

Šta imam u IT sistemu?

## Karakteristike tipičnog IT sistema:

- Korisnici se autentifikuju korišenjem "username\password"
- Za uspostavljanje šifrovanih tunela koristi se "pre-shared secret"

Šta želim u IT sistemu?

## Prvi korak u podizanju nivoa bezbednosti IT sistema treba da obezbedi:

- Poverljivost
- Autentičnost
- Integritet
- Neporicivost

Kako to mogu da postignem?

## PKI (Public Key Infrastructure) Infrastruktura Javnih Ključeva

je tehnologija kojom se ovo postiže.

Deo naziva Javni Ključevi asocira na to da se koristi par ključeva za kriptografske operacije. Informacija koja se šifrjuje sa jednim ključem može da se dešifrjuje sa drugim. Jedan ključ je dostupan svima i nazivamo ga javnim ključem, a drugi ključ je tajni i njega nazivamo privatnim ključem.

Deo naziva Infrastruktura znači da postoji sistem kojim se obezbeđuje pravljenje para ključeva, sertifikata i objavljivanje relevantnih javnih informacija.

Digitalni sertifikat sadrži javni ključ sa informacijama o vlasniku, periodu važenja, kao i o tome ko je tvorac sertifikata. Sertifikat je javno dostupan svima. Digitalni identitet predstavlja digitalni sertifikat sa odgovarajućim parom ključeva.

Šta mogu sa PKI?

## Korišćenjem Infrastrukture Javnih Ključeva može da se obezbedi:

- Interaktivni logon Smart Karticama
- Korišćenje Digitalnog identiteta za autentifikaciju zaštićenim web sajtovima
- Korišćenje Digitalnog identiteta za autentifikaciju VPN serveru
- Korišćenje Digitalnog identiteta za IPSec tunel do VPN servera
- Digitalni potpis office dokumenata
- Enkcipcija fajlova na sistemu
- Enkcipcija mail poruka

Čemu služe smart kartice?

Najkritičnija tačka za upotrebu digitalnog identiteta je baratanje privatnim ključem. Najpouzdaniji hardverski uređaj za smeštanje privatnog ključa korisnika je Smart Kartica. Ona obezbeđuje da privatni ključ u fazi kreiranja i korišćenja nikad ne napušta smart karticu. A šta ćemo sa servisima? Kod servisa ne postoji user interface, pa se koriste HSM (Hardware Security Modul) uređaji.

Šta su problemi sa implementacijom PKI (366-i dan...)

Osnovni principi bezbednosti nalažu da privatni ključ, koji služi za neporicivost i autentičnost, mora postojati samo u jednoj instanci. Operacija enkripcije maila, sa druge strane, nalaže da se sertifikat kojim je podatak zaštićen mora i arhivirati (gubitak sertifikata za enkripciju ne sme da povlači gubitak samog enkriptovanog podatka).

Out-of-the-box sertifikat za Smart Card Login dozvoljava enkripciju maila, ali se taj sertifikat ne može arhivirati.

Ne postoje mehanizmi za praćenje životnog veka sertifikata na smart kartici.

Ne postoje Microsoft alati za upravljanje samim smart karticama.

Nekontrolisana enkripcija lokalnih podataka (EFS) može da prouzrokuje probleme u dekripciji. Svaki korisnik po definiciji ima mogućnost izdavanja sertifikata za EFS samom sebi (self-signed EFS sertifikat važi 100 godina!). EFS se lako uključuje, ali nema alata za centralizovano upravljanje.

## Rešenja

(odgovori na poslovne potrebe)

Kroz više projekata implementacije PKI i Smart Card tehnologije u velikim okruženjima (Hemofarm, EPS, Grad Beograd – Gradska Uprava) razvili smo aplikacije kojima konfiguriramo, upravljamo, rešavamo incidentne situacije. Standardni projekat sadrži sledeće faze: obuku (PKI Laboratorija – tehnički deo, PKI workshop – poslovni deo), dizajn PKI, dizajn Smart Card okruženja, dizajn serverskog okruženja i dokumentacioni i procesni okvir održavanja sistema.

### **Kroz višegodišnje iskustvo su razvijeni brojni aplikativni moduli, od kojih izdvajamo:**

- Osnovnu aplikaciju na Enrolment stanicama
- Logon skript za EFS
- Logon skript za Smart Kartice

### **Modulima se obezbeđuje:**

- Jasno definisanje tipova kartica u sistemu
- Centralizovano upravljanje kompletnim sistemom smart kartica sa rešavanjem incidentnih situacija
- Kontrolisano korišćenje EFS sa podrškom za recovery procese
- Rešava se problem digitalne enkripcije i potpisivanja uvođenjem kartice sa dva profila
- EFS radi enkripcije My Documents na osnovu članstva u grupi
- Jedna kartica sposobna da digitalno potpiše i dekriptuje e-mail
- Automatizovano i kontrolisano zadržavanje sertifikata na karticama
- Zaštita transporta smart kartice od trenutka izdavanja sertifikata do trenutka dostavljanja korisniku smart kartice
- Izdavanje i dostavljanje sertifikata VPN korisniku koji nije član domena
- Pokrivanje incidentnih situacija (zaboravljena ili izgubljena kartica)
- Pokrivanje incidentnih situacija (blokirana kartica)
- Povećanje opšteg nivoa bezbednosti informacionog sistema
- Povećanje nivoa znanja i veština u domenu PKI i Smart Card tehnologije na Windows platformi
- Značajne uštede u primeni infrastrukture javnih ključeva za najširi skup slučajeva korišćenja (digitalni dokumenti, zaštita web aplikacija i servisa)
- Optimizacija administrativnih aktivnosti vezanih za svakodnevnu podršku krajnjim korisnicima

## Zanimljivi slučajevi iz prakse

## Benefiti

## Kontakt

### **E-Smart Systems d.o.o.**

Blagoja Parovića 19, 11030 Beograd, Srbija

Tel: +381 (0) 11 30 50 200

Fax: +381 (0) 11 30 50 222

PKITeam@e-smart.co.yu

www.e-smart.co.yu