

MONET +

Životní cyklus klíčů a certifikátů

Jakub Kolařík

19. 11. 2025



Obsah

01 MONET+ Identity Solutions

02 Technical ID

03 Certificate Lifecycle Management

04 Key Management System

05 Dotazy / diskuze





**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.

0 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



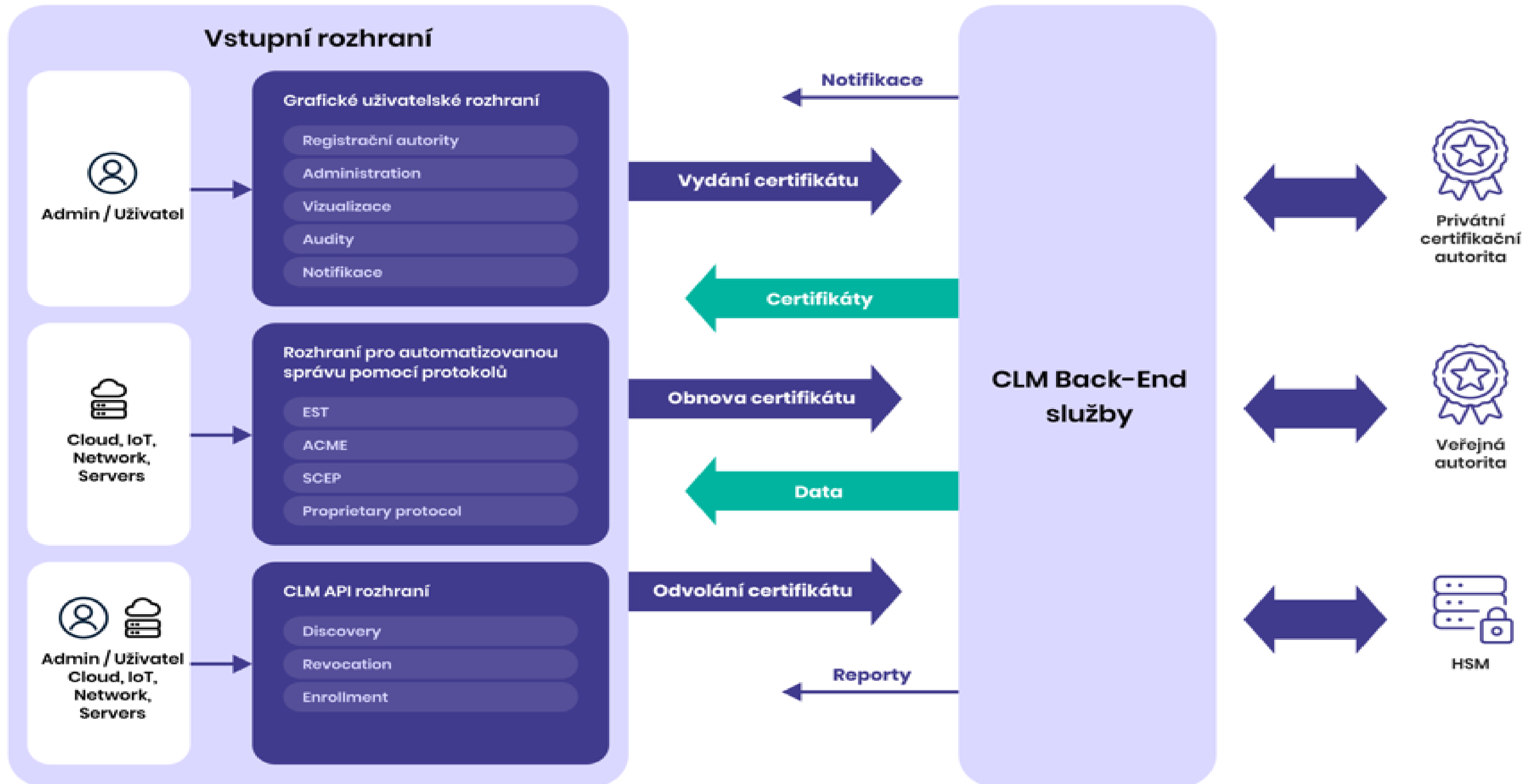
VS



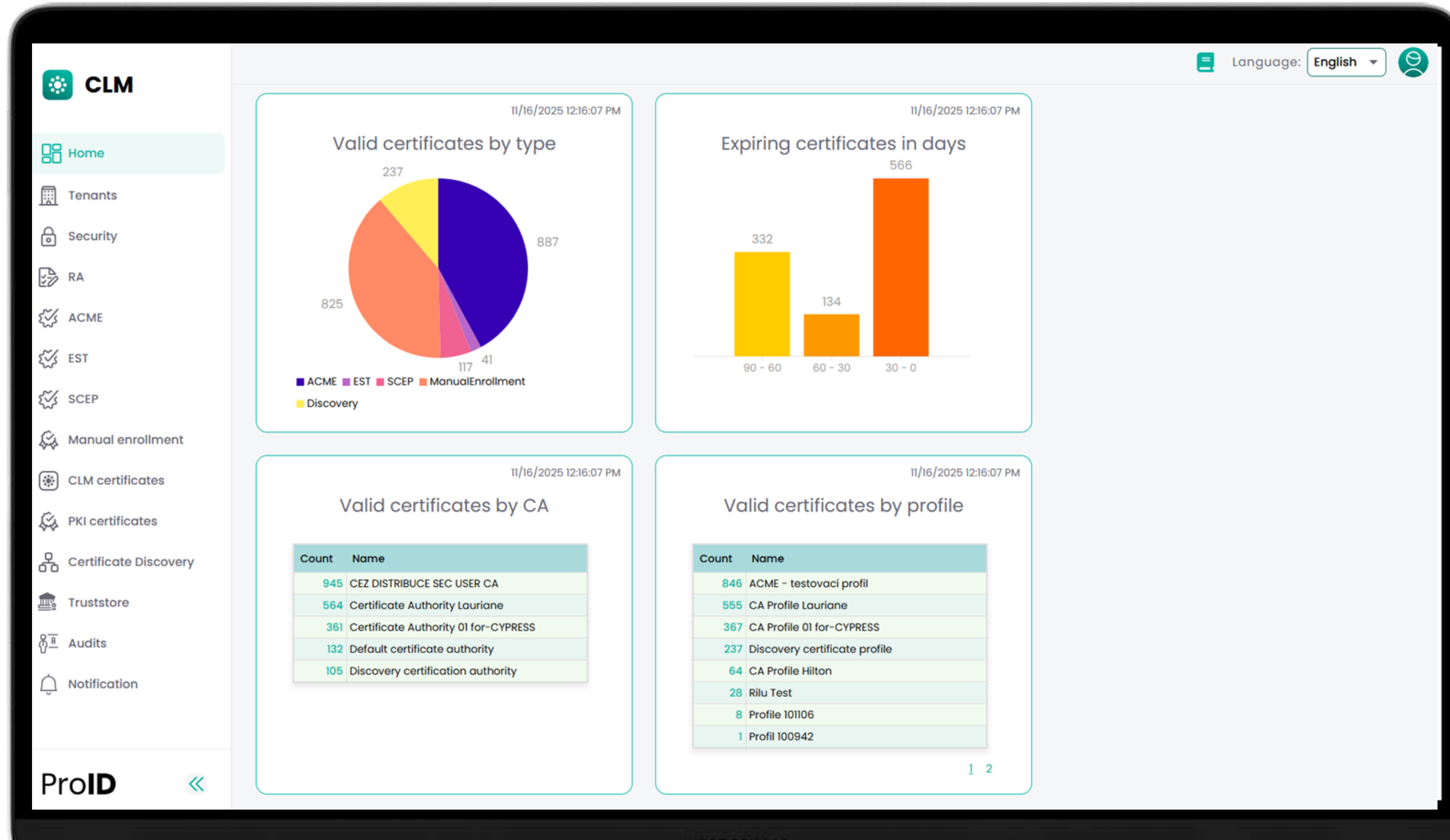
- Ruční evidence v excelových tabulkách
- Žádná automatizace
- Nepříliš velký důraz na bezpečnost - kdo může žádat o jaké certifikáty, resp. s jakými identifikačními daty žadatele

