

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 +

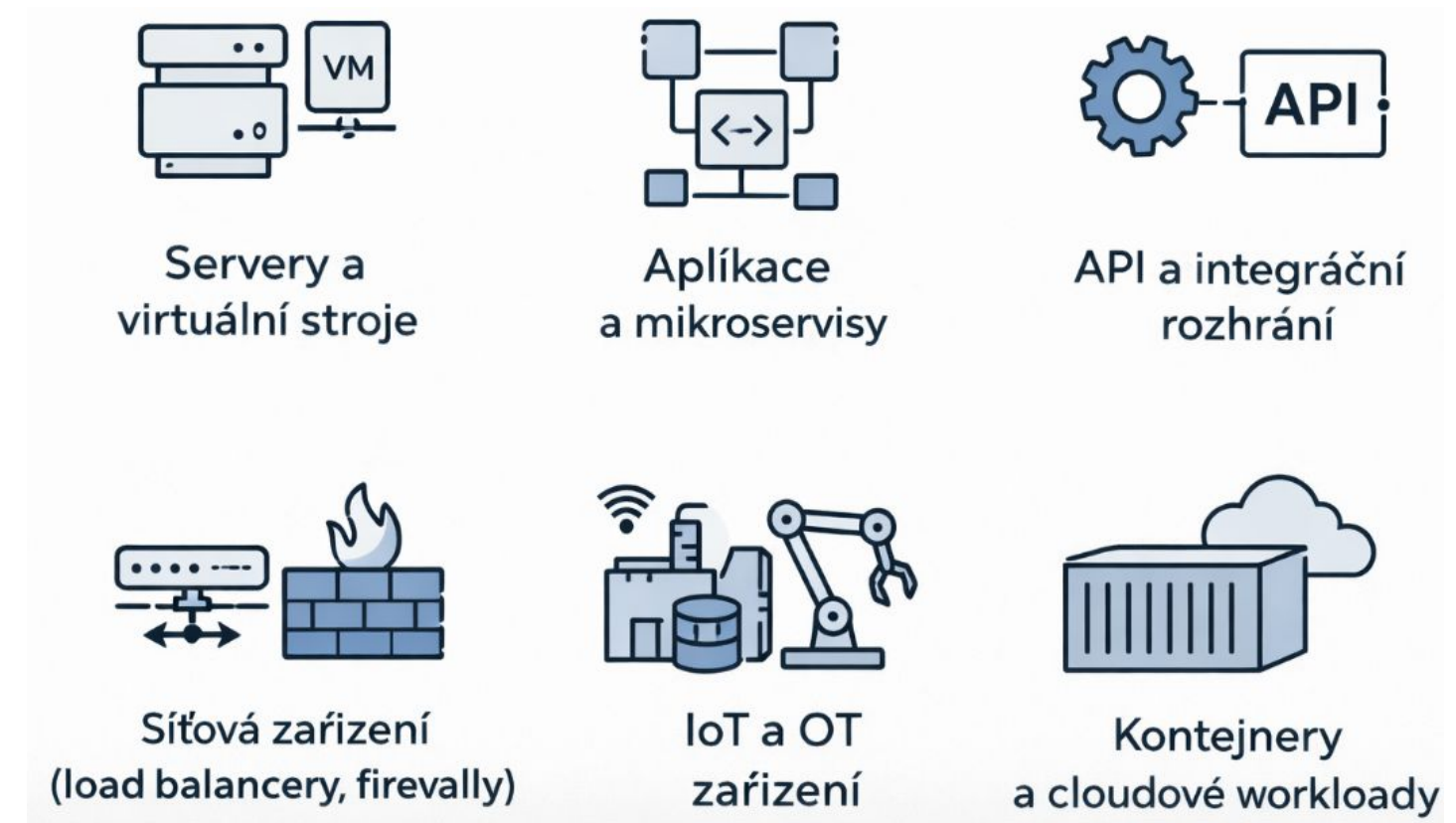
Technologická identita

- **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 expirací 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.

