Centar Informacijske Sigurnosti

HSM moduli

veljača 2012.

CIS-DOC-2012-02-041

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. UVOD 4

2. HSM MODULI 5

2.1. FUNKCIONALNOSTI HSM MODULA 6

2.1.1. Šifriranje podataka 6

2.1.2. Digitalni potpis 6

2.1.3. Izračunavanje sažetka 7

2.1.4. Kod za ovjeru poruke 8

2.1.5. Upravljanje ključevima 9

3. PREDNOSTI I NEDOSTACI HSM MODULA 10

3.1. PREDNOSTI HSM MODULA 10

3.2. NEDOSTACI HSM MODULA 11

4. PRIMJENE HSM MODULA 12

4.1. INFRASTRUKTURE S JAVNIM KLJUČEM 12

4.2. SUSTAVI S KARTIČNIM PLAĆANJEM 12

4.3. SSL POVEZANOST 13

5. NAČIN RADA HSM MODULA 14

6. CERTIFICIRANJE HSM MODULA 15

7. ZAKLJUČAK 17

8. LEKSIKON POJMOVA 18

9. REFERENCE 20

1. Uvod

Ljudi se od davnina bave problematikom slanja poruka nesigurnim kanalima i oduvijek žele sigurno komunicirati. Iako su se kroz stoljeća načini prenošenja poruka znatno promijenili, još uvijek je prisutan osnovni problem - kako onemogućiti onoga tko može nadzirati kanal kojim se prenosi poruka da dozna njen sadržaj.

Jedan od načina zaštite poruke je upotrijebiti znanje kriptografije i šifrirati poruku tako da je može razumjeti samo onaj kome je ona namjenjena. Razvojem tehnologije, a posebno Interneta, potreba za sigurnošću prijenosa podataka raste. Kako znati da poruka nije putem izmijenjena? Kako znati da je sugovornik onaj za koga se izdaje? Na papiru je potpis dovoljan dokaz vjerodostojnosti, ali kako provjeriti indentitet pošiljatelja poruke poslane preko Interneta ?

Osim toga, pojedini algoritmi za kriptiranje podrazumijevaju uz javni ključ postojanje i tajnog ključa pa se kao dodatan problem javlja i potreba za zaštitom tajnih ključeva.

Sve spomenute probleme vezane uz zaštitu podataka i sigurnost alata kojima se ta zaštita postiže nastoje riješiti HSM moduli. HSM moduli se mogu koristiti za razne zadatke kao što su stvaranje ključeva i njihova sigurna pohrana, pomoć pri autentikaciji provjerom digitalnog potpisa, zatim kao sredstvo za sigurno šifriranje osjetljivih podataka za pohranu u relativno nesigurnim lokacijama kao što su baze podataka, sredstvo za verifikaciju integriteta podataka pohranjenih u bazi podataka, generator ključeva za pametne kartice i sl.

Na početku ovog dokumenta je objašnjeno što su to HSM moduli i čemu služe funkcionalnosti koje mogu obavljati. Nakon toga su opisane prednosti i nedostaci HSM modula, područja u kojima se oni primjenjuju te kratak opis načina rada. Posebno poglavlje posvećeno je certificiranju HSM modula. Na kraju se nalazi poglavlje koje opisuje što se može očekivati u budućnosti HSM modula.

2. HSM moduli

Slopovski sigurnosni moduli ili skraćeno HSM (eng. *hardware security module*) moduli su vrsta sigurnih kriptoprocesora čiji je cilj upravljanje ključevima te ubrzanje kriptografskih procesa kao što su digitalni potpisi, provjere valjanosti i integriteta prilikom pristupa ključevima poslužiteljskih aplikacija itd.

Smatraju se kriptoprocesorima s visokim stupnjem zaštite i uobičajeno se koriste na poslužiteljima u poduzećima (eng. *Enterprise servers*). HSM moduli mogu imati više stupnjeva fizičke zaštite s kriptoprocesorom na jednom čipu (ili više kriptoprocesora) kao svojom najosiguranijom komponentom. Kriptoprocesori ne otkrivaju ključeve ili instrukcije koje izvode na sabirnici, osim u šifriranoj formi, i automatski brišu podatke ako se pojavi naznaka fizičkog proboja sigurnosti. Uz sam kriptoprocesor, HSM obično sadrži još nekoliko procesora i memorijskih čipova koji pohranjuju i obrađuju šifrirane podatke.

Kao što je već spomenuto, HSM moduli su fizički uređaji s pripadnim programom i dolaze u obliku „plug-in“ kartice (slika 1) ili vanjskog TCP/IP (eng. *Transmission Control Protocol / Internet Protocol*) sigurnosnog uređaja (slika 2) koji se mogu spojiti izravno na poslužitelj ili računalo opće namjene.

Slika 1. Plug-in kartica (Stariji Luna HSM, PCMCIA)
Izvor: Wikipedia, armedforces-int.com

Slika 2. HSM kao vanjski uređaj (SafeNet Luna XML)
Izvor: cyprotect.com

2.1. Funkcionalnosti HSM modula

HSM modul može izvoditi različite funkcije vezane uz sigurnost i zaštitu kriptografskih ključeva. Također omogućuje ubrzane kriptografske operacije kao što su šifriranje, digitalni potpis ili izračunavanje sažetka. U nastavku će biti objašnjene neke od tih funkcija.

Danas se za pristup i korištenje HSM modula najčešće koristi PKCS #11[1] API koji definira najčešće korištene tipove kriptografskih objekata (razni ključevi i certifikati) i sve funkcije potrebne za njihovo korištenje, stvaranje, izmjenu ili brisanje.

2.1.1. Šifriranje podataka

Šifriranje (eng. *encryption*) je pretvaranje izvornog teksta (eng. *plaintext)* u šifrirani tekst *(eng. ciphertext)* pomoću određene šifre (tj. algoritma kao što je AES[2] ili 3DES[3]). [5]

Postupak se sastoji od izmjene dijelova teksta,primjerice na način da sva slova u abecedi pomaknemo za tri mjesta naprijed u abecedi (tzv. Cezarova šifra), tako da riječ INFORMACIJA postaje LQIRUPDFLMD. Moderni postupci su naravno mnogo složeniji.

Obrnuti postupak – dešifriranje (eng. *decryption*) – odnosi se na omogućavanje čitanja šifriranih podataka korisnicima koji posjeduju ključ. Time su podaci zaključani na način da je tijelo informacije (tekst) nečitljivo korisnicima koji ne posjedu ključ (*password*) – u primjeru je ključ informacija da su slova pomaknuta za tri mjesta.