- 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

The image shows a laptop screen displaying the CLM (Certificate Lifecycle Management) interface. The main content area is titled "Certificate filtering" and contains a list of filter criteria on the left and their corresponding input fields on the right. The criteria include: Certificate authority name, Certificate profile, Valid from, Valid to, Serial number, Certificate name, Subject, DNS names, IP address, Issuer, Source, Exclude expired certificates, and Exclude revoked certificates. The input fields for "Valid from" and "Valid to" are date pickers. The "Filter" button is highlighted in green.

CLM

Home / Certificates

Certificate filtering

Certificate authority name: - Not selected -

Certificate profile: - Not selected -

Valid from: dd.mm.rrrr To: dd.mm.rrrr

Valid to: 23.06.2025 To: dd.mm.rrrr

Serial number: Serial number

Certificate name: Certificate name

Subject: Subject

DNS names: DNS names

IP address: IP address

Issuer: Issuer

Source: - Not selected -

Exclude expired certificates:

Exclude revoked certificates:

Clear Filter

ProID <<

Certificates

Visibility & Discovery

The screenshot displays the CLM interface with a sidebar on the left and a main content area. The sidebar includes navigation options: Home, Security, RA, ACME, Manual enrollment, CLM certificates (highlighted), Certificates, Private keys, Revocation, Audits, and Notification. The main content area shows the details for a certificate authority named 'CANEW'. A dropdown menu is open over the certificate details, offering 'Download certificate' and 'Revoke certificate' options. The certificate details include serial number, validity dates, subject, thumbprint, issuer, source, and private key status. Below this, the 'Extensions' section lists various attributes like UPN name, email name, DNS names, IP address, URL name, template, subject key ID, and auth key ID.

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: DIADE9004115658B89279FB499D0B5288319AEB3

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

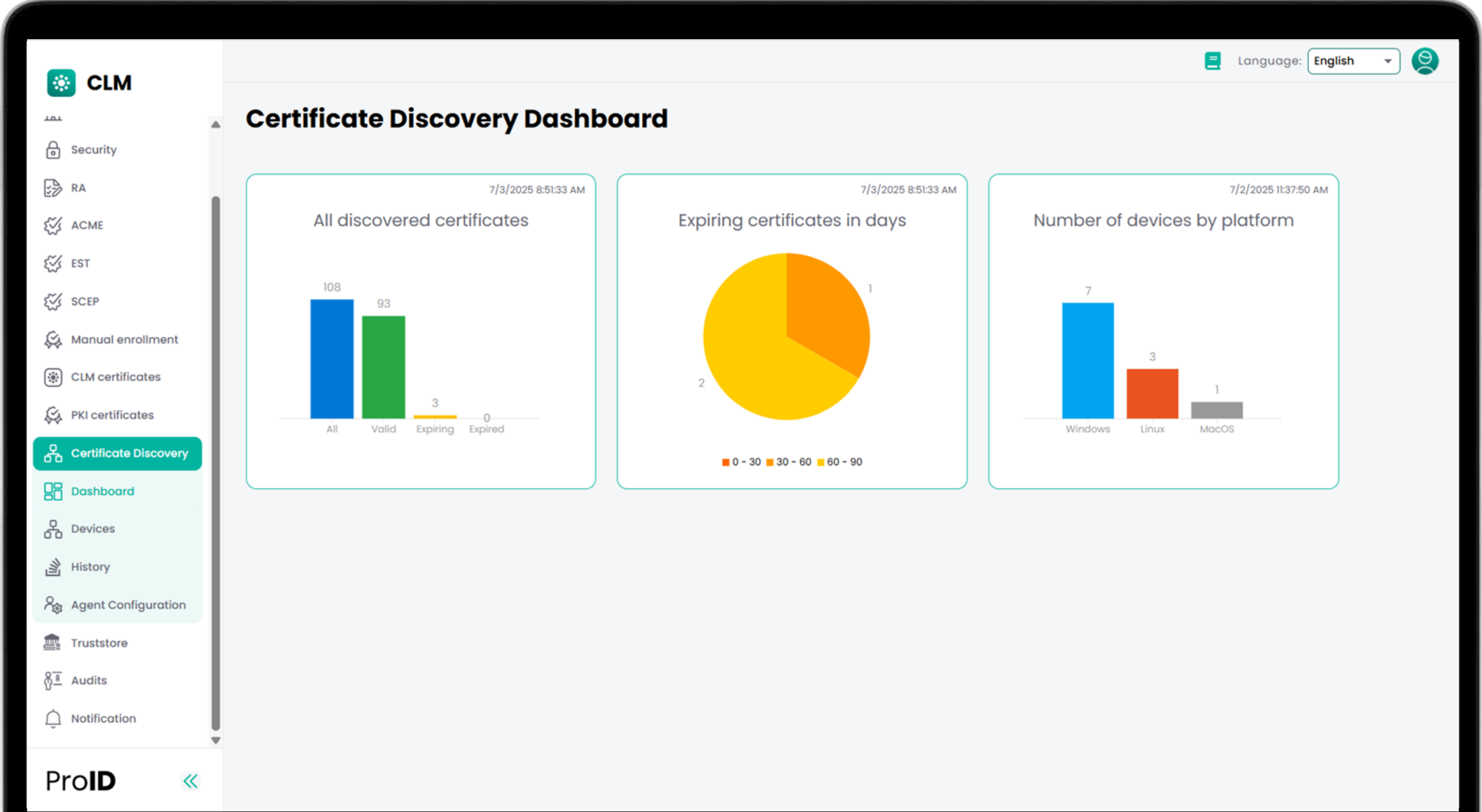
Template: 1.3.6.1.4.1.311.21.8.14192724.4682562.14827945.714657.14454345.186.6783213.9287898

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



Discovery Across Environment

CLM

Language: English

Home / Devices

Devices

Device filtering

Name:

Platform:

IP address:

MAC address:

Added since:

Added to:

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	CACLUSTRER2	CACLUSTRER2.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.cmsscsl.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

ProID

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

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
49000004606BFD6FFD2A5E5780000100000460	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 10:04:27 AM
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
490000013005A37476EC46169000000000013	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
361F27F3F1308993475C898F5A8D9EB1	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
6C0000A64680B30468927469E10000000A646	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

ProID
⏪

Discovery Across Environment

The screenshot displays the CLM (Certificate Lifecycle Management) interface. The left sidebar contains navigation options: Home, Tenants, Security, RA, ACME, EST, SCEP, Manual enrollment, CLM certificates, PKI certificates, Certificate Discovery (highlighted), Dashboard, Devices, History, Agent Configuration, Truststore, Audits, and Notification. The main content area is titled "Certificate Discovery History" and includes a "History filtering" section with input fields for Device, Operation (set to "Certificate linked to device"), Added since (dd.mm.rrrr), and Added to (dd.mm.rrrr). A table below lists the discovery history with columns for Date, Operation, Device, and Certificate.