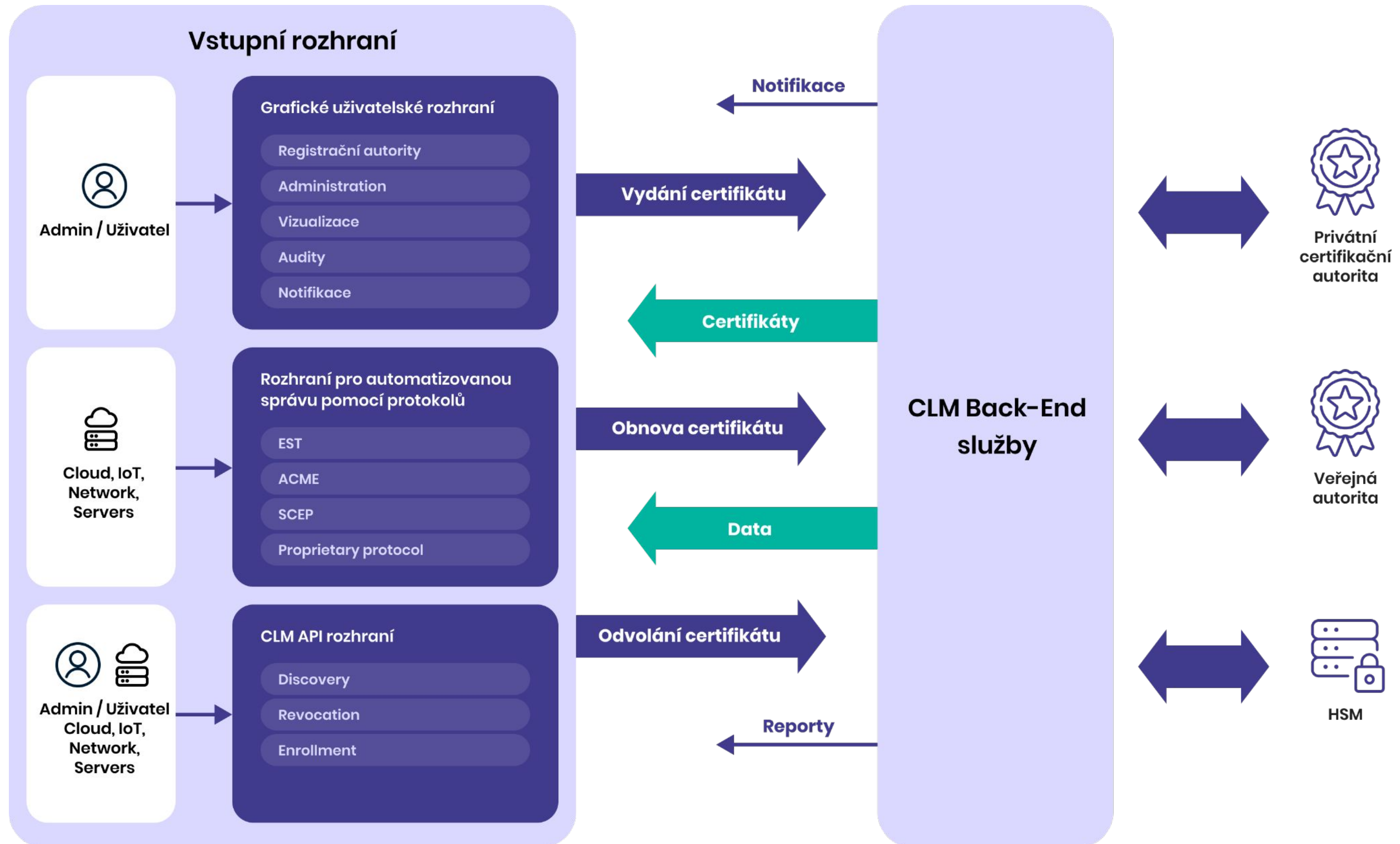
Kompletní životní cyklus certifikátu

- 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:
 - interními 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

