Zavod za elektroniku, mikroelektroniku, računalne i inteligente sustave
Fakultet elektrotehnike i računarstva
Sveučilište u Zagrebu

Seminarski rad iz predmeta Operacijski sustavi 2:

EMV standard

Knjiga 2: Sigurnost i rukovanje ključevima

Student: Radovan Aleksander
Matični broj: 0036374849

Siječanj, 2003.

Uvod

Zbog naglog porasta kupovine preko Interneta i plaćanjem kreditnim karticama (koje ionako čine 99% svih plaćanja u svijetu), financijske institucije i njihove banke članice odlučile su napraviti pametnu kreditnu karticu kako bi si postigli veću sigurnost kod on-line plaćanja. Naime, gubici nastali zbog pronevjere kartica i raznih razmirica prilikom kupovine preko Interneta ogromni su. Visa je, naprimjer, dosad gubila oko 250 milijuna dolara godišnje na razne zloupotrebe nastale kupovinom preko Interneta. Zbog sigurnosne infrastrukture implementirane na smart kartici, navedeni iznos smanjuje se do 40%, a općenito pronevjere u bankarskoj industriji (ne samo na Internetu) smanjuje se i do 70%. U pitanju su veliki vrijednosni iznosi pa smart kartica daje veliki doprinos sigurnosti i veliki je izum na tom području.

Da bi se omogućila multiaplikacijska kompatibilnost, potrebno je donijeti standard. EMV standard to omogućuje s tim da je funkcija plaćanja postala središnja aplikacija. Standard EMV je nastao 1993. godine kao rezultat zajedničkog rada vodećih svjetskih platnih institucija: **E**uropaya, **M**astercarda i **V**ise, po čemu je i standard dobio ime (početna slova udruženih institucija). Glavni zadatak im je bio definirati skup standarda za platne aplikacije temeljene na smart karticama. Ti standardi omogućuju siguran i nesmetan rad pametne kartice s uređajima za prihvat, tzv. CAD (Card Acceptance Device), tj. daju skup pravila o njihovoj međusobnoj komunikaciji. EMV specifikacije napisane su sa slijedećim ciljevima:

- Kartica i CAD uređaj (npr. bankomat, platni EFTPOS terminal, PC čitač), moraju moći zajedničkom komunikacijom odrediti koje su im zajedničke aplikacije i funkcije.
- CAD uređaj može izvoditi uobičajene aplikacije i osigurati minimalne sigurnosne standarde za kreditne aplikacije.
- Mikroprocesorske platne kartice moraju biti interoperabilne i prihvaćene u cijelom svijetu.

EMV specifikacije temeljene su na ISO (International Organization of Standardisation) setu standarda za čip-kartice i uređaje za njihov prihvat. EMV sprecifikacije su ustvari implementacijski orjentirani podskup ISO 7813-3 standarda.

Ovaj rad se koncentrira na jednu od knjiga najnovijeg standarda EMV 4.0 izdanog u prosincu 2000. godine. On se sastoji od četiri dijela, tj. knjige:

1. knjiga – specifikacije zajedničkog sučelja CAD uređaja i kartice koja ne ovisi o aplikaciji.
- opisuje minimalnu funkcionalnost potrebnu za ispravan rad i interoperabilnost kartica i terminala neovisno o aplikaciji koja se izvršava
2. knjiga – specifikacije sigurnosti i upravljanja kriptografskim ključevima
- definira neophodni sigurnosni minimum koji kartice i uređaji za prihvat moraju zadovoljiti s obzirom na on-line komunikaciju između kartice i izdavača te upravljanje kriptografskim ključevima u cijelom sustavu plaćanja
3. knjiga – specifikacije aplikacija
- definira procedure neophodne da bi terminali i pametne kartice vršili međunarodne platne transakcije
4. knjiga – specifikacija sučelja (interface-a) za platne sustave
- daje obvezne, preporučljive i opcionalne zahtjeve za terminale s obzirom na vlasnika kartice, trgovca i izdavača kartice radi prihvaćanja pametnih kartica usklađenih s prve tri knjige

Zbog usklađivanja teme seminara sa temom predmeta, izabrana je 2. knjiga standarda kao tema ovog seminara. Ovo je malo skraćena verzija s obzirom na original, tako da čitatelj može pročitati više o temi na web stranicama navedenih u literaturi.

