# Technická specifikace – Část 4 Aktivita 2 Vybudování PKI

Obsah

[1) Popis obecných požadavků na řešení 3](#_Toc197342712)

[Řešení správy digitálních certifikátů a klíčů (Public Key Infrastructure) 3](#_Toc197342713)

[2) Architektura pki a postup při realizaci aktivity 4](#_Toc197342714)

[Architektura navrženého PKI 4](#_Toc197342715)

[Postup při realizaci aktivity 5](#_Toc197342716)

# Popis obecných požadavků na řešení

## Řešení správy digitálních certifikátů a klíčů (Public Key Infrastructure)

Koncept správy digitálních certifikátů a klíčů (dále jen **PKI**) je postaven na jedné sdílené Root CA a dvou podřízených Enterprise vydávajících CA. Klíče CA budou chráněny prostředky operačního systému. PKI bude postaven na platformě Windows Server a v rámci výstavby bude upřednostněna možnost využití virtuálních serverů.

# Architektura pki a postup při realizaci aktivity

## Architektura navrženého PKI

Doporučená infrastruktura využívá následující prvky:

1. Kořenovou Standalone OffLine CA (např. notebook bez připojení do sítě a uložený na bezpečném místě). V případě, že bude využit algoritmus RSA, pak doporučujeme délku klíče 4096b, případně využití algoritmu ECC.

Zdůvodnění: V případě kybernetického útoku může dojít ke kompromitaci certifikačních autorit. V případě, že nebude vybudována kořenová CA, tak je v rámci zotavení po havárii nutné celé PKI budovat zcela znovu. Při použití offline kořenové CA je dopad útoku na kořenovou CA zcela minimalizován a kořenová autorita tak zůstane nedotčena. PKI je nutné obnovovat jen v útokem postižených částech. Doba obnovy i náklady na obnovu po útoku se tak výrazně snižují.

1. Enterprise certifikační vydávající autoritu *CA Uživatelé*, která bude vydávat certifikáty autorizovaným uživatelům.

Zdůvodnění: Jedná se o oddělení rolí. Kdy certifikáty jasně identifikovaných uživatelů vydává jiná CA než certifikáty služeb, počítačů a infrastruktury, které se vydávají zpravidla automaticky (*autoenrolment*). Správu mohou zajišťovat samostatní správci oddělení od ostatních CA.

1. Enterprise certifikační vydávající autoritu *CA technologie / Případně pro jiné autentizační metody,* která bude vydávat certifikáty technologickým zařízením (servery, sítové prvky, KDC certifikáty), případně pro jiné autentizační metody uživatelů než CA uživatelé.

Zdůvodnění: Jedná se o oddělení rolí. Kdy certifikáty jasně identifikovaných uživatelů vydává jiná CA než certifikáty služeb, počítačů a infrastruktury, které se vydávají zpravidla automaticky (*autoenrolment*).

Tato architektura je do budoucna jednoduše rozšiřitelná o další vydávající enterprise CA.



Obrázek 1: Návrh architektury PKI

1. Důrazně oddělit role jednotlivých vydávajících CA:

Kořenová CA bude vydávat výhradně jen:

* Certifikáty podřízených CA
* CRL

CA Uživatelé bude vydávat certifikáty výhradně identifikovaným uživatelům.

CA Technologie nebude vydávat certifikáty uživatelům, ale výhradně aplikacím, systémům a infrastruktuře.

1. Vytvořit další distribuční bod pro CRL a AIA na protokolu HTTP. HTTP protokol lze v budoucnu použít i pro externí publikaci CRL a AIA. Dostupnost CRL je kritický prvek infrastruktury PKI a je potřeba zajistit jeho dostupnost. Přidáním dalšího distribučního bodu dojde ke zvýšení dostupnosti CRL a AIA.
2. Implementovat jednu nebo více registračních autority (RA), které budou identifikovat a autentizovat uživatele (např. v rámci personalistů):

A to minimálně před vystavením prvního uživatelského certifikátu, pokud nebyl identifikován odpovídajícím způsobem jinou cestou.

Stávající uživatelé, kteří již byli identifikováni, využijí existující autentizaci pro vystavení uživatelských certifikátů (po přechodnou dobu).

## Postup při realizaci aktivity

Realizace aktivity vybraným dodavatelem se bude skládat ze tří základních částí:

* Sběr požadavků a příprava návrhové dokumentace
* Instalace v prostředí zákazníka
* Test, Školení a předání do ostrého provozu

Celkový čas odhadovaný pro provedení projektu bude 8 týdnů od zahájení. V rámci projektu budou postupně řešena tato témata:

* Analytická schůzka se zadavatelem, kde budou přesně identifikovány UC, které bude budovaný PKI systém pokrývat
* Vytvoření návrhové dokumentace Návrh PKI pro Nemocnice Vyškov, kde budou popsána následující témata:
  + Základní parametry kořenové a vydávajících CA
  + Integrace CA do infrastruktury
  + Distribuční body CRL, AIA
  + Šablony certifikátů
  + Role PKI
  + Návrh zálohování
  + Aktiva systému a návrh jejich obnovy
  + Fyzická bezpečnost
* Revize a schválení návrhové dokumentace
* Předání podkladů pro přípravu infrastruktury
* Příprava infrastruktury na straně zákazníka
* Instalace PKI systému
  + Root CA
  + 2x Enterprise vydávající CA
  + Zavedení důvěry v rámci domény
  + Zavedení a start AIA a CRL
  + Zavedení šablon certifikátů do LDAP a jejich publikace
  + Test systému
* Zaškolení obsluhy, představení kompletního řešení
* Příprava dokumentů
  + Havarijní plány PKI
  + Provozní dokumentace PKI
* Revize a schválení dokumentací
* Předání do rutinního provozu