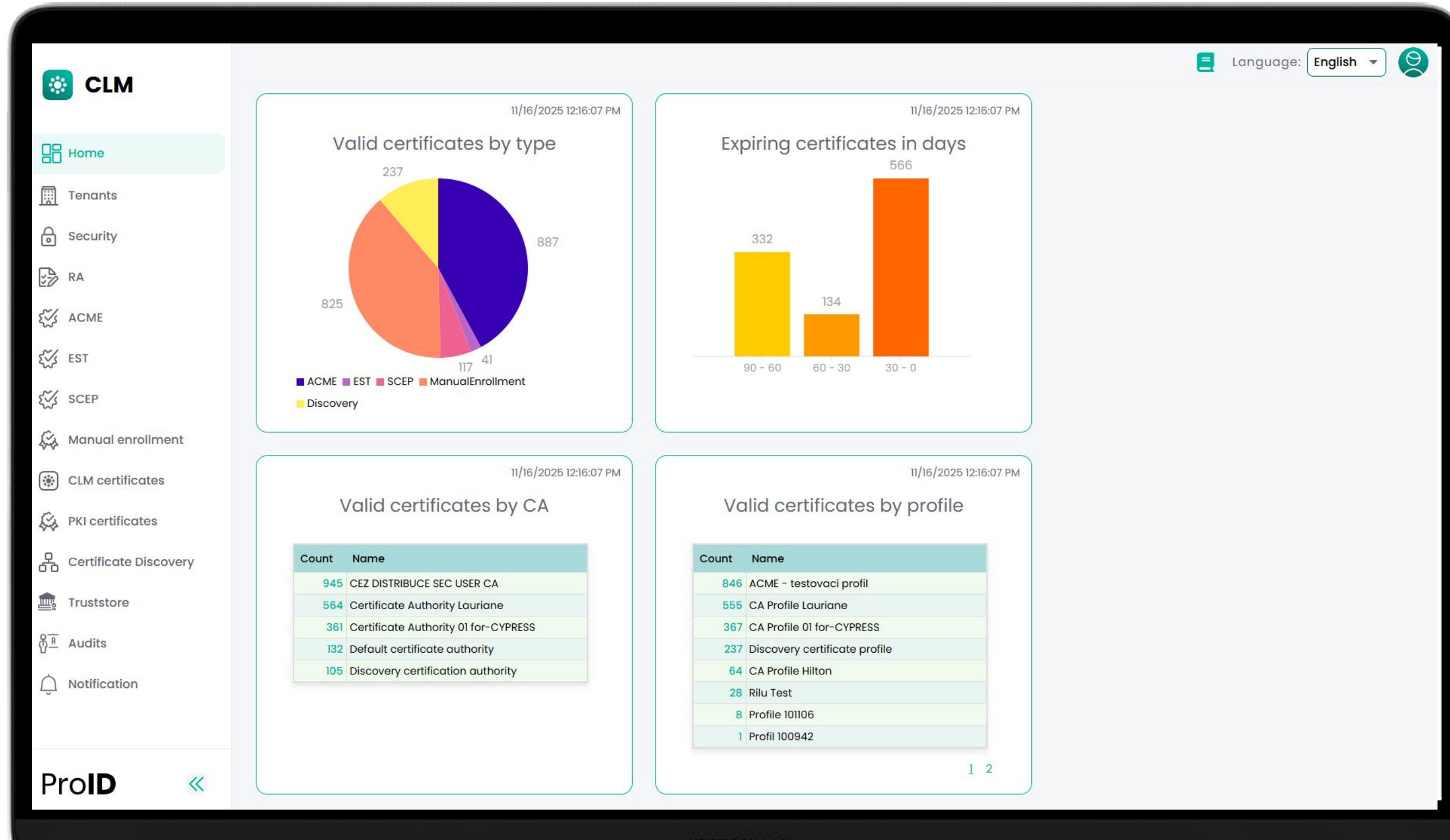
Filtrování certifikátů

Přehledy a reporty

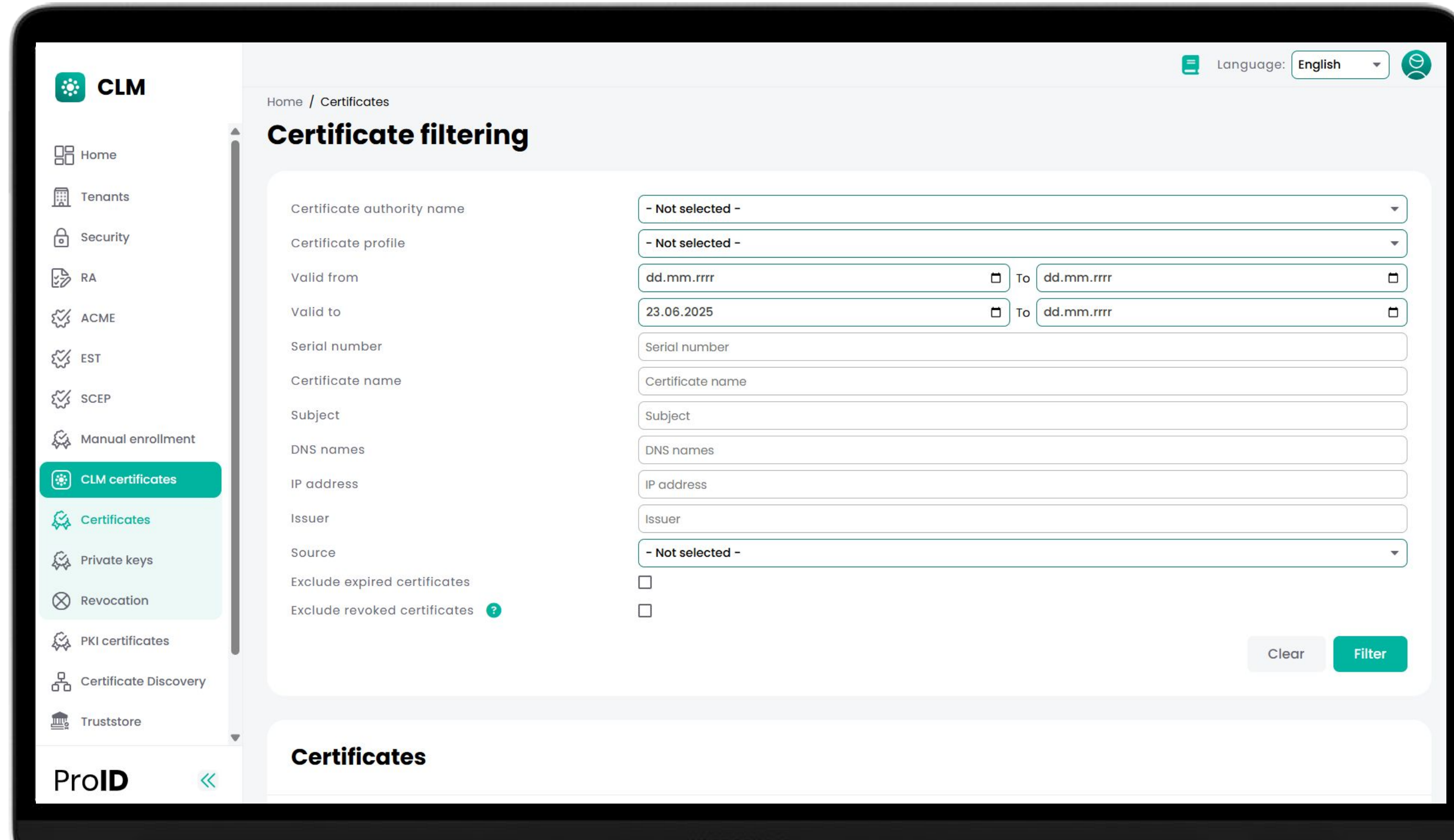
Validace žádostí o certifikát

Autorizace žádostí o certifikát

Visibility & Discovery



Visibility & Discovery



Visibility & Discovery

The screenshot displays the CLM interface on a laptop. The left sidebar contains navigation options: Home, Security, RA, ACME, Manual enrollment, CLM certificates (highlighted), Certificates, Private keys, Revocation, Audits, and Notification. The top right shows a language dropdown set to 'English' and a user profile icon. The main content area is divided into two sections: 'Certificate authority name' and 'Extensions'.

CLM

Language: English

Certificate authority name
CANEW

Serial number	3F00001B1239285A51429C59D3000000001B12
Revoked	No
Valid from	6/20/2025 9:47:20 AM
Valid to	6/20/2026 9:47:20 AM
Subject	CN=clm.mvcr.loc
Simple name	clm.mvcr.loc
Thumbprint	DIAD9004115658B89279FB499D0B5288319AEB3
Issuer	CN=CANEW, DC=mvcr, DC=loc
Source	ACME
Private key	No

Download certificate
Revoke certificate

Extensions

UPN name	
Email name	
DNS names	clm.mvcr.loc, cacluster2.mvcr.loc, est.mvcr.loc, lsi.mvcr.loc
IP address	
URL name	
Template	1.3.6.1.4.1.311.21.8.14192724.4682562.14827945.714657.14454345.186.6783213.9287898
Subject key ID	B1A1112363A117DC2E88714D252115E7AA17A3AF
Auth key ID	05 79 5E 88 DB 36 F3 27 5A 0E 60 13 A6 96 DB EE B3 94 C1 27

ProID <<

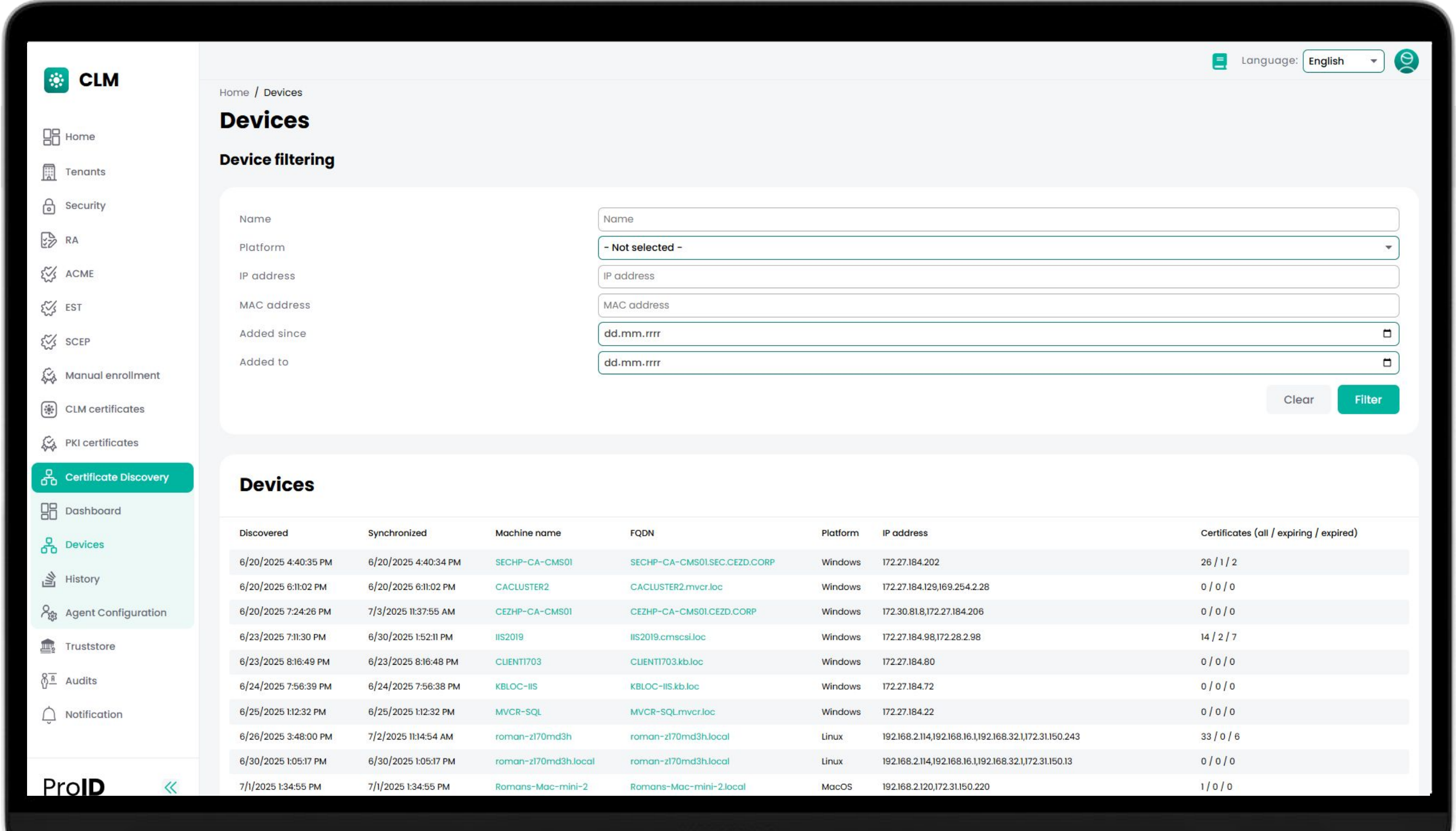
Discovery Across Environment

The dashboard displays the following data:

