SISTEMI ELEKTRONSKOG PLAĆANJA 2021/2022

VEŽBE

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

ŠTA JE PCI DSS ?

- PCI DSS je nastao sa ciljem da poboljša bezbednost podataka vlasnika kartica, kao i da olakša usvajanje bezbednosnih mehanizama i mera na globalnom nivou
- PCI DSS obezbeđuje tehničke i operativne zahteve koji su dizajnirani da zaštite podatke o računu
- Standard se odnosi na sve entitete koji su uključeni u proces obrade platnih kartica


VISA
MasterCard
JCB
AMERICAN EXPRESS
DISCOVER
PCI DSS V1.0

DA LI MORAM DA SE PRIDRŽAVAM PCI DSS ?

- Sve organizacije koje prihvataju kartice, skladište ih, obrađuju ili prenose njihove podatke moraju da ispune sve zahteve iz standarda

6 grupa - 12 zahteva

I Build and Maintain a Secure Network and Systems

II.Protect Cardholder Data

III.Maintain a Vulnerability Management Program

IV Implement Strong Access Control Measures

V Regularly Monitor and Test Networks

VI Maintain an Information Security Policy

I BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS

~~Requirement 1: Install and maintain a firewall configuration to protect cardholder data~~

~~Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters~~

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Nije dovoljno samo instalirati firewall

~~1.Podesiti firewall i ruter tako da se ograniče konekcije između nepouzdanih mreža i komponenata sistema, koje rade sa osetljivim podacima~~
~~2. Zabraniti direktan pristup komponentama sistema na Internet~~
~~3. Zaštiti uređaje koji se koriste van mreže~~
~~4. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za upravljanje firewall-om~~

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Napadači mogu da zloupotrebe inicijalno postavljenje, podrazumevane lozinke i podešavanja

1. ~~Uvek promeniti podrazumevane lozinke i onemogućiti upotrebu podrazumevanih naloga~~
2. ~~Kreirati konfiguracione standarde za sve komponente sistema~~
3. ~~Šifrovati administrativni pristup~~
4. ~~Redovno vršiti popis sistemskih komponenti koje su u opsegu PCI DSS~~
5. ~~Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za upravljanje podrazumevanim vrednostima i drugim sigurnosnim parametrima~~

II PROTECT CARDHOLDER DATA

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 3: Protect stored cardholder data

Napadači mogu da zloupotrebe skladištene podatke koji nisu zaštićeni

1. Svesti podatke koji se skladište na minimum
   - Čuvamo samo ono što moramo. Pan broj, ime vlasnika i ostali podaci o kartici su skladišteni u bazi. Rezultate transakcija ne čuvamo, nego logujemo.
2. Podatke za autentifikaciju ne treba čuvati nakon autorizacije
   - Ne čuvamo authenitfication header sa jwt tokenom. Sa svakim zahtevom šalje se token i vrši se autorizacija.
3. Ceo PAN broj ne sme da se prikaže
   - Ne prikazujemo ceo pan broj, prikazujemo prve 4 i poslednje 4 cifre kako ne bi neko drugi mogao da vidi pan broj i zloupotrebi ga. Ima smisla da neko može da vidi pan broj, ali za to mora imati poslovnu potrebu.
4. Onemogućiti čitanje PAN broja iz baze
   - Pan broj se svuda šalje enkriptovan i u bazi je zapisan u enkriptovanom obliku. Za enkripciju i dekripciju korišćen je AES algoritam sa CBC operacijom (AES/CBC/PKCS5PADDING). Za enkripciju je korišćen taj algoritam, secret key i enkriptovani vector.
5. Dokumentovati i implementirati procedure za zaštitu ključeva
   - Koristimo ključ koji je 128-bitni enkriptovani ključ koji je dodatno enkriptovan kako ne bi svako imao pristup njegovoj vrednosti.
6. Dokumentovati i implementirati sve procese i procedure za upravljanje ključevima
   - Ključ i vektor koji smo koristili smo dodatno enkriptovali pomoću JASYPT encryptor-a. Čuvamo ih na jednom mestu u application.properties. JASYPT za algoritam koristi PBEWithMD5AndTripleDES, a lozinka je sačuvana kao varijabla u lokalnom sistemu.
7. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za zaštitu podataka koji se skladište
   - Svi koji rade na implementaciji projekta su upoznati sa bezbednosnim propisima i operativnim procedurama za zaštitu podataka koji se skladište.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Napadači mogu da zloupotrebe podatke, koji nisu zaštićeni, a šalju se sa jedne na drugu lokaciju