Home / Devices

Certificate Discovery History

History filtering

Device:

Operation:

Added since:

Added to:

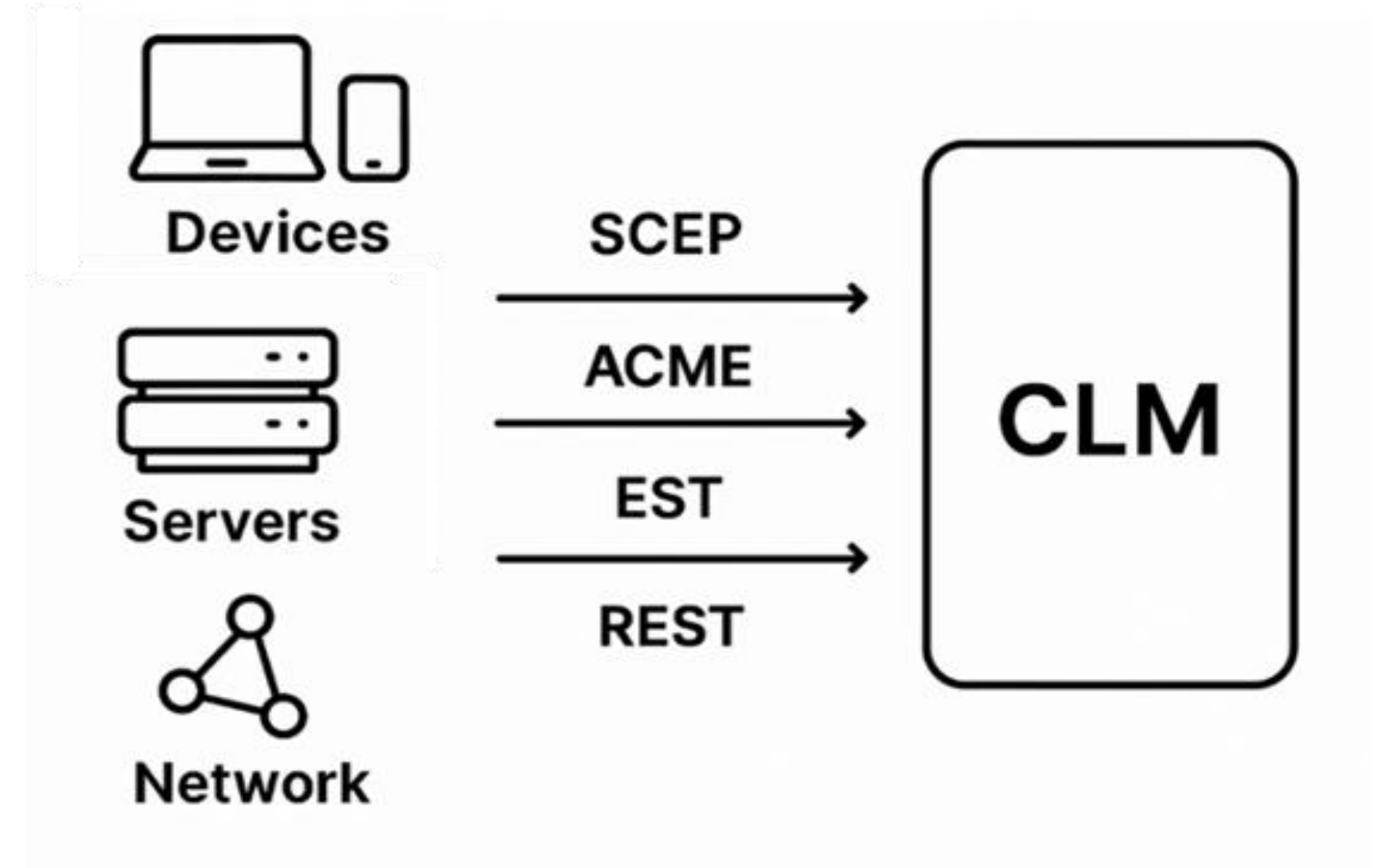
Date	Operation	Device	Certificate
7/1/2025 3:35:26 PM	Certificate linked to device	roman-zl70md3h.local	3679CA35668772304D30A5FB873B0FA77BB70D54
7/1/2025 3:35:25 PM	Certificate linked to device	roman-zl70md3h.local	3BC0380B33C3F6A60C86152293D90FF54B81C004
7/1/2025 3:35:24 PM	Certificate linked to device	roman-zl70md3h.local	D8EB6B41519259E0F3E78500C03DB68897C9EEFC
7/1/2025 3:35:23 PM	Certificate linked to device	roman-zl70md3h.local	76E27EC14FD882C1C0A67585058E3D29B4EDD8BB
7/1/2025 3:35:23 PM	Certificate linked to device	roman-zl70md3h.local	37F76DE6077C90C5813E931AB74110B4F2E49A27
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	75E0ABB6138512271C04F85FD0DE38E4B7242EFE
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

ProID <<

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:

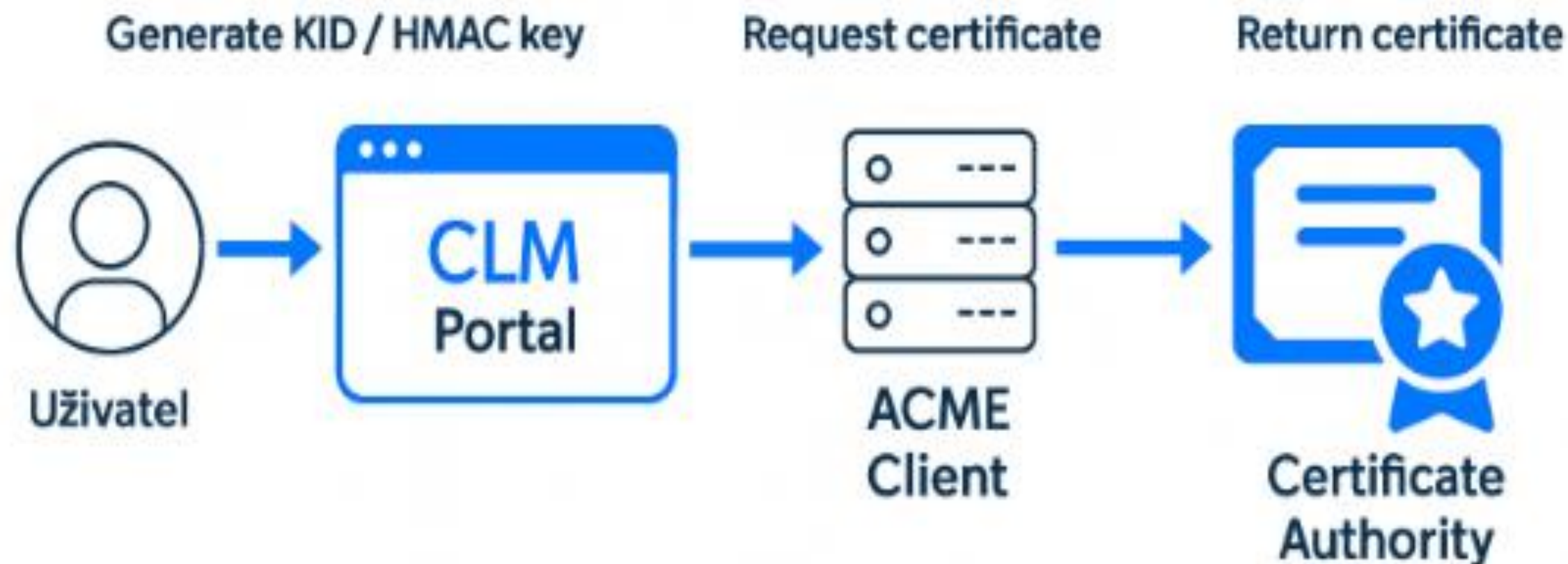
- ACME External Account Binding
 - Proč řešit ACME challenge v interním perimetru?
- MONET+ ACME flow:

