Konkrétne problémy a skúsenosti pri nasadzovaní PKI (2)

Andrej Vávra

Komponenty Entrust PKI

V nasledujúcej časti sa budeme venovať konkrétnemu systému Entrust PKI, s ktorým máme bohaté skúsenosti. Ide o riešenie firmy Entrust Technologies (www.entrust.com) poskytujúce všetky stavebné kamene, nutné na implementáciu PKI.

V krátkosti si popíšeme základné komponenty Entrust PKI a načrtneme kritériá ich umiestnenia a nastavenia. Vychádzame z toho, že ide o architektúru klient/server, kde určité systémy poskytujú služby (servery) a iné systémy tieto služby využívajú (klienti). V tomto popise budeme predpokladať, že budujeme kompletnú PKI, t. j. aj s certifikačnou autoritou. Existujú aj iné možnosti, napr. že naša PKI bude využívať služby externej certifikačnej autority.

Základné serverové komponenty:

- Entrust/-Authority — poskytuje funkcionalitu certifikačnej autority. Znamená to, že -zodpovedá hlavne za manipuláciu s certifikátmi (ich vydávanie, rušenie) a spravuje najväčšie aktívum – tajný kľúč certifikačnej autority, od ktorého je odvodená všetka dôvera.
- Databáza Entrust/Authority – obsahuje všetky informácie certifikačnej autority, tajné aj verejné (certifikáty, definovaných používateľov).
- Entrust/Authority Master Control – je to rozhranie pomocou ktorého hlavný používateľ spravuje certifikačnú autoritu (pozri nižšie).
- Entrust/RA – registračná autorita, ktorá je vlastne predĺženou rukou certifikačnej autority a poskytuje v jej mene služby. Pracujú s ňou pokročilí používatelia okrem hlavného používateľa (pozri nižšie).
- Adresár (directory) – úložisko verejne dostupných informácií, najmä všetkých certifikátov a zoznamov zrušených certifikátov. Ako z názvu vyplýva, ide vlastne o telefónny zoznam – ak chceme poslať niekomu zašifrovanú správu alebo overiť si jeho elektronický podpis, tak všetky potrebné informácie získame práve v adresári.

Voliteľné serverové komponenty (zoznam nie je kompletný):

- Entrust/WebConnector – ide o webovú stránku, pomocou ktorej možno spravovať nemanažované certifikáty (v terminológii Entrust – webové certifikáty).
- Entrust/SelfAdmin – ide o webovú stránku, pomocou ktorej môže koncový používateľ vykonávať určité administratívne činnosti (napr. zrušenie svojho certifikátu) a nemusí preto kontaktovať registračnú autoritu.
- Entrust/Timestamp – aplikácia, ktorá vydáva časové pečiatky. Ide o elektronický podpis odtlačku súboru a presného časového údaja, ktorý môže byť použitý ako dôkaz, že daný dokument existoval v danom čase.

Klientske komponenty:

- Desktopové prístupy – poskytujú riešenia na úrovni používateľskej pracovnej plochy. Ide najmä o šifrovanie, dešifrovanie, elektronické podpisovanie a časové pečiatky súborov (Entrust/Entelligence), automatické šifrovanie a dešifrovanie celých adresárov (Entrust/ICE), automatické prihlásenie sa do aplikácií Entrust ready a prostredia Windows (Entrust/SignOn), a tiež bezpečné odstraňovanie súborov (Entrust/TrueDelete).
- E-mailové prístupy (napr. Entrust/Express) – poskytujú riešenia na úrovni elektronickej pošty, hlavne šifrovanie a dešifrovanie e-mailov, elektronické podpisovanie e-mailov a overovanie elektronicky podpísaných e-mailov.
- Zariadenia (mobilné zariadenia, sieťové komponenty) – do PKI je možné zakomponovať zariadenia (napr. smerovače), ktoré sú schopné prevádzkovať virtuálne privátne siete (VPN).