1. Koristiti bezbednosne protokole, kao što je SSL/TLS, SSH itd. da bi se zaštitili osetljivi podaci tokom prenosa
   - Sva moguća komunikacija se odvija pomoću HTTPS. Napravljeni su self-signed sertifikati. Za mikroservise je implementirana two-way SSL komunikacija. Pristup ka bazi podataka je takođe osiguran putem SSL-a.
2. Nezaštićen PAN broj ne sme da se šalje preko platformi za razmenu poruka (e-mail, instant messaging, chat..)
   - Nezaštićen PAN broj se ne šalje preko platforme za razmenu poruka.
3. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za zaštitu podataka, koji se šalju sa jedne na drugu lokaciju
   - Svi koji rade na implementaciji projekta su upoznati sa bezbednosnim propisima i operativnim procedurama za zaštitu podataka koji se šalju sa jedne na drugu lokaciju.

III MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

~~Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs~~

Requirement 6: Develop and maintain secure systems and applications

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Maliciozni softver može da izvrši napad, ako ne postoji odgovarajući antivirus

1. ~~Postaviti antivirus na sve sisteme koji su često meta napada~~
2. ~~Obezbediti redovno održavanje antivirusa~~
3. ~~Obezbediti da antivirus aktivno radi i da korisnici ne mogu da ga onemoguće ili izmene~~
4. ~~Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za zaštitu sistema od malvera~~

Requirement 6: Develop and maintain secure systems and applications

Napraviti i održavati bezbedne sisteme i aplikacije

1. Uspostaviti mehanizam za identifikovanje ranjivosti i njihovo rangiranje
   - Model pretnji je specificiran u dokumentu za najviše ocene.
2. Osigurati da su sve sistemske komponente zaštićene od ranjivosti blagovremenim update-om
   - Prvo će se rešavati ranjivosti koji imaju najveći prioritet iz specificiranog modela pretnji.
3. Razvojno/test okruženje odvojiti od produkcije; podela dužnosti; ne koristiti prave PAN brojeve
   - Trenutno smo u fazi razvoja, kada bude rađena produkcija okruženje će biti izmenjeno. Neće biti isti ljudi u razvojnom i produkcijskom okruženju. Za test aplikacije se ne koriste pravi PAN brojevi kako ne bi došli u situaciju da ih neko drugi vidi.
4. Best practices
   - Koristimo tehnike sigurnog kodiranja kao što su validacija input-a, smanjenje upozorenja na back-end-u, najjednostavnija rešenja, podrazumevane akcije su deny/false, samo osobe koje su zadužene za neku funkcionalnost je stvarno i obavljaju, XSS (ESAPI), svaki mikroservis ima zasebne provere, penetraciono testiranje.
5. Kontinuirana procena i rad sa ranjivostima
   - Kontinuirano testiranje i otklanjanje ranjivosti.
6. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za održavanje bezbednih sistema i aplikacija
   - Svi koji rade na implementaciji projekta su upoznati sa bezbednosnim propisima i operativnim procedurama za održavanje bezbednih sistema i aplikacija.

IV IMPLEMENT STRONG ACCESS CONTROL MEASURES

Requirement 7: Restrict access to cardholder data by business need to know

Requirement 8: Identify and authenticate access to system components

~~Requirement 9: Restrict physical access to cardholder data~~

Requirement 7: Restrict access to cardholder data by business need to know

Veoma je bitno *ko, zašto* i *kako* može da pristupi podacima

1. Ograničiti pristup komponentama sistema i podacima
   - Implementirana je autentifikacija i autorizacija za uloge CUSTOMER i ADMIN.
2. Smernice za kontrolu pristupa
3. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za ograničavanje pristupa podacima
   - Svi koji rade na implementaciji projekta su upoznati sa bezbednosnim propisima i operativnim procedurama za ograničavanje pristupa podacima.