Prednosti EMV standarda

Postoje tri primarne prednosti koje dobivamo upotrebom EMV platnih terminala i čitača pametnih kartica:

1. Povećana sigurnost i smanjena zloupotreba

Smanjena zloupotreba najviše se očituje u on-line trgovini, gdje je ona i najveća. Strah zbog zloupotrebe jedan je od glavnih razloga sporijeg razvoja trgovanja putem javne mreže. Poznato je da se oko dvije trećine potencijalnih internetskih transakcija prekidaju u trenutku kada se od korisnika zatraže njegovi financijski podaci. Ogroman je problem i velik broj kasnije poreknutih transakcija.

Povećanjem sigurnosti korisnika platnih kartica na Internetu uveliko doprinosimo povećanju broja korisnika on-line trgovine. Pritom se smanjuju troškovi izdavača kartica.

Povećanjem prometa bi Internet-trgovci osigurali povoljnije popuste i nabavne cijene, što bi doprinijelo i povoljnijoj kupovini za krajnjeg korisnika. Moguće je i smanjenje postotka provizije izdavača kartice zbog povećanog prometa i smanjenih troškova zlouporabe, što opet može pozitivno odraziti na trgovca i na kupca.

EMV definira korištenje pametnih kartica u e-trgovini koristeći SET protokol (Secure Electronic Transaction).

Postoje dvije glavne vrste pronevjere kartica: tzv. skimming (u slobodnom prijevodu, krađa zapisa) i tzv. counterfeiting (krivotvorenje). Skimming je slučaj kad se podaci sa zapisa "skinu" i kasnije koriste u nelegalne svrhe kada kartica nije više prisutna, na Internetu na primjer. EMV rješava taj problem kriptografskom zaštitom broja kartice i autentifikacijom.

Kod krivotvorenja, kartice su na prvi pogled jednake legitimnima (npr. u slučaju magnetskih kartica), s time što, najčešće, podaci embosirani (otisnuti na kartici, ispupčeni) na tijelu kartice ne odgovaraju zapisanim podacima. Zapisani su podaci ili ukradeni skimmingom ili uopće ne postoje pa se kartica čini oštećenom. U tom slučaju se trgovac koristi ručnom naplatom. EMV infrastruktura to sprečava autentifikacijom čipa na terminalu i obrnuto te opcionalno on-line autentifikacijom na serveru banke.

2. Učinkovitost procesiranja stalno rastućeg broja transakcija

Broj kreditnih transakcija rapidno se povećavao prošlih godina, a tendencija se nastavlja i u budućnosti. POS terminali koji prihvaćaju magnetske kartice traže on-line vezu s bankom radi autorizacije kartica. EMV smart kartice povećavaju učinkovitost takvih transakcija, a većina ih se može izvoditi u off-line modu, krateći pri tome vrijeme odvijanja transakcije i štedeći novac, bez stalno dostupnih telefonskih i računalnih mreža. To sve ovisi o tzv. risk management politici banke izdavača kartice. EMV platna aplikacija može se dobro konfigurirati za off-line način rada. Za kontrolu rizika i pojednostavljenje procesiranja potebno je definirati tzv. Lower Consecutive Offline Limit (LCOL), tj. niži uzastopni off-line limit, i Upper Consecutive Offline Limit (UCOL), tj. viši uzastopni off-line limit. Ukoliko je prilikom transakcije dosegnut jedan od ovih parametara, iduća se transakcija odvija on-line. Tada banka pokreće skripte za prikupljanje transakcijskih podataka i opcionalno, za update EMV parametara.