- All discovered certificates:** A bar chart showing 108 All, 93 Valid, 3 Expiring, and 0 Expired certificates as of 7/3/2025 8:51:33 AM.
- Expiring certificates in days:** A pie chart showing 1 certificate in the 0-30 day range, 2 in the 30-60 day range, and 1 in the 60-90 day range as of 7/3/2025 8:51:33 AM.
- Number of devices by platform:** A bar chart showing 7 Windows, 3 Linux, and 1 MacOS device as of 7/2/2025 11:37:50 AM.

The interface includes a sidebar with navigation options: Security, RA, ACME, EST, SCEP, Manual enrollment, CLM certificates, PKI certificates, Certificate Discovery (selected), Dashboard, Devices, History, Agent Configuration, Truststore, Audits, and Notification. The bottom left shows 'ProID' and a back arrow. The top right shows 'Language: English' and a user profile icon.

Discovery Across Environment



- CLM
- Home
- Tenants
- Security
- RA
- ACME
- EST
- SCEP
- Manual enrollment
- CLM certificates
- PKI certificates
- Certificate Discovery
- Dashboard
- Devices
- History
- Agent Configuration
- Truststore
- Audits
- Notification

Home / Devices

Devices

Device filtering

Name	<input type="text" value="Name"/>
Platform	<input type="text" value="- Not selected -"/>
IP address	<input type="text" value="IP address"/>
MAC address	<input type="text" value="MAC address"/>
Added since	<input type="text" value="dd.mm.rrrr"/>
Added to	<input type="text" value="dd.mm.rrrr"/>

Devices

Discovered	Synchronized	Machine name	FQDN	Platform	IP address	Certificates (all / expiring / expired)
6/20/2025 4:40:35 PM	6/20/2025 4:40:34 PM	SECHP-CA-CMS01	SECHP-CA-CMS01.SEC.CEZD.CORP	Windows	172.27.184.202	26 / 1 / 2
6/20/2025 6:11:02 PM	6/20/2025 6:11:02 PM	CACLUSTR2	CACLUSTR2.mvcr.loc	Windows	172.27.184.129,169.254.2.28	0 / 0 / 0
6/20/2025 7:24:26 PM	7/3/2025 11:37:55 AM	CEZHP-CA-CMS01	CEZHP-CA-CMS01.CEZD.CORP	Windows	172.30.81.8,172.27.184.206	0 / 0 / 0
6/23/2025 7:11:30 PM	6/30/2025 1:52:11 PM	IIS2019	IIS2019.cmscsl.loc	Windows	172.27.184.98,172.28.2.98	14 / 2 / 7
6/23/2025 8:16:49 PM	6/23/2025 8:16:48 PM	CUENTI703	CUENTI703.kb.loc	Windows	172.27.184.80	0 / 0 / 0
6/24/2025 7:56:39 PM	6/24/2025 7:56:38 PM	KBLOC-IIS	KBLOC-IIS.kb.loc	Windows	172.27.184.72	0 / 0 / 0
6/25/2025 1:12:32 PM	6/25/2025 1:12:32 PM	MVCR-SQL	MVCR-SQL.mvcr.loc	Windows	172.27.184.22	0 / 0 / 0
6/26/2025 3:48:00 PM	7/2/2025 11:14:54 AM	roman-z170md3h	roman-z170md3h.local	Linux	192.168.2.114,192.168.16.1,192.168.32.1,172.31.150.243	33 / 0 / 6
6/30/2025 1:05:17 PM	6/30/2025 1:05:17 PM	roman-z170md3h.local	roman-z170md3h.local	Linux	192.168.2.114,192.168.16.1,192.168.32.1,172.31.150.13	0 / 0 / 0
7/1/2025 1:34:55 PM	7/1/2025 1:34:55 PM	Romans-Mac-mini-2	Romans-Mac-mini-2.local	MacOS	192.168.2.120,172.31.150.220	1 / 0 / 0

Discovery Across Environment

CLM

Language: English

- Home
- Tenants
- Security
- RA
- ACME
- EST
- SCEP
- Manual enrollment
- CLM certificates
- PKI certificates
- Certificate Discovery
- Dashboard
- Devices
- History
- Agent Configuration
- Truststore
- Audits
- Notification

ProID
<<

Device

Machine name	SECHP-CA-CMS01
FQDN	SECHP-CA-CMS01.SEC.CEZD.CORP
Platform	Windows
IP address	172.27.184.202
Created	6/20/2025 4:40:34 PM
Domain	SEC.CEZD.CORP
Type	VirtualMachine
Manufacturer	vmware, inc.
Model	vmware7,1
Architecture	X64
Version	Microsoft Windows Server 2022 Standard
Role	Server
Virtual	True
Hypervisor host	False
MAC address	00505692881E
UID	cabe0cd7-5cba-4274-bdf7-d799db708065

[Show less...](#)