Kao što je već spomenuto, HSM moduli nude mogućnost šifriranja podataka, a PKCS #11 API između ostalih kriptografskih objekata definira i DES/Triple DES ključeve kao i sve funkcije za njihovo korištenje.

2.1.2. Digitalni potpis

Digitalni potpis (eng. *digital signature*) predstavlja prvi stupanj u identifikaciji stranaka koje razmjenjuju poruke. Postupak digitalnog potpisa prikazan je na slici 3.

Iz poruke pošiljatelj izračunava sažetak poruke (korištenjem nekog matematičkog alata za izračunavanje sažetka). Sažetak se kriptira privatnim ključem pošiljatelja i dodaje se izvornoj poruci.

[1] PKCS#11 (eng. *Public-Key Cryptography Standard*) - standard kojeg je izdao RSA laboratorij, a koji definira platformno nezavisan API prema kriptografskim tokenima.(kao što su HSM moduli i pametne kartice)

[2] AES (eng. *Advanced Encryption Standard*) je specifikacija za šifriranje elektroničkih podataka. To je vrsta algoritma sa simetričnim ključem, što znači da se isti ključ koristi za kodiranje i dekodiranje podataka.

[3] 3DES (eng. *Triple Data Encryption Algorithm*) je algoritam koji pri šifriranju podataka primjenjuje DES šifru tri puta na svaki blok podataka.

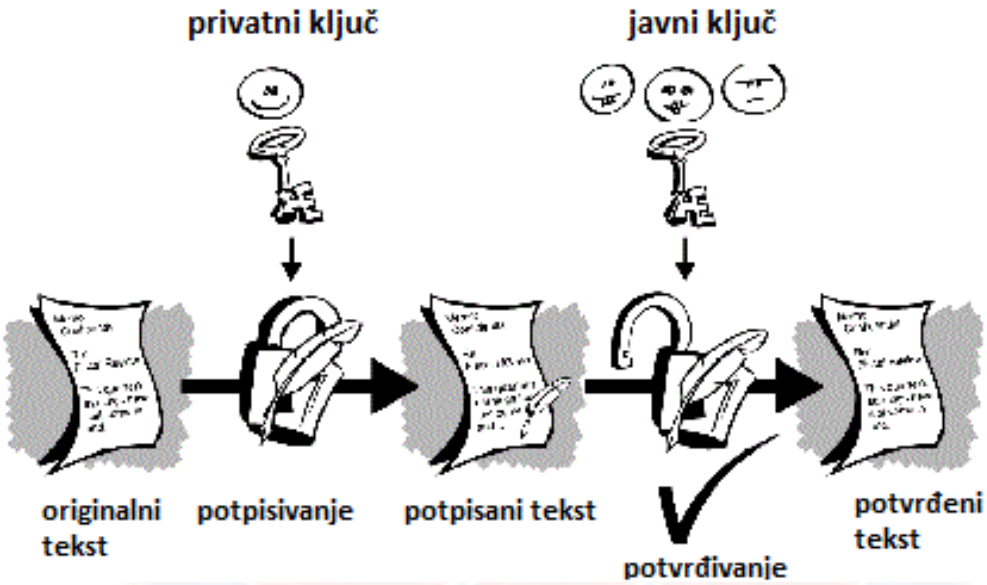
Primatelj može utvrditi autentičnost pošiljatelja takve poruke, kao i potvrditi integritet poruke dekriptirajući digitalni potpis javnim ključem pošiljatelja i uspoređujući rezultat s izračunatim sažetkom primljene poruke dobivenim korištenjem istog matematičkog algoritma kojeg je primijenio i pošiljatelj. [6]

Dakle, digitalni potpis osigurava:

- autentičnost (identitet pošiljatelja utvrđuje se dešifriranjem sažetka poruke),
- integritet (provjerom sažetka poruke utvrđuje se je li poruka izmijenjena na putu do primatelja) i
- neporecivost (pošiljatelj ne može poreći sudjelovanje u transakciji jer jedino on ima pristup do svog privatnog ključa kojim je potpisao poruku).

Današnje tehnike digitalnog potpisivanja temelje se na algoritmima kao što su RSA[4] i DSA[5].

Zahvaljujući PKCS #11 API-ju aplikacije mogu koristiti i ovu funkcionalnost HSM modula jer spomenuti API definira i ključeve potrebne za ispravan rad funkcije digitalnog potpisivanja.



Slika 3. Princip potpisivanja poruke
Izvor: tspace.library.utoronto.ca

2.1.3. Izračunavanje sažetka

Na području zaštite podataka hash funkcija predstavlja deterministička proceduru koja uzima blok podataka i vraća niz bitova definirane duljine (tzv. hash vrijednost) takav da slučajna ili namjerna promjena danog bloka podataka automatski mijenja i hash vrijednost. Podaci koji se hashiraju uobičajeno se nazivaju "poruka" (eng *message*), a dobivena hash vrijednost "sažetak" (eng. *message digest*).

U današnje vrijeme dvije najpopularnije hash funkcije su MD5[6] i SHA-1[7]. Na slici 4 prikazan je rad hash funkcije SHA-1. Osobito valja primjetiti kako i malena promjena ulaznog bloka podataka vodi do velike promjene u hash vrijednosti. [7]