🔒 Koncepte 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](#)

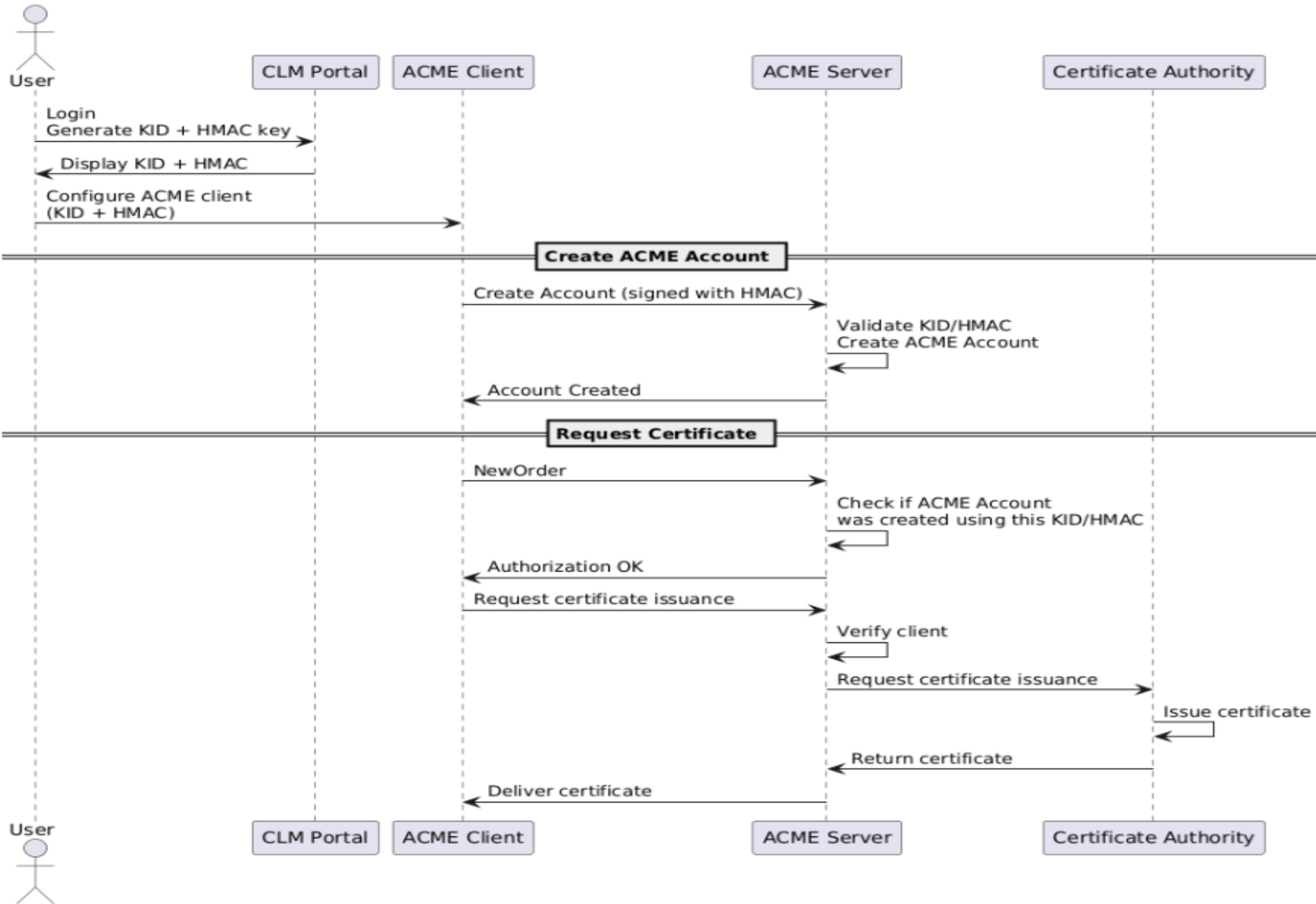
Configuration management tools

- [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



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

The screenshot displays the 'ACME profile' configuration page in the CLM (Certificate Lifecycle Management) system. The interface includes a sidebar with navigation options and a main content area for editing the profile and its DNS identifiers.

CLM

Home
Tenants
Security
RA
ACME
ACME profiles
EAB management
Accounts
Orders
EST
SCEP
Manual enrollment
CLM certificates
PKI certificates
Certificate Discovery

ProID <<

Language: English

ACME profile

Name: ACME Profile
Description: ACME Profile
EAB key type: Permanent
Account key type: Permanent
Scenario: ACME Test
Roles: +
Security: +

Cancel Save

Identifiers

Type	Value	
Dns	domena.cz	🗑️
Dns	sub.domena.com	🗑️
Dns	muj.web.pro.info	🗑️
Dns	domena-s-pomlckou.net	🗑️
Dns	123.cisla.org	🗑️
Dns	*.domena.net	🗑️
Dns	*.sub.domena.org	🗑️
Dns	*.e-shop.co.uk	🗑️

CSR Validation

The screenshot displays the CLM web interface for CSR validation. The left sidebar contains navigation options: Home, Tenants, Security, RA, ACME, EST, SCEP, Manual enrollment (highlighted), Profiles, Enrollment, CLM certificates, PKI certificates, Certificate Discovery, Truststore, and Audits. The main content area is titled "Language: English" and includes a user profile icon. It is divided into three sections: "Algorithms", "Roles", and "Subject names".