3. Interoperabilnost različitih platnih aplikacija i dodatnih usluga

Preduvjet je za nastajanje globalne kartične platne sheme da sve transakcije budu procesirane bilo gdje u svijetu, neovisno o zemljopisnim granicama. Taj se preduvjet generalno naziva interoperabilnost i ima sva važna aspekta. S perspektive financijske platne industrije znači da uređaji mogu procesirati platne kartice različitih platnih shema. S gledišta izdavača kartice znači mogućnost korištenja kreditne kartice na svakoj lokaciji na kojoj je prikazan odgovarajući logotip, neovisno o tehnologiji uređaja za prihvat. To uključuje međudržavne transakcije i kupovine prilikom kojih se ne pokazuje kartica, kao što je kupovina preko Interneta. Gdje god je prikazan odgovarajući logotip, plaćanje karticom mora funkcionirati. Korisnici su u mogućnosti koristiti svoju kreditnu karticu u bilo kojoj državi s istom lakoćom i na isti način kao i u svojoj zemlji.

Kronologija EMV

1993: Formiranje EMV radne grupe
1994: Nastanak prvih specifikacija
1996: Izdaju se osnovne EMV specifikacije
1996: UKIS 3.0 (VISA) specifikacije
1996: Objavljivanje VIS 1.2 specifikacije
1997: Prvi EMV pilot (UKIS) u Engleskoj
1998: VIS 1.3.1 specifikacije
1998: Objava EMV '96 3.1.1 – prve verzije EMV standarda
1998: "EPI minimum requirements" specifikacije
1998: "EPI Card Technical Specs." V. 3.0.2
1998: Prvi EPI pilot (Off the Shelf) u Istočnoj Evropi
1999: Nacionalni rollout UKIS u Engleskoj
1999: "EPI Off the Shelf 3.0.3" specifikacije
1999: Nacionalni rollout UKIS u Slovačkoj
2000: VISA EMV projekt (VSDC) u SAD-u
2000: Izdane EMV 2000 4.0 specifikacije

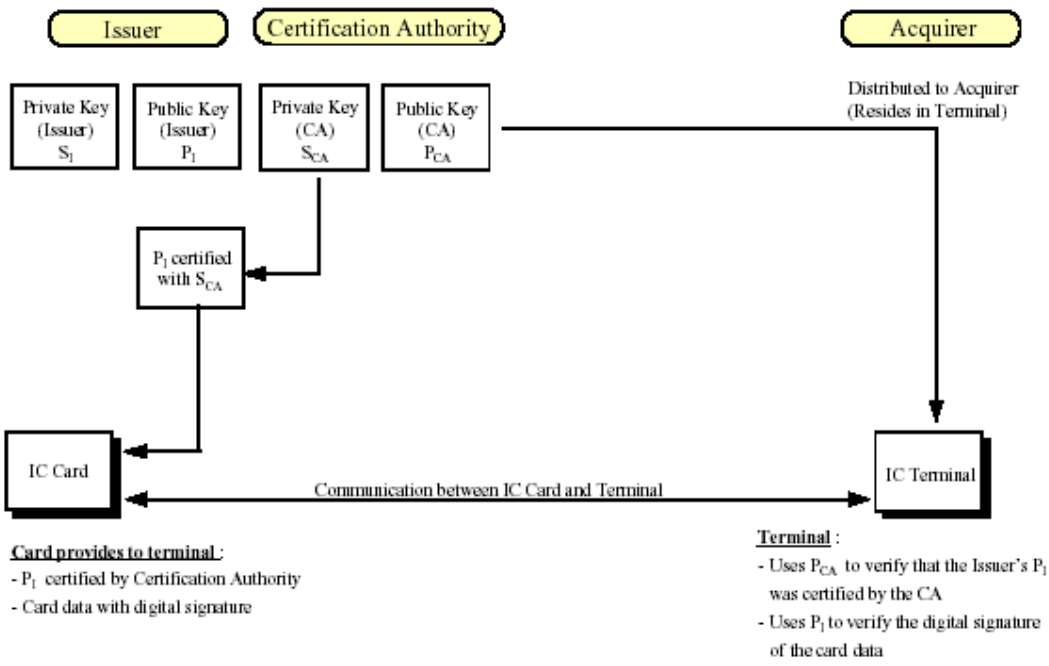
Sigurnost i rukovanje ključevima kod pametnih kartica

U ovome dijelu standarda opisuju se minimalni funkcionalni zahtjevi za sigurnost komunikacije između kartice i terminala koji usiguravaju ispravnu operaciju i interoperatibilnost. U to spada offline statička i dinamička autentifikacija podataka, offline PIN enkripcija, aplikacija koja generira kriptogram i autentificira izdavača, sigurnosno slanje poruka, principi rukovanja javnim ključem i sigurnost terminala.