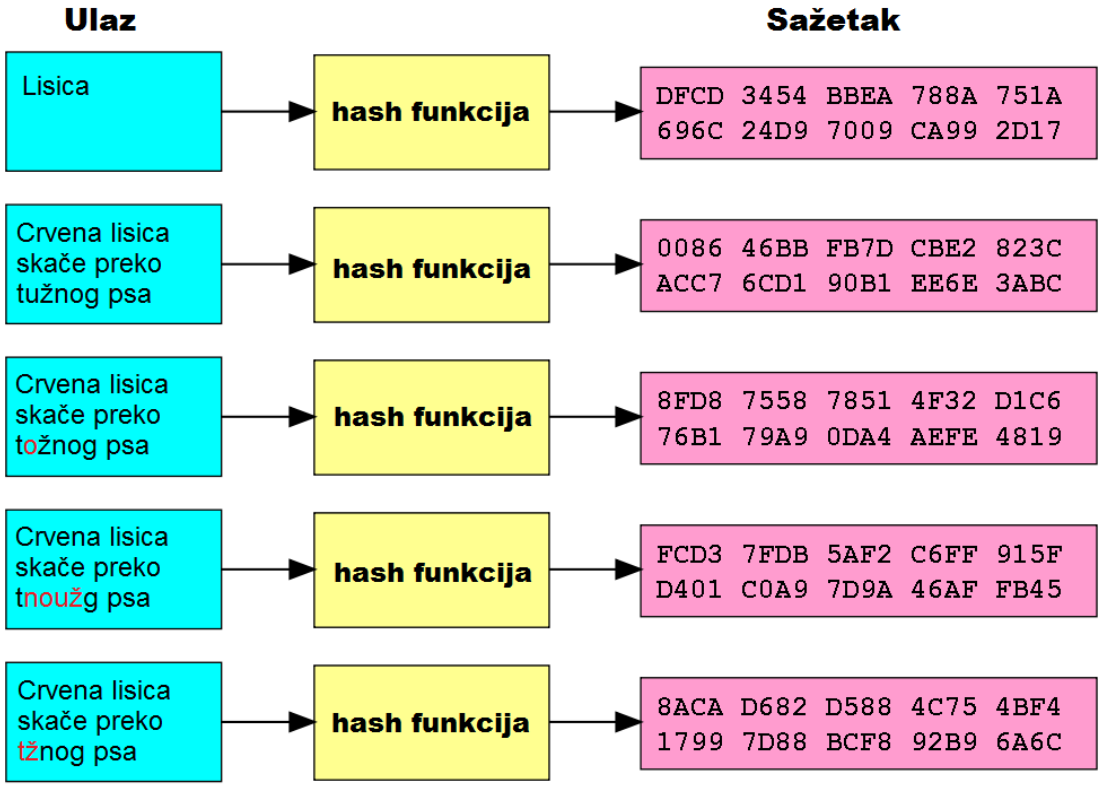
[4] RSA - Ovaj algoritam je predstavljen u javnosti 1977. godine od strane tri američka znanstvenika - Ronalda Rivesta, Adija Shamira i Leonarda Adlermana. Algoritam je skraćenica od tri prezimena: Rivest, Shamir i Adlerman. To je algoritam šifre javnog ključa (eng. *public-key encryption*), i bio je prvi algoritam koji se koristio za potpisivanje (utvrđivanje izvornosti poruke) te za šifriranje podataka. Još se koristi u računarstvu za zaštitu podataka i u elektronskom poslovanju.

[5] DSA (eng. *Digital Signature Algorithm*) je standard za digitalne potpise predstavljen u kolovozu 1991. godine.

[6] MD5 je ime za kriptografsku hash funkciju koja je dugačka 128 bita, ratificiranu internetskim standardom RFC 1321. Koristi se u sigurnosne svrhe za ratificiranje izvornosti datoteka ili podataka. Ovu funkciju je dizajnirao amerikanac Ronald Rivest 1991. godine.

[7] SHA-1 (eng. *Secure Hash Algorithm*) je kriptografska hash funkcija, najrasprostranjenija među postojećim SHA hash funkcijama (uz nju postoje SHA-0 i SHA-2) i koristi se u nekoliko širokorasprostranjenih sigurnosnih aplikacija i protokola.

HSM moduli nude i ovu funkcionalnost, a zbog prije spomenutog PKCS #11 API-ja njeno korištenje je uvelike olakšano.



Slika 4. Rad hash funkcije SHA-1
Izvor : Wikipedia

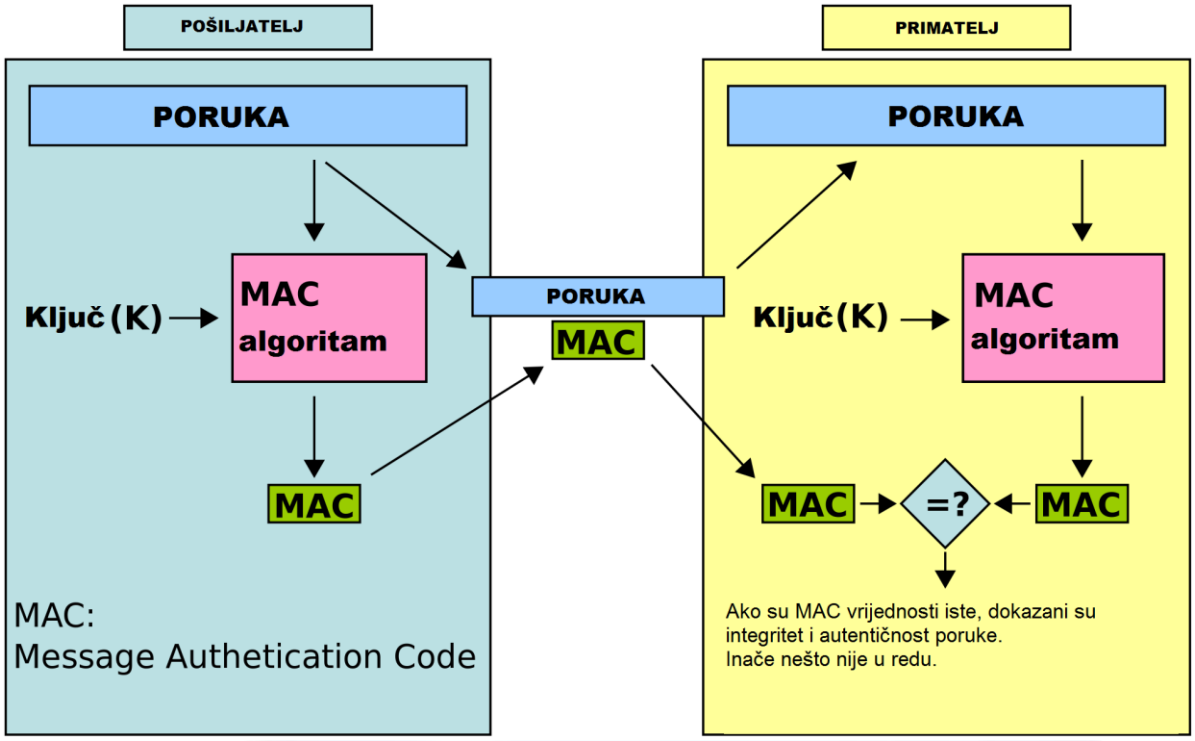
2.1.4. Kod za ovjeru poruke

Kod za ovjeru poruke (eng. *Message Authentication Codes,* skraćeno MAC) je algoritam sličan hash funkcijama. Kao ulaze prima tajni ključ i poruku koju treba zaštititi, a kao izlaz daje MAC vrijednost koja služi kao zaštita integriteta i autentičnosti podataka. Razlika u odnosu na digitalne potpise je u tom što MAC algoritam koristi isti tajni ključ i za stvaranje MAC vrijednosti i za provjeru valjanosti poruka. [8]

Na primjer, pretpostavimo da baza podataka sadrži listu bankovnih računa. Iz perspektive sigurnosti jako je poželjno moći spriječiti neovlaštenog korisnika u ručnom mijenjanju podataka. Dakle, kada se autorizirani korisnik spoji, HSM bi proslijedio podatke i tajni ključ MAC-u. Budući da HSM štiti tajni ključ, nitko drugi teoretski ne može reproducirati valjan MAC za dani bankovni račun. Zbog toga, kada autorizirani program dohvati podatke o bankovnom računu, automatski se šalje zahtjev HSM modulu da potvrdi valjanost MAC vrijednosti. Ako se uspostavi da vrijednost nije valjana, program zna da je netko mijenjao podatke i može poduzeti odgovarajuću akciju kao što je npr. uključenje alarma.