Algorithms

- RSA 2048
- RSA 3072
- RSA 4096
- ECDH_P256
- ECDH_P384
- ECDH_P521
- ECDSA_P256
- ECDSA_P384
- ECDSA_P521

Roles

- Administrator
- CLM_Security_Admins

Buttons: Cancel, Save

Subject names

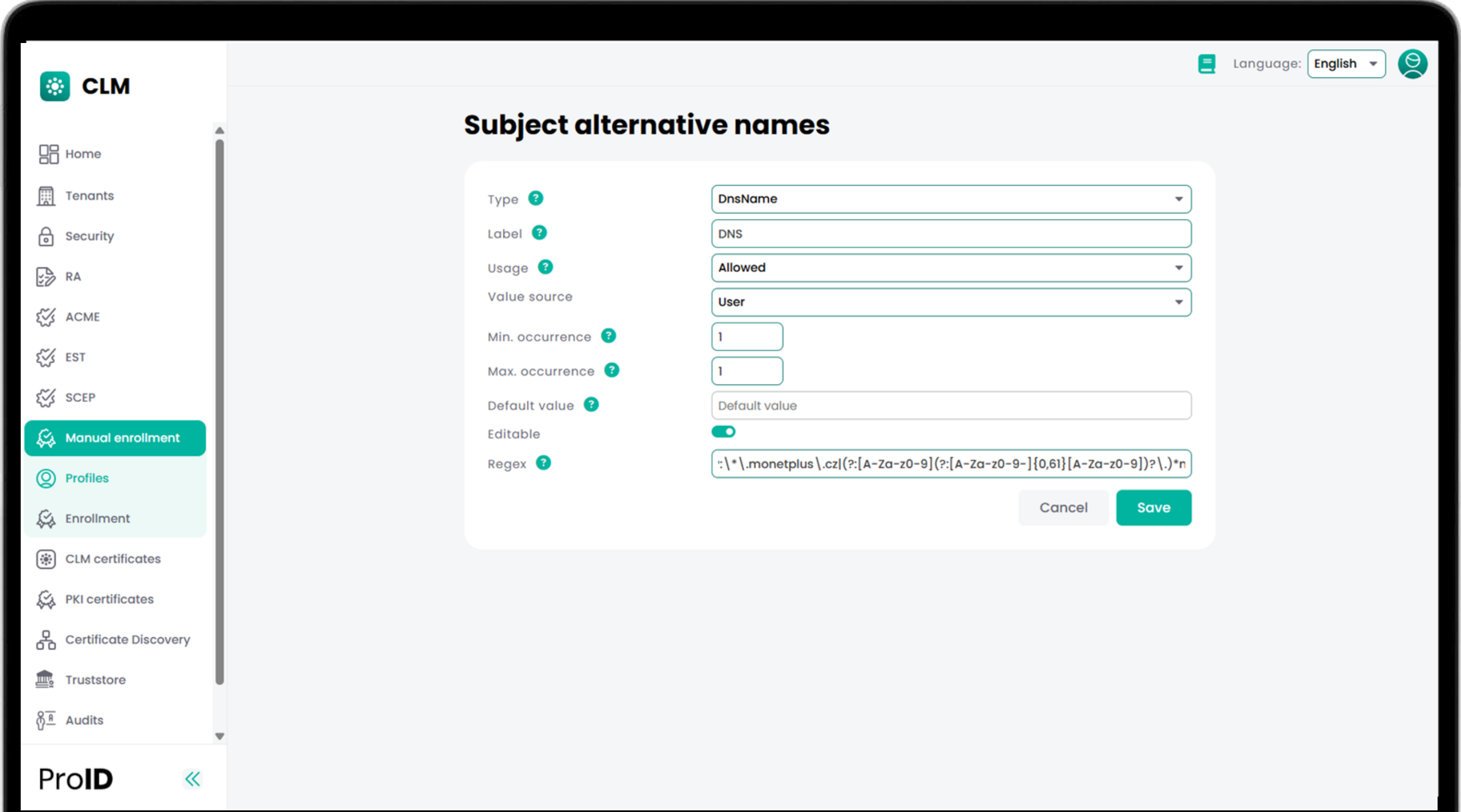
Type	Min. occurrence	Max. occurrence	Default value	Regex	Usage	
CommonName	2	2	--		Allowed	

Button: New

Subject alternative names

Type	Min. occurrence	Max. occurrence	Default value	Regex
DnsName	1	1	--	^(?:*\.\monetplus\.cz)(?:[A-Za-z0-9](?:[A-Za-z0-9-]{0,61}[A-Za-z0-9])?)

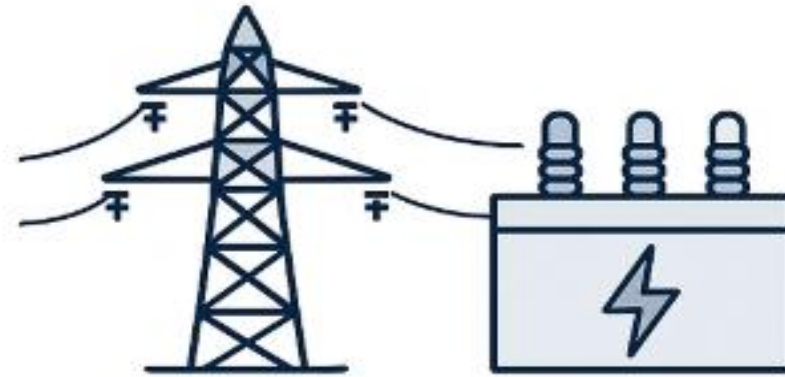
CSR Validation



MONET+ EST / SCEP

Síťové a další prvky:

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



Elektrická síť



Zdravotnictví



Doprava



Vládní budovy




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)

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	<div style="border: 1px solid #ccc; height: 100px;"></div>

Available subject names

Common Name (4)

Email (5)

