Technická specifikace

ProID

MONET+ Certificate Lifecycle Management

Správa životního cyklu digitálních certifikátů organizace

Správa digitálních certifkátů představuje pro organizaci náročnou agendu, která je většinou realizována manuálními činnostmi administrátorů.

Správci organizace ručně spravují svou PKI infrastrukturu, výsledky své práce (např. vydávání certifikátů) zaznamenají do textových nebo tabulkových dokumentů a spoléhají se na to, že v budoucnu dokument včas zkontrolují a certifikát obnoví.

Tento přístup vede nejen k neefektivnímu využití času zaměstnanců, ale může končit až kritickým výpadkem části infrastruktury organizace, která se opírá o využívání digitálních certifikátů.

S MONET+ Certificate Lifecycle Management (CLM) lze efektivně a bezpečně spravovat životní cyklus technologických certifikátů organizace. Produktová rodina CLM zajišťuje všechny **kritické scénáře** (automatizované vydávání certifikátů s využitím globálně používaných protokolů, kontrola schválených identifikačních údajů v žádosti o certifikát, kontrola podporovaných kryptografických algoritmů, atp.) i **podpůrné procesy** pro správu certifikátů (přehledy vydaných certifikátů organizace, notifikace o vydaných certifikátech nebo certifikátech, kterým se blíží expirace, automatické či manuální odvolání certifikátu, atd.).

MONET+ Certificate Lifecycle Management **zvyšuje stabilitu a bezpečnost oganizace** při současném šetření lidských zdrojů.

info@proid.cz | www.proid.cz

Klademe důraz na:

- Dodání vysoce škálovatelného systému pro správu životního cyklu certifikátů organizace a jejich infrastruktury
- Splnění potřeb menších organizací i velkých firem, které spadají do kritické infrastruktury státu
- Automatizované i manuální procesy v rámci řízení správy PKI organizace
- Zajištění bezpečnosti organizace vynucením kontroly security compliance pravidel v procesu správy certifikátů
- Zajištění používání moderních kryptografických algoritmů v procesu správy certifikátů
- Znemožnění vydání certifikátu neautorizované roli nebo certifikátu s neautorizovanými identifikačními údaji žadatele

Centrální správa nastavení systému

ROLE SYSTÉMU

- globální nastavení a správa rolí systému
- přiřazení uživatelů / rolí do předdefinovaných bezpečnostních profilů
- možnost vytváření vlastních bezpečnostních profilů
- role systému jsou následně svázané se scénáři vydávání certifikátů, pro každý certifikát tak lze definovat, kdo má být notifikován před jeho expirací (nebo při vydání), kdo má právo vydaný certifikát revokovat, atd.

ZABEZPEČENÍ VYDÁVÁNÍ CERTIFIKÁTŮ

- dynamická validace podporovaných identifikačních údajů žadatele v žádosti o certifikát, včetně validace podporovaných algoritmů a délky veřejného klíče v žádosti
- před odesláním do CA možnost podpisu žádosti o certifikát autorizačním certifikátem (podpora klíče v HSM)
- bezpečnostní nastavení lze následně napojit do libovolného scénáře - automatizovaného (ACME, EST, atd.), manuálního (Webová registrační autorita)

SESTAVOVÁNÍ SCÉNÁŘŮ PRO VYDÁNÍ CERTIFIKÁTU

- scénář vydání certifikátu je v CLM systému entita, která nese informace o posloupnosti akcí, které vedou k vydání certifikátu
- scénář se skládá z komponent, které definují např. adresu certifikační autority, profil certifikační autority, validační pravidla žádosti o certifikát, atp.
- CLM systém umožňuje dynamicky sestavovat scénáře z předem vytvořených komponent, které lze znovu použít u nově vytvářených scénářů
- rozhraní protokolů (např. ACME, EST) se následně napojují na vzniklé scénáře

CLM systém lze provozovat jako:

- OnPremise řešení integrované do domény Active Directory s využitím komponent MS - IIS Web Server, MS SQL Server
- OnPremise řešení provozované v kontejnerizované architektuře (aktuálně ve vývoji)
- Multitenantní cloudové řešení, konzumované jako SaaS, s možností integrace na PKI organizace (plánované v příštích release)

Rozhraní pro automatizovanou správu životního cyklu certifikátů

ACME

- implementace obecného ACME serveru dle RFC 8555
- kompatibilita s globálně nejčastěji využívanými ACME klienty
- unikátní koncept ACME External Account Binding - vytvořen na míru pro koncept interního ACME serveru pro vydávání certifikátů z interní certifikační autority
- vhodné pro SSL certifikáty (Domain Validation certifikáty)

SCEP

- implementace SCEP protokolu dle RFC 8894
- vhodné (nejen) pro certifikáty síťových prvků

