

Infinity a.s.

Staročernská 1799, 530 03 Pardubice
Tel.: +420 - 467 005 111, fax: +420 - 467 005 555
Kontaktní osoba: Ing. Dana Ouhrabková
e-mail: douhrabkova@infinity.cz
<http://www.infinity.cz>



Vztah k řešení: producent

Budování infrastruktury veřejných klíčů (PKI)

České/slovenské uživatelské prostředí: **ano/ne**

Podporovaná legislativa: **česká**

Počet instalací ve světě/ČR/SR: **0/2/0**

Typický počet uživatelů aplikace: **více než 20**

Orientační cena typické instalace

včetně nasazení systému (v Kč): **desetitisíce**

Reference v ČR/SR: **Hradecká lesní a dřevařská společnost a.s.**



státní správa a samospráva
finančnictví, bankovníctví, pojišťovnictví, leasing
energetika (vodovody, plyn, elektřina, teplo, ...)
doprava nebo spoje (telekomunikace, pošta, ...)
prům. výroba, zemědělství, stavebnictví, zpracov. prům.
velkoobchod, maloobchod, služby
zdravotnictví
jiná úzká specializace

řešení ERP, ekonomické agendy, personalistika
intranetové portály, správa dokumentů, workflow, helpdesk, správa zákazníků
nástroje pro analýzu finančních, obchodních a marketingových dat (Business Intelligence)
nástroje a řešení pro řízení projektů
Six Sigma
integrace podnikových aplikací (Enterprise Application Integration – EAI)
komunikace s dodavateli a odběrateli (B2B scénáře)
podnikové portály (Internet Business)
průmyslová automatizace, vizualizace, CAD, SCADA, GIS
řešení pro architekturu systémů
bezpečnost a PKI (ochrana dat, firewally, smartcards, apod.)
nástroje pro řízení a správu systémů
mobilní řešení

Microsoft Windows Server	Microsoft Exchange Server	Microsoft SQL Server	Microsoft Biztalk Server	Microsoft Content Management Server	Microsoft Commerce Server	Microsoft SharePoint Portal Server	Integrace s Microsoft Office	Microsoft Visio	Microsoft Project	Podpora clusterových řešení Microsoft	Podpora mobilních zařízení	Komunikace v XML
VYŽADUJE	VYUŽÍVÁ		VYUŽÍVÁ			VYUŽÍVÁ	VYUŽÍVÁ				VYUŽÍVÁ	VYUŽÍVÁ

BUDOVÁNÍ INFRASTRUKTURY VEŘEJNÝCH KLÍČŮ (PKI)

Všude kolem nás se skloňuje pojem „elektronický podpis“. Jak ale jeho využití vypadá v praxi? Skutečně využíváme všechny možnosti, které nám moderní bezpečnostní technologie přinášejí? Soudobé a perspektivní způsoby užívání IT předpokládají, že podporu ze strany infrastruktury veřejných klíčů (Public Key Infrastructure) budou při své každodenní činnosti potřebovat prakticky všichni uživatelé sítě.

Firma Infinity a.s. úspěšně aplikovala PKI infrastrukturu u velkých i malých organizací do 50 uživatelů. Řešení pro malé firmy využívá certifikační služby integrované do Active Directory ve Windows 2000/2003 a dalších technologiích firmy Microsoft. Pro větší organizace Infinity používá komplexní certifikační autoritu integrovanou do specializovaného hardwarového boxu pod názvem Cosign od firmy Algorithmic Research (viz <http://www.arx.com>). Tato komplexní aplikace certifikačních služeb je určena cíleně pro Intranety a umožňuje mnohem efektivnější práci s elektronickými dokumenty ve vnitřní síti organizace.

CO ZÁKAZNÍK ZÍSKÁ VYBUDOVÁNÍM PKI?

Koncového uživatele nezajímají technické detaily řešení, a proto vždy maximálně zohledňujeme transparentnost vůči ověřeným postupům a minimalizaci dopadů PKI na klienty PC. Také klademe

důraz na přidanou hodnotu a zvýšení bezpečnosti celého IS. Hlavní přínosy pro uživatele jsou detailně popsány v následujícím přehledu:

Bezpečná pošta:

Pro zajištění bezpečné pošty je použito e-mail klientů podporujících standard S/MIME zahrnutý např. v Outlook, Outlook Express. Certifikáty jsou vyžadovány cestou WWW prohlížeče a následně instalovány do email aplikací. S použitím certifikátů je zaručeno soukromí uživatelů a prokazování jejich identity u e-mailových zpráv a jejich příloh. Tato vlastnost je velmi důležitá pro výměnu citlivých dokumentů např. smluv. Certifikáty mohou být získávány ze specializovaného úložiště v MS Exchange Serveru nebo v Active Directory, popř. v boxu aplikace Cosign.

Bezpečný WWW:

Vytvořená firemní certifikační autorita zajišťuje vydávání certifikátů do všech populárních prohlížečů a rovněž vydává certifikáty pro WWW servery. S pomocí certifikátů je poskytnuta vysoká záruka za bezpečné zpracování informací pomocí kryptografických mechanismů v protokolu SSL. Celé řešení nabízí Infinity v rámci integrace s MS SharePoint portálem.

Virtual Private Networking (VPN):

Komunikace pomocí VPN technologií se rovněž mohou opřít o vybudované řešení PKI. Vzhledem k použití standardu PKCS#10/7 mohou být využity libovolné hardwarové i softwarové produkty třetích stran pro vzdálené přístupy. Správce systému

může využívat vzdálených přístupů přes libovolný firewall k firemním serverům pomocí VPN mechanismů firmy Microsoft. Stejný mechanismus je používán i pro vzdálený dohled certifikačních služeb vnitřní sítě našimi pracovníky.

Přidaná hodnota

Uživatelé používají čtečku s kartou a klientský software firmy ActiveCard (<http://www.activcard.fr>), který jim umožňuje bezpečné přihlašování do systému Windows 2000/XP. Dále je na kartě bezpečně uloženo statických hesel pro přístup např. k WWW stránkám jiných systémů. Tato funkce má tu přednost, že si uživatelé nemusí pamatovat velké množství hesel a stačí jim znát pouze jeden přístupový PIN na kartu. Pro naplnění rozšiřujících požadavků uživatelů na šifrování souborů používáme doplňkový šifrovací software využívající certifikáty od firmy Finmatica/MSI pod názvem SecurityBox. Více informací je k dispozici na adrese <http://www.securitybox.net>.

Typická PKI zahrnuje nástroje pro transparentní vydávání digitálních certifikátů uživatelům a serverům. Samozřejmě jsou nástroje pro integraci s různými druhy seznamů certifikátů, nástroje pro správu, odvolávání (revokaci), prokazování a obnovu platnosti certifikátů a podpůrné prostředí pro uplatnění PKI služeb. Vytvořit celé prostředí PKI do jednoho funkčního celku není vůbec jednoduché, a proto byste se měli obrátit na kvalifikovaného a nezávislého partnera, jakým je Infinity a.s.