Available subject alternative names

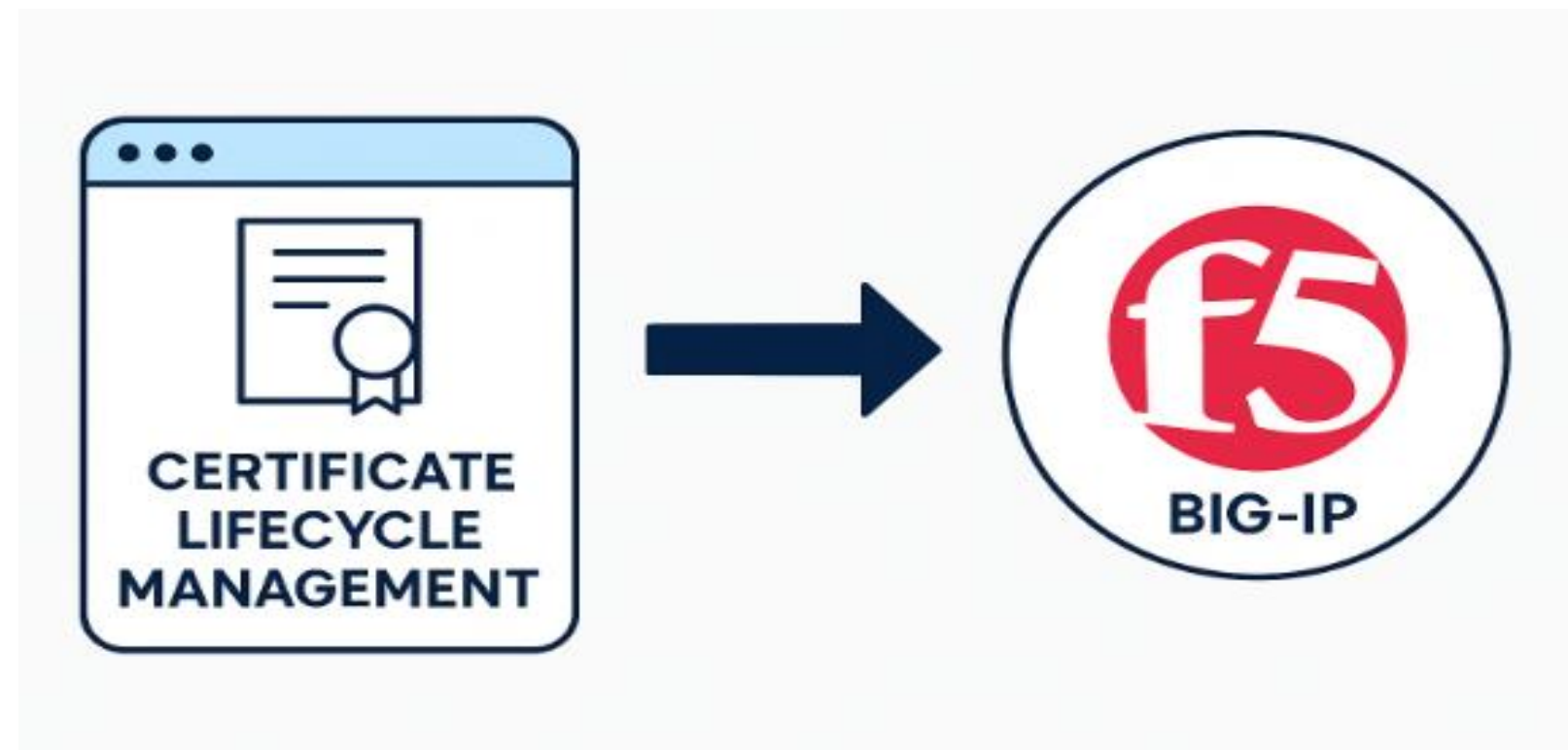
DNS (199)

URL (2)

Email (5)

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.

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

Step 2: Upload the Private Key

Similarly, upload the private key file:

```
1 curl -i -sk -u admin:your-password -X POST \  
2 -H "Content-Type: application/octet-stream" \  
3 -H "Content-Range: 0-1253/1254" \  
4 --data-binary "@test.key" \  
5 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:

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

Step 4: Install the Private Key

Next, install the private key:

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

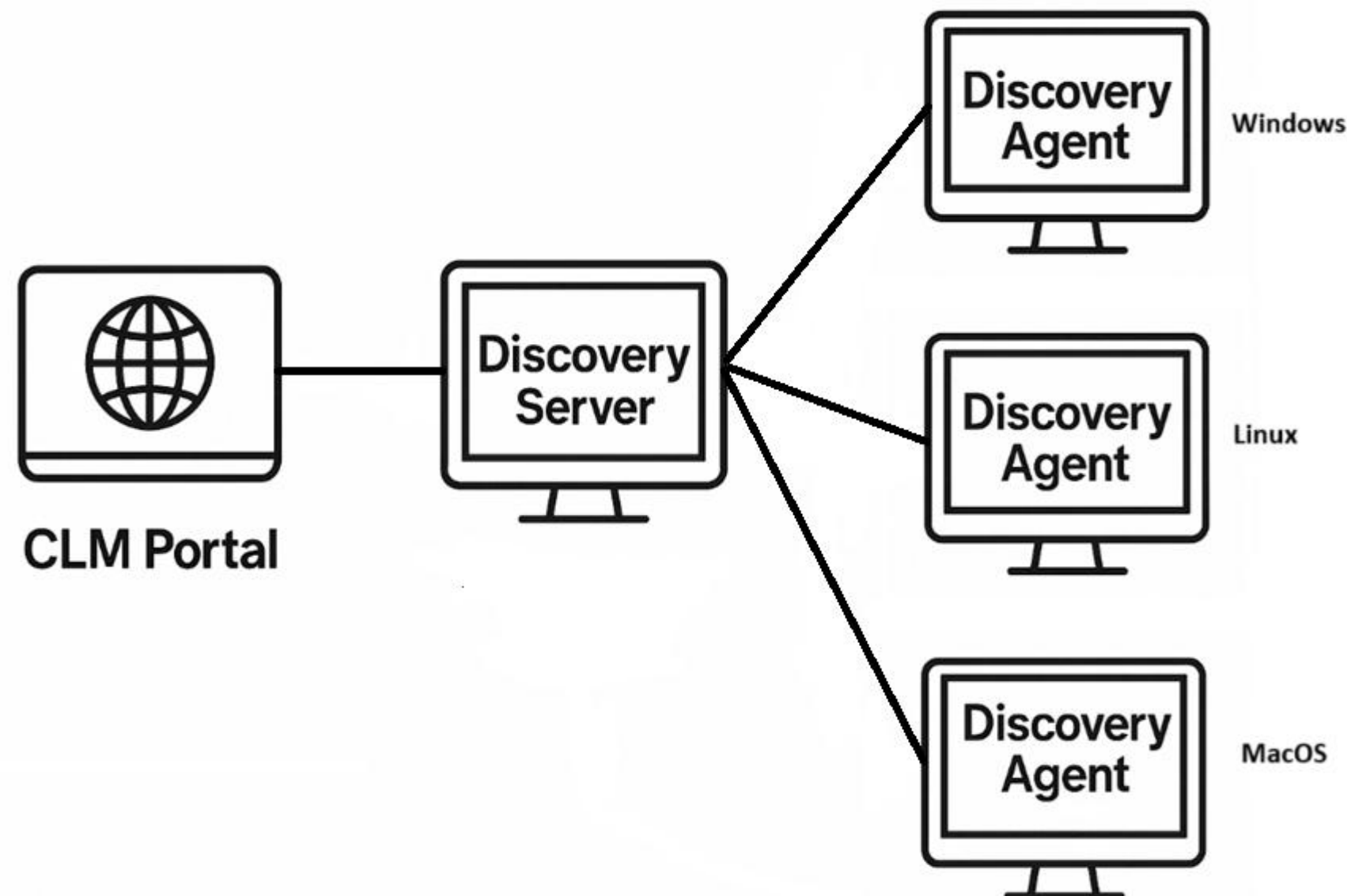
Step 5: Update the SSL Profile

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

