ProID

Datasheet

Automatizovaná správa digitálních certifikátů

info@proid.cz | www.proid.cz

PKI a certifikační autority

V digitálním světě se organizace stále více spoléhají na bezpečnou identitu, šifrování a ověřování uživatelů i zařízení. Moderní PKI (**Public Key Infrastructure**) je klíčem k ochraně firemních dat a digitálních operací – ale pouze tehdy, pokud je správně implementována a efektivně řízena.

Společnosti využívající **Microsoft infrastrukturu** (Active Directory, Intune, Entra ID, Windows Server) potřebují robustní PKI řešení, které se plně integruje s jejich technologickým ekosystémem. Efektivní management certifikátů je navíc klíčový pro minimalizaci bezpečnostních rizik, eliminaci ručních procesů a zajištění plné kontroly nad digitální identitou uživatelů i zařízení.

ProID, součást společnosti **Monet+**, přináší řešení pro automatizovanou správu certifikátů, integraci s Microsoft prostředím a zajištění maximální bezpečnosti bez složité správy. S našimi moduly získáte jednoduché, škálovatelné a bezpečné PKI, které odpovídá moderním požadavkům organizací na ochranu digitálních identit.

Proč použít platformu Microsoft?

Přestože máme zkušenosti s implementací certifikačních autorit (CA) na platformě Linux, doporučujeme zákazníkům využívat certifikační autority integrované v **Microsoft Windows Server**. Důvodem jsou jejich široké možnosti integrace, nativní podpora pro firemní infrastrukturu a efektivní správa v prostředí Microsoft.

Hlavní důvody využití technologie Microsoft:

- **Standardy a interoperabilita:** Implementace certifikační autority dodržuje platné průmyslové standardy. Díky tomu garantuje CA vysokou míru interoperability s aplikacemi třetích stran, např. na žádostí, certifikátů, formátů dat, komunikačních protokolů.

- **Kompatibilita:** Certifikáty vydávané z CA lze používat i na non-Windows platformách, jako jsou Linux, OpenShift/Kubernates, macOS, Android, atd.

- **Plná kontrola nad celým životním cyklem certifikátů:** Organizace si sama určuje podmínky vydávání, platnost, možnosti revokace a další parametry certifikátů podle svých potřeb.

- **Snadná integrace s podnikovými službami:** Certifikáty z interní CA lze použít pro zabezpečení interních webů, emailové komunikace (S/MIME), VPN připojení, WiFi autentizace (802.1x) a dalších služeb.

- **Výrazně nižší náklady oproti komerčním certifikátům:** Interní CA umožňuje vydávat prakticky neomezené množství certifikátů bez dodatečných poplatků.

- **Bezpečnost:** Certifikační autorita poskytuje šifrování a autentizaci, což zvyšuje bezpečnost komunikace a dat v síti.

- **Integrace s Active Directory:** Certifikační autorita je plně integrovaná s Active Directory, což usnadňuje správu certifikátů a uživatelů.

- **Automatizace:** Certifikační autorita umožňuje automatické vydávání a obnovování certifikátů, což snižuje administrativní zátěž.

- **Důvěryhodnost:** Certifikáty vydané certifikační autoritou jsou důvěryhodné pro všechny zařízení a aplikace v doméně.

- **Group Policy integrace:** Možnost centrálně nastavit důvěryhodnost CA a distribuovat kořenové certifikáty přes Group Policy na všechny počítače v doméně.

- **Variabilita:** integrovaná podpora různých scénářů a mechanismů vydávání certifikátů a autorizace žádostí.

- **Podpora různých typů certifikátů:** Certifikační autorita podporuje různé typy certifikátů, jako jsou SSL/TLS, S/MIME, VPN a další. Nové typy certifikátů lze snadno přidávat, prostřednictvím grafické konzoly.

- **Podpora ověření stavu certifikátů:** CA vydává seznam zneplatněných certifikátů (CRL). Navíc lze aktivovat službu i OCSP, která umožňuje zjišťovat stav certifikátů online, mechanismem dotaz-odpověď.

- **Centralizovaná správa:** Umožňuje centralizovanou správu certifikátů, což usnadňuje jejich sledování a správu.

- **Separace rolí:** CA podporuje systém separace rolí pro administraci, správu certifikátů, zneplatňování, podávání žádostí apod… Jednotlivým účastníkům lze snadno přidělovat potřebná oprávnění – zařazením do role.