Requirement 8: Identify and authenticate access to system components

Dodeliti ID svakom pojedincu, da bi se lako otkrili odgovorni

1. Definisati i implementirati procedure za pravilno upravljanje korisnicima, koji nisu potrošači, i administratorima, koji ne koriste sve komponente sistema
   - Svaki korisnik se jedinstveno identifikuje tj. dodeljen mu je jedinstveni UUID.
2. Najmanje jedan mehanizam za potvrdu identiteta
   - Logovanje putem email-a i lozinke koja mora biti sačinjena od minimum 8 karaktera, od toga minimum jedan karakter mora biti veliko slovo, malo slovo, broj i specijalni karakter.
3. Dvostruka potvrda identiteta
   - Udaljeni korisnici koji pristupaju podacima.
4. Dokumentovati procedure za autentifikaciju (smernice kako zaštiti kredencijale, uputstvo za promenu lozinke..)
   - Pri registraciji korisnik će dobiti smernice za dobru lozinku i naknadno uputstvo za promenu lozinke.
5. Ne koristiti grupne, deljene ili generičke IDs, lozinke..
   - Koristimo UUID, lozinke su bikriptovane.
6. Mehanizam za potvrdu identiteta dodeliti pojedinačnom nalogu
   - Svaki se identifikuje pomoću jedinstvene email adrese.
7. Svaki pristup bazi podataka treba da bude ograničen
   - Korisnici sistemski pristupaju bazi podataka, a admin pomoću unesene lozinke ima mogućnost ručne izmene podataka u bazi.
8. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za potvrdu identiteta i da su dokumentovani, u upotrebi i poznati svim stranama
   - Svi koji rade na implementaciji projekta su upoznati sa bezbednosnim propisima i operativnim procedurama za potvrdu identiteta i dokumentovani, u upotrebi i poznati svim stranama.

Requirement 9: Restrict physical access to cardholder data

Ako se fizički pristup uređajima, koji sadrže podatke sa kartica, ne ograniči, omogućava se lak pristup podacima

1. ~~Koristiti odgovarajuće kontrole ulaska u objekte, da bi se ograničio i nadzirao fizički pristup sistemima, koji rade sa osetljivim podacima~~
2. ~~Razviti procedure za lako razlikovanje osoblja od posetilaca~~
3. ~~Kontrolisati fizički pristup osoblja u delovima gde se nalaze osetljivi podaci~~
4. ~~Implementirati mehanizme za identifikovanje i autorizaciju posetilaca~~
5. ~~Fizički osigurati sva skladišta~~
6. ~~Održavati strogu kontrolu nad unutrašnjom ili spoljašnjom distribucijom bilo koje vrste skladišta~~
7. ~~Održavati strogu kontrolu nad skladištenjem i dostupnošću media~~
8. ~~Uništavanje skladišta kada više nisu potrebni iz poslovnih ili pravnih razloga~~
9. ~~Onemogućiti da uređaji, koji hvataju podatke sa platnih kartica direktnom fizičkom interakcijom, izvrše neovlašćene promene~~
10. ~~Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za ograničavanje fizičkog pristupa osetljivim podacima, da su dokumentovani, u upotrebi i poznati svim stranama~~

V REGULARLY MONITOR AND TEST NETWORKS

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 10: Track and monitor all access to network resources and cardholder data

Voditi evidenciju svih aktivnosti

1. Postupak za povezivanje svih pristupa komponentama sa pojedinačnim korisnikom
   - Vodimo evidenciju o aktivnostima korisnika putem log fajla.
2. Mehanizam za praćenje svih događaja (pojedinačan pristup, akcije administratora, neuspešna prijava,..)
   - Korišćenje logova.
3. Za svaki događaj sačuvati: tip događaja, datum i vreme, izvor...
   - Za logovanje koristimo logback pomoću kog znamo kada i šta se desilo. Logovanje se vrši obavezno na početku, u toku i na kraju svake aktivnosti.
4. Sinhronizacija vremena
   - U application.properties je dodata vremenska zona Europe/Berlin. Koristi se ISO6801 standard.
5. Review logova
   - Review logova se radi svaki vikend.
6. Čuvati istoriju
   - Čuvamo logove u log fajlu.
7. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za nadgledanje svih pristupa podacima
   - Svi koji rade na implementaciji projekta su upoznati sa bezbednosnim propisima i operativnim procedurama za nadgledanje svih pristupa podacima.

