Primarni Fokus: Smart Card Logon

Klijent: Hemofarm AD
Web Site: www.hemofarm.com
Br. Zaposlenih: 1000+
Zemlja: Srbija
Industrija: Farmaceutsko Hemijska

Profil Klijenta
Hemofarm koncern je međunarodna farmaceutska grupacija sa sedištem baziranim u Vršcu, Srbija. Pored proizvodnje farmaceutskih proizvoda i preparata, Hemofarm se bavi i proizvodnjom medicinskih sredstava, kozmetike, kućne hemije, ambalaže, veterinarskih preparata, sredstava za zaštitu bilja. Od 29 preduzeća u sklopu Hemofarm koncerna, 5 se bavi razvojem, proizvodnjom i prodajom lekova. Preduzeća u okviru Koncerna specijalizovana su i za trgovinsku, spoljnotrgovinsku delatnost, inženjering i pružanje širokog spektra usluga.

• Pregled Rešenja

• Namena

• Tehnički Izazovi

• Implementacija

• Obuka Korisnika

• Ključne Koristi

• Jedinstvenost Rešenja

Pregled Rešenja
Ovo rešenje realizovano je za Hemofarm koncern, jednu od vodećih farmaceutskih korporacija

na Balkanu.

Rešenje je imalo za cilj da obezbedi visok nivo integracije i primene PKI i smart card tehnologije u Windows Server 2003 Enterprise infrastrukturi. Hemofarm koncern je pre početka realizacije projekta već raspolagao stabilnom i pouzdanom infrastrukturom, koja je uspešno pružala podršku poslovanju centrale u Vršcu i distribuiranim organizacionim jedinicama u Rusiji, Americi, Bosni i Srbiji.

Osnovna namera bila je da se uvođenjem PKI i smart card tehnologije podigne opšti nivo bezbednosti u pristupu i rukovanju IT sredstvima, a da se pri tom ne naruši ni jedan od već postignutih nivoa raspoloživosti i performansi IT usluga.

Realizacija projekta tekla je u tri faze:
1. Prezentacija mogućnosti i obuka stručnog tima
2. Izbor i ispitivanje ciljnih funkcionalnosti
3. Dizajn sistema i primena ciljnih tehnologija u produkcionom okruženju

Zahtevani skup rezultata specificiran od strane stručnog tima korisnika obuhvatao je:
- Uspostavljanje adekvatne, fleksibilne PKI spremne da odgovori na izazove poslovne i geografske distribuiranosti kompanije
- Primena EFS uz visoko automatizovano upravljanje EFS sertifikatima, kontrola primenjenog sertifikata i automatsko kriptovanje sadržaja na osnovu postavljene konfiguracije (mogućnost specifikacije direktorijuma koji se automatski štite mehanizmima EFS-a)
- Primena smart card tehnologije u procesu interaktivnog logona i prilikom uspostavljanja VPN konekcija, potpisa Word dokumenata, generisanja digitalnog potpisa nad e-mail porukama i formiranja digitalne envelope oko e-mail poruka
- Potpuna kontrola i backup svih ključeva koji se koriste za potrebe enkripcije unutar baze CA servisa (EFS i enkripcija e-mail poruka)
- Jedinstveno administrativno okruženje namenjeno: inicijalizaciji smart kartica (priprema fajl strukture kartice), izdavanju sertifikata na smart karticama, upravljanju ključevima za pristup kartici i daljinskoj administraciji kartica
- Kontrola PIN-a na smart kartici – forsirana politika kompleksnosti PIN-a
  Nakon procene performansi, raspoloživosti i podrške, izabrana je Axalto Cryptoflex 32k smart kartica, kao hardverski nosilac RSA ključeva i digitalnog sertifikata krajnjeg korisnika.

