Smart karta

Bezpečná autorizace uživatelů

Pomocí technologie přihlašování uživatelů pomocí Smart karet získává společnost zvýšení bezpečnosti pro přístup do infrastruktury k interním datům.

Dvoufaktorová autentizace, tj. uživatel musí něco mít (Smart karta) a něco znát (PIN či heslo), je bezpečnou kombinací pro autorizaci uživatele v prostředí informačních technologií. Smart karta je svázána s identitou uživatele, a tak je možné ji aplikovat pro přístupy nejen do operačních systémů v rámci přihlášení aplikací, ale také pro fyzické vstupy do prostor, platby za stravování či uložení šifrovacích klíčů v kartě. Smart karty jsou ve standardizované velikosti kreditní karty s možností personifikace pro snadnou identifikaci jejího držitele například fotografií držitele, barvou na kartě pro snadné rozpoznání, zdali se uživatel pohybuje v prostorách kartou povolených. Je možné také připravit karty pro speciální účely, například administrátorské karty, karty pro VIP přístupy apod.

Co řešení přináší

Pomocí dvoufaktorové autentizace je obtížné odcizení identity a přihlášení se místo jiného uživatele. Ztráta karty neznamená ohrožení tajemství, karta je sama o sobě chráněna heslem či pinem a může být konfigurována tak, aby po zadání počtu špatných pokusů byla zcela zablokována. Operační systém může být nakonfigurován tak, že pouze při připojení karty je možné v zařízení pracovat a po odpojení karty je zařízení uzamčeno. Nehrozí tak zneužití dat v případě opuštění zařízení. Smart karta může obsahovat volitelně kontaktní i bezkontaktní část. Karta obsahující oba čipy, kontaktní a bezkontaktní, je nazývána hybridní.

Smart karty

Kontaktní část Smart karty je čip, s implementovanou asymetrickou kryptografií (RSA), umožňuje bezpečné uložení privátních RSA klíčů. Všechny operace s privátním klíčem probíhají uvnitř čipu, klíč tedy nikdy neopustí čip karty a nelze jej z karty vyexportovat. Kontaktní část v sobě ukládá certifikáty. Těmi uživatel prokazuje svou identitu ve světě informačních technologií, ověřuje tak svou identitu v aplikacích, jako například přihlášení do operačního systému, šifruje data, elektronickou poštu, uloženým elektronickým podpisem podepisuje dokumenty, ověřuje se vůči internetovému bankovnictví aj. Kontaktní část potřebuje hardware zařízení, tzv. čtečku karet. Některé čtečky jsou již integrovány například v klávesnicích či v noteboocích.

Bezkontaktní část karty je čip integrovaný do jejího těla. Ten pak lze v organizaci využít v rámci bezkontaktních systémů. Například v docházkovém systému, pro vyhrazený přístup do určitých částí budovy, platbu v závodních jídelnách, oprávněnost pro tisk, kopírování atp. Nabízené řešení na Smart kartách podporuje technologie bezkontaktního čipu Mifare, DESfire a EM Marine (dotaz - jsou čipy aktuální?). Podporu jiných je možné řešit individuálně.

Certifikační autorita

je služba Active Directory Certification Services obsažená již v licenci Microsoft Windows Serveru. Funkce role AD CS je pomocí certifikátů zajistit v elektronickém světě ověření identity, integrity, nepopiratelnost a privátnost. Certifikační autorita je ideální produkt pro spojení se Smart kartami.

Mezi obvyklé důvody, proč si organizace pořizují Smart karty k Certifikační autoritě, patří:

- Dvoufaktorová autentizace do doménových počítačů
- Bezpečná autentizace do VPN, Wifi Access Pointů
- Elektronické podepisování a šifrování e-mailů
- Zaručené elektronické podpisy (kvalifikované certifikáty)
- Šifrování disků a souborů
- Autentizace certifikátem na webové servery (HTTPS)