1. Statička autentifikacija podataka

Statičku autentifikaciju podataka izvršava terminal upotrebljavajući digitalni potpis. Shema digitalnog potpisa je bazirana na tehnici javnog ključa pomoću koje se potvrđuje legitimnost kritičnih kartičnih podataka. Kritični statični podaci se identificiraju pomoću AFL-a (Application File Locator). Pomoću toga se detektiraju neautorizirane izmjene nad podacima nakon identifikacije izdavača.

Statička autentifikacija podataka zahtijeva postojanje certifikatora (engl. Certification Authority, tj. povjerena treća strana koja dokazuje vezu između javnog ključa (Public Key) i izdavača (Issuer)), kao sredstva visoke razine sigurnosti za označavanje javnog ključa izdavača. Svaki terminal koji odgovara toj specifikaciji mora sadržavati prikladan certifikator javnih ključeva koji prepoznaje svaka aplikacija u terminalu. Ta specifikacija dopušta višestruke AID-ove (Applications Identifier) koji dijele isti certifikator javnog ključa. Poveznost između podataka i kriptografskih ključeva je prikazana na slici 1:



Slika 1: Dijagram statičke autentifikacije podataka

Kartice koje podržavaju statičku autentifikaciju bi morale sadržavati slijedeće podatkovne elemente:

- Indeks certifikatora javnog ključa: jednobajtni element podataka koji sadrži binarni broj koji određuje koji će aplikacijski javni ključ sa svojim asocijativnim algoritmom biti upotrebljen u operaciji između kartice i terminala.
- Certifikat javnog ključa izdavača: element podataka promjenjive veličine koji osigurava odgovarajući certifikator izdavača kartice. Nakon što terminal ispita taj element podataka, autentificira javni ključ izdavača sa dodatnim podacima.
- Označeni statički aplikacijski podaci: element podataka promjenjive veličine generirani od izdavača upotrebom privatnog ključa koji korespondira sa javnim ključem autentificiranim sa certifikatom javnog ključa izdavača.
- Podsjetnik javnog ključa proizvođača
- Predstavnik javnog ključa proizvođača

Za podržavanje statičke autentifikacije, svaki terminal mora imati mogućnost spremanja šest certifikatora javnih ključeva pomoću RID-a (Registered Application Provider Identifier). Isto tako mora znati povezivati svaki ključ sa određenom informacijom koja onda može biti upotrebljena zajedno sa ključem. Terminal mora još biti u mogućnosti locirati ključ i relevantnu informaciju danu RID-u osiguranu od kartice.

