MONET +

Technologická identita

Jakub Kolařík

22. 1. 2026

Digital Identity Solutions
Identita
Platby
MONET +

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.

Digital Identity

Technical ID

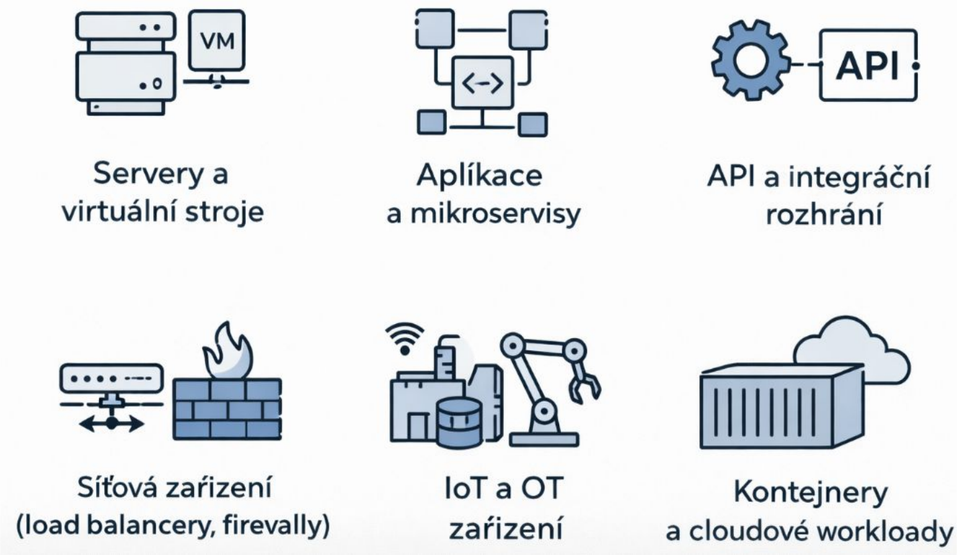
MONET +

Technologická identita

- **Technologická identita** je **jednoznačná a ověřitelná identita ne-lidského subjektu** v IT prostředí.
- Umožňuje systémům, aplikacím a zařízením **prokázat, kdo jsou**, a **bezpečně spolu komunikovat** bez zásahu člověka.
- Realizována:
  - **digitálním certifikátem**
  - kryptografickým klíčem
  - …

Co může mít technologickou identitu

- servery a virtuální stroje
- aplikace a mikroservisy
- síťová zařízení
  (load balancery, firewally)
- IoT a OT zařízení
- kontejnery a cloudové workloady



Počet technologických identit **násobně převyšuje lidské identity**

Proč vydáváme certifikáty technickým prvkům?

Bezpečnost komunikace

- šifrování dat

Důvěryhodná identita systémů

- víme, kdo s kým mluví

Nahrazení hesel

- menší riziko úniku

Automatizace

- bez ruční správy

Soulad s regulacemi

- audit, dohledatelnost

Scénáře použití certifikátů

1. Autentizace mezi systémy (mTLS)

- vzájemné ověření **server** ↔ **server** nebo **služba** ↔ **služba**

2. Šifrování komunikace

- ochrana dat **za běhu (in-transit)**
- TLS/HTTPS

3. Zabezpečení API a integračních rozhraní

- autentizace klienta pomocí certifikátu místo tokenu nebo hesla

Scénáře použití certifikátů

4. Cloud a kontejnery (workload identity)

- identita pro:
  - kontejnery
  - Kubernetes pody
  - cloudové služby
- krátkodobé certifikáty

5. IoT / OT zařízení

- jednoznačná identita každého zařízení
- bezpečné připojení k backendu

6. Autentizace serverů a síťových prvků

- load balancery, firewally, reverse proxy
- bezpečná komunikace v rámci infrastruktury

Výzvy spojené se správou certifikátů

1) Zkracování platnosti veřejných TLS certifikátů

- Od **15. 3. 2026** se **maximální délka platnosti veřejných TLS certifikátů zkracuje na 200 dní** (vs. 398 dříve), další redukce v roce 2027 na 100 dní a cílově do **47 dní do roku 2029**.
- To znamená **častější obnovování certifikátů** — přibližně 2–8× více než dnes.

2) Doporučení zkracovat platnost i interních certifikátů

- Minimalizace dopadu kompromitace klíče
- Soulad s principy Zero Trust - identita musí být pravidelně obnovována
- Cloud-native a moderní architektury (Kontejnery, Kubernetes atp. počítají s certifikáty s platností v řádu hodin až dnů)

Krátká platnost výrazně snižuje časové okno, po které lze zneužít odcizený certifikát nebo privátní klíč.

3) Nutnost automatizace životního cyklu certifikátů

- S kratšími životnostmi **ruční správa je neudržitelná**.
- Automatizace **vystavení** → **instalace** → **obnova** → **audit** se stává základním požadavkem, nikoli volitelnou výhodou.

Rizika spojená s expiracemi certifikátů

Provozní rizika (nejkritičtější)

Nedostupnost služeb

- TLS handshake selže → **služba se vůbec nespustí**
- Typicky weby, API, integrační rozhraní, load balancery (např. F5), reverse proxy

Selhání automatizovaných procesů

- CRON joby, integrace, middleware, message brokery přestanou komunikovat
- Často **bez okamžité viditelné chyby** (tiché selhání)

Výpadky v řetězu služeb

- Jediný expirovaný certifikát může „shodit“ celý aplikační stack

Rizika spojená s expiracemi certifikátů

Bezpečnostní rizika

Nucené obcházení bezpečnosti

- Administrátoři pod tlakem:
    - vypínají TLS validaci

Ruční generování certifikátů:

- slabé klíče
- špatné CN/SAN
- neznámý původ privátního klíče

Co může pomoci?

Implementace CLM systému.

CLM systém (Certificate Lifecycle Management) je **centrální platforma pro řízení životního cyklu digitálních certifikátů a technologických identit** napříč celým IT prostředím organizace.