Serial number	Subject	Issuer	DNS names	IP address	Valid from	Valid to
6C0000A75D659208F65C107CFE0000000A75D	CN=acme-dev.sec.cezd.corp	CN=CEZ DISTRIBUCE SEC USER CA, O=CEZ Distribuce a...	acme-dev.sec.cezd.corp, acmeclient.sec.cezd.corp, ...		6/28/2025 10:37:31 AM	6/28/2026 10:37:31 AM
18E84DE3	SERIALNUMBER=IC-27112489, OID.2.5.4.97=VATCZ-27112...	CN=TEST - ACAeID - Qualified Issuing Certificate (...)			4/1/2025 7:49:21 AM	4/1/2026 7:49:21 AM
490000046068FD6FFD2A5E5780000100000460	CN=TBO CertRegApi Login, C=CZ	CN=KB Interni CA Osobni, O=Komerční banka a.s., C=...			8/11/2023 1:04:27 PM	8/10/2025 1:04:27 PM
6C0000A6D3B32AFE21308AA65C0000000A6D3	CN="CN=DTSXD-DPU-20230926-1.dts.cezd.corp", SERIAL...	CN=CEZ DISTRIBUCE SEC USER CA, O=CEZ Distribuce a...			6/23/2025 1:52:11 PM	6/23/2027 2:52:11 PM
490000013005A37476EC4616900000000013	CN=Monet Renewal Test CA, O=Monet, C=CZ	CN=KB Root 3 CA, O="Komerční banka, a.s.", OID.2.5...			1/2/2025 10:04:28 AM	1/20/2025 10:04:28 AM
6C0000A68199C7E7C854D8A21300000000A681	CN="CN=DTSXD-DPU-20230926-1.dts.cezd.corp", SERIAL...	CN=CEZ DISTRIBUCE SEC USER CA, O=CEZ Distribuce a...			6/13/2025 3:29:22 PM	6/13/2027 3:29:22 PM
6F0000016F9777DD527C35C6C00000000016	CN=CEZ DISTRIBUCE SEC USER CA, O=CEZ Distribuce a...	CN=CEZ Root CA2, O="CEZ, a.s.", C=CZ			3/24/2022 2:03:21 PM	3/24/2032 2:03:21 PM
361F27F3F130B993475C898F5A8D9EB1	CN=CEZ Root CA2, O="CEZ, a.s.", C=CZ	CN=CEZ Root CA2, O="CEZ, a.s.", C=CZ			7/10/2019 9:42:48 AM	7/10/2039 9:42:48 AM
6C0000A64660B30468927469E10000000A646	CN=clm-auto.sec.cezd.corp	CN=CEZ DISTRIBUCE SEC USER CA, O=CEZ Distribuce a...	clm-auto.sec.cezd.corp		6/4/2025 5:28:34 PM	6/4/2027 5:28:34 PM
6C00008E402D39A0F950A53712000000008E40	CN=Acme CSR Signature	CN=CEZ DISTRIBUCE SEC USER CA, O=CEZ Distribuce a...			10/31/2023 12:38:29 PM	10/30/2025 12:38:29 PM

Discovery Across Environment

CLM

Home / Devices

Certificate Discovery History

History filtering

Device:

Operation:

Added since:

Added to:

Date	Operation	Device	Certificate
7/1/2025 3:35:26 PM	Certificate linked to device	roman-zl70md3h.local	3679CA35668772304D30A5FB873B0FA77BB70D54
7/1/2025 3:35:25 PM	Certificate linked to device	roman-zl70md3h.local	3BC0380B33C3F6A60C86152293D9DF54B81C004
7/1/2025 3:35:24 PM	Certificate linked to device	roman-zl70md3h.local	D8EB6B41519259E0F3E78500C03DB68897C9EEFC
7/1/2025 3:35:23 PM	Certificate linked to device	roman-zl70md3h.local	76E27EC14FDB82C1C0A675B505BE3D29B4EDDBBB
7/1/2025 3:35:23 PM	Certificate linked to device	roman-zl70md3h.local	37F76DE6077C90C5B13E931AB74110B4F2E49A27
7/1/2025 3:35:22 PM	Certificate linked to device	roman-zl70md3h.local	74F8A3C3EFE7B390064B83903C21646020E5DFCE
7/1/2025 3:35:21 PM	Certificate linked to device	roman-zl70md3h.local	2A1D6027D94AB10A1C4D915CCD33A0CB3E2D54CB
7/1/2025 3:35:21 PM	Certificate linked to device	roman-zl70md3h.local	30D4246F07FFDB91898A0BE9496611EB8C5E46E5
7/1/2025 3:35:21 PM	Certificate linked to device	roman-zl70md3h.local	D273962A2A5E399F733FE1C71E643F033834FC4D
7/1/2025 3:35:21 PM	Certificate linked to device	roman-zl70md3h.local	E1C950E6EF22F84C5645728B922060D7D5A7A3E8
7/1/2025 3:35:20 PM	Certificate linked to device	roman-zl70md3h.local	75E0ABB6138512271C04F85FDDDE38E4B7242EFE
7/1/2025 3:35:20 PM	Certificate linked to device	roman-zl70md3h.local	6969562E4080F424A1E7199F14BAF3EE58AB6ABB
7/1/2025 3:35:20 PM	Certificate linked to device	roman-zl70md3h.local	8D1784D537F3037DEC70FE578B519A99E610D7B0
7/1/2025 3:35:20 PM	Certificate linked to device	roman-zl70md3h.local	DE28F4A4FFE5892FA3C503DIA349A7F9962A8212
7/1/2025 3:35:19 PM	Certificate linked to device	roman-zl70md3h.local	5F43E5B1BF8788CACICC7CA4A9AC6222BCC34C6

- Home
- Tenants
- Security
- RA
- ACME
- EST
- SCEP
- Manual enrollment
- CLM certificates
- PKI certificates
- Certificate Discovery**
- Dashboard
- Devices
- History
- Agent Configuration
- Truststore
- Audits
- Notification

