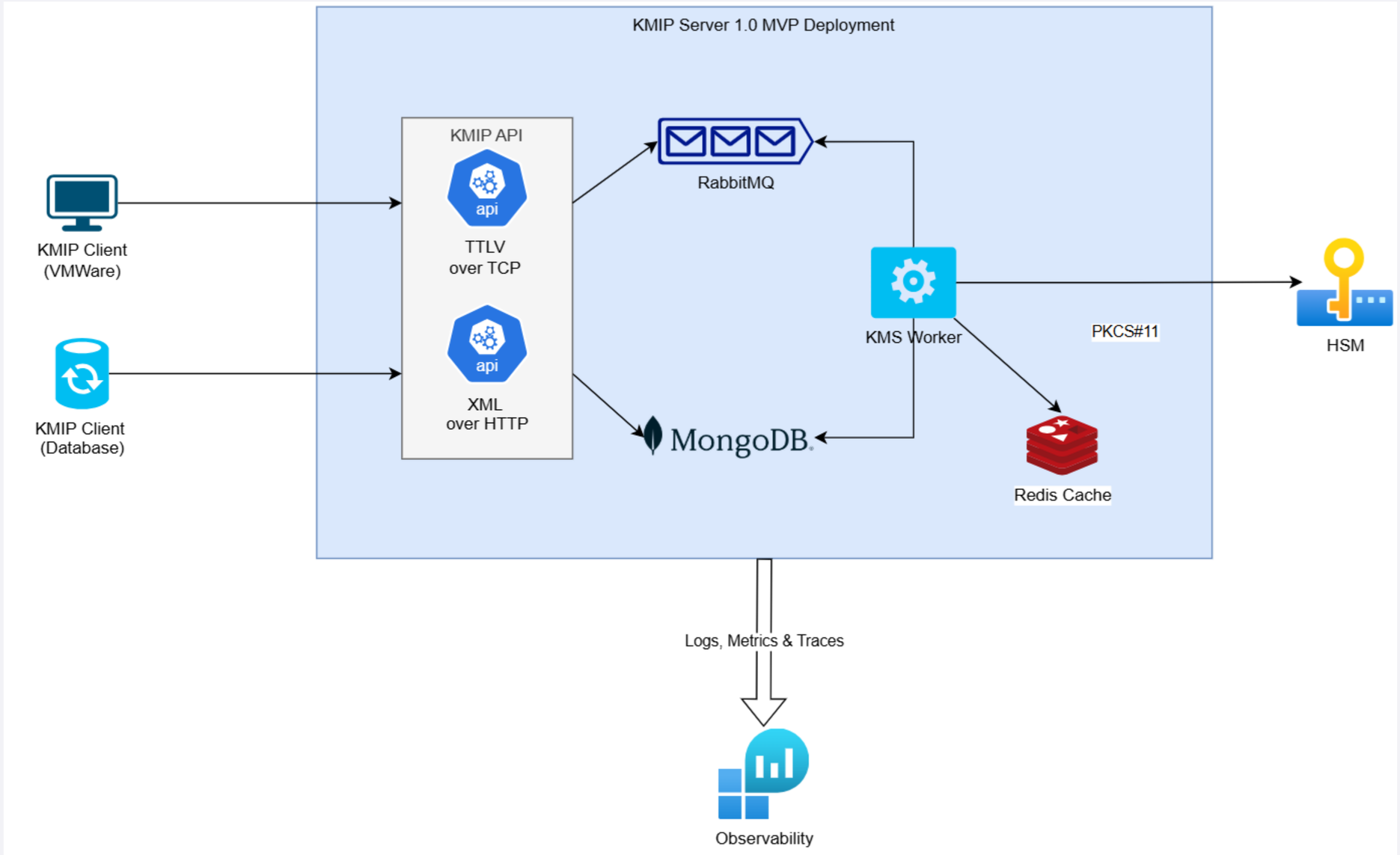
This is where the master encryption keys are physically created and securely stored.

Language (KMIP & PKCS#11 Protocols)

KMIP: Allows “The Broker” to talk to client applications (e.g., CommVault).
PKCS#11: Allows “The Broker” to talk to the certified hardware (HSM).

Key Benefit: Centralized, audited control over keys protected by the highest hardware standard.

Key Management Server (KMIP protocol)



Key Management Server (KMIP protocol)

- Klíčové vlastnosti:
  - Standardizace (OASIS KMIP)
  - Více verzí protokolu
  - Centrální správa klíčů
- Otestované scénáře:
  - VMware vSphere/ vSAN Encryption
  - Databázová šifrování
  - Zálohovací SW (např. CommVault)

Provides keys to applications (e.g. Commvault) for encrypting data before it is stored on disk or tape.

Manages keys for encrypting Virtual Machines (VMs) and disks (e.g., in a VMWare environment).