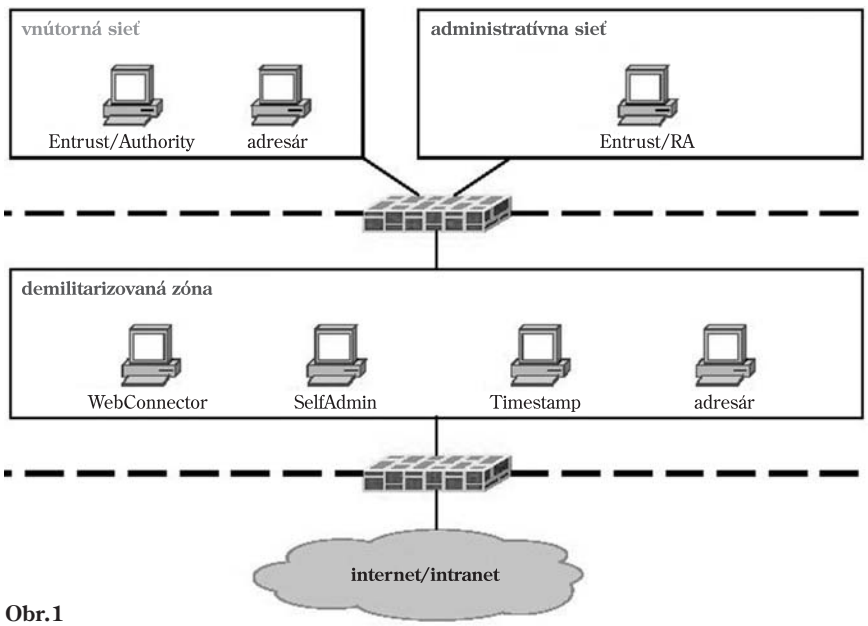
Vybudovaná infraštruktúra na strane servera môže vyzerať ako na obr. 1.

Infraštruktúra sa skladá z troch podsietí, ktoré vytvárajú dva firewally. Patrí sem demilitarizovaná zóna (iba do nej majú prístup používatelia z internetu, resp. intranetu), ďalej vnútorná sieť (obsahuje najkritickejšie komponenty) a administratívna sieť (obsahuje iba Entrust/RA, ale môže obsahovať aj pracovné stanice správcov jednotlivých systémov).

Kritériá umiestnenia a nastavenia komponentov Entrust/PKI

Z pohľadu bezpečnosti:

- Umiestnenie vo vnútornej chránenej sieti, kde je zabezpečený špeciálny režim fyzickej bezpečnosti (kontrola prístupu, kamerové monitorovanie) a procedurálnej bezpečnosti (napríklad nutnosť viacnásobnej autentizácie).
- Nasadenie HSM (Hardware Security Modul) na ochranu tajných kľúčov CA – týmto chránime najväčšie aktívum certifikačnej autority zariadeniami, ktoré by mali spĺňať FIPS 140-2 Level 3.
- Monitorovanie systémov a prienikov – nevyhnutnosťou je nasadenie systémov na detekciu prienikov (IDS), ktoré je však nutné monitorovať a pravidelne spravovať.



Obr.1

- Havarijné plány, plány obnovy a stratégia zálohovania.

Z pohľadu dostupnosti služieb a dát:
- Clustering, redundancia hardvéru, diskové polia RAID – ide o štandardné mechanizmy zabezpečenia dostupnosti služieb.
- Load balancing (distribúcia záťaže) – o tomto mechanizme je vhodné uvažovať hlavne pri adresári (directory).
- Monitorovanie systémov – v tomto prípade najmä z pohľadu dostupnosti.
- Havarijné plány a plány obnovy.

Ak sa vrátime k obr. 1, tak vo vnútornej sieti sa nachádzajú komponenty kritické z pohľadu bezpečnosti a v demilitarizovanej zóne komponenty kritické z pohľadu dostupnosti služieb a dát.