Requirement 11: Regularly test security systems and processes

Zlonamerni pojedinci teže otkrivanju ranjivosti u sistemima, te je veoma važno redovno sprovođenje testiranje komponenti, softvera i procesa

1. ~~Implementirati procese za testiranje prisustva bežičnih pristupnih tačaka~~
2. Skeniranje ranjivosti interne i eksterne mreže najmanje kvartalno i nakon bilo kakvih značajnih promena na mreži
   - Pokretanje testiranja na svaka tri meseca.
3. Penetraciono testiranje
   - Izvršeno je penetraciono testiranje.
4. Koristiti tehnike za sprečavanje i/ili otkrivanje upada na mrežu. Nadgledati sav saobraćaj na obodu CDE, kao i na kritičnim tačkama CDE
5. Primeniti mehanizam za otkrivanje promena (alati za praćenje integriteta datoteka) kako bi se osoblje upozorilo na neovlašćenu modifikaciju kritičnih sistemskih datoteka, konfiguracionih datoteka itd.
6. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za nadzor i testiranje, da su dokumentovani, u upotrebi i poznati svim stranama
   - Svi koji rade na implementaciji projekta su upoznati sa bezbednosnim propisima i operativnim procedurama za nadzor i testiranje, da su dokumentovani, u upotrebi i poznati svim stranama.

VI MAINTAIN AN INFORMATION SECURITY POLICY

Requirement 12: Maintain a policy that addresses information security for all personnel

Requirement 12: Maintain a policy that addresses information security for all personnel

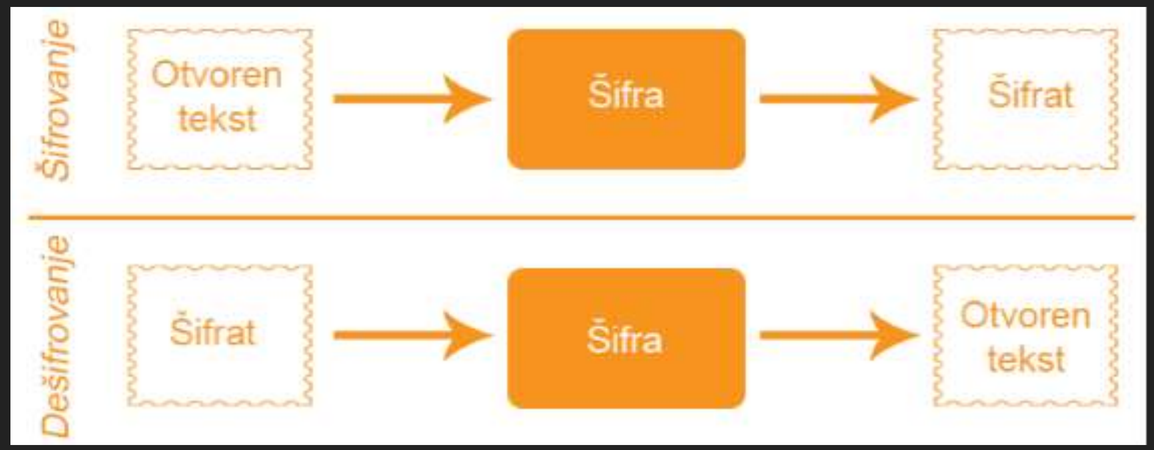
Dobro razvijene, sveobuhvatne procedure za očuvanje bezbednosti podataka su osnova za usklađenost sa PCI DSS

1. Uspostaviti i održavati bezbednosne procedure
2. Procena rizika
3. Definisati pravilnu upotrebu tehnologija
4. Procedure sa jasno definisanim odgovornostima
5. Dodeliti pojedincu ili timu odgovornost za upravljanje bezbednosnim procedurama
6. Organizovati treninge/seminare za osoblje
7. Proveriti da li osoba koja se zapošljava na ključnu poziciju ima kriminalnu prošlost
8. Primeniti i održavati procedure za eksterne servise koji rade sa podacima
9. Dodatni zahtev za eksterne servise
10. Plan reagovanja na incidente