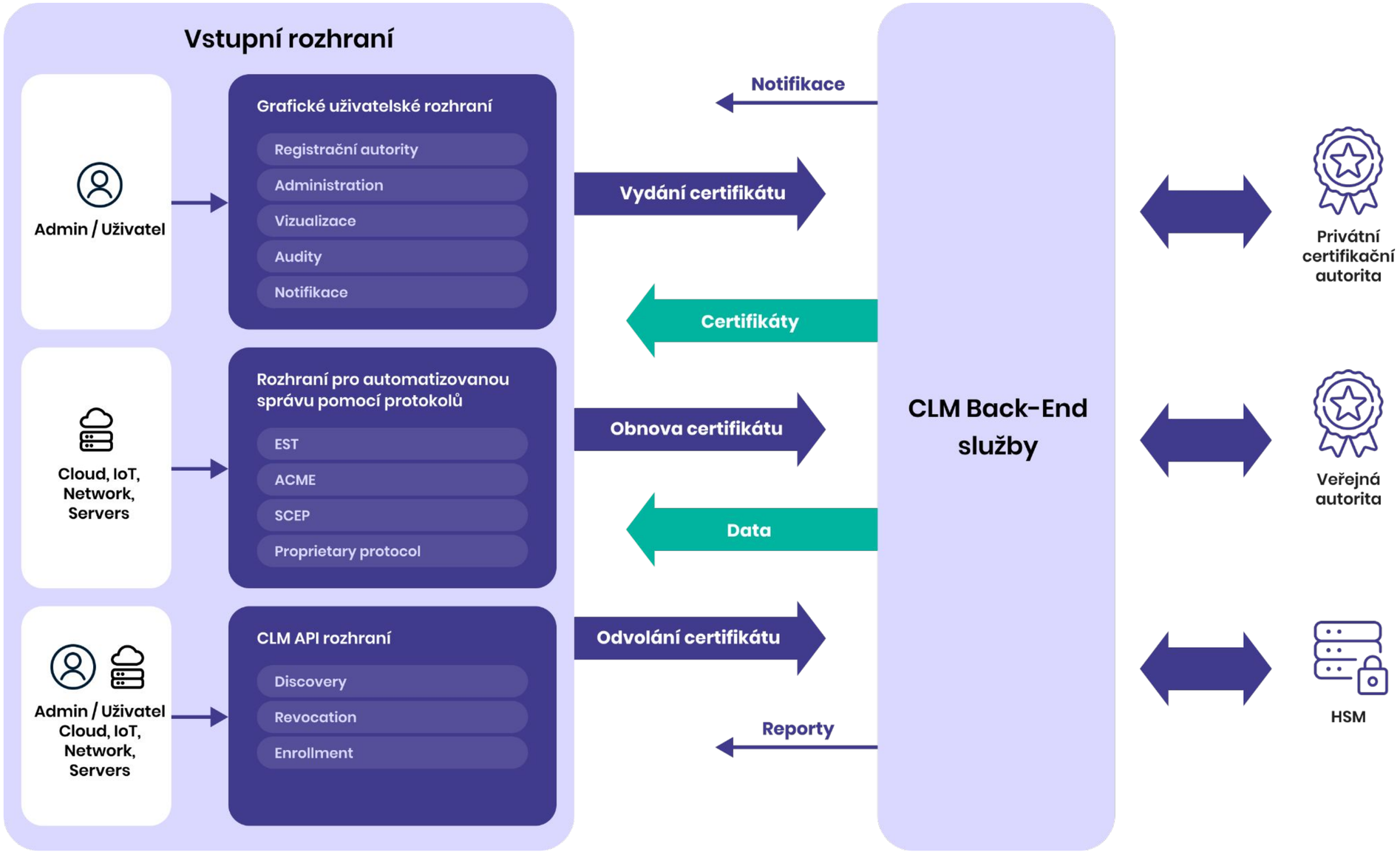
Kompletní životní cyklus certifikátu

- žádost (automatická i manuální)
- schválení / RA procesy
- vydání certifikátu
- instalace a distribuce
- obnova (renewal)
- revokace a expirace

Automatizace a integrace

- protokoly: ACME, EST, SCEP
- integrace s:
  - internímí i veřejnými CA
  - cloudem, Kubernetes, DevOps pipeline
  - síťovými prvky (LB, FW, API GW)