Všimnime si, že na obrázku sa nachádzajú dva adresáre, jeden vo vnútornej a druhý v demilitarizovanej zóne. Ide o mechanizmus zabezpečenia dostupnosti, keďže adresár v demilitarizovanej zóne vystupuje ako replika adresára vo vnútornej sieti. K adresáru vo vnútornej sieti pristupuje iba Entrust/Authority, preto nie je vystavený žiadnej záťaži od koncových používateľov. Naopak adresár v demilitarizovanej zóne je pod neustálym tlakom koncových používateľov, preto je jeho výpadok pravdepodobný. Vďaka vzťahu replikácie je ho však možné veľmi jednoducho a efektívne obnoviť pomocou adresára vo vnútornej sieti. Napokon, replikovaných adresárov môže existovať niekoľko, takže takéto riešenie je veľmi flexibilné.

Zaujímavé je aj umiestnenie Entrust/Timestamp. Teoreticky môže byť umiestnený vo vnútornej sieti alebo aj v demilitarizovanej zóne. Tajný kľúč Entrust/Timestamp môže byť pokladaný za veľké aktívum organizácie (na rovnakej úrovni ako tajný kľúč certifikačnej autority), a preto môže padnúť strategické rozhodnutie, že aplikácia bude umiestnená vo vnútornej sieti.

Používatelia Entrust PKI

Okrem systémov sú dôležití a možno aj omnoho dôležitejší konkrétni ľudia, ktorí tieto systémy obsluhujú a zodpovedajú za ich bezchybnú činnosť. Rozvedieme teda hierarchiu používateľov Entrust PKI, ich povinnosti a oprávnenia.

V tomto zozname nie sú zahrnuté špecifické funkcie, ako napríklad pracovníci Help Desk alebo administratívni pracovníci.

Entrust PKI definuje 4 stupne používateľov:
1. stupeň: pokročilý používateľ (power user),
2. stupeň: bezpečnostný technik (security officer),
3. stupeň: administrátor RA, audítor, adresárový administrátor,
4. stupeň: koncový používateľ (fyzická osoba, zariadenie).

Prvé tri stupne definujú tzv. pokročilých používateľov a hierarchia určuje aj stupeň privilégií, čo znamená, že hlavný používateľ (master user) je „najmocnejšia“ osoba v Entrust PKI.

Niektoré povinnosti pokročilých používateľov (power users):

V pozícii hlavný používateľ (master user):
– môžu byť maximálne traja, ide o najdôveryhodnejšie osoby,
– môže spustiť alebo zastaviť certifikačnú autoritu,
– môže vygenerovať nový kľúč certifikačnej autority, zrevokovať (zrušiť) certifikát certifikačnej autority a certifikáty všetkých používateľov,
– zodpovedá za nastavenie certifikačnej autority, za implementáciu a realizáciu zálohovania, obnovu údajov zo záloh.

V pozícii bezpečnostný technik:
– musí existovať minimálne jeden,
– nastavuje bezpečnostnú politiku, t. j. definuje typy a vlastnosti používateľov (okrem hlavného používateľa), definuje typy certifikátov, definuje vzťahy s inými certifikačnými autoritami (podriadené, krížovo certifikované).

Administrátor RA:
– nemusí existovať ani jeden,
– spravuje koncových používateľov – vkladá ich do systému, revokuje (ruší) im certifikáty, mení konkrétne hodnoty (meno, priezvisko).

Audítor:
– nemusí existovať ani jeden,
– monitoruje činnosť ostatných pokročilých používateľov.

Adresárový administrátor:
– spravuje adresár (directory), jeho povinnosti a právomoci vyplývajú z typu používaného adresára,
– táto funkcia je v Entrust PKI vyčlenená, pretože Entrust dokáže využiť ľubovoľný adresár podporujúci protokol LDAP v. 2, v. 3.

Na vybudovanie a prevádzku Entrust PKI s vlastnou certifikačnou autoritou by sme teda potrebovali minimálne 5 pokročilých používateľov. Toto je však v podmienkach SR stav, ktorý môže akceptovať len malý počet spoločností, preto je zaujímavá otázka vyťaženosti jednotlivých postov a ich možná kumulácia.