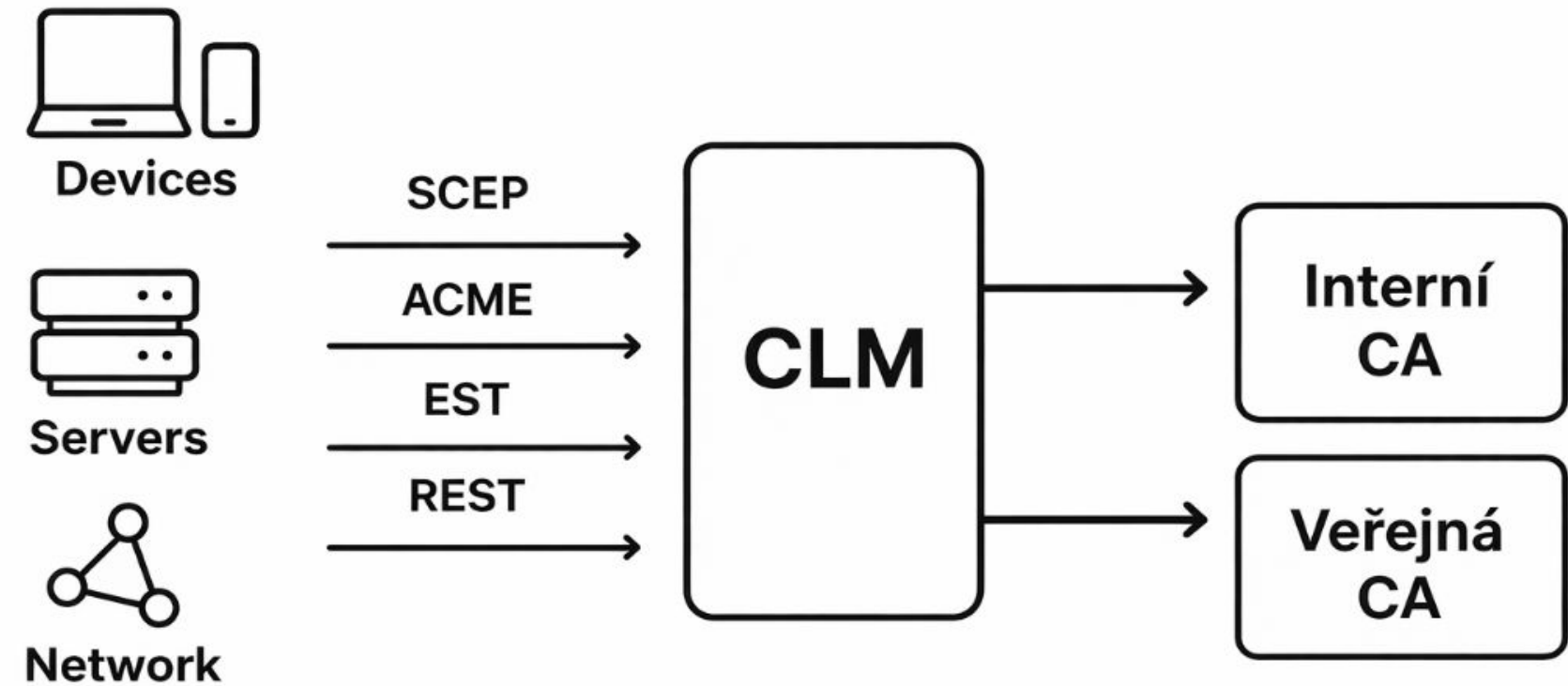
ProID <<

Language: English

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 na 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)

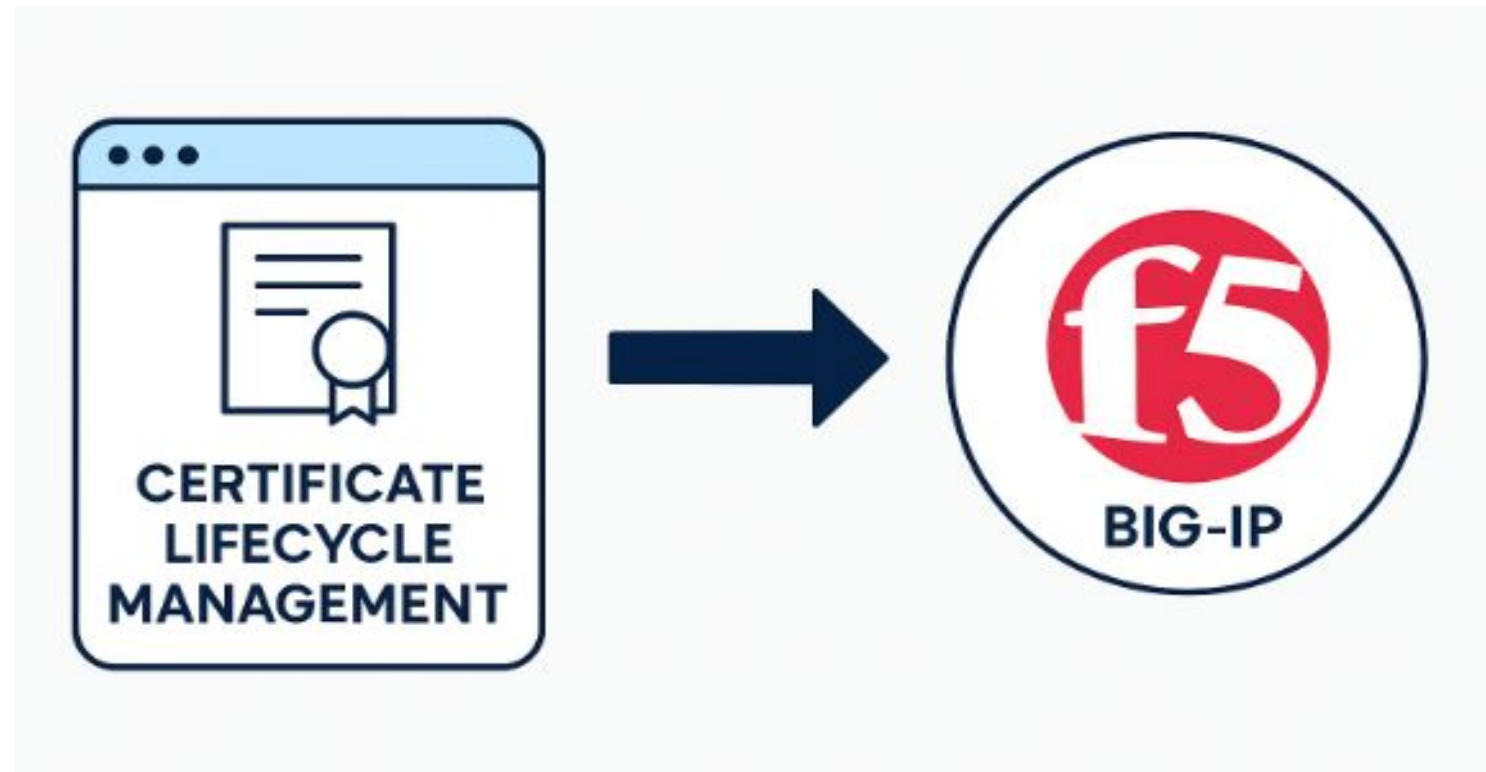
Certificate name	<input type="text" value="Test certifikat"/>
Algorithm	<input type="text" value="ECDSA_P521"/>
Subject name	
Common Name	<input type="text" value="Server Monet"/>
Organizace	<input type="text" value="Monetplus"/> 
Země	<input type="text" value="CZ"/> 
Subject alternative name	
DNS	<input type="text" value="monetplus.cz"/> 
Additional information	
Note	<input type="text"/>

