Standard pro PKI

Verze 1.00

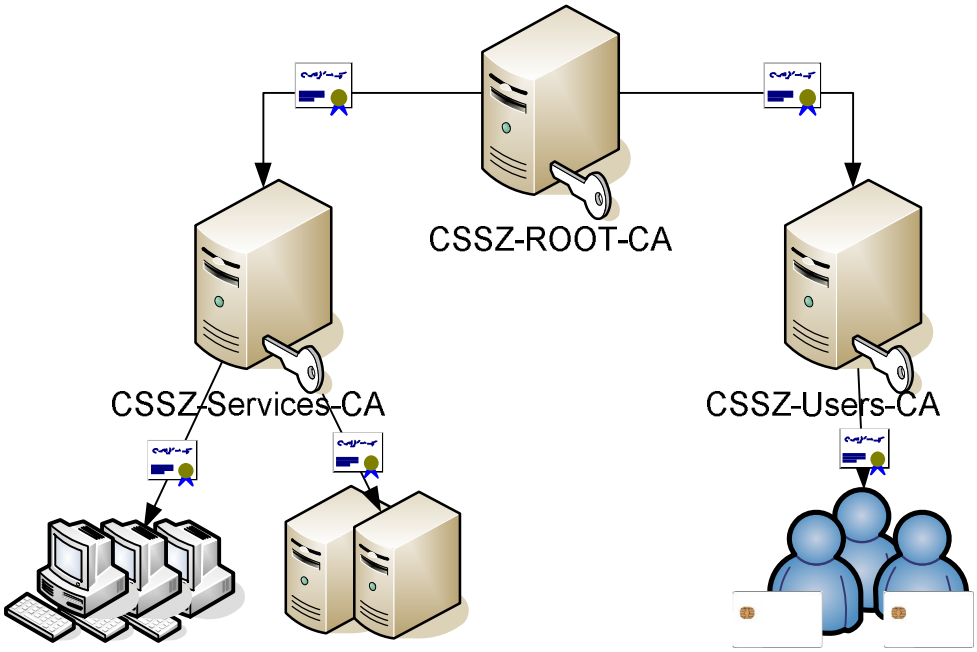
Změny:

Datum vydání	Verze	Změna proti předchozí verzi	Změnil (jméno)
18.6.2008	1.00	Finální verze po oddělení DB z AD	Chlupáč

Obsah

1.1 Certifikační autority

Hlavní součástí infrastruktury PKI ČSSZ jsou 3 certifikační autority. CSSZ-ROOT-CA je kořenovou Off Line certifikační autoritou, která vydává certifikáty podřízeným certifikačním autoritám: „Servery a služby"(CSSZ-Services-CA) a „Zaměstnanci"(CSSZ-Users-CA).



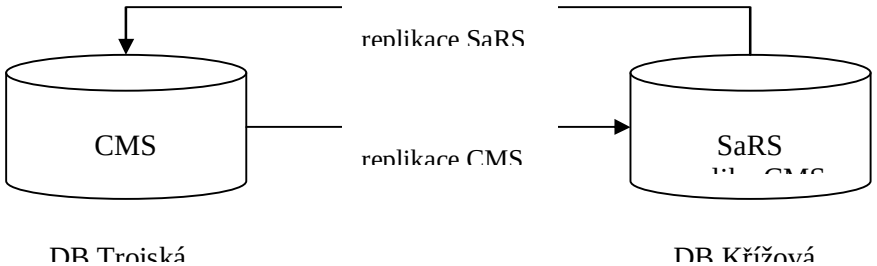
Certifikační autorita „Servery a služby" slouží k vydávání technologických certifikátů serverům,stanicím a síťovým prvkům, šifrovacích EFS certifikátů pro notebooky a certifikátů pro podpis softwarových komponent.

Certifikační autorita „Zaměstnanci" slouží výhradně k vydávání certifikátů zaměstnancům ČSSZ a externím zaměstnancům. Autorita „Zaměstnanci" obsahuje exit modul pro uložení údajů o certifikátech do databáze certifikátů SARS. Jak certifikační autorita„Zaměstnanci" tak i certifikační autorita „Servery a služby" jsou integrovány do Active Directory.

Certifikační autority „Servery a služby" a „Zaměstnanci" jsou zálohovány formou „studené zálohy" v lokalitě Trojská.

1.2 Databázové servery

Součástí infrastruktury PKI jsou 2 geograficky oddělené databázové servery. Jeden je umístěn v lokalitě Křížová a druhý v lokalitě Trojská. Dabázové servery infrastruktury PKI obsahují databáze SARS a CMS. Databáze SARS je primárním zdrojem dat o zaměstnaneckých certifikátech, databáze CMS je primárním zdrojem dat pro správu čipových karet. Databázové servery jsou vzájemně replikovány(Standardní nastavení jednosměrné DB replikace MS SQL Serveru 2005).



1.3 Rozhraní pro přístup k databázím

Informace z databází SaRS A CMS nejsou klientům a pracovištím registračních autorit dostupná přímo. Přístup k databázím zprostředkovává rozhraní tvořené dvěma geograficky oddělenými webovými servery. Stejně jako u databázových serverů je jeden webový server umístěn v lokalitě Trojská a druhý v lokalitě Křížová. Oba webové servery jsou schovány pod jednou virtuální adresou wpki.cssz.cz. Tato adresa je adresou Content switche, který se stará o směrování požadavku na cílový webový server. Součástí webového serveru je i rozhraní pro čerpání dat z databází SaRS a CMS externími systémy(AAA,COMINFO).

1.4 Registrační autority a kartové centrum

Důležitou součástí infrastruktury PKI jsou též pracoviště registračních autorit a kartového centra.

Registrační autority jsou kontaktním místem certifikační autority „Zaměstnanci“, kde pracovník registrační autority (označovaný též jako operátor registrační autority) ověří totožnost žadatele o certifikát předtím, než je zaměstnanci certifikát vydán. RA též provádí odvolávání a obnovu certifikátů. Pracoviště RA jsou umístěna v centrále a na každé KSSZ, MSSZ,PSSZ.

Zaměstnanecké certifikáty jsou zásadně vydávány na čipové karty. Běžný zaměstnanec má na své čipové kartě tři certifikáty(po provedení obnovy 4 – původní šifrovací certifikát je na kartě ponechán) :

- Certifikát pro přihlášení do sítě
- Šifrovací certifikát
- Certifikát pro elektronický podpis (interní elektronický podpis v rámci ČSSZ)

Platnost zaměstnaneckých certifikátů je dva roky. 2 měsíce před vypršením platnosti certifikátů je zaměstnanci umožněno prostřednictvím aplikace pro automatickou obnovu (Reenrollment.exe), z PC jež je členem domény ČSSZ, obnovení certifikátů. Na konec doby platnosti je zaměstnanec a jemu místně příslušná RA upozorněn též emailovou zprávou zaslanou prostřednictvím aplikace NTFMAIL.

Pro administrátory Windows jsou vydávány druhé čipové karty pouze s certifikátem pro přihlášení do sítě. Vlastní postupy pro vydávání karet a certifikátů jsou určeny interními směrnicemi ČSSZ.

Pracoviště kartového centra slouží k dávkovému vydávání certifikátů a recyklaci čipových karet. Pracoviště je umístěno v ústředí ČSSZ.