Vyťaženosť

Hlavný používateľ (master) zasahuje iba výnimočne. Pravidelne vykonáva iba zálohovanie, takže je vyťažený iba na pár hodín v rámci týždňa.

Bezpečnostný technik implementuje hlavne bezpečnostnú politiku. Jeho vyťaženosť závisí od frekvencie zmien bezpečnostnej politiky. Teoreticky sa raz nastavená bezpečnostná politika nemusí zmeniť vôbec.

Administrátor RA pracuje s koncovými používateľmi. Jeho vyťaženosť závisí od ich počtu. Väčšinou táto funkcia vyťažuje pracovníka na 100 %.

Audítor kontroluje činnosť ostatných hlavných používateľov. Jeho vyťaženosť závisí od definovaného auditného plánu. Obyčajne vykonáva svoju činnosť v pravidelných intervaloch – napr. jedenkrát do týždňa alebo mesiaca.

Adresárový správca je správca adresárov (directories). Keďže typ adresára nie je v Entrust PKI presne daný, jeho vyťaženosť sa odhaduje veľmi ťažko. Teoreticky nastavenie adresárov je potrebné meniť iba pri inštalácii a konfigurácii Entrust Authority.

Kumulácia

Najprirodzenejšia je kumulácia funkcie bezpečnostného technika a administrátora RA, pretože bezpečnostný technik má všetky právomoci administrátora RA.

Ďalšou prirodzenou kumuláciou je spojenie funkcie adresárového administrátora a existujúceho správcu systému.

Funkciu Entrust audítora môže vykonávať existujúci vnútorný audítor alebo externý audítor.

Z povahy funkcie hlavného používateľa (mastera) ako najdôveryhodnejšej osoby vyplýva, že ju pravdepodobne bude vykonávať existujúci dôveryhodný zamestnanec organizácie, ktorý určite nejakú funkciu (pravdepodobne dosť významnú) v rámci organizácie už zastáva.

Z uvedeného vyplýva, že pri budovaní certifikačnej autority na báze Entrust PKI budeme v „ideálnom“ prípade potrebovať zamestnať jediného pracovníka na kumulovanú funkciu administrátor RA a bezpečnostný technik.. Ostatných pokročilých používateľov vieme obsadiť existujúcimi pracovníkmi.

Niektoré problémy

V poslednej časti spomenieme niektoré problémy, s ktorými sme sa stretli pri nasadzovaní PKI.

Registrácia v systéme Entrust PKI

Na to, aby sa koncový používateľ stal plnoprávnym členom Entrust PKI, si musí vygenerovať tajný kľúč a dať si vystaviť certifikát verejného kľúča. Oprávnenie na túto operáciu získa tým, že od administrátora RA dostane aktivačný kód.

Pri distribúcii aktivačného kódu od administrátora RA ku koncovému používateľovi môže byť porušená zásada nepopierateľ-

nosti, ak aktivačný kód použije neoprávnená osoba. Riešenie je v tom, že aktivačný kód sa skladá z dvoch častí, ktoré administrátor RA môže zasielať nezávislými kanálmi (napr. SMS, e-mail, klasická pošta).

Existuje však aj nebezpečenstvo, že sám administrátor RA zneužije aktivačný kód. Tomuto sa dá zabrániť tak, že aktivačný kód sa bude automaticky zasielať bezpečnými kanálmi (napr. automatické zasielanie SMS, e-mailov, tlačenie na špeciálnej tlačiarni a vkladanie do zalepenej obálky). V tomto prípade je možnosť zneužitia aktivačného kódu administrátorom RA minimalizovaná, keďže administrátor RA aktivačný kód nikdy v otvorenom tvare neuvidí.