```
1 curl -sk -u admin:your-password \  
2 -X PATCH \  
3 https://<BIG-IP-ADDRESS>:8443/mgmt/tm/ltm/profile/client-ssl/clientssl_te \  
4 -H "Content-Type: application/json" \  
5 -d '{ \  
6   "cert": "/Common/mycert", \  
7   "key": "/Common/mycert" \  
8 }'
```

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 seriózně řešit ani globální konkurence



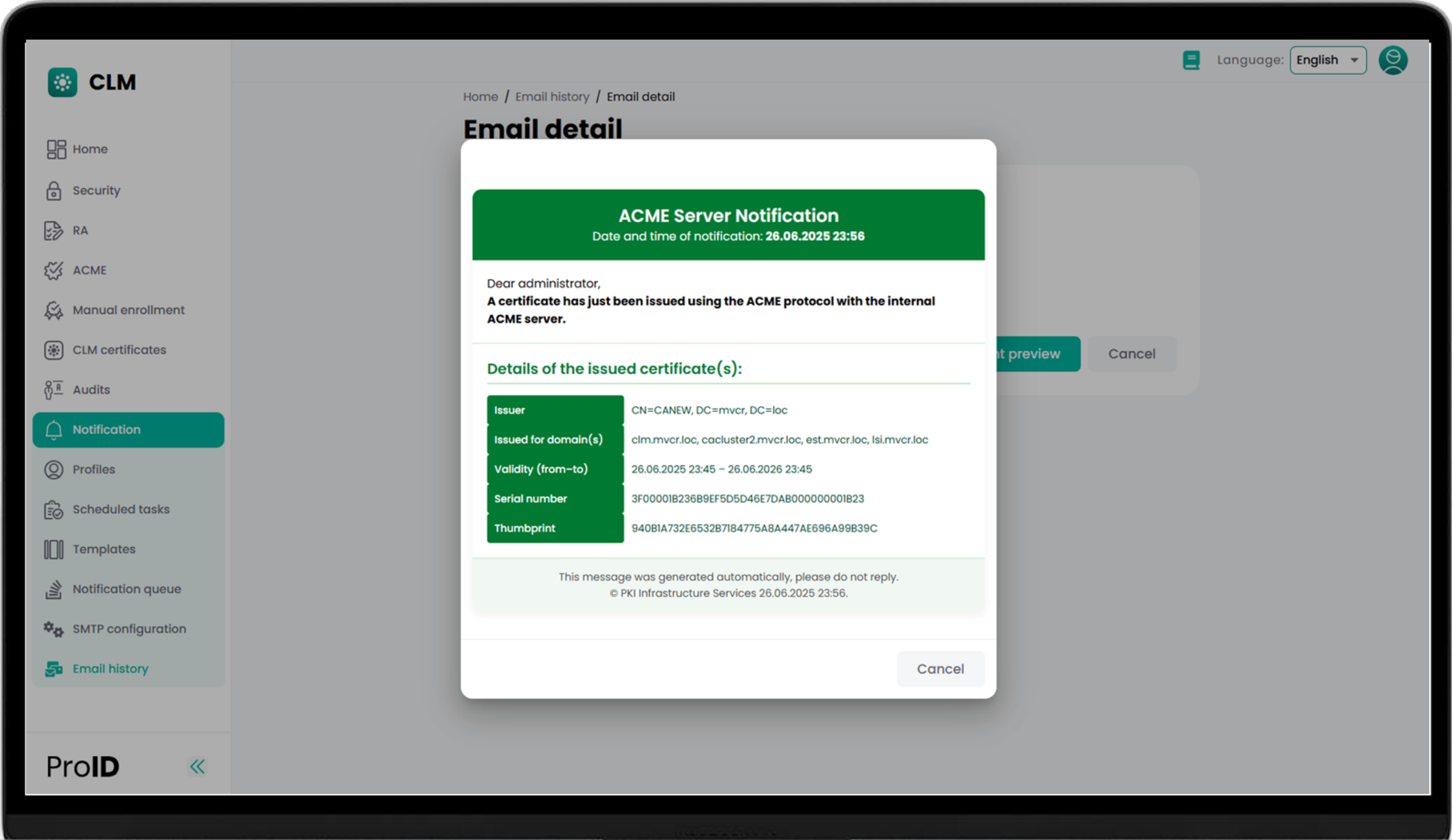
Notifikace

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 form with the following fields: 'Date from' and 'To' (both with 'dd.mm.rrrr' placeholder and calendar icons), '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 form. Below the form is the 'Email history' section, which is a table with the following data:

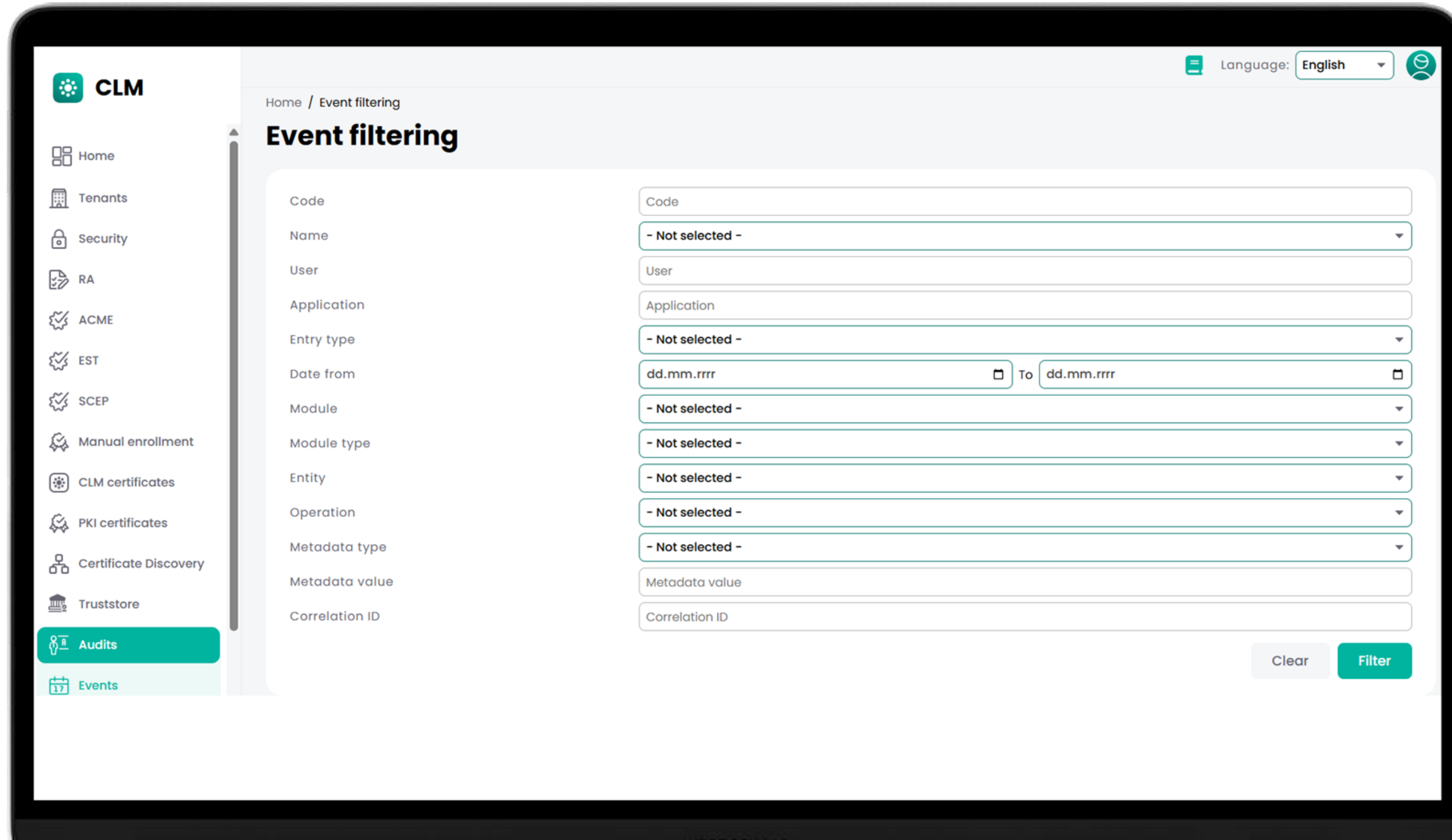
Date	Recipients	Notification profile	Event type	State	
13.06.2025 16:38:52	bockino.t@gmail.com, bocek.tomas7@gmail.com	PROFILE - Davonte	Certificate expired	Sent	