Rešenje obuhvata:
- Upravljačke aplikacije za izdavanje, kontrolu i upravljanje događajima iz životnog veka kartice za više organizacionih i poslovnih nivoa (za Intranet korisnike, za Internet korisnike i izdavanje privremenih kartica za Intranet korisnike)
- Fini dizajn infrastrukture javnih ključeva (izabrana je troslojna infrastruktura), i posebno obrazaca sertifikata koji pokrivaju sve poslovne potrebe i različite metode izdavanja i zanavljanja sertifikata na smart karticama, a povezani su sa profilima fajl struktura na smart karticama
- Logon skriptove namenjene kontroli EFS okruženja, preko koga se forsira upotreba sertifikata za EFS v2, sa obezbeđenim bekapom ključeva unutar baze CA
- Logon skriptove namenjene kontroli sertifikata na smart kartici, izdavanju sertifikata za enkripciju e-mail poruka, automatsko zanavljanje sertifikata na karticama sa dva profila i izdavanje sertifikata za uspostavljanje VPN konekcija (sa specifičnim OID-om) na osnovu postojećeg, validnog interactive logon sertifikata
- Uslužne aplikacije za promenu PIN-a sa forsiranom PIN politikom

Namena: zamena postojećeg rešenja
Hemofarm koncern je pre primene ovog rešenja posedovao ranije podignutu PKI.
Ova infrastruktura je prevashodno korišćena za potrebe generisanja Web Server sertifikata za

interne web aplikacije. Infrastruktura nije izdavala klijentske sertifikate.
U toku primene našeg rešenja, postojeća PKI je zaustavljena, depublikacijom svih obrazaca na Issuing CA, a zatim su svi izdati sertifikati zamenjeni novim, izdatim od nove PKI.
Na kraju procesa, prethodna PKI je deinstalirana i po referencama uklonjena iz AD.

Tehnički Izazovi i načini njihovog prevazilaženja
Osnovni izazov u realizaciji i primeni ovog rešenja, bila je slaba podrška kompanije Microsoft upravljanju crypto strukturama na smart kartici i visoka očekivanja klijenta u pogledu nivoa njihove stabilnosti i upravljivosti. Ovo se pre svega odnosi na pouzdano upravljanje sertifikatima za enkripciju e-mail poruka koji se nalaze na smart kartici na alternativnom profilu. Sa druge strane, klijent je insistirao na integrisanom upravljačkom okruženju (jedinstvene aplikacije) koje u potpunosti podržava proces personalizacije.
Ovo očekivanje rezultiralo je formiranjem specifičnih aplikacija koje su integrisale upravljanje iz domena čiju podršku obezbeđuje proizvođač kartice, kao i iz domena za čiju podršku obezbeđuje Microsoft.

Ozbiljan izazov predstavljao je i visoko kontrolisan proces eksploatacije EFS. Zbog visoke distribuiranosti sistema, neraspoloživosti bezbednosno pouzdanog IT kadra na svim poslovno značajnim lokacijama, odustalo se od Data Recovery Agenata kao metode oporavka sadržaja zaštićenog EFS. Umesto toga iskorišćena je Key Recovery opcija, koja je uslovila razvoj pouzdanih mehanizama za upravljanje i kontrolu sertifikata koji se koriste za EFS.
Ova funkcionalnost je podržana namenski razvijenim logon skriptovima.

Implementacija
U implementaciju projekta krenulo se vrlo oprezno. Kao pilot sajt uzeti su IT sektor i sektor spoljne trgovine, s obzirom na to da su njihovi zahtevi za raspoloživošću i performansama, različite opcije korišćenja različitih servisa, potrebe za zaštitom tajnosti (EFS), kao i intenzivno korišćenje VPN pristupa, predstavljali etalon za kompletnu organizaciju koncerna.
Nakon uspešne primene u ovom okruženju, rešenje je prošireno na kompletnu infrastrukturu centrale u Vršcu kao i na sajt u Moskvi.

Osnovne koristi uvođenja rešenja:
- Ušteda sredstava planiranih za nabavku softvera za digitalnu enkripciju e-maila (razmatrana je nabavka PGP licenci)
- U roku od tri meseca preko 1000 korisnika Hemofarm koncerna je obučeno i aktivno koristi postavljenu PKI, u procesima interaktivnog logon-a i VPN pristupa za digitalno potisivanja pošte, enkripciju e-mail poruka i zaštitu podataka na disku (EFS).
- Integracija Windows identity-ja u SAP sistem (zahtevan smart card logon i politike provere raspoloživosti kartice u toku rada), odnosno optimizacija procesa administracije korisnika centralnog poslovnog sistema.
- Unapređenje bezbednosti VPN konekcija, kao čestog metoda povezivanja važnih korisnika IT infrastrukture
- Primenjena troslojna PKI obezbeđuje jednostavno proširenje infrastrukture i bolju mogućnost posvećivanja određenih Issuing CA izdavanju određenih sertifikata. Obezbeđena je podrška i za funkcionalnu i geografsku distribuciju funkcija izdavanja, čime je podignut opšti nivo raspoloživosti CA servisa
- Rešenjem su visoko automatizovane aktivnosti izdavanja sertifikata i nadzora nad korišćenjem PKI i smart card tehnologije, tako da se ovaj proces uklopio u postojeće procese administracije i upravljanja IT resursima, bez proširenja ljudskih resursa.