Distribúcia a správa aplikácií Entrust-ready

Entrust poskytuje celý rad aplikácií pre koncových používateľov a pomocou Entrust Desktop Solutions je možné vytvárať z kombinácií týchto aplikácií jeden inštalačný balík. Toto umožňuje vytvoriť pre konkrétneho koncového používateľa prostredie, ktoré presne vyhovuje jeho potrebám. Problém je však v správe takýchto balíkov, pretože po určitom čase by sme mohli stratiť prehľad, aké aplikácie má konkrétny používateľ nainštalované, takže by vznikali nejasnosti hlavne pri riešení problémov. Odporúčame definovať iba zopár typov balíkov s presne definovanými aplikáciami. Ich updatovanie je plne automatizované aplikáciou UpToDate.

Identifikácia vlastníka certifikátu

Predovšetkým pri komunikácii s orgánmi štátnej správy (daňové úrady) je nevyhnutné jednoznačne identifikovať vlastníka certifikátu, ktorý vytvoril elektronický podpis. Ak je v certifikáte uvedené, že patrí Andrejovi Vávrovi, táto informácia určite nepostačuje na jednoznačnú identifikáciu. Otázka znie, či máme nejaký jednoznačný identifikátor osoby. Odpoveď znie – nie. Existujú síce rodné čísla (aj tam však existujú duplicity), ale musíme si uvedomiť, že certifikát je verejná informácia, a preto všetky údaje v ňom zahrnuté sú verejne dostupné. V prípade zaradenia rodného čísla do certifikátu by sme sa však dostali do konfliktu so Zákonom o ochrane osobných údajov č. 428/2002 Z. z.

Určite bude nevyhnutné definovať verejne dostupný jednoznačný identifikátor osoby. Toto je však otázka skôr politická a súvisí aj so začleňovaním Slovenska do európskych štruktúr.

Dokumentácia

V pravom slova zmysle dokumentácia nepredstavuje problém. Chceme skôr upozorniť, že je to podceňovaná časť nasadzovania PKI, pritom sa však odhaduje, že tvorba dokumentácie tvorí až 70 % prác pri nasadzovaní systémov PKI. Medzinárodné štandardy aj slovenská legislatíva (hlavne vyhlášku NBÚ číslo 541/2002 Z. z.) predpisujú, aké typy dokumentácie musí mať vypracované certifikačná autorita. Okrem týchto povinných dokumentov vznikajú aj dokumenty súvisiace so zmenami pracovných postupov pri zavádzaní PKI. Napríklad môže ísť o interné smernice, ako majú používatelia pracovať s aplikáciami, ako a kde môžu používať elektronický podpis. Rozsah tejto následnej dokumentácie sa stanoví pri analýze požiadaviek a pri definovaní záberu nasadenia PKI. Často sa však až pri reálnom používaní zistí, že je nutné vytvoriť alebo modifikovať niektoré dokumenty. Tento proces nie je nikdy ukončený.

Manažované verzus nemanažované PKI

Entrust PKI dokáže poskytovať manažované aj nemanažované služby súčasne. Rozhodnutie, či poskytovať výlučne iba jeden typ služieb, je skôr strategické a obchodné. Závisí od typov koncových používateľov a hlavne od aplikácií, ktoré koncoví používatelia pri svojej práci používajú.

Výhody manažovaného PKI sú zrejmé už z názvu. Nemanažované PKI realizujú manipuláciu s kľúčmi tak, že napríklad výmena kľúčov a vystavovanie certifikátov prebieha automaticky. Ďalšou významnou vlastnosťou je história kľúčov. V prípade manažovaného PKI sa nemôže stať, že používateľ si zmení svoj kľúč a už sa nedostane k dátam, ktoré sú zašifrované so starým kľúčom. Aplikácie, ktoré umožňujú využiť výhody manažovaného Entrust PKI sa nazývajú aplikácie Entrust ready. Ak teda nasadzujeme Entrust PKI v internom prostredí organizácie, tak je prirodzené nasadiť manažované PKI, pretože sme schopní kontrolovať používané aplikácie koncových používateľov.

Mgr. Andrej Vávra 36

Tempest, s. r. o.
Landererova 1
811 09 Bratislava
Tel.: 02/50 26 71 11
e-mail: andrej_vavra@tempest.sk