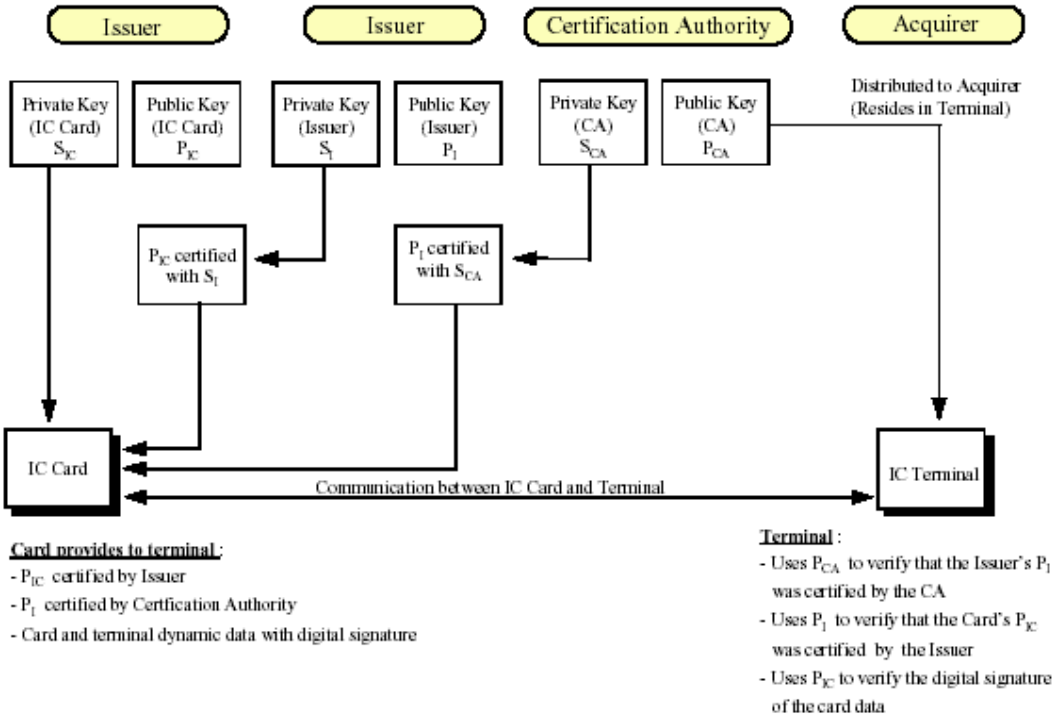
2. Dinamička autentifikacija podataka

Dinamičku autentifikaciju podataka provodi terminal koji upotrebljava digitalni potpis. Shema digitalnog potpisa se bazira na tehnikama javnog ključa za autentifikaciju kartice i potvrdu legitimnosti kritičnih kartičnih podataka (rezidentnih i generiranih od kartice) i podataka primljenih od terminala.

Postoje dvije opcije:

- Standardna dinamička autentifikacija podataka izvršava se prije analize akcije sa karticom, gdje kartica generira digitalni potpis nad kartičnim rezidentnim/generiranim podacima.
- Kombinacija dinamičke autentifikacije podataka i aplikacije za generiranje kriptograma (rezultata kriptografske operacije) se izvršava kod izdavanja prve GENERATE AC naredbe.

Dinamička autorizacija podataka zahtijeva postojanje certifikatora kao sredstva visoke razine sigurnosti za označavanje javnog ključa izdavača. Svaki terminal koji odgovara toj specifikaciji mora sadržavati prikladnu autorizaciju certifikata javnog ključa koji prepoznaje svaka aplikacija u terminalu. Ta specifikacija dopušta višestruke AID-ove (Applications Identifier) koji dijele istu autorizaciju certifikata javnog ključa. Poveznost između podataka i kriptografskih ključeva je prikazana na slici 2:



Slika 2: Dijagram dinamičke autentifikacije podataka

Kartica koja podržava dinamičku autentifikaciju podataka mora sadržavati slijedeće elemente podataka:

- Indeks certifikatora javnog ključa: jednobajtni element podataka koji sadrži binarni broj koji određuje koji će aplikacijski javni ključ sa svojim asocijativnim algoritmom biti upotrebljen u operaciji između kartice i terminala.
- Certifikat javnog ključa izdavača: element podataka promjenjive veličine koji osigurava odgovarajući certifikat autorizacije izdavača kartice. Nakon što terminal ispita taj element podataka autentificira javni ključ izdavača sa dodatnim podacima.
- Kartični certifikat javnog ključa: element podataka promjenjive veličine koji osigurava proizvođač kartice. Nakon što što terminal ispita taj element podataka autentificira javni ključ kartice sa dodatnim podacima.
- Podsjetnik javnog ključa proizvođača
- Predstavnik javnog ključa proizvođača
- Podsjetnik javnog ključa kartice
- Predstavnik javnog ključa kartice
- Privatni ključ kartice

Kartica koja podržava dinamičku autentifikaciju podataka mora generirati slijedeći podatkovni element:

- Označena dinamička aplikacija podataka: element podataka promjenjive veličine generiran od kartice koristeći privatni ključ koji korespondira sa javnim ključem autentificiranim u kartičnom certifikatu javnog ključa.

Za podržavanje dinamičke autentifikacije, svaki terminal mora imati mogućnost spremanja šest certifikatora javnih ključeva pomoću RID-a (Registered Application Provider Identifier).

Isto tako mora znati povezivati svaki ključ sa određenom informacijom koja onda može biti upotrebljena zajedno sa ključem. Terminal mora još biti u mogućnosti locirati ključ i relevantnu informaciju danu RID-u osiguranu od kartice.