Na slici 5 prikazan je primjer izvođenja MAC algoritma.

Komunikacija između HSM modula koji čuva tajni ključ i provodi potvrdu valjanosti te programa koji ga koriste moguća je zahvaljujući PKCS #11 API-ju.



Slika 5. Rad MAC algoritma
Izvor: Wikipedia

2.1.5. Upravljanje ključevima

Upravljenje ključevima (eng. *key management*) se odnosi na rukovanje ključevima za šifriranje/dešifriranje podataka u sustavima za šifriranje. To uključuje stvaranje, razmjenu, pohranu, korištenje i zamjenu ključeva. Uspješno upravljanje ključevima je nužno za sigurnost sustava za šifriranje. U praksi je to i najteži aspekt kriptografije jer zahtijeva usklađen rad između više čimbenika kao što su pravila sustava, korisnici i slično. [9]

Da bi pružio najbolju sigurnost, HSM modul pohranjuje sve ključeve na fizički uređaj. Sigurnosne kopije ključeva trebale bi se pohraniti korištenjem sigurne veze na drugi HSM modul ili na jednu ili više pametnih kartica (eng. *smart card*). Čitač kartica se pri tom treba spojiti izravno na uređaj kako bi se spriječilo potencijalno presretanje podataka.

Upravljanje ključevima jedan je od osnovnih i najvažnijih zadataka HSM modula. Oni ne samo da nude sigurnu pohranu ključeva, nego i stvaranje, izmjenu ili brisanje istih, a PKCS #11 API omogućuje aplikacijama da koriste sve te mogućnosti.

3. Prednosti i nedostaci HSM modula

Postoje mnoge prednosti korištenja HSM modula, ali i neki nedostaci. Naravno, svaki proizvođač nastoji istaknuti one prednosti koje će njegov proizvod prikazati superiornijim nad konkurentskim proizvodom. Neke od najčešće isticanih prednosti prikazane su u nastavku [1].

3.1. Prednosti HSM modula

- **FIPS 140 certificiranje**

  FIPS 140 je priznati standard koji nudi 4 dobro definirane razine za provjeru valjanosti HSM modula. O njemu će detaljnije biti riječ u nastavku dokumenta. Ipak, valja istaknuti kako certifikat ne znači da je HSM modul koji ga ima savršen. No, ako ga ima, kupac može biti siguran da je HSM kojeg koristi barem prošao osnovnu razinu testova sigurnosti koje su proveli kvalificirani profesionalci u FIPS akreditiranim laboratorijima.

- **Širokoprihvaćeni i dostupni sigurni kriptografski algoritmi**

  Mnogi proizvođači u svojim proizvodima nude vlastite tajne algoritme za kriptiranje. Ipak, preporuča se takve HSM module izbjegavati. Umjesto takvih, preporuča se koristiti HSM module koji koriste dobro poznate i sigurne algoritme, kao što su, npr. RSA i DSA bazirani algoritmi za digitalne potpise, SHA-1 ili MD5 za izračunavanje sažetaka ili 3-DES za kodiranje podataka. Također postoje i proizvođači koji uz standardne algoritme nude i vlastite. Pri korištenju takvih HSM modula bitno je HSM ispravno konfigurirati da koristi samo standardne algoritme u radu.

- **Jaki generatori slučajnih brojeva**

  Generator slučajnih brojeva (RGB, eng. *random number generator*) ili generator pseudo-slučajnih brojeva je bitan za mnoge kriptografske funkcije. Ako je RGN slab, cijeli proizvod je kriptografski nesiguran. Budući da HSM moduli obavljaju kriptografske funkcije, mnogi od njih sadrže jake generatore slučajnih brojeva.

- **Siguran izvor podataka o vremenu**

  Sigurno potvrđivanje i priznavanje ispravnosti poruka zahtjeva poruke koje uključuju vrijeme i datum koji dolaze iz pouzdanog izvora. Sistemski sat poslužitelja se lako može izmjeniti pa ne predstavlja pouzdani izvor. Naime, ako je digitalno potpisana poruka nastala korištenjem nesigurnog izvora podataka o vremenu, vrijeme i datum poruke, kao i ispravnost cijele transakcije se lako može osporiti. Zbog toga HSM moduli dopuštaju izmjenu vremena samo ovjerenom administratoru i pri čemu taj događaj sigurno zabilježe.

- **Standardizirano sučelje**

  Pri kupnji HSM modula potrebno je razmotriti i kriptografske zahtjeve. Ako se modul namjerava koristiti za naprednije potrebe, onda je vjerojatno najbolji izbor pri kupnji proizvod koji zadovoljava PKCS#11 čime se osigurava standardizirano sučelje za programere i olakšava im se rad.

- **Sigurno i jednostavno korisničko sučelje**

  Korisničko sučelje HSM modula najčešće je intuitivno, jednostavno za korištenje i ima dobro dokumentirane upute. Time se nastoji spriječiti korisnike da slučajno zbog nerazumijevanja sučelja ne naprave skupe pogreške (npr. izbrišu pohranjene ključeve).

- **Detaljne upute za instalaciju**

  Prekidači na uređaju, sukladnost sa drugim uređajima, način zamjene baterije te detaljan popis drugih uređaja s kojima pojedini HSM modul nije kompatibilan su samo neke od stvari koje su najčešće jasno naznačene i detaljno dokumentirane kako si se spriječile pogreške vezane uz ispravan rad HSM modula.

- **Sigurnosna kopija ključeva**

  Ako se HSM modul koristi za kriptiranje ili provjeru valjanosti podataka u bazi podataka nužno je da HSM ima sigurnosne kopije ključeva u slučajevima da modul zakaže. U idealnom slučaju, sigurnosna kopija bi trebala biti pohranjena na 3 ili više pametnih kartica, pri čemu bi svaka kartica sadržavala dio ključa i bila pohranjena na posebnoj lokaciji.