MONET+ Certificate Lifecycle Management



CLM Aplikace

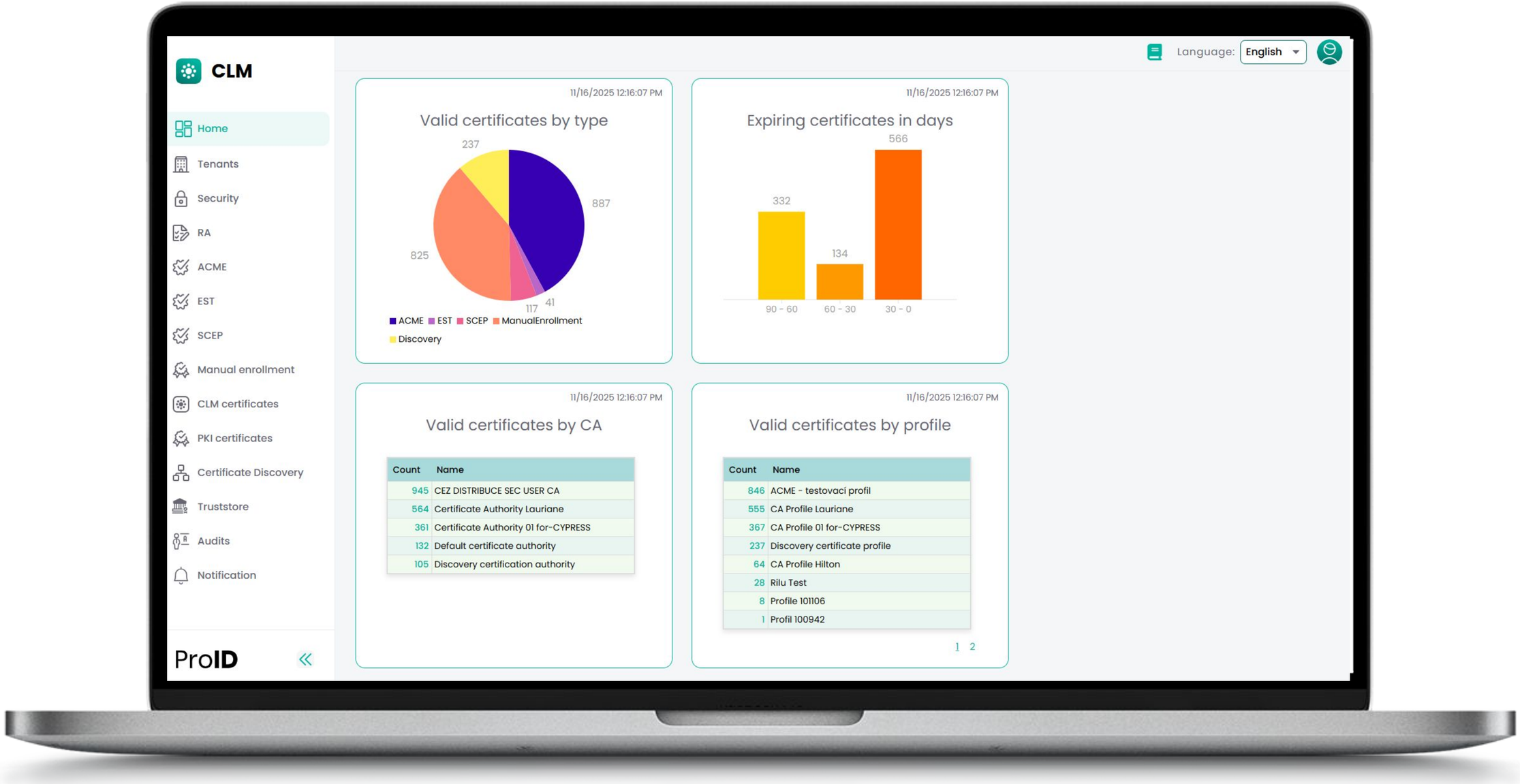
Primární procesy

- Vydání certifikátů
- Obnova certifikátů
- Odvolání certifikátů

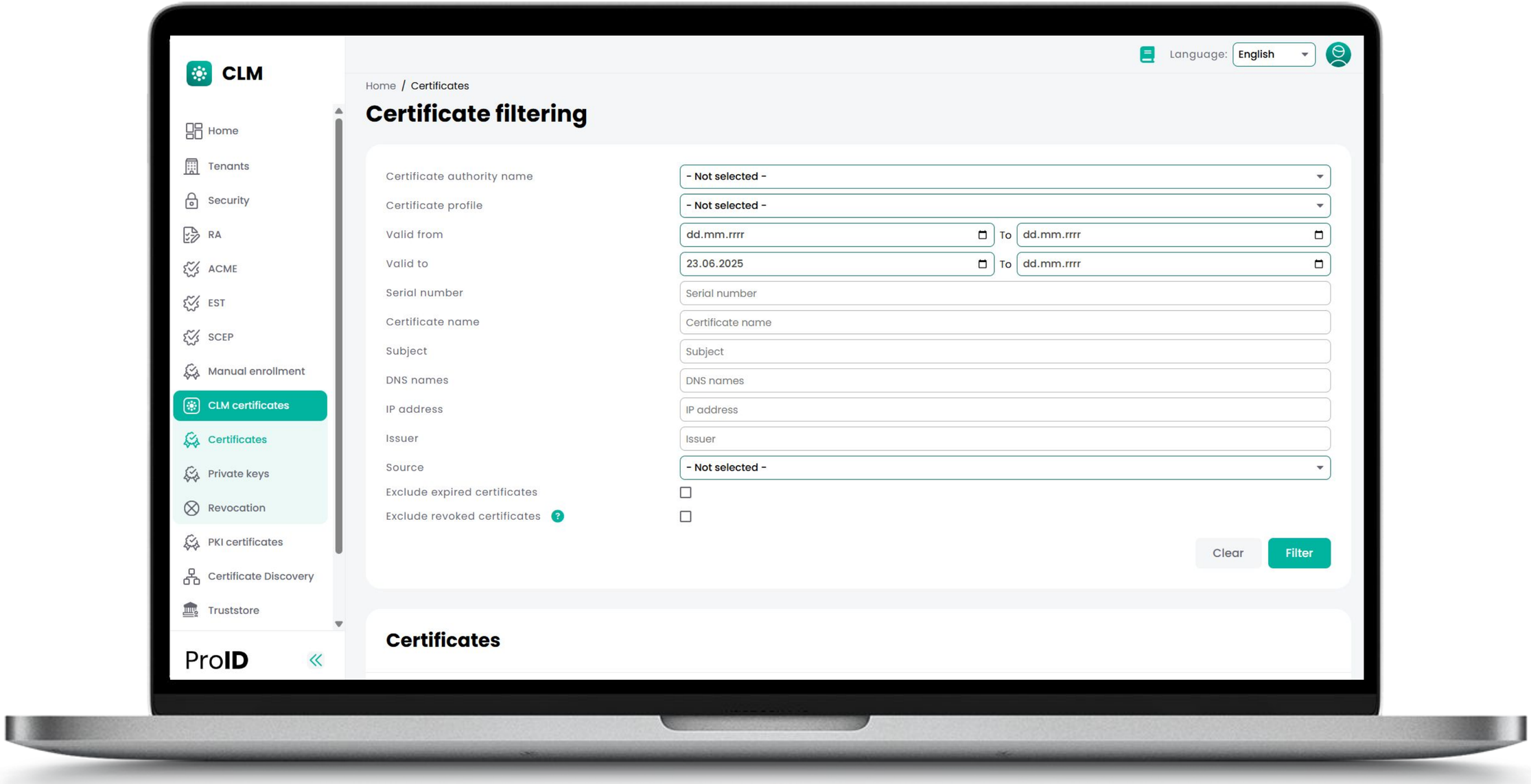
Podpůrné procesy a funkce

- Správa uživatelů a rolí
- Audit
- Discovery certifikátů
- Notifikace
- Filtrování certifikátů
- Přehledy a reporty
- Validace žádostí o certifikát
- Autorizace žádostí o certifikát