3. Enkripcija osobnog identifikacijskog broja (PIN)

Ako je podržana, enkripcija osobnog identifikacijskog broja (PIN) za offline provjeru se izvodi od strane terminala koji upotrebljava asimetrični mehanizam enkripcije za sigurno prenošenje identifikacijskog broja sa tipkovnice do kartice. Preciznije, kartica mora posjedovati par javnih ključeva povezanih sa kriptiranim identifikacijskim brojem. Javni ključ upotrebljava tipkovnica za unošenje identifikacijskog broja ili sigurna komponeneta terminala (koja nije tikovnica) za enkripciju identifikacijskog broja, a privatni ključ upotrebljava kartica za provjeru kriptiranog identifikacijskog broja.

Sigurna komponenta terminala se upotrebljava za enkripciju identifikacijskog broja, jer transfer identifikacijskog broja sa tipkovnice do sigurne komponente mora biti na visokoj razini sigurnosti.

4. Aplikacijski kriptogram i autentifikacija izdavača

Pod aplikacijskim kriptogramom se podrazumijeva protokol komunikacije između kartice i terminala.

Cilj ovog dijela je opisivanje metoda generiranja aplikacijskog kriptograma (TC – Transaction Certificate, ARQC – Authorisation Request Cryptogram, AAC – Application Authentication Cryptogram). Kriptogrami se generiraju pomoću kartice (ICC – Integrated Circuit Card). U ovom dijelu se još opisuju i ARPC (Authorisation Response Cryptogram) koje generiraju izdavači, a verificiraju ih kartice.

4.1. Generiranje aplikacijskog kriptograma

Aplikacijski kriptogram se sastoji od poruke autentifikacijskog koda:

- poslanog od strane terminala prema kartici (izvršavanjem GENERATE AC ili neke druge naredbe)
- preuzetog interno sa kartice

Preporučeni minimalni set podataka od kojih bi se moralo sastojati generiranje kriptograma se nalaze u slijedećoj tablici 1:

Value	Source
Amount, Authorised (Numeric)	Terminal
Amount Other (Numeric)	Terminal
Terminal Country Code	Terminal
Terminal Verification Results	Terminal
Transaction Currency Code	Terminal
Transaction Date	Terminal
Transaction Type	Terminal
Unpredictable Number	Terminal
Application Interchange Profile	ICC
Application Transaction Counter	ICC

Tablica 1: Preporučeni minimalni set podataka za generiranje kriptograma

Algoritam za generiranje kriptograma uzima kao ulaz 16-bajtni glavni ključ (Master Key) i ostale potrebne podatke te iz njih izračunava 8-bajtni kriptogram u slijedeća dva koraka:

1. Prvi korak se sastoji u deriviranju funkcije sjedničkog ključa koji se sastoji od 16-bajtnog sjedničkog ključa kriptograma i 2-bajtnog ATC-a (Application Transaction Counter)

2. Drugi korak se sastoji u generaciji 8-bajtnog kriptograma uz pomoću MAC algoritma (Message Authentication Code) i sjedničkog ključa kriptograma iz prethodnog koraka.

4.2. Authentifikacija izdavača

Postupak generiranja 8-bajtnog ARPC-a (Authorisation Response Cryptogram) se sastoji upotrebom Triple-DES algoritma. Kao ulazni podaci za algoritam su 8-bajtni ARQC generiran od strane kartice i 2-bajtni ARC. Upotrebljava se još i sjednički ključ kriptograma SKac na slijedeći način:

1. ARC se proširuje sa 6 bajtova da bi postao 8-bajtni broj:

X := (ARC || ‘00’|| ‘00’ || ‘00’ || ‘00’ || ‘00’ || ‘00’).

2. Izračunavanje Y: = ARQC ⊕ X.

3. 8-bajtni ARPC se na kraju dobiva:

ARPC := DES3(SKac)[Y].

5. Sigurno slanje poruka

Ciljevi sigurnog slanja poruka su osiguravanje povjerljivosti, intergritet podataka i autentifikacija pošiljatelja. Integritet podataka i autentifikacija izdavača su postignute pomoću MAC-a (Message Authentication Code). Povjerljivost podataka se ostvaruje