- **Zaštita ključeva**

  HSM uređaj nikada ne smije dopustiti pohranu ili prijenos izvornog (eng. *plaintext*) privatnog ili tajnog ključa izvan svojih fizičkih granica. Svaki ključ koji izlazi izvan tih granica trebao bi biti šifriran.

- **Otpornost na fizičke pokušaje provale**

  Neki od skupljih i boljih HSM modula automatski brišu sve osjetljive podatke (eng. *zeroize data*) u slučaju otkrivanja fizičkih pokušaja provale. Pod tim se podrazumijevaju nasilni pokušaji pristupa, nenormalna električna aktivnost ili nenormalne temperature. To je način na koji se štite ključevi pohranjeni u uređaju od neprijatelja koji je dobio fizički pristup HSM modulu.

  Zaštita od fizičkih prijetnji je upravo ono što razlikuje HSM module od uobičajenih poslužiteljskih računala koja služe za ubrzavanje kriptografskih procesa.

- **Prilagodljivost**

  Ako se veličina mrežne arhitekture mijenja, i HSM arhitektura bi se trebala moći mijenjati u skladu s njom. Zato je preporučljivo pri kupnji pripaziti na ovu stavku željenog uređaja, osobito ako postoje planovi proširenja mrežne arhitekture. Naravno, uvijek je moguće dodati novi HSM modul, ali ako već unaprijed postoje planovi za proširenje možda je bolja opcija već u startu razmišljati o kupnji HSM modula koji ima mogućnost pohranjivanja podataka na "oblak" (eng. *clustering*) i balansiranja opterećenja.

3.2. Nedostaci HSM modula

Najveći nedostatak pri korištenju HSM modula je njihova cijena. Rasponi u cijeni ovih uređaja su jako veliki i ovise o stupnju funkcionalnosti i sigurnosti koju nude.

Također, proizvođači skrivaju mnogo informacija o radu svojih uređaja. Jedan od primjera je i skrivanje detalja o generatoru slučajnih brojeva, pri čemu proizvođači navedu samo da "uređaj sadrži" generator slučajnih brojeva ili da je generator slučajnih brojeva "jak" ili "baziran na sklopovlju". Dio problema je i činjenica da trenutno ne postoji adekvatan standard za "slučajnost".

Drugi nedostatak HSM modula u usporedbi sa programima za kriptiranje su problemi u nadogradnji. Ako se, na primjer, otkrije slabost u algoritmu za kriptiranje, ugradnja novog kriptografskog programa u dobro dizajniranu programsku arhitekturu neće predstavljati problem, dok s HSM modulima to nije tako.

4. Primjene HSM modula

HSM modul se može koristiti za bilo koju primjenu koja podrazumijeva korištenje digitalnih kriptografskih ključeva. U praksi se uglavnom koriste kada je riječ o ključevima visoke vrijednosti, tj. onda kada kompromitiranje ključa vodi do jako velikog negativnog utjecaja na vlasnika ključa. Mogućih primjera primjene ima bezbroj, no najvažnije se mogu podijeliti u sljedeće kategorije [2]:

1. Infrastrukture s javnim ključem (eng. *public key infrastructure*, skraćeno PKI),
2. Sustavi s kartičnim plaćanjem (eng. *card payment system*) i
3. SSL povezanost[8].

U nastavku će biti više riječi o navedenim kategorijama.

4.1. Infrastrukture s javnim ključem

PKI je skup sklopovlja, programskih rješenja, ljudi, pravila i procedura koje su potrebne za stvaranje, upravljanje, distribuiranje, upotrebu i pohranu digitalnih certifikata.

Na području kriptografije PKI je sporazum koji veže javni ključ s odgovarajućim korisničkim identitetom, a izdaje ga organizacija za izdavanje certifikata (eng. *certificate authority*, skraćeno CA).

U PKI okruženju HSM module mogu koristiti organizacije zadužene za izdavanje certifikata ili organi za registraciju kako bi obavljali već spomenute radnje stvaranja, pohrane i upravljanja parovima ključeva. HSM moduli koji se koriste u PKI infrastrukturi moraju imati neke osnovne značajke kao što su:

- visok stupanj zaštite i na fizičkoj i na logičkoj razini,
- autorizaciju korisnika koja se sastoji od više dijelova (eng. *Multi-part user authorization schema*),
- bilježenje svih događaja te
- sigurno stvaranje sigurnosnih kopija.

Očito je da HSM uređaji koji se koriste u PKI okruženjima imaju velik naglasak na sigurnost, a manji na same performanse.

4.2. Sustavi s kartičnim plaćanjem

HSM moduli korišteni na području sustava s kartičnim plaćenjem mogu se podijeliti u dvije kategorije :

1. **Integrirani moduli** koji se koriste u bankomatima i blagajnama

   Ovi moduli koriste se za kriptiranje PIN broja prilikom korištenja kartice te za prijenos ključeva u zaštićenu memoriju.

2. **Moduli za autorizaciju i personalizaciju**

   Ovi moduli koriste se za usporedbu on-line PIN-a[9] sa kriptiranim PIN blokom[10], za ovjeravanje transakcija učinjenih putem kreditne kartice na bankomatima, stvaranje skupa ključeva kao pomoć u personalizaciji pametnih kartica, zatim stvaranje podataka za kartice s magnetnom vrpcom itd.

Najveća organizacija koja se bavi pisanjem i održavanjem standarda HSM modula namjenjenih bankarskom tržištu je Payment Card Industry Security Standards Council. Na slici 6 je prikazan

[8] SSL (eng. *Secure Sockets Layer*) je transportni protokol unutar TCP/IP stoga koji omogućava sigurnu komunikaciju preko interneta za razne aplikacije kao što su e-pošta, web preglednik, trenutne komunikacije (eng. *instant messaging*)...

[9] Online PIN - PIN kojeg korisnik pametne ili debitne kartice unosi prilikom plaćanja karticom, a koji se zatim šalje na verifikaciju banci koja je izdala karticu.

[10] Kriptirani PIN blok - PIN koji je pohranjen u šifriranom obliku u banci koja je izdala karticu i s kojim banka uspoređuje PIN koji joj je pristigao na verifikaciju prilikom kartičnog plaćanja.

uređaj "*ARX network-attached PrivateServer HSM*", HSM modul namjenjen korištenju u bankarskim poslovima.