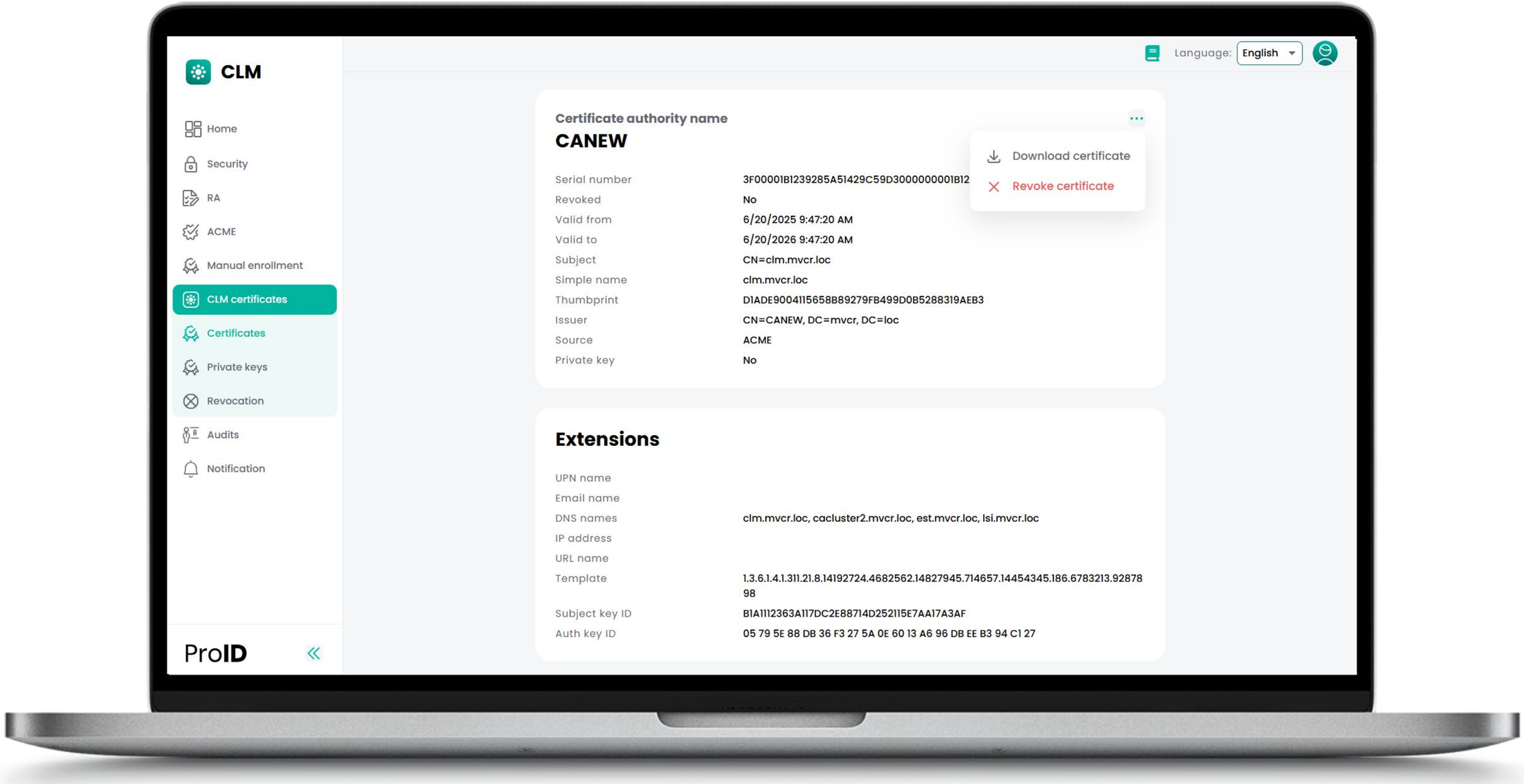
Visibility & Discovery



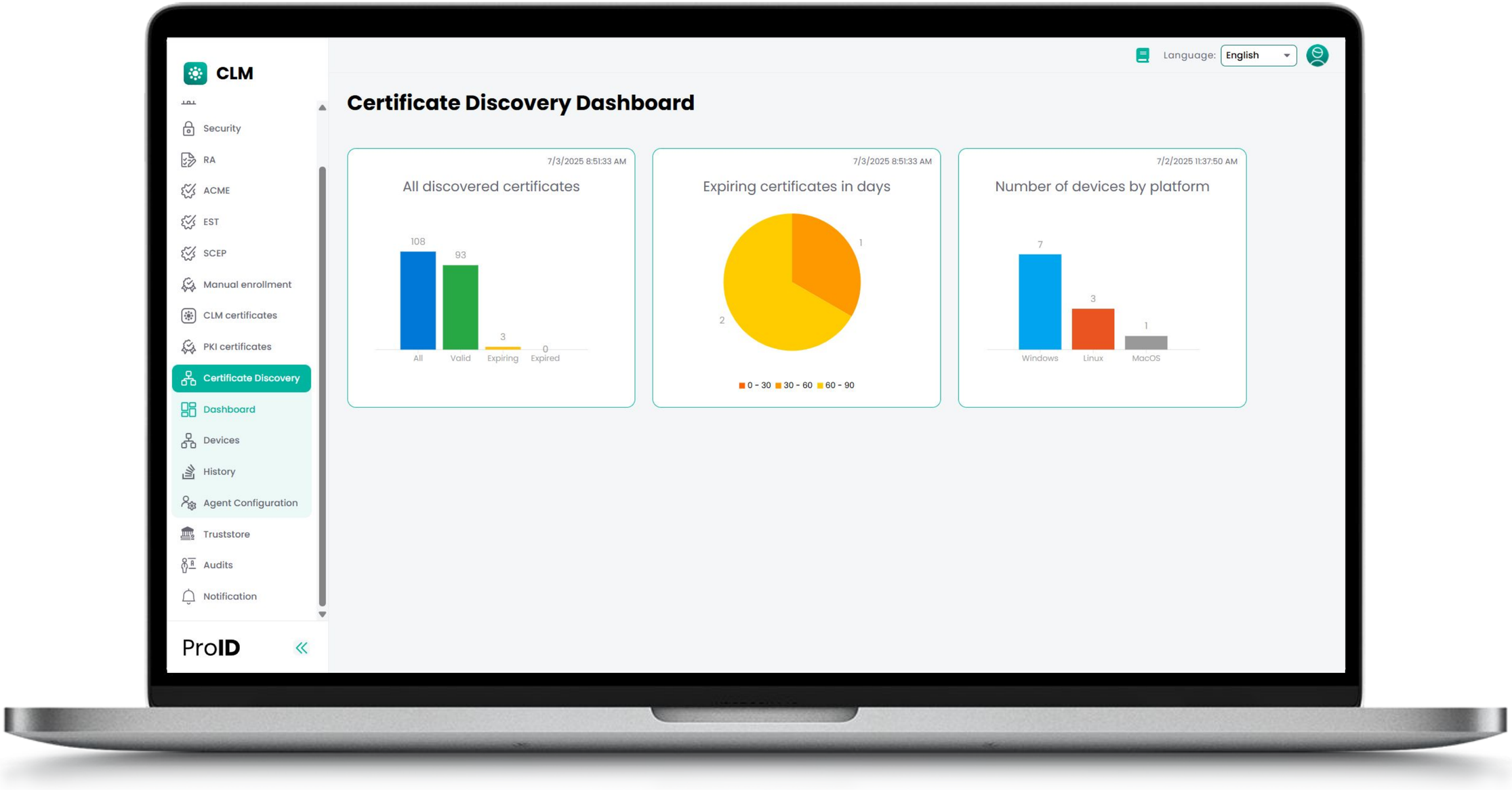
Visibility & Discovery



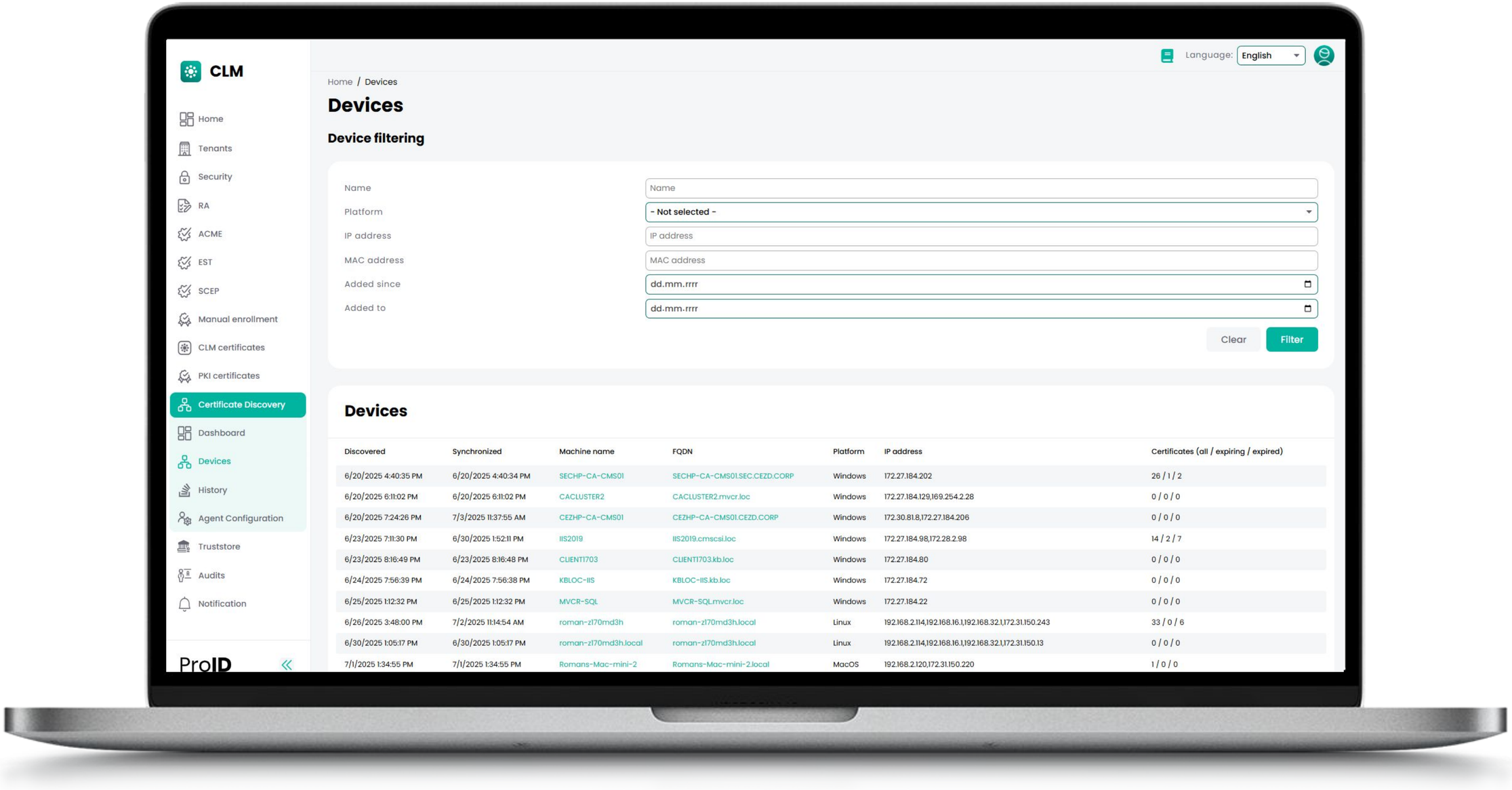
Visibility & Discovery



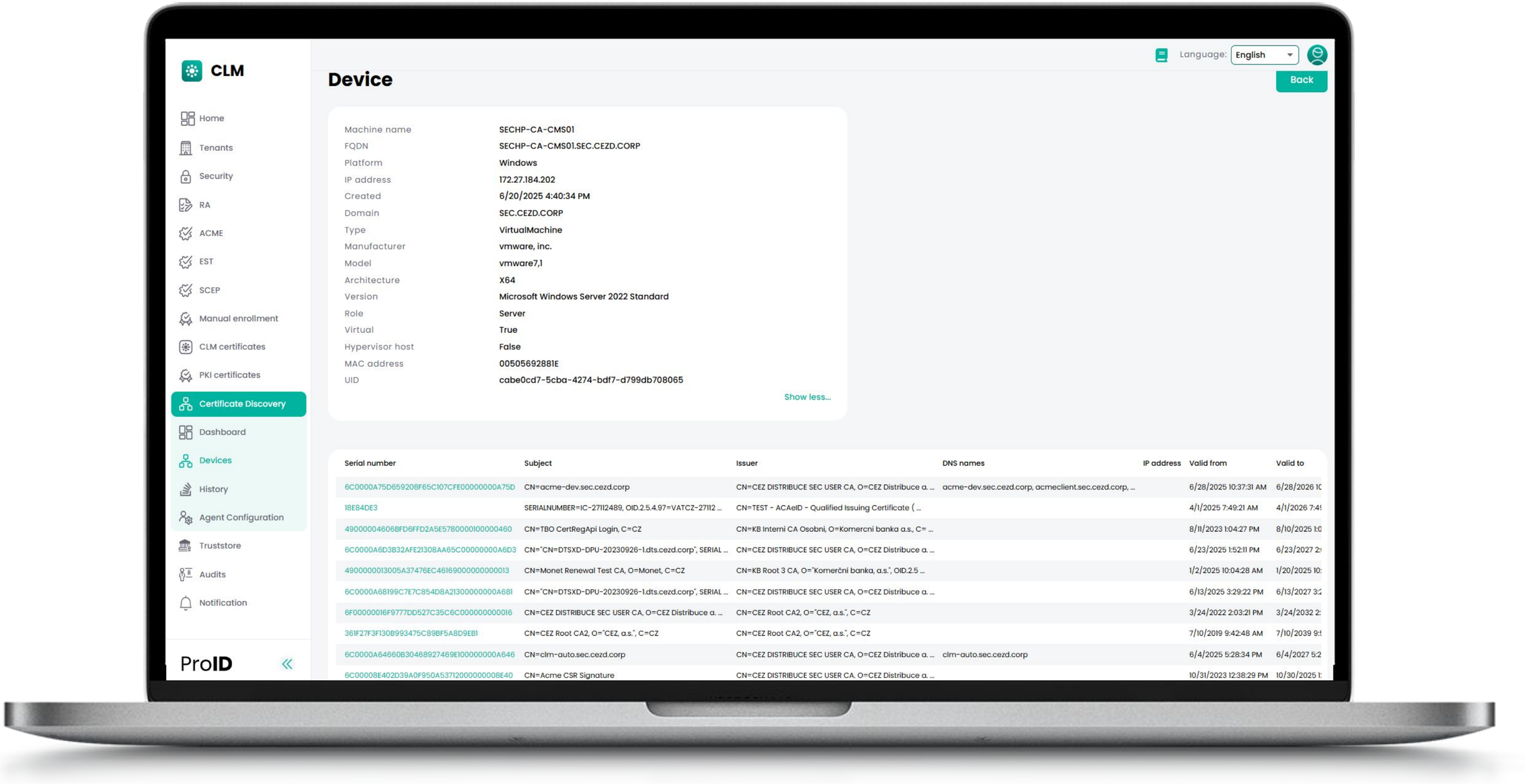
Discovery Across Environment



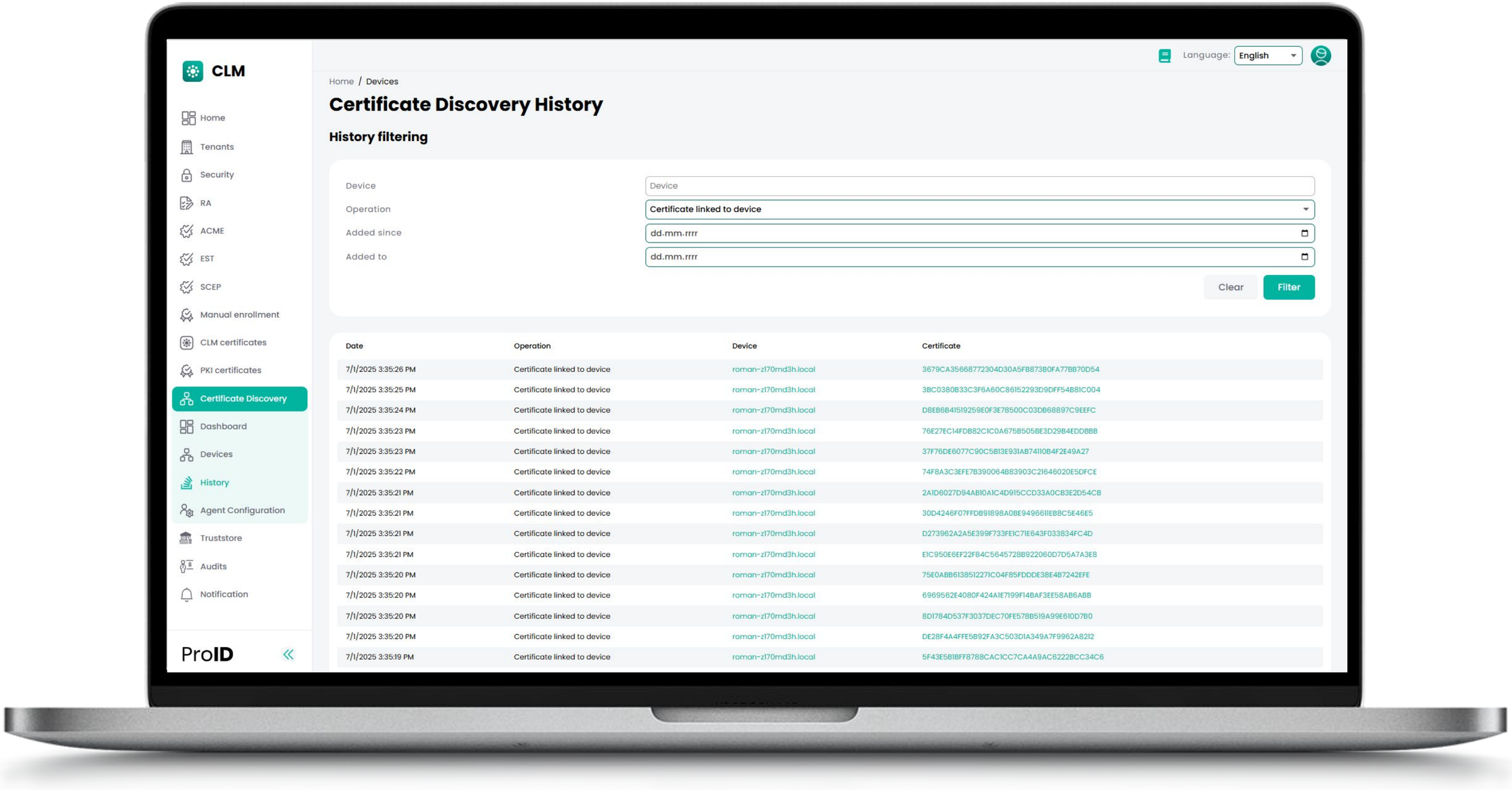
Discovery Across Environment



Discovery Across Environment



Discovery Across Environment

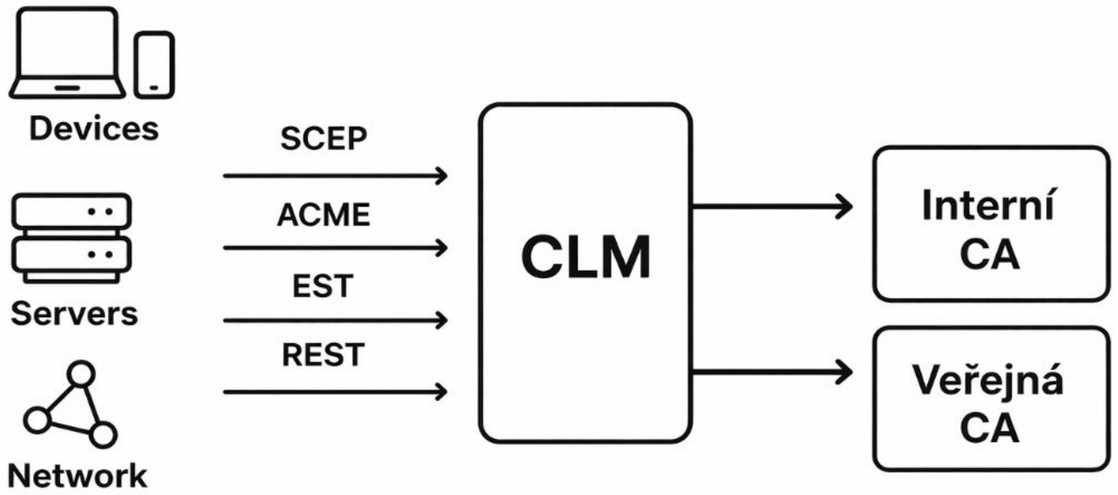


Full Lifecycle Automation

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

- CLM jako ACME / SCEP / EST Server, resp. online registrační autorita
  - slouží jako prostředník mezi klienty ACME / SCEP / EST a certifikačními autoritami
- možnost napojení ne interní i veřejnou CA



Protokoly pro automatizovanou správu certifikátů – stručně

- **ACME (Automated Certificate Management Environment)**
  - Protokol pro **plně automatizované vydávání a obnovu certifikátů** bez lidského zásahu.
    Typicky používaný pro **TLS certifikáty serverů, API a cloudové služby**.

- **SCEP (Simple Certificate Enrollment Protocol)**
  - Starší protokol pro **automatizované vydávání certifikátů zařízení**.
    Často používaný pro **MDM, Wi-Fi, VPN, síťová a mobilní zařízení**.