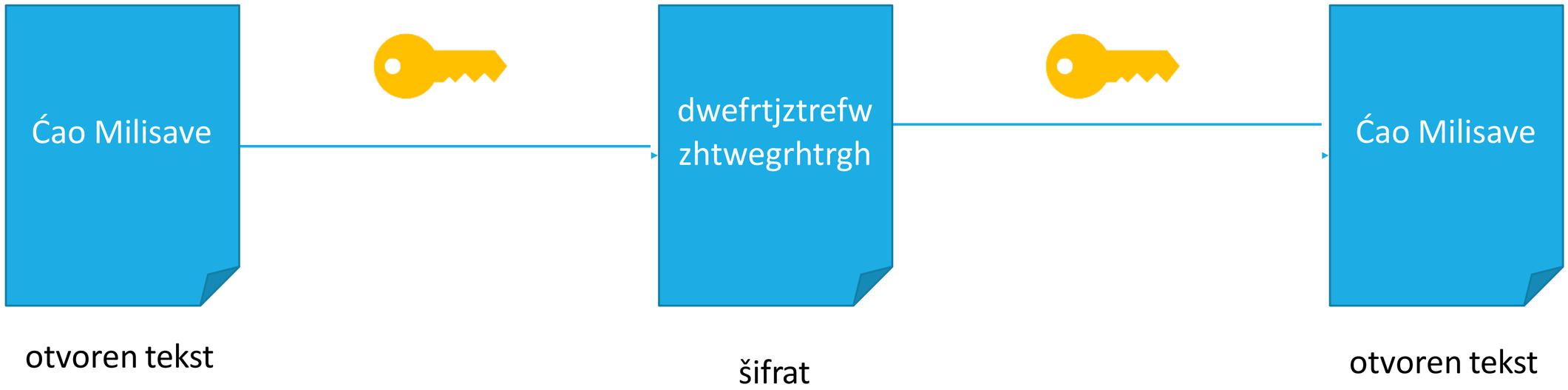
PODSETNIK - KRIPTOGRAFSKE PRIMITIVE, SERTIFIKATI

KRIPTOGRAFSKE PRIMITIVE

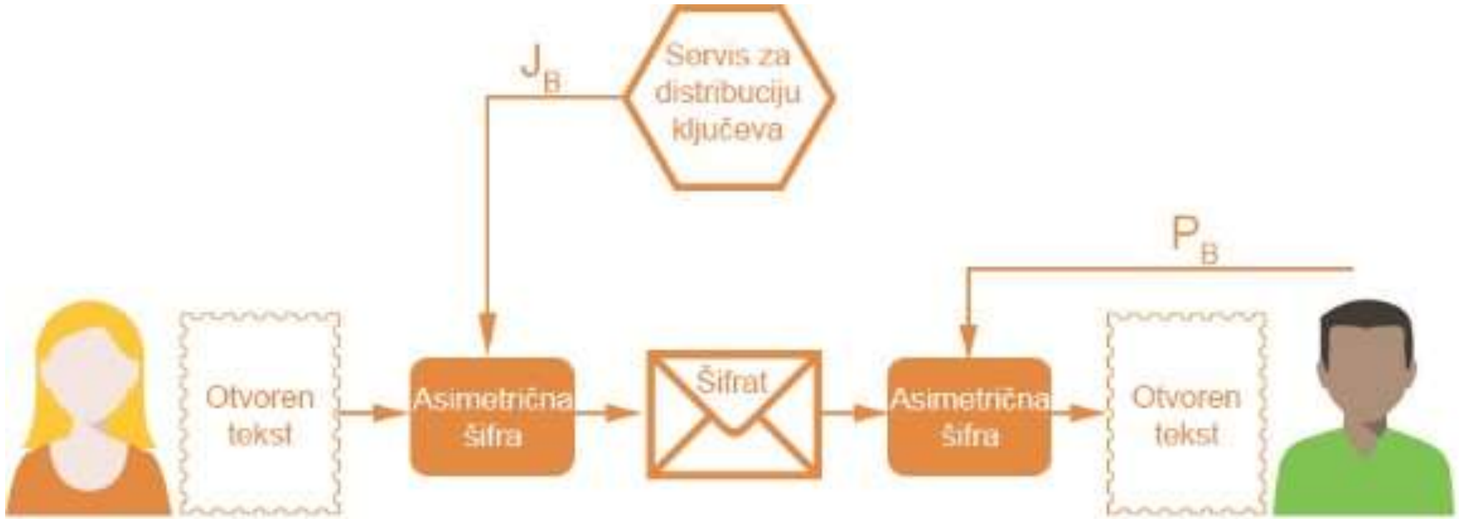
- Simetrične šifre
- Asimetrične šifre
- Heš funkcije