Slika 6. ARX network-attached PrivateServer HSM
Izvor: Wikipedia

4.3. SSL povezanost

Postoje određene primjene HSM modula u kojima se veliki naglasak stavlja na performanse, ali se zahtjeva i sigurnost koju oni pružaju. Većina takvih aplikacija se predstavlja kao sigurna *web* usluga koja koristi HTTPS protokol (eng. *Hypertext Transfer Protocol Secure*). Neke od tih usluga su e-pošta, web preglednici, slanje trenutačnih poruka (eng. *instant messaging*) i sl.

HTTPS protokol je kombinacija HTTP (eng. *Hypertext Transfer Protocol*) protokola s SSL i TLS (eng. *Transport Layer Security*) protokolnim dodacima. Budući da je zadatak SSL protokola ostvariti zaštićen prijenos podataka kroz mrežu koji uključuje identifikaciju poslužitelja, identifikaciju klijenta i šifriranu razmjenu podataka među njima, očito je da je za nesmetan i siguran rad potrebno omogućiti visok stupanj sigurnosti ključeva koji se koriste pri kriptiranju, ali i brz rad.

Zbog toga se u takvom okruženju uglavnom koriste uređaji koji uz osnovne usluge HSM modula nude i ubrzanje SSL protokola. Performanse takvih uređaja su jače od onih kod običnih HSM modula, a neki od njih mogu doseći čak i 7000 operacija po sekundi.

Dakle, uz sigurnost, ovakvi uređaji pružaju i značajno ubrzanje koje uklanja potencijalno zagušenje SSL prometa koje usporava ili zaustavlja transakcije preko mreže, izazivajući frustracije korisnika i time predstavlja rizik za kompanije. Na slici 7 prikazan je nForce 1600, HSM modul koji nudi kombinaciju sigurnosti ključeva za šifriranje s ubrzanjem SSL protokola.

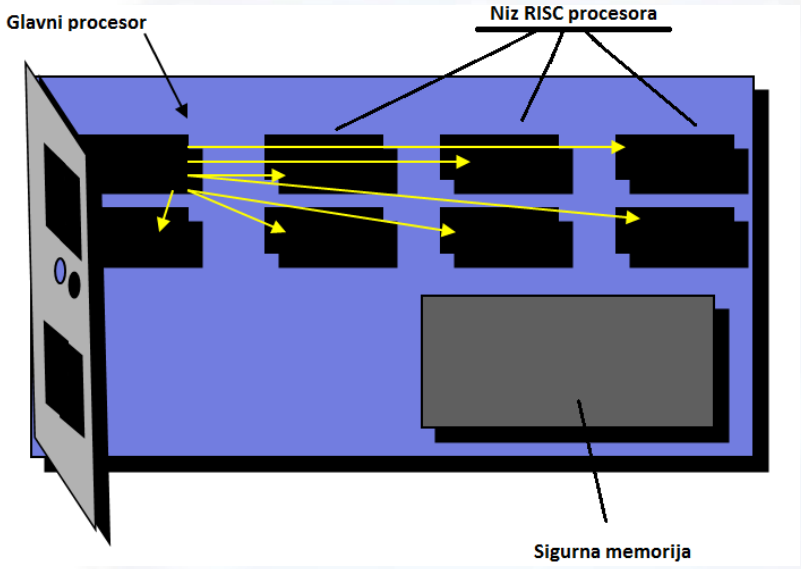
Slika 7. HSM modul nForce 1600
Izvor: net-security.org

5. Način rada HSM modula

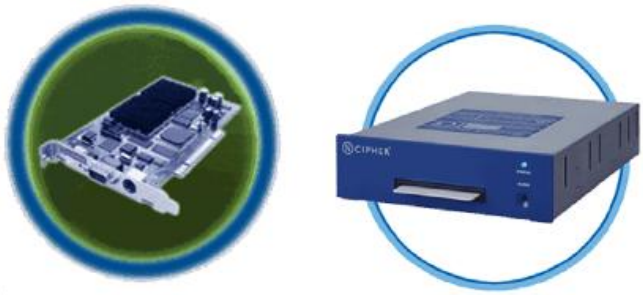
Kao što je već rečeno, HSM moduli izvode kriptografske operacije unutar sklopovlja koje služi kao zaštita. HSM moduli dolaze u raznim oblicima kao što su pametne kartice, SCSI kutije[11], PCI ploče[12] i sl.

HSM moduli se u pravilu priključuju izravno na poslužitelj i pružaju zaštićeno područje za stvaranje i pohranu privatnih ključeva kao i za korištenje tih ključeva u osjetljivim procesima kao što su potpisivanje i dešifriranje. Time je omogućeno da se privatni ključ nikada ne nađe u aktivnoj memoriji ili programu u nekriptiranom izdanju. To je osobito bitno jer je aktivna memorija ranjiva na napade i kopiranje privatnog ključa ako se on nalazi u nekriptiranom obliku.

Ono što je zajedničko svim HSM modulima pri njihovu radu jest da kriptoprocesor prima instrukcije u kriptiranom obliku, dekriptira te instrukcije u otvoreni tekst i izvede ih unutar modula. Kriptoprocesor nikada ne otkiva ključeve (koji su pohranjeni u sigurnoj memoriji) ili izvršne naredbe na sabirnici, osim u šifriranom obliku. HSM modul može uz jedan glavni procesor imati i druge procesore. Glavni procesor obavlja kriptografske operacije i delegiranje dešifriranih instrukcija drugim procesorima, dok drugi procesori samo obavljaju kriptografske operacije. Na slici 8 je prikazano sklopovlje HSM modula nCipher, a primjeri modula nCipher dani su na slici 9.



Slika 8. Sklopovlje HSM modula nCipher
Izvor: pkiforum.org



Slika 9. Primjer nCipher HSM modula (lijevo: PCI, desno: SCSI)
Izvor: pkiforum.org

[11] SCSI (*Small Computer System Interface*) skup je standarda za priključivanje perifernih jedinica na sustav, te za prijenos podataka.

[12] PCI (eng. Peripheral Component Interconnect) je sabirnica za spajanje hardverskih uređaja na računalo.

6. Certificiranje HSM modula

FIPS 140-1 (eng. *Federal Information Processing Standards*) je izvorni standard za certificiranje HSM modula, izdan u siječnju 1994. godine. Noviji standard, FIPS 140-2 izdan je u lipnju 2001. godine.

Standarde je izdao National Institute of Standards and Technology (NIST) kako bi stvorio jedinstveni standard za kriptografske module koji bi uključivao i sklopovski i programski dio uređaja.