- **EST (Enrollment over Secure Transport)**
  - Modernější nástupce SCEP pro **bezpečné vydávání certifikátů přes TLS**.
  - Silnější bezpečnost, lepší ověření identity než SCEP

MONET+ EST / SCEP / ACME

- desítky tisíc aktivních prvků spravovaných CLM MONET+
- např. kritická infrastruktura státu
- veřejné i státní subjekty

Manuální vydání certifikátu

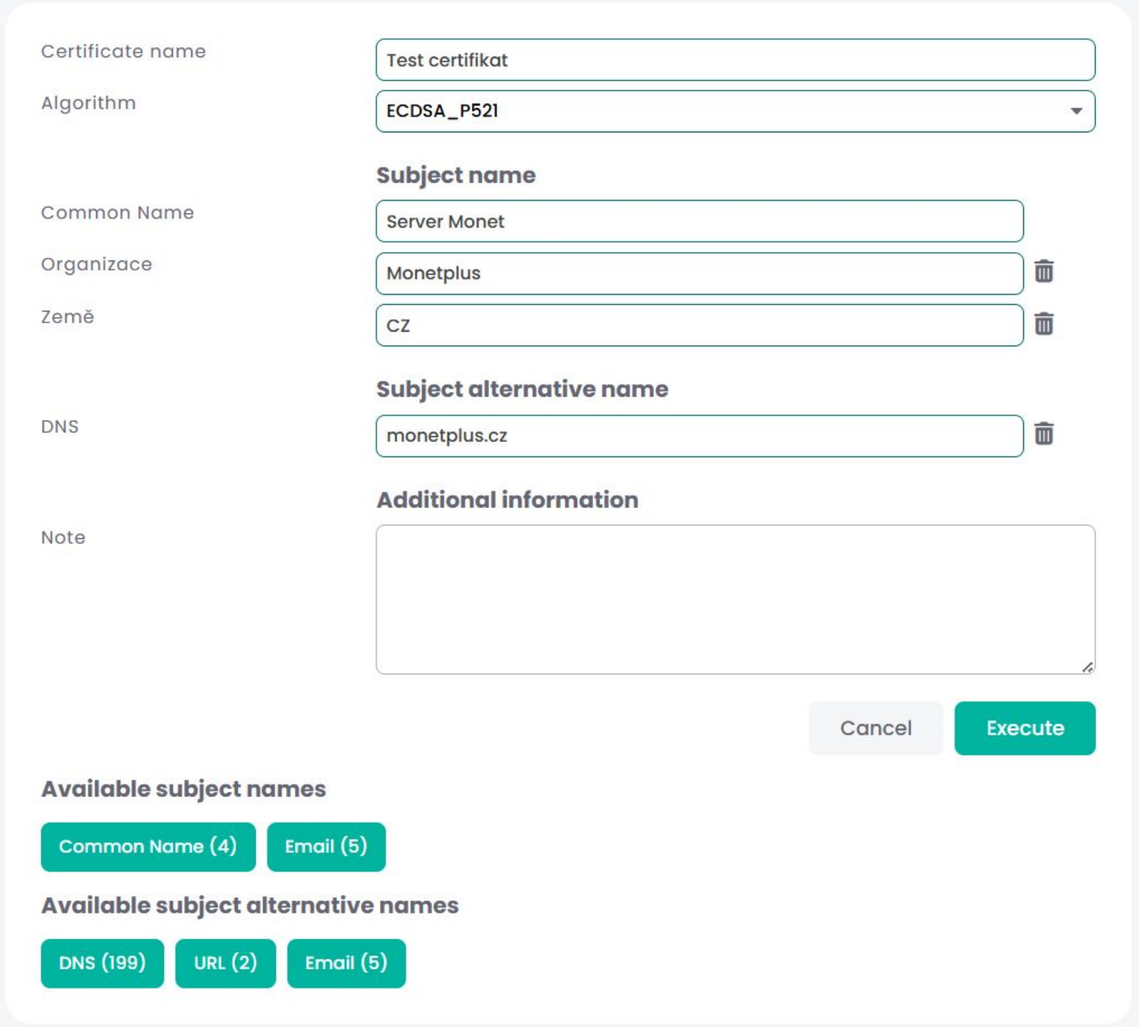
Generování klíčů v CLM

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

Importem vytvořené žádosti o certifikát

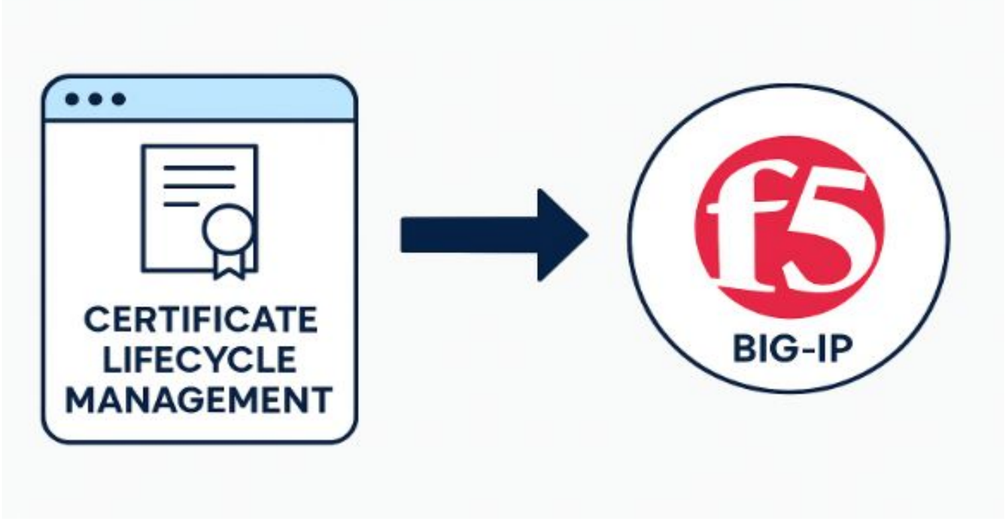
- ze souboru
- textem CSR (base64 / PEM)

Interní CA i veřejná CA (ACME CA)



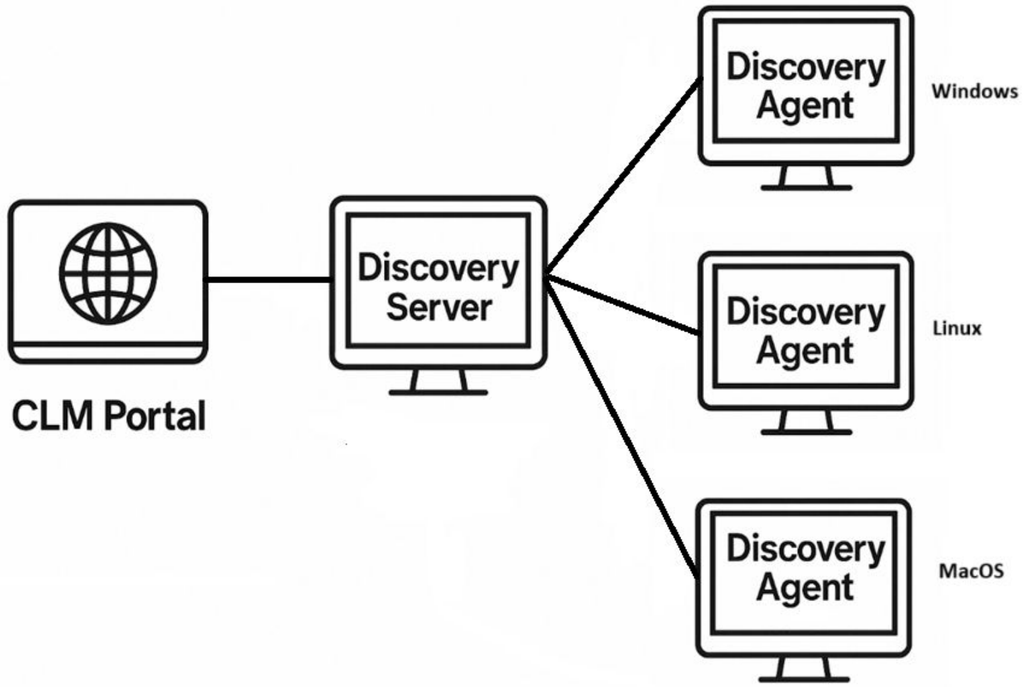
F5 management

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



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



Security & Compliance v MONET+ CLM

CLM systém vynucuje bezpečnostní a compliance pravidla v celém životním cyklu certifikátu:

- **Validace žádostí o certifikát**
  Kontrola obsahu CSR / požadavku (Subject, SAN, typ certifikátu, účel použití)

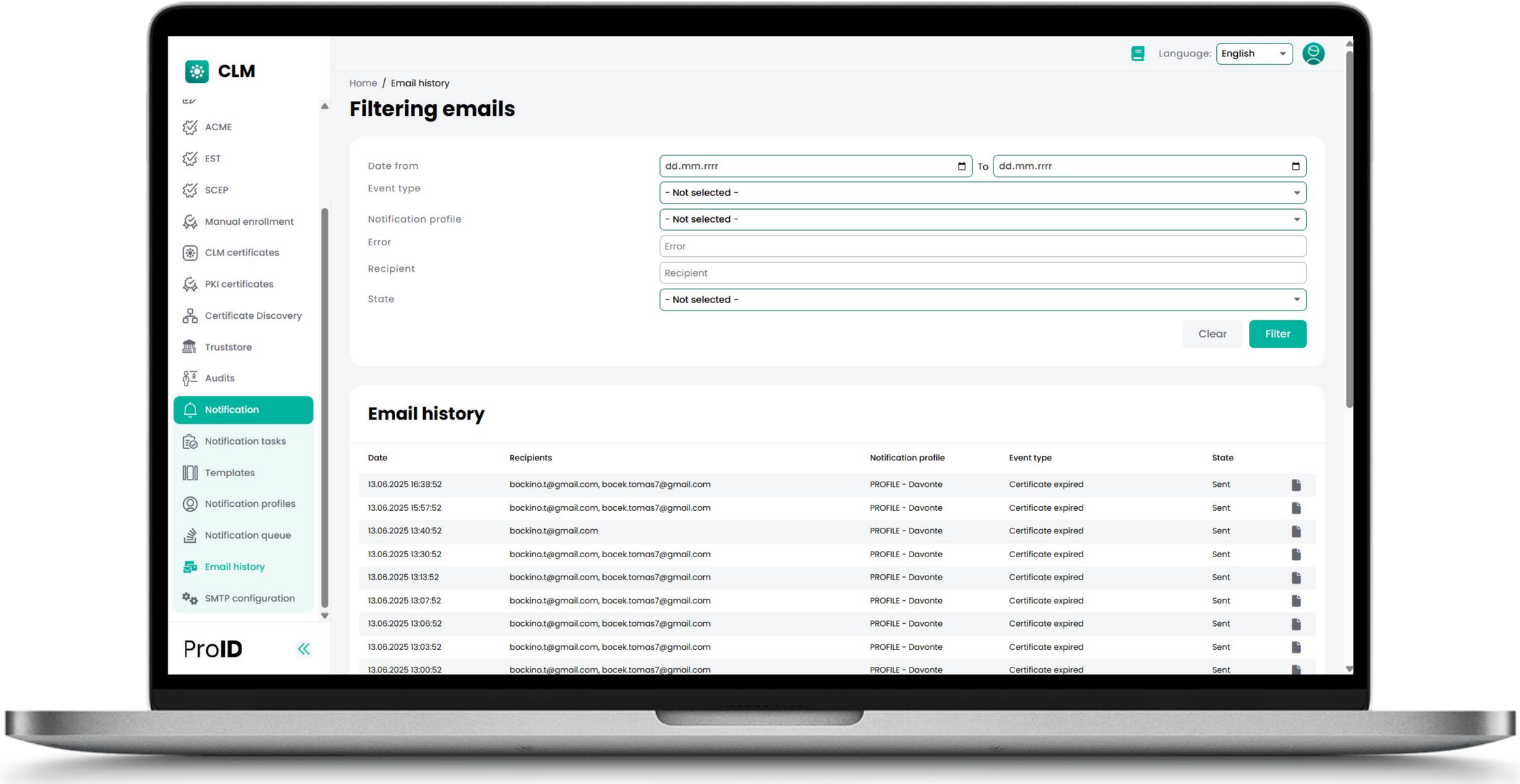
- **Kryptografická politika**
  - povolené algoritmy (RSA, ECC)
  - minimální délky klíčů
  - zákaz slabé nebo nevyhovující kryptografie

- **Policy enforcement**
  Vydání certifikátu je možné pouze při splnění definovaných bezpečnostních pravidel

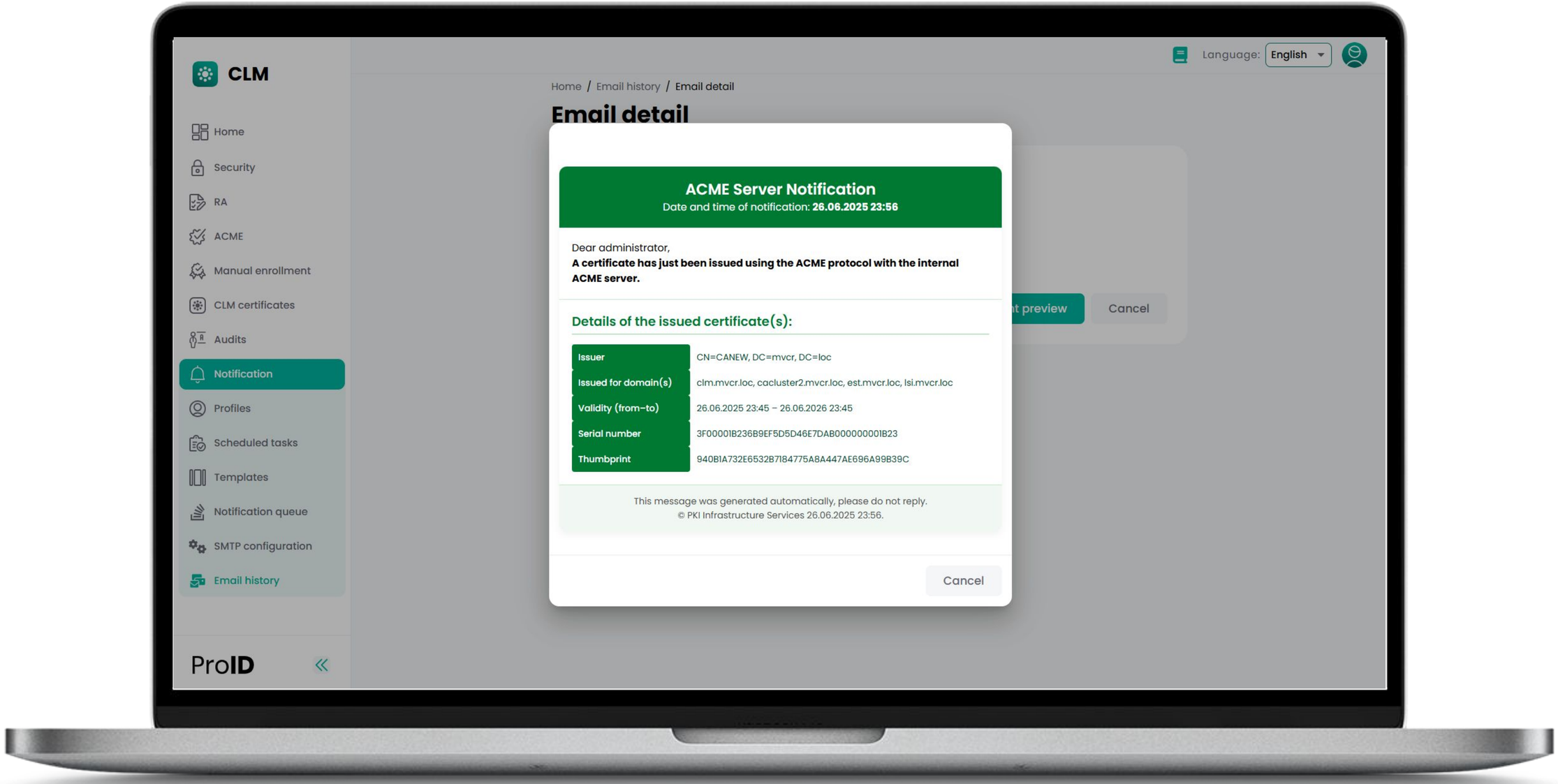
- **Prevence chyb a rizik**
  Zamezení vydání nekompatibilních, slabých nebo neautorizovaných certifikátů