Available subject names

Available subject alternative names

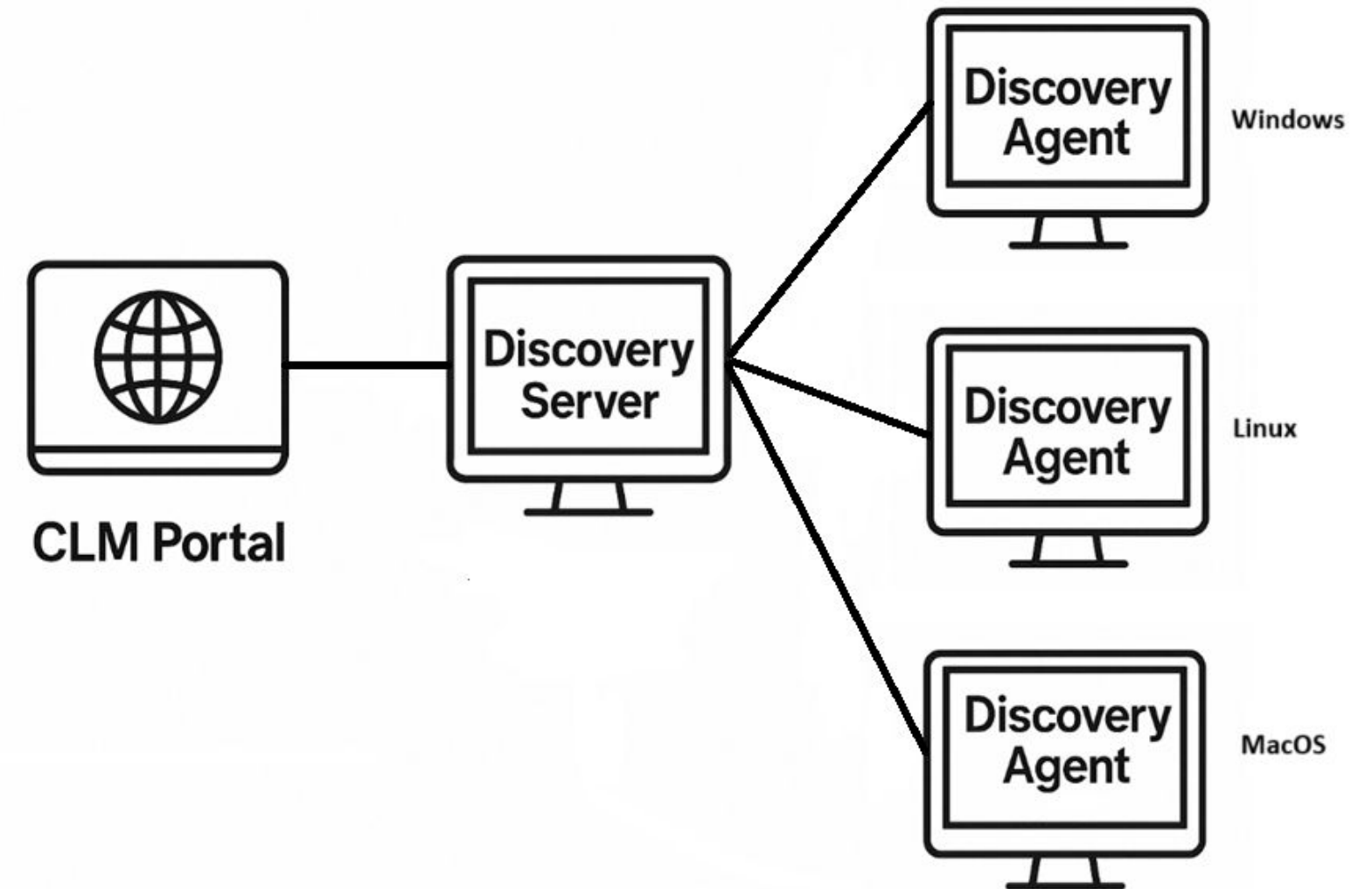
F5 management

- **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

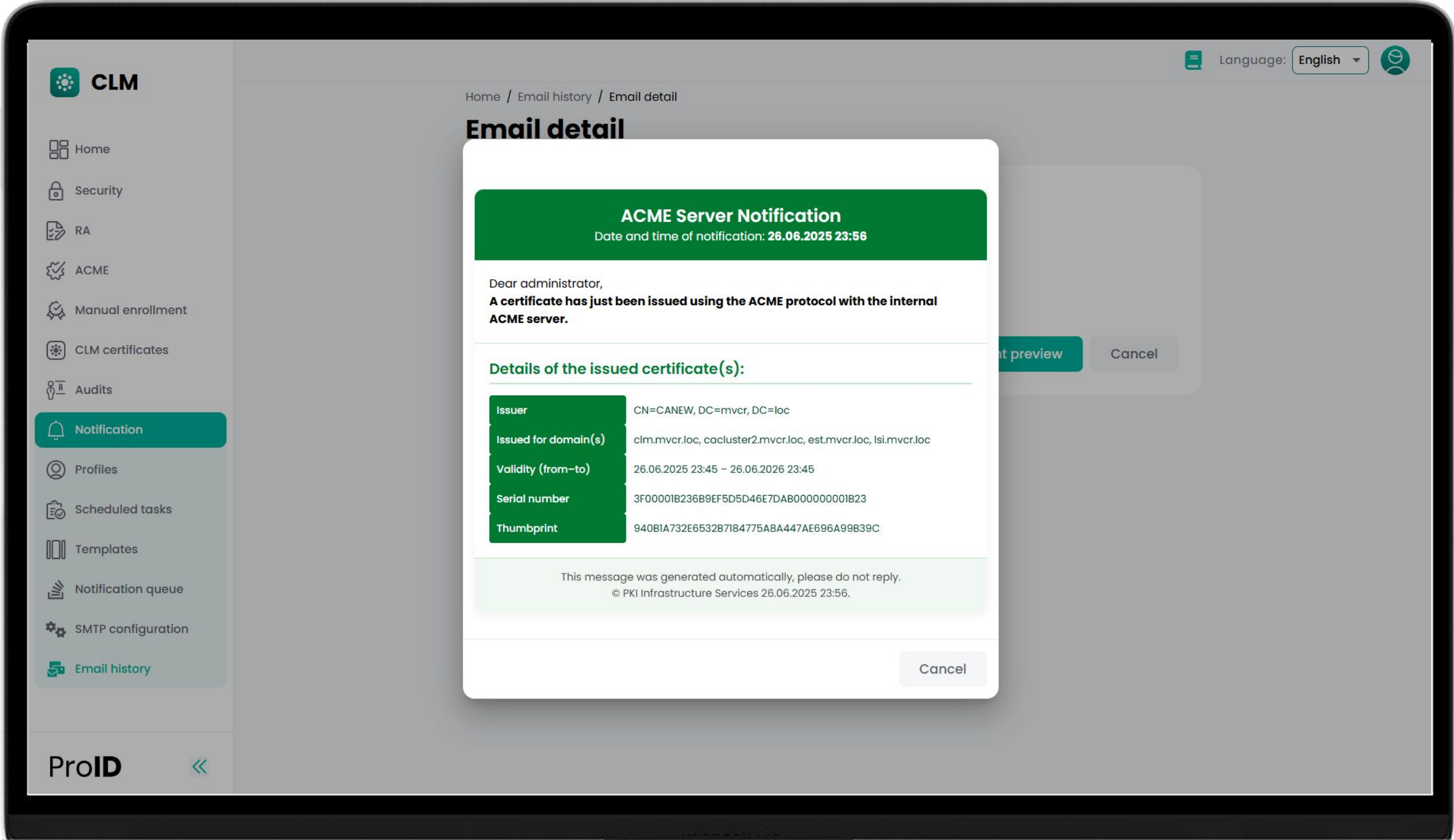
Notifikace

The screenshot displays the 'Notifikace' web application interface. On the left is a sidebar with the 'CLM' logo and a list of navigation items: ACME, EST, SCEP, Manual enrollment, CLM certificates, PKI certificates, Certificate Discovery, Truststore, Audits, Notification (highlighted), Notification tasks, Templates, Notification profiles, Notification queue, Email history, and SMTP configuration. The main content area is titled 'Home / Email history' and 'Filtering emails'. It contains a filtering panel with the following fields: 'Date from' and 'To' (both with date pickers and placeholder 'dd.mm.rrrr'), 'Event type' (dropdown: '- Not selected -'), 'Notification profile' (dropdown: '- Not selected -'), 'Error' (text input: 'Error'), 'Recipient' (text input: 'Recipient'), and 'State' (dropdown: '- Not selected -'). 'Clear' and 'Filter' buttons are at the bottom right of the panel. Below the panel is the 'Email history' section, which is a table with the following data:

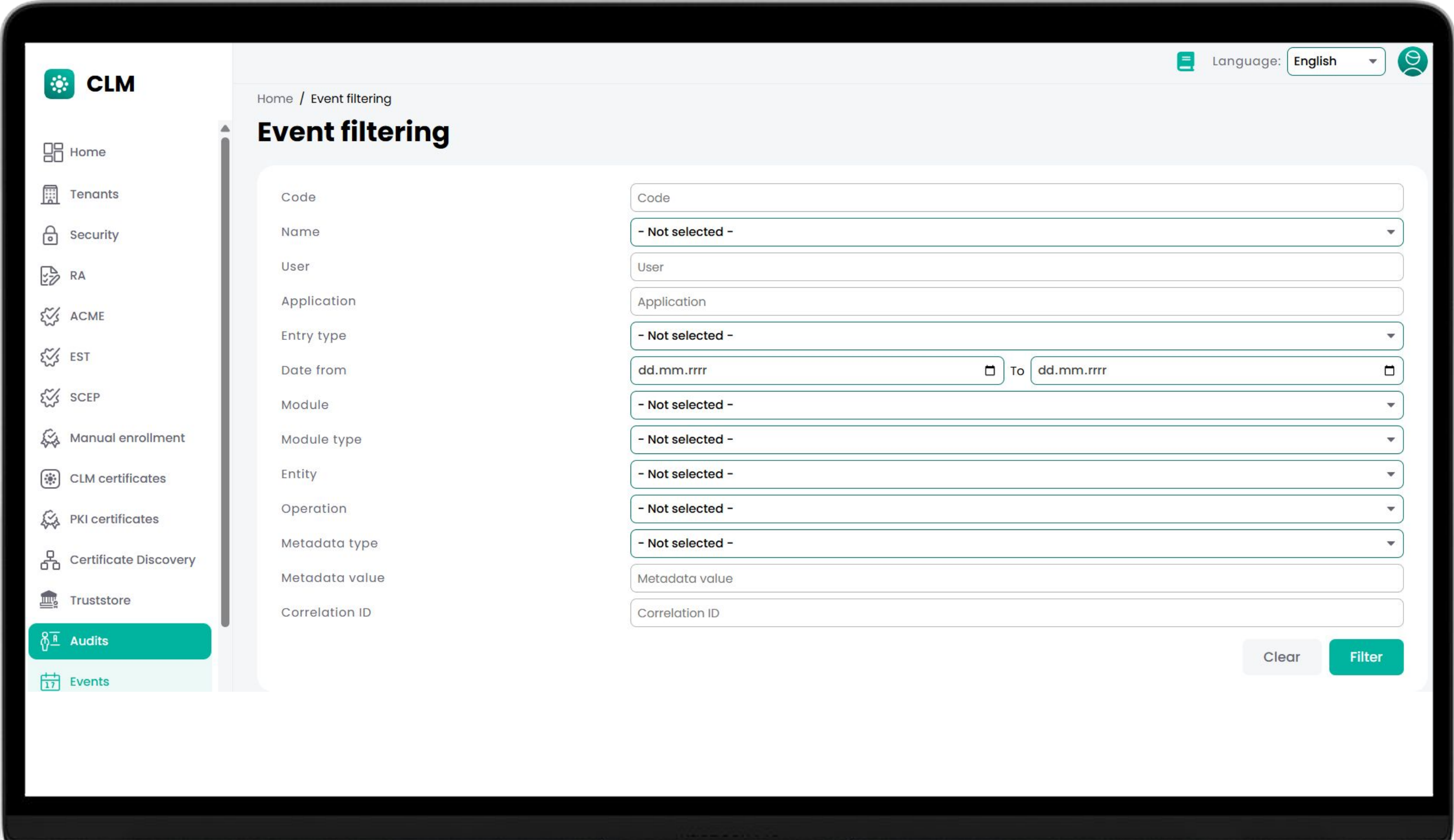
Date	Recipients	Notification profile	Event type	State	
13.06.2025 16:38:52	bockino.t@gmail.com, bocek.tomas7@gmail.com	PROFILE - Davonte	Certificate expired	Sent	
13.06.2025 15:57:52	bockino.t@gmail.com, bocek.tomas7@gmail.com	PROFILE - Davonte	Certificate expired	Sent	