U oba standarda postoje 4 razine certificiranja, pri čemu četvrta razina predstavlja najveću razinu sigurnosti. Razine su jednostavno nazvane "Razina 1" do "Razina 4". FIPS ne navodi koja je razina sigurnosti potrebna za neku primjenu, ali navodi svojstva pojedinih razina koja su dana u nastavku.

- **Razina 1** je najniža razina i potrebno je zadovoljiti najmanje zahtjeva da se stekne certifikat ove razine. U globalu, potrebno je samo da su komponente uređaja ispravne i da ne postoje prevelike nesigurnosti u radu.
- **Razina 2** postavlja dodatne zahtjeve na upozorenja na fizičke prijetnje te autentikaciju različitih korisnika na temelju njihovih uloga.
- **Razina 3** postavlja zahtjeve na otpornost na fizičke prijetnje (otežavanje napadačima da dođu do osjetljivih informacija pohranjenih u modulu), autentikaciju korisnika na temelju njihovog identiteta te na fizičko i logičko odvajanje sučelja preko kojeg važni sigurnosni parametri ulaze i izlaze iz modula.
- **Razina 4** postavlja dodatne zahtjeve na fizičku sigurnost uređaja i zahtjeva robusnost po pitanju napada iz okoline.

FIPS 140 navodi 11 specifičnih područja i zahtjeva koje modul mora zadovoljiti kako bi dobio certifikat određenog stupnja. Navedene kategorije su [4]:

1. Specifikacija kriptografskog modula (što treba biti dokumentirano).
2. Sučelje i priključnice uređaja (koje informacije ulaze i izlaze iz modula i kako trebaju biti razdvojene).
3. Uloge, usluge i autentifikacija (tko može što raditi s modulom i kako se to provjerava).
4. Model s konačnim brojem stanja (dokumentiranje stanja visoke razine u kojima se modul može naći i načine kako se događa prijelaz iz jednog stanja u drugo).
5. Fizička sigurnost uređaja (bilježenje napada i obrana od napada te robusnost na napade iz okoline).
6. Operacijska okolina (OS koji upravlja radom HSM modula ili pak OS koji upravlja radom uređaja u sklopu kojeg se HSM modul koristi).
7. Upravljanje ključevima za šifriranje (stvaranje, unošenje, prenošenje, pohrana i uništavanje ključeva).
8. EMI/EMC[13] - razina otpornosti na smetnje uzrokovane elektromagnetskom indukcijom ili elektromagnetskim zračenjem iz vanjskog izvora.
9. Samotestiranje (što se treba ispitati, kada i što se treba napraviti u slučaju da test ne prođe).
10. Dokaz o sigurnosti dizajna (koje dokaze treba pokazati kako bi se potvrdilo da je modul dobro dizajniran i implementiran).
11. Smanjenje drugih napada (ako je modul dizajniran za smanjenje neke posebne vrste napada treba dokumentirati protiv koje i kako).

[13] EMI (eng. *Electromagnetic interference*) - smetnje koje utječu na rad električnih krugova uzrokovane ili elektromagnetskom indukcijom ili elektromagnetskim zračenjem iz vanjskog izvora.

EMC (eng. *Electromagnetic compatibility*) - grana znanosti koja se bavi proučavanjem EMI smetnji i načinima njihova spriječavanja.

Popis svih kriptografskih modula koji posjeduju neki od FIPS 140-1 ili FIPS 140-2 certifikata moguće je pronaći na internet stranici :

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

FIPS standard je najlakši način provjere sigurnosti nekog HSM modula. Program povezan s FIPS-om, nazvan Program za vrednovanje kriptografskih modula (eng. *Cryptographic Module ValidationProgram,* skraćeno CMVP) zadužen je za ovjeravanje i vrednovanje danog HSM modula u skladu s razinama certifikata.

Ipak, program vrednovanja ne jamči ništa u potpunosti. Kao primjer se često navodi slučaj HSM modula IBM 4758 (slika 10).

Slika 10. HSM modul IBM 4758
Izvor: http://www.cl.cam.ac.uk/

IBM 4758 je prvi HSM modul koji je dobio certifikat razine 4. Ipak, dvojica istraživača za Sveučilišta u Cambridgeu demonstrirala su kako je moguće postići da 3-DES ključevi modula postanu ranjivi ako se modul implementira s opcionalnim rješenjem arhitekture Common Cryptographic Ahitecture (CCA) kojeg nudi IBM.

Iako ova ranjivost uzrokovana CCA arhitekturom ne narušava valjanost FIPS 140 standarda, ipak donosi pitanje pokriva li FIPS dovoljno širok raspon sigurnosnih pitanja. [1]

U konačnici se sve svodi na to da pri odabiru bilo koje metode ili sredstva za pojačavanje sigurnosti ne postoje prečaci. Bitno je da bilo koje rješenje prije upotrebe dobro istraže i ispitaju profesionalni stručnjaci na području sigurnosti.

7. Zaključak

Kao što je pokazano, HSM moduli se mogu koristiti za razne zadatke: stvaranje ključeva i njihovu sigurnu pohranu, kao sredstvo za sigurno šifriranje osjetljivih podataka koje treba pohraniti u relativno nesigurnim lokacijama kao što su baze podataka itd.

Ipak, postoje i programi koji pružaju jednake funkcionalnosti, a većina ih je čak i besplatna, pa se postavlja pitanje zašto platiti između 500$ i 10 000$ za HSM modul?

U osnovi postoje 3 glavna razloga: pojačana sigurnost, ubrzanje kriptografskih performansi i industrijski standardizirani certifikacijski i validacijski programi. Ako je pažljivo izabran i ispravno implementiran, HSM modul nudi povećanje u performansama od jedan do dva reda veličine u odnosu na program.

U principu većina HSM modula radi u skladu s očekivanjima i pruža funkcionalnosti koje pojedinac treba od sigurnog kriptoprocesora. Koji HSM modul odabrati ovisi o raspoloživom iznosu novca, zahtjevima performansi i specifičnim zahtjevima pojedine aplikacije. [3]

Problem koji se može istaknuti je razlika u načinu na koji svaki proizvođač implementira neke značajke kao što je hijerarhija uloga, autorizacija i stvaranje sigurnosne kopije ključeva. Upravo se zbog te razlike teško naviknuti na HSM modul novog proizvođača nakon korištenja HSM modula drugog proizvođača. Procesu prilagodbe ne pridonosi ni činjenica da je popratna dokumentacija proizvoda najčešće jako sažeta, bez potrebnih detalja.