- **Auditovatelnost**
  Všechny kontroly a rozhodnutí jsou logovány pro audit a compliance účely

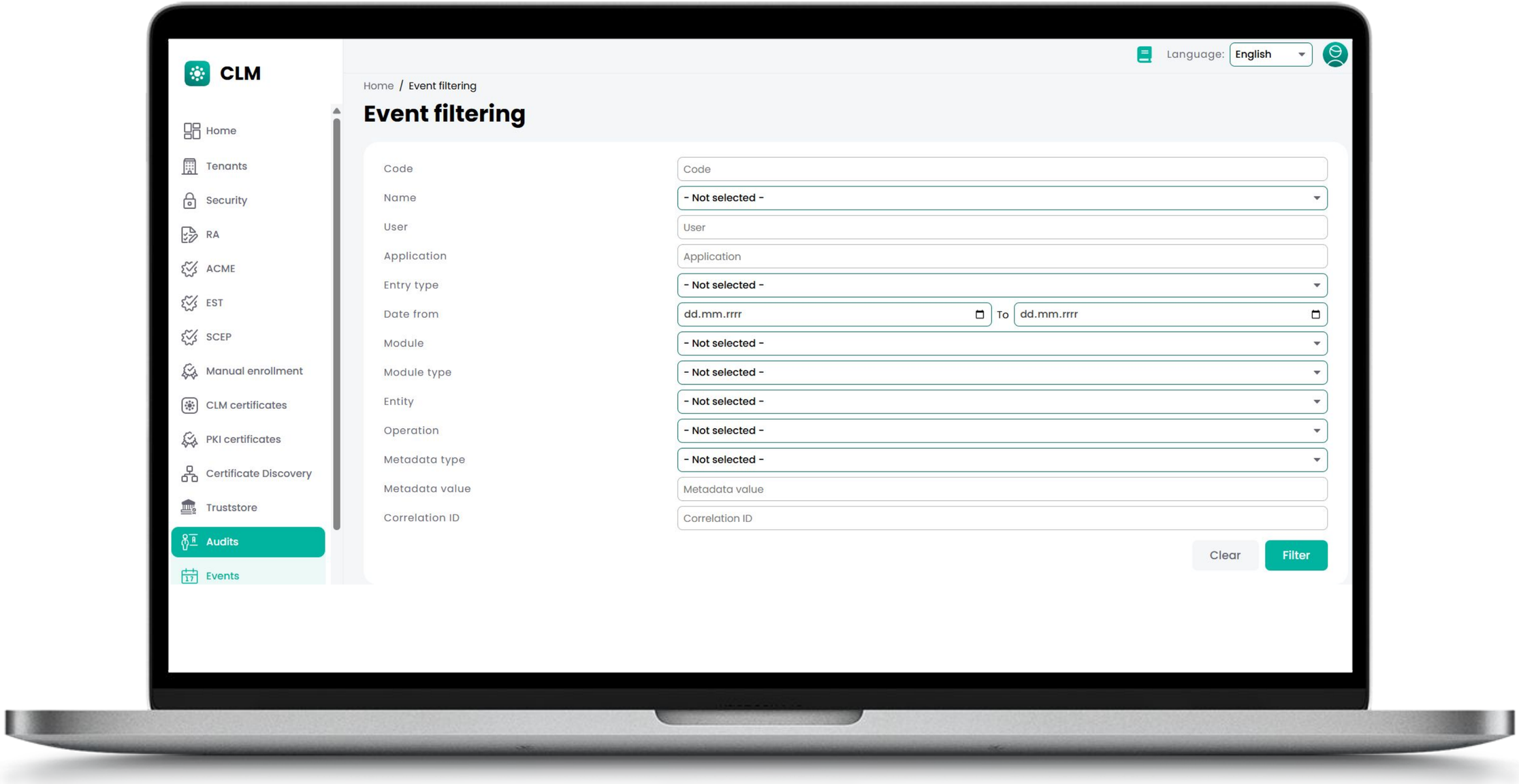
Notifikace


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
Error
Recipient
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

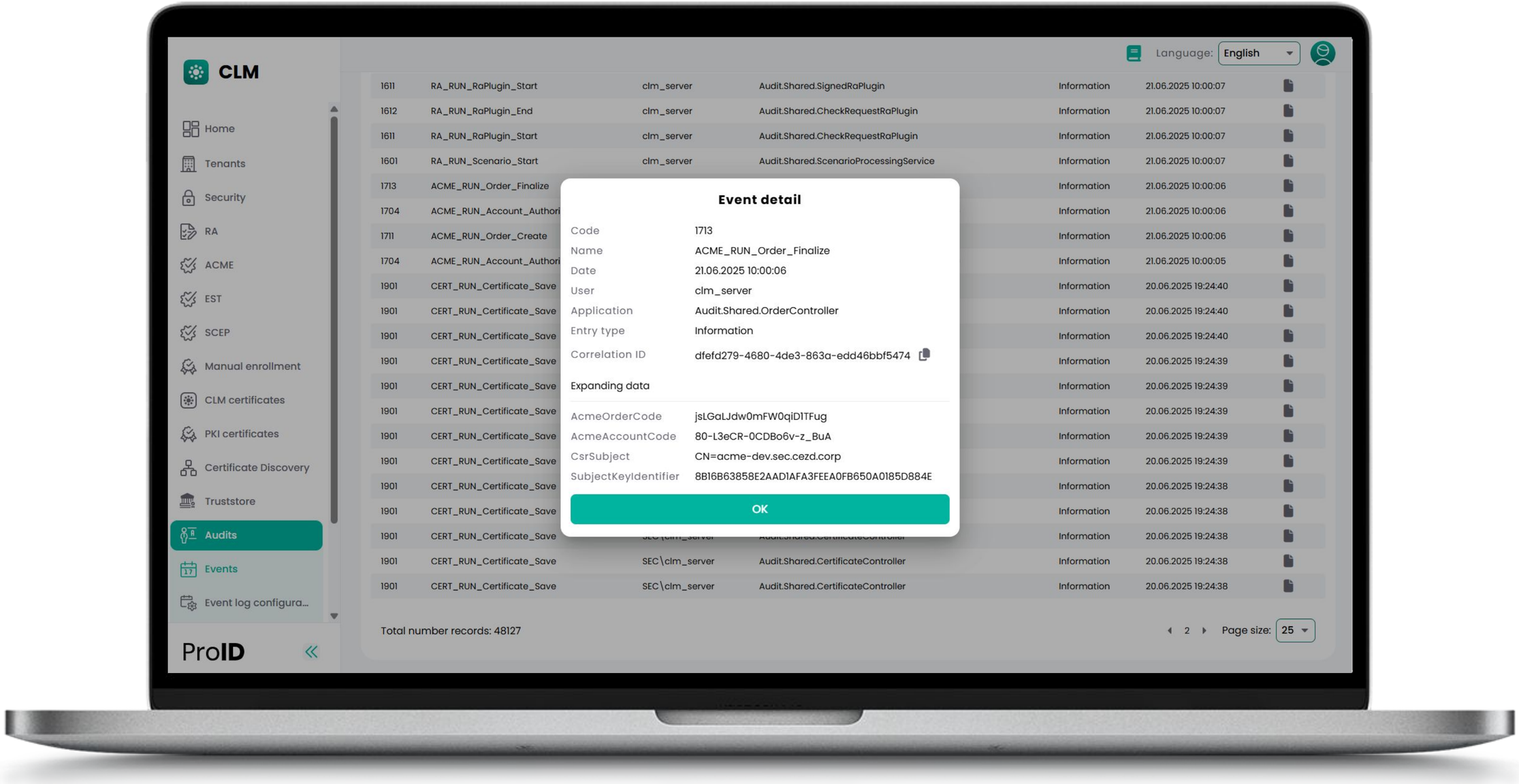
Notifikace


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
Home
Tenants
Security
RA
ACME
EST
SCEP
Manual enrollment
CLM certificates
PKI certificates
Certificate Discovery
Truststore
Audits
Events
Event log configura...
ProID
Language: English
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
Total number records: 48127
2
Page size: 25
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

Děkuji!

proid.cz