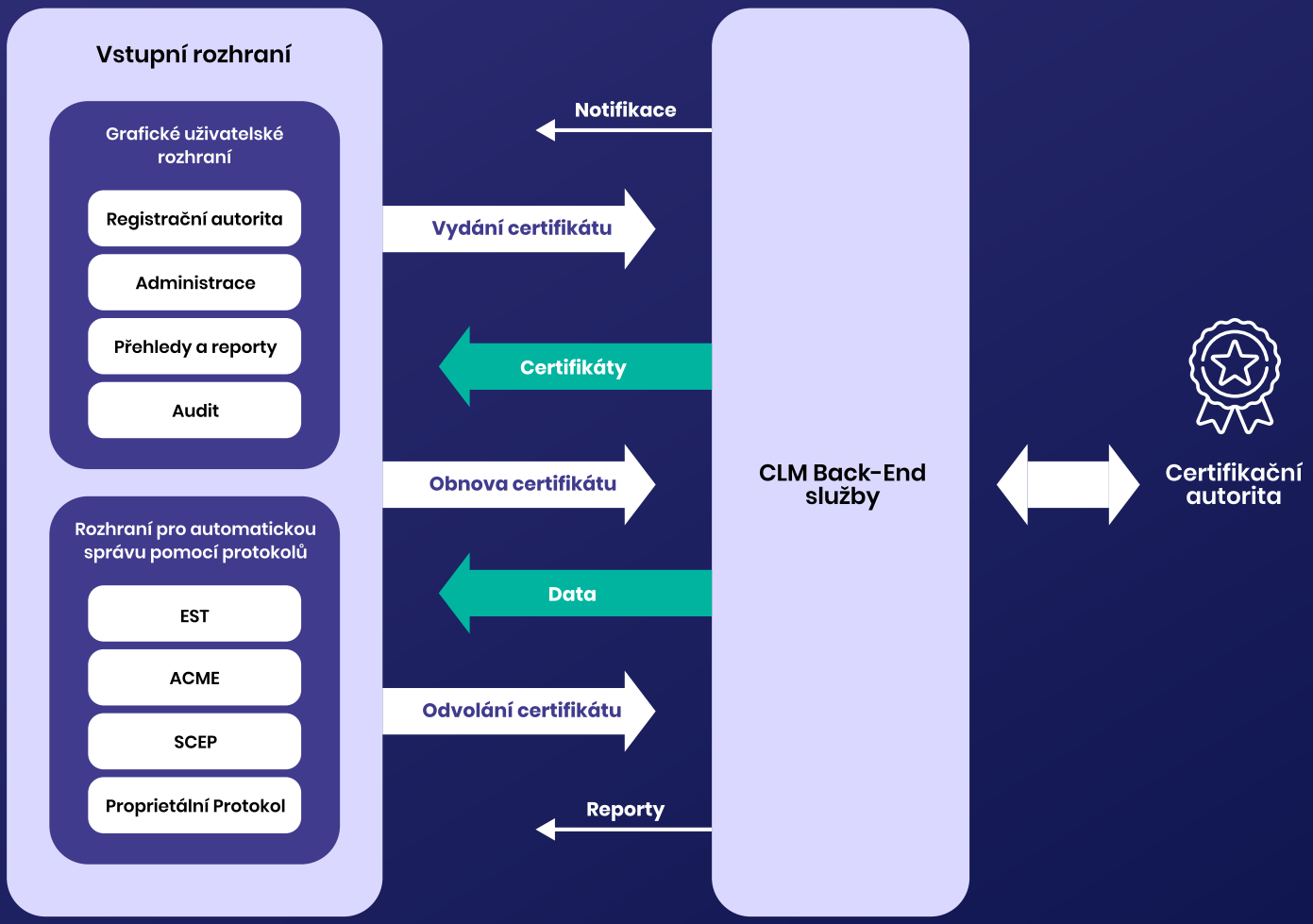
EST

- implementace EST protokolu dle RFC 7030
- dynamická konfigurace autorizačních pravidel EST endpointů (pro autentizaci klientským certifikátem nebo jménem / heslem)
- možnost zapojení kontroly seriových čísel zařízení v žádosti o certifikát
- vhodné (nejen) pro certifikáty síťových prvků

PROPRIETÁRNÍ PROTOKOL

- S našim vývojovým týmem jsme schopni vyvinout podporu proprietárního protokolu na míru zákazníkovi
- Lze využít, pokud již zákazník používá zařízení nebo systémy, které mají implementované vlastní rozhraní na PKI systém

Architektura řešení



Uživatelské rozhraní pro manuální vydávání certifikátů

WEBOVÁ REGISTRAČNÍ AUTORITA

- uživatelské rozhraní pro možnost obslužného vydání certifikátu podle definovaného profilu
- možnost vydání certifikátu podle předem vytvořené žádosti, nebo s možností vygenerování klíčů a žádosti v CLM systému
- v budoucím release bude moci být RA přes technologii ProID Web Bridge propojena s prostředky počítače klienta (např. čipová karta, úložiště klíčů / certifikátů operačního systému, HSM, atp.) - klíčový pár tak bude moci vzniknout přímo v HW prostředku klienta

LICENCOVÁNÍ

Licenční model MONET+ Certificate Lifecycle Management je postaven na licencování za jednotlivý funkční modul.

Funkční moduly aktuálně představují:

Webová registrační autorita | **ACME** | **SCEP** | **EST**

Licence za funkční modul zahrnuje neomezený počet instancí modulu.
Tohoto benefitu lze využít v případě více prostředí zákazníka, více domén, atp.

Onboarding Certificate Lifycycle Management dále zahrnuje fixní licenční poplatek za obecné funkcionality systému:

- Administrativní funkce systému
- Přehledy certifikátů
- Notifikační funkce
- Revokační funkce

Vybrané reference

SKUPINA ČEZ | ČSSZ | KB | albert | eli

Zaujalo vás naše řešení?
Kontaktujte nás.

info@proid.cz | www.proid.cz