13.06.2025 15:57:52	bockino.t@gmail.com, bocek.tomas7@gmail.com	PROFILE - Davonte	Certificate expired	Sent	
13.06.2025 13:40:52	bockino.t@gmail.com	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. In the top right corner, there is a language selector set to 'English' and a user profile icon.

Notifikace



Audit



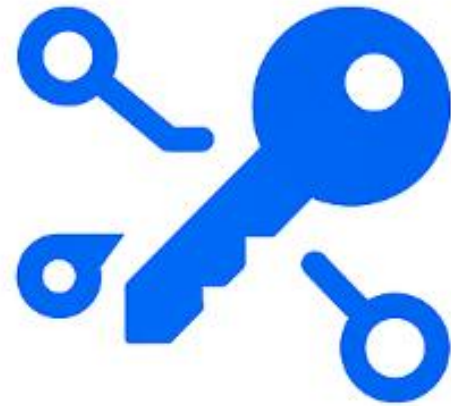
Audit

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 document icon. At the bottom of the interface, it says 'Total number records: 48127' and 'Page size: 25'.

Key Management Server (KMIP protocol)



KMS / KMIP

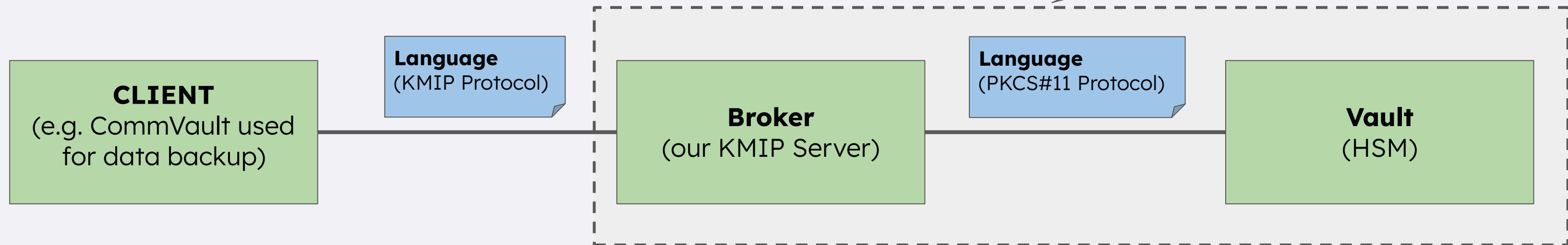
Symetrická kryptografie

Šifrování

- zálohy
- VMWare
- DBs
- atp.

"What is it?"

ProID Key Manager (KMS)



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.

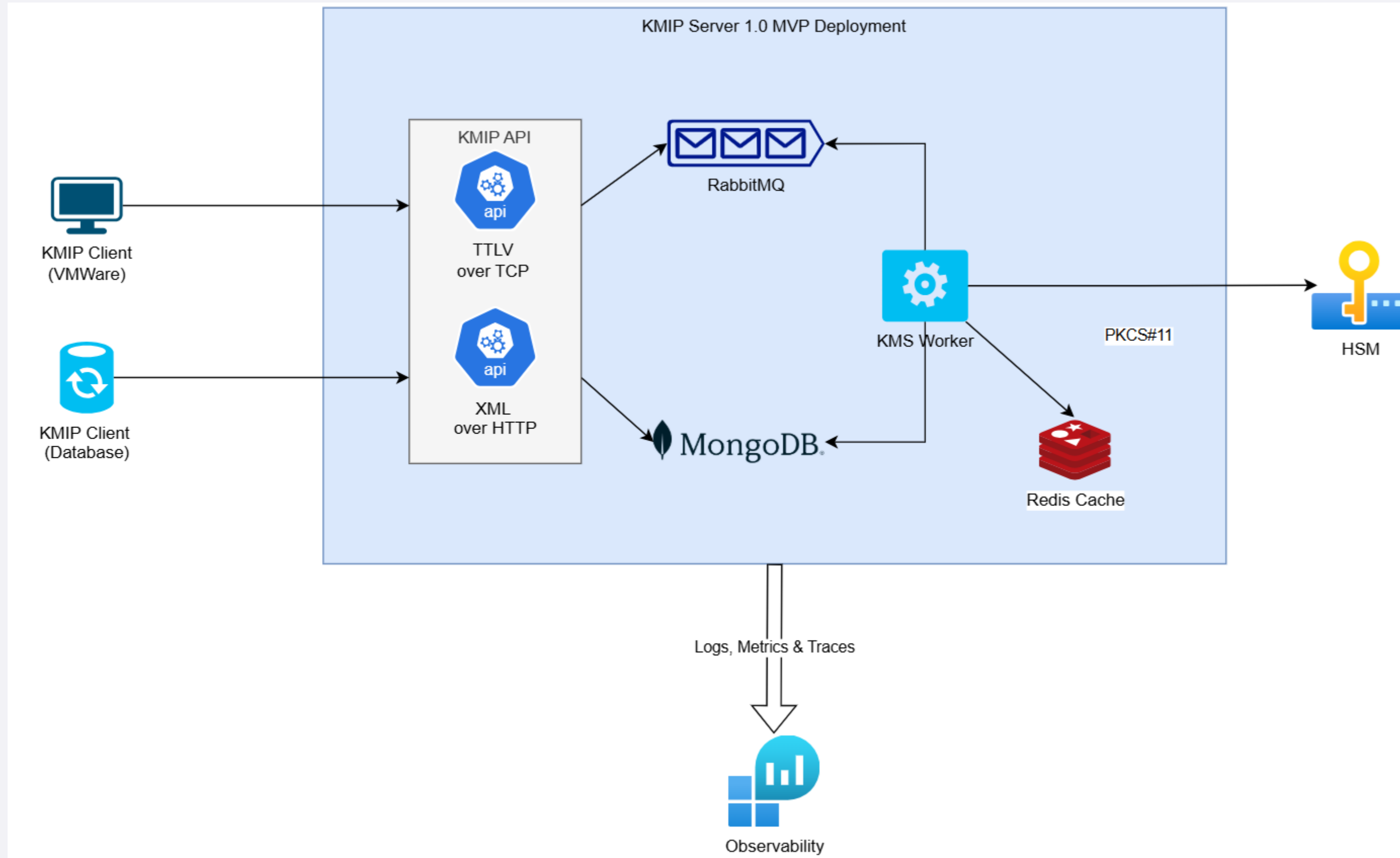
Language (KMIP & PKCS#11 Protocols)

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).