- **Archivace klíčů:** CA podporuje bezpečnou archivaci šifrovacích klíčů, včetně obnovy klíčů ze zálohy. (Šifrovací klíče je vhodné zálohovat).

- **Audit a sledování:** Zapisuje informace o bezpečnostně relevantních událostech do auditu, což zvyšuje transparentnost a bezpečnost.

- **Snadná rozšiřitelnost:** Velmi snadno lze CA doplnit o komunikační kanály, kterými lze požádat o certifikát, např. některý ze standardizovaných protokolů: SCEP, EST, ACME.

- **Podpora politik:** Umožňuje definovat a implementovat bezpečnostní politiky pro vydávání a správu certifikátů.

- **Škálovatelnost:** Certifikační autorita může být snadno škálována podle potřeb organizace.

Moduly pro pokročilou správu a automatizaci digitálních certifikátů

Digitální certifikáty jsou klíčovým prvkem bezpečnosti – zajišťují šifrování, ověřování identity a ochranu dat. S rostoucím počtem digitálních identit a zařízení se však správa certifikátů stává čím dál složitější a časově náročnější.

Řešením jsou moduly pro pokročilou správu a automatizaci, které organizacím umožňují efektivně řídit celý životní cyklus certifikátů, minimalizovat manuální zásahy a eliminovat rizika spojená s jejich expirací či nesprávným použitím. Díky integraci s Microsoft infrastrukturou zajišťují tyto nástroje snadné nasazení, škálovatelnost a vysokou úroveň zabezpečení v podnikovém prostředí.

CLM – Systém pro management certifikátů

CLM **(Certificate Lifecycle Management)** je pokročilý systém pro efektivní správu celého životního cyklu digitálních certifikátů, a to nejen v prostředí Microsoft certifikačních autorit. Nabízí širokou škálu funkcí, které zajišťují automatizaci, bezpečnost a přehlednost pro správce systémů.

Mezi jeho klíčové výhody patří:

- **Kompletní správa certifikátů** – Řízení celého životního cyklu certifikátu od podání žádosti, přes jeho vydání až po evidenci a správu.
- **Uživatelský portál** – Přehledné rozhraní umožňující snadný přístup k informacím o certifikátech a jejich stavu.
- **Registrační autority (RA)** – Systém zahrnuje ověřovací místa, kde dochází k potvrzení identity žadatelů o certifikát. Registrační autorita umožňuje vydání certifikátu i jménem jiné osoby nebo zařízení (např. zaměstnanecký certifikát, certifikát serveru).
- **Automatizovaná obnova certifikátů** – Zajišťuje automatické prodlužování platnosti certifikátů (např. pro webové servery), čímž eliminuje riziko jejich neplatnosti a následných výpadků služeb. Podporuje standardní protokoly ACME, EST a SCEP.

Automatizovaná správa certifikátů – Protokoly ACME, SCEP a EST

V prostředí **Certificate Lifecycle Management** (CLM) je klíčová automatizace vydávání a správy certifikátů, která eliminuje manuální zásahy a snižuje bezpečnostní rizika. K tomu slouží standardizované protokoly ACME, SCEP a EST, které umožňují efektivní distribuci certifikátů pro různé systémy a zařízení.

ACME – Automatizovaná správa SSL/TLS certifikátů

ACME **(Automatic Certificate Management Environment)** je protokol určený k automatizovanému získávání, obnovování a správě SSL/TLS certifikátů. Umožňuje serverům bezpečně komunikovat s certifikační autoritou (CA), provádět ověření domény a získat certifikát bez nutnosti ručních zásahů.

ACME server funguje jako online registrační autorita, která zprostředkovává komunikaci mezi klientskými systémy a certifikační autoritou.

Využití ACME:

- **Webové servery** – automatická obnova HTTPS certifikátů
- **Cloudové služby** – ověřené a šifrované komunikace
- **IoT zařízení a interní infrastruktura** – snadná správa certifikátů
- **VPN a e-mailové servery** – bezpečné šifrování komunikace

SCEP – Protokol pro správu certifikátů

SCEP **(Simple Certificate Enrollment Protocol)** je starší, ale stále využívaný. V podnikových sítích má za úkol automatizaci vydávání a správu PKI certifikátů. Ve srovnání s novějšími protokoly je méně flexibilní.