U budućnosti se očekuje značajan razvoj HSM modula na području performansi, osobito na ubrzanju SSL protokola. Također se predviđa da će sve veći broj HSM modula imati certifikate viših razina, sa jakom zaštitom od fizičkih prijetnji.

S razvojem modula očekuje se i daljni razvoj standardizacije kako bi se izbjegli trenutni problemi prelaska na novi HSM modul drugog proizvođača.

8. Leksikon pojmova

HSM moduli

Slopovski sigurnosni moduli (eng. *hardware security module*) ili skraćeno HSM moduli su vrsta sigurnih kriptoprocesora čiji je cilj upravljanje ključevima te ubrzanje kriptografskih procesa kao što su digitalni potpisi, provjere valjanosti i integriteta prilikom pristupa ključevima poslužiteljskih aplikacija itd.

http://en.wikipedia.org/wiki/Hardware_security_module

Kriptoprocesor

Kriptoprocesor je računalo na čipu ili mikroprocesoru zaduženo za kriptografske operacije, koje je zaštićeno s više razina fizičke zaštite čime mu se pruža otpornost na fizičke napade. Namjena kriptoprocesora je predstavljati centar sigurnosti podsustava, tako da nije potrebno štititi preostale djelove podsustava od fizičkih prijetnji, već samo njega.

http://en.wikipedia.org/wiki/Secure_cryptoprocessor

Šifriranje podataka

Šifriranje (eng. *encryption*) je pretvaranje izvornog teksta (eng. *plaintext)* u šifrirani tekst *(eng. ciphertext)* pomoću određene šifre (tj. algoritma).

http://en.wikipedia.org/wiki/Encryption

Digitalni potpis

Digitalni potpis (eng. digital signature) je matematički algoritam za dokazanje autentičnosti digitalne poruke ili dokumenta.Valjan digitalni potpis pruža primatelju razlog za vjerovanje da je poruku poslao poznati pošiljatelj i da poruka nije mijenjana pri prijenosu.

http://en.wikipedia.org/wiki/Digital_signature

Hashing

Kriptografska hash funkcija se može definirati kao deterministička procedura koja uzima proizvoljni blok podataka i vraća niz bitova definirane duljine, tzv. hash vrijednost. Slučajna ili namjerna promjena podataka automatski mijenja i hash vrijednost, pa se hashing često koristi u kriptografiji za kao pomoć pri autentifikaciji.

http://en.wikipedia.org/wiki/Cryptographic_hash_function

Kod za ovjeru poruke

Kod za ovjeru poruke (eng. *Message Authentication Codes,* skraćeno MAC) je algoritam sličan hash funkcijama. Kao ulaze prima tajni ključ i poruku koju treba zaštititi, a kao izlaz daje MAC vrijednost koja služi kao zaštita integriteta i autentičnosti podataka. Razlika u odnosu na digitalne potpise je u tom što MAC algoritam koristi isti tajni ključ i za stvaranje MAC vrijednosti i za provjeru valjanosti poruka.

http://en.wikipedia.org/wiki/Message_authentication_code

Upravljanje ključevima

Upravljenje ključevima (eng. *key management*) se odnosi na upravljanje ključevima za šifriranje/dešifriranje podataka u sustavima za šifriranje. To uključuje stvaranje, razmjenu, pohranu, korištenje i zamjenu ključeva.

http://en.wikipedia.org/wiki/Key_management

Generator slučajnih brojeva

Generator slučajnih brojevaključevima (eng. *random number generator*) je računalni ili fizički uređaj namijenjen stvaranju slijeda brojeva ili simbola koji ne slijede nikakav uzorak, tj. doimaju se slučajnim.

http://en.wikipedia.org/wiki/Random_number_generation

Infrastrukture s javnim ključem

Infrastruktura s javnim ključem (eng. *public key infrastructure*, skraćeno PKI) je skup sklopovlja, programa, ljudi, pravila i procedura koje su potrebne za stvaranje, upravljanje, distribuiranje, upotrebu i pohranu digitalnih certifikata.

Na području kriptografije PKI je sporazum koji veže javni ključ a odgovarajućim korisničkim identitetom a izdaje ga stručnjak za certifikate (eng. *certificate authority*, skraćeno CA).

http://en.wikipedia.org/wiki/Public_key_infrastructure

SSL protokol

Secure Sockets Layer (SSL) protokol ostvaruje identifikaciju dva sugovornika povezana preko računalne mreže i zaštićeni prijenos podataka među njima. SSL protokol uključuje identifikaciju poslužitelja, identifikaciju klijenta i šifriranu razmjenu podataka među njima.

http://fly.srk.fer.hr/~peloquin/SSL/ssl.html

FIPS 140-1 i FIPS 140-2

FIPS 140-1 (eng. *Federal Information Processing Standards*), izdan u siječnju 1994. godine je izvorni standard za certificiranje HSM modula. Noviji standard, FIPS 140-2 izdan je u lipnju 2001. godine.

Standarde je izdao National Institute of Standards and Technology (NIST) kako bi stvorio jedinstveni standard za kriptografske module koji bi uključivao i sklopovski i programski dio uređaja.

U oba standarda postoje 4 razine certificiranja, pri čemu četvrta razina predstavlja najveću razinu sigurnosti.

http://en.wikipedia.org/wiki/FIPS_140

9. Reference

[1] SANS Institute InfoSec Reading Room: An Overview of Hardware Security Modules, http://www.sans.org/reading_room/whitepapers/vpns/overview-hardware-security-modules_757, 02. 2012.

[2] Wikipedia: Hardware security module http://en.wikipedia.org/wiki/Hardware_security_module, 02.2012.

[3] CERTEZZA: A Review of Hardware Security Modules Fall 2010, http://www.opendnssec.org/wp-content/uploads/2011/01/A-Review-of-Hardware-Security-Modules-Fall-2010.pdf , 02.2012.

[4] Wikipedia: FIPS 140 http://en.wikipedia.org/wiki/FIPS_140, 02.2012

[5] Wikipedia: Šifriranje podataka http://en.wikipedia.org/wiki/Encryption, 02.2012.

[6] Wikipedia: Digitalni potpis http://en.wikipedia.org/wiki/Digital_signature, 02.2012.

[7] Wikipedia: Hashing http://en.wikipedia.org/wiki/Cryptographic_hash_function, 02.2012.

[8] Wikipedia: Kod za ovjeru poruke http://en.wikipedia.org/wiki/Message_authentication_code,02.2012.

[9] Wikipedia: Upravljanje ključevima http://en.wikipedia.org/wiki/Key_management,02.2012.