Obuka Korisnika
Prva faza realizacije projekta posvećena je obuci i treningu IT osoblja u domenu primene PKI i smart card tehnologije u Windows 2003 okruženju.

Obukom su pokriveni svi poznati slučajevi korišćenja ovih tehnologija vezanih za postojeće Microsoft platforme i osnovni slučajevi korišćenja hardverskih uređaja za sigurno čuvanje i korišćenje privatnih ključeva (HSM i smart card).
Obuka je izvedena u namenski izgrađenoj PKI laboratoriji u kojoj je simulirano produkciono okruženje (korišćenjem tehnologije Virtual server-a) i različite konfiguracije klijentskih i servisnih okruženja. Ovo okruženje je kasnije korišćeno u procesu evaluacije i testiranja namenski razvijenih aplikacija i skriptova.
Obuka poslovnog segmenta izvršena je od strane IT osoblja Hemofarm koncerna.

Ključne Koristi

Rešenjem je:
- Unapređena bezbednost procesa autentikacije (uvođenjem logon-a putem digitalnog sertifikata, eliminacijom password-a, uvođenjem smart kartice kao two-factor sredstva autentikacije)
- Povećan nivo bezbednosti značajnih poslovnih podataka na najnižem nivou (EFS)
- Unapređen nivo bezbednosti elektronske pošte upotrebom mehanizama digitalnog potpisa i digitalne envelope u kojima učestvuju različiti sertifikati, izdati po obrascima različite namene, a prisutni na istoj smart kartici.
- Obezbeđeno arhiviranje ključeva koji učestvuju u procesima digitalne enkripcije i ojačan je proces restauracije ključeva smeštanjem sertifikata Key Recovery agent-a na smart karticu.

Jedinstvenost Rešenja
Ovo rešenje pre svega predstavlja primer uspešne primene Microsoft PKI u Windows 2003 Enterprise okruženju. Dakle svi bezbednosni ciljevi koje adresira PKI: autentičnost, integritet i tajnost adresirani su i ovim projektom. Rešenje je dodatno adresiralo i bezbednost samih ključeva koje koristi PKI.
U realizaciji je korišćena smart kartica koja ne dozvoljava eksport privatnog ključa i obezbeđuje obavljanje kriptoloških operacija privatnim ključem na samoj kartici.
Rešenje je generalno namenjeno Microsoft Windows 2003 Enterprise okruženjima.
U ovom okruženju instaliraju se Enterprise CA servisi na Windows 2003 Serverima, koji će predstavljati Issuing CA tela. U ovoj konfiguraciji na raspolaganju nam je mehanizam formiranja novih Certificate obrazaca i uvođenje naprednih šema izdavanja sertifikata. Na ovoj infrastrukturi Enrollment stanice mogu biti standardni korisnički računari sa dva čitača na kojima se instaliraju aplikacije za upravljanje smart karticama (inicijalizacija kartice, izdavanje logon sertifikata, promena i deblokada PIN-a).

Aplikacija ima tri verzije:
- Verziju za enterprise pokriva sve tipove profila kartica
- Verziju za branch office pokriva izdavanje samo privremenih kartica
- Verziju za eksterne klijente pokriva izdavanje kartica samo za klijente koji koriste sertifikate u procesu logona na HTTS resurse

Shodno konfiguracijama podržanim kroz grupne polise na klijentskim računarima se instaliraju adekvatna verzija CSP - a, uslužne crypto, PKI i smart card aplikacije, i primenjuju odgovarajući namenski razvijeni skriptovi namenjeni upravljanju EFS sertifikatima i sertifikatima na smart karticama. Sve instalacije su pripremljene kao .msi paketi.