Hlavní vlastnosti SCEP:

- Podporuje šifrovanou komunikaci mezi klientem a CA pomocí RSA
- Využíván pro autentizaci zařízení v podnikových sítích
- Oproti EST nabízí omezené bezpečnostní mechanismy

Využití SCEP:

- **Síťová zařízení** – switche, routery, firewally
- **VPN brány** – autentizace uživatelů a zařízení
- **Mobilní zařízení (MDM)** – správa certifikátů pro mobilní infrastrukturu
- **Starší IT infrastruktura** – servery, tiskárny, starší IoT zařízení

EST – Moderní a bezpečnější nástupce SCEP

EST **(Enrollment over Secure Transport)** je pokročilejší alternativa SCEP, která poskytuje vyšší úroveň zabezpečení pro automatizovanou správu certifikátů prostřednictvím TLS.

Proč zvolit EST?

- Zvýšená bezpečnost díky mutual TLS (mTLS)
- Podpora moderních kryptografických algoritmů (ECC, postkvantové algoritmy)
- Funguje přes HTTPS, což zajišťuje kompatibilitu s moderními bezpečnostními standardy

Využití EST:

- **Moderní síťová zařízení** – firewally, switche, IoT
- **Podnikové VPN infrastruktury** – zabezpečení komunikace
- **Cloudové a hybridní prostředí** – vyšší úroveň ochrany certifikátů

Výběr správného protokolu závisí na potřebách organizace:

- **ACME** – Ideální pro webové servery, cloudové služby a IoT
- **SCEP** – Použitelný pro starší infrastrukturu a podnikové sítě
- **EST** – Nejlepší volba pro moderní, bezpečné a škálovatelné PKI řešení

Díky plné podpoře ACME, SCEP i EST umožňuje CLM efektivní správu certifikátů ve všech IT prostředích, od tradičních serverů po moderní cloudové platformy.

Modul SaRS – Rozšíření pro bezpečnou obnovu MS CA

SaRS **(Save and Recovery System)** je specializovaný modul doplňující certifikační autority (CA) v prostředí Microsoft Windows Server. Přestože Windows nativně podporuje zálohování CA, jeho mechanismus není dostatečně robustní a nemusí zajistit kompletní obnovu dat po havárii.

Při obnově CA pomocí standardních Microsoft nástrojů se mohou objevit kritické problémy, jako například:

- **Nejasná evidence vydaných certifikátů** – Chybějící certifikáty mohou být v provozu, ale nelze je odvolat, a navíc CA může omylem vydat nový certifikát se stejným sériovým číslem (riziko duplicit).
- **Neúplná správa zneplatněných certifikátů** – Certifikáty, které byly dříve odvolány, mohou být po obnově opět považovány za platné.
- **Chybějící informace o CRL** (seznamu zneplatněných certifikátů) – Po obnově není jasné, jaké CRL bylo naposledy vydáno, což může vést k nesprávné validaci certifikátů.

Modul SaRS eliminuje tyto nedostatky a poskytuje spolehlivý způsob obnovy certifikačních autorit v prostředí Microsoft. Díky němu lze minimalizovat riziko výpadků, ztráty dat a zajistit rychlou a bezpečnou obnovu CA, čímž se snižuje pravděpodobnost expirace CRL a dalších kritických bezpečnostních incidentů.

Modul AUREVO – Automatizované zneplatnění certifikátů

V různých situacích (např. ukončení pracovního poměru) dochází k deaktivaci zaměstnaneckých účtů, avšak certifikáty těchto zaměstnanců často zůstávají aktivní, což představuje bezpečnostní riziko a možnost jejich zneužití. AUREVO tento problém eliminuje díky automatizovanému procesu zneplatňování certifikátů.

Modul AUREVO umožňuje:

- **Pravidelné skenování databáze certifikátů** – v definovaných intervalech prochází dostupné certifikáty.
- **Filtrování podle konfiguračních parametrů** – umožňuje přizpůsobit pravidla pro identifikaci certifikátů určených k odvolání.
- **Automatické kontroly a zneplatnění certifikátů** – v případě splnění podmínek jsou certifikáty ihned odvolány, čímž se eliminuje bezpečnostní riziko.

Díky modulu AUREVO je správa digitálních identit v organizaci bezpečnější, efektivnější a plně automatizovaná.