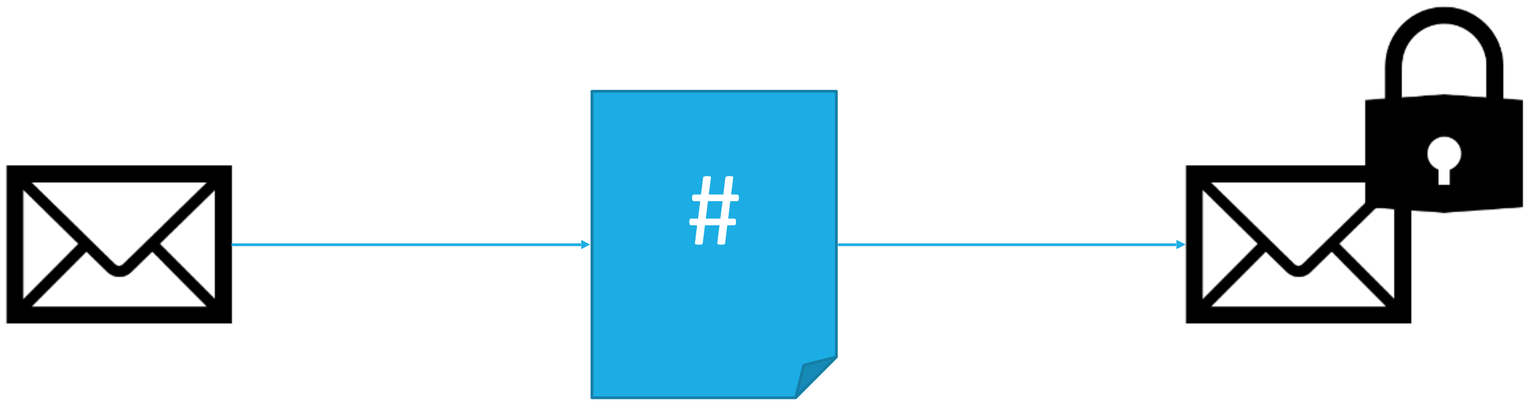
SIMETRIČNE ŠIFRE



ASIMETRIČNE ŠIFRE



HEŠ FUNKCIJE

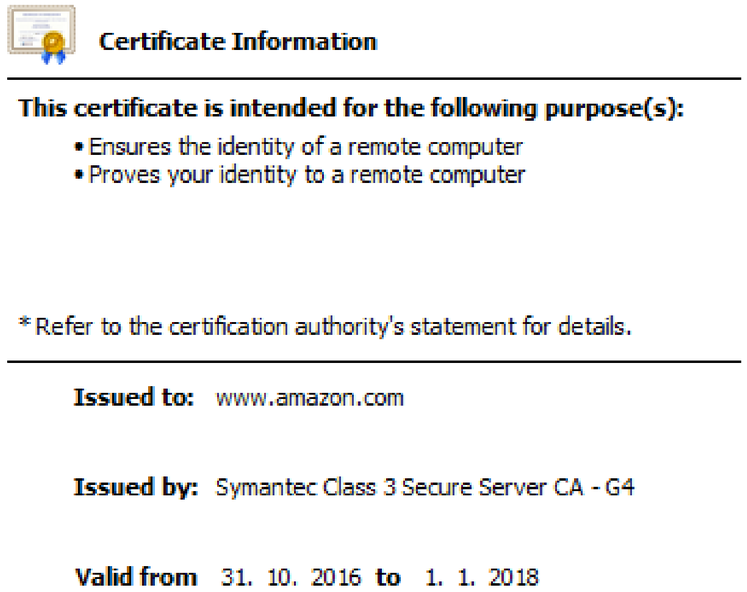


DIGITALNI SERTIFIKAT

Digitalni sertifikat je elektronski dokument koji sadrži sledeće podatke:

- Ko je izdao sertifikat;
- Kome je sertifikat izdat;
- Kada je sertifikat izdat;
- Do kada je sertifikat validan;
- Javni ključ povezan sa sertifikatom i identitetom kom je sertifikat izdat;
- Digitalni potpis formiran od strane izdavaoca sertifikata

… … .



HIJERARHIJA SERTIFIKATA

Sertifikaciono telo (Certificate Authority) izdaje digitalni sertifikat