13.06.2025 13:40:52	bockino.t@gmail.com	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	

At the bottom left of the interface, the 'ProID' logo and a double-left arrow icon are visible. The top right corner shows a language selector set to 'English' and a user profile icon.

Notifikace



Audit



Audit

The screenshot displays the CLM Audit interface. On the left is a navigation sidebar with the following items: Home, Tenants, Security, RA, ACME, EST, SCEP, Manual enrollment, CLM certificates, PKI certificates, Certificate Discovery, Truststore, **Audits** (highlighted), Events, and Event log configura... At the top right of the main area, there is a language dropdown set to 'English' and a user profile icon. The main area contains a table of audit events. A modal window titled 'Event detail' is open over one of the rows, showing the following information:

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	jsLGaLJdw0mFW0qiDITFug
AcmeAccountCode	80-L3eCR-0CDBo6v-z_BuA
CsrSubject	CN=acme-dev.sec.cezd.corp
SubjectKeyIdentifier	8B16B63858E2AAD1AFA3FEEA0FB650A0185D884E

At the bottom of the modal is an 'OK' button. The background table shows a list of events with columns for ID, Name, User, Application, Entry type, Date, and a download icon. At the bottom of the table, it says 'Total number records: 48127'. On the far right, there is a pagination control showing 'Page size: 25'.

Děkuji!

proid.cz