Modul NTFmail – Automatizované notifikace o expiraci certifikátů

Každý digitální certifikát má omezenou dobu platnosti, po jejímž uplynutí se stává neplatným a nelze jej dále používat. Pro zachování kontinuity a bezpečnosti je nezbytné certifikát obnovit.

Obnova certifikátu je však často ponechána na samotném držiteli, který nemusí sledovat blížící se expiraci. Pokud certifikát exspiruje, jeho obnova bývá komplikovanější – například v případě, kdy se žádost o obnovu autorizuje elektronickým podpisem předchozího certifikátu, který je již neplatný.

Modul NTFmail tento problém eliminuje tím, že **automaticky upozorňuje držitele certifikátů** a správce na blížící se expiraci. Díky tomu mohou včas podniknout potřebné kroky a předejít výpadkům služeb způsobeným neplatnými certifikáty.

Klíčové funkce modulu NTFmail:

- Automatizované e-mailové notifikace o expiraci certifikátů či vydání nových.
- Možnost zasílání upozornění i přes SMS bránu pro ještě vyšší spolehlivost.
- Přizpůsobitelné parametry pro zasílání notifikací konkrétním uživatelům nebo správcům.

NTFmail pomáhá organizacím minimalizovat riziko neplatných certifikátů, zvyšuje bezpečnost a zajišťuje plynulý provoz IT infrastruktury.

Modul OCSP – Ověřování platnosti certifikátů

OCSP **(Online Certificate Status Protocol)** server je klíčovou součástí infrastruktury pro ověřování platnosti certifikátů. Microsoft Windows Server obsahuje nativní OCSP službu, která generuje informace o stavu certifikátů na základě seznamů odvolaných certifikátů (CRL). Tento přístup však přináší významnou nevýhodu – časové zpoždění mezi odvoláním certifikátu a jeho skutečnou propagací v OCSP odpovědích.

Proto nabízíme vlastní implementaci OCSP serveru, která zásadním způsobem **zkracuje časový interval** mezi odvoláním certifikátu a propagací informace o odvolání.

Hlavní výhody našeho OCSP serveru:

- Okamžitá aktualizace informací o odvolání certifikátů díky přímému propojení s databází SaRS.
- Plná kompatibilita s RFC 6960, zajišťující standardizované OCSP rozhraní.
- Rychlé odpovědi přes HTTP protokol pro efektivní ověřování certifikátů.
- Synchronizace s lokálním operačním systémem pro přesné časové údaje.

Nasazením našeho OCSP serveru organizace minimalizují bezpečnostní rizika, zajistí si rychlejší revokaci certifikátů a získají stabilní a výkonné řešení pro správu digitálních identit.

Závěr

Efektivní správa digitálních certifikátů je klíčovým prvkem bezpečnostní politiky každé organizace. **Certificate Lifecycle Management** (CLM) přináší automatizaci, centralizovanou kontrolu a vyšší bezpečnost, čímž eliminuje rizika spojená s ruční správou certifikátů.

Díky podpoře standardizovaných protokolů jako ACME, SCEP a EST umožňuje CLM snadnou integraci s Microsoft infrastrukturou, moderními cloudovými službami i rozsáhlými podnikovými sítěmi. Správné řízení životního cyklu certifikátů pomáhá minimalizovat bezpečnostní hrozby, snižovat provozní náklady a zajišťovat plynulý chod IT infrastruktury.

Nasazením CLM řešení od ProID/Monet+ získáte spolehlivý a škálovatelný systém pro správu digitálních identit, který odpovídá nejnovějším bezpečnostním standardům a požadavkům moderních organizací.

ProID solutions by Monet+

Monet+ je česká technologická společnost s více než 25 lety zkušeností v oblasti digitální identity, bezpečnosti a platebních řešení. Zaměřuje se na vývoj a implementaci pokročilých autentizačních a kryptografických technologií, které chrání digitální svět před kybernetickými hrozbami.

Produktová linie ProID (www.proid.cz) představuje komplexní řešení pro správu digitální identity, autentizaci a certifikátů. ProID nabízí bezpečnostní moduly pro PKI infrastrukturu, správu certifikátů, silné ověřování uživatelů a ochranu přístupu k IT systémům. Díky integraci s Microsoft technologiemi a podporou nejnovějších bezpečnostních standardů je ProID ideálním řešením pro veřejný i soukromý sektor.

Zaujalo vás naše řešení?

www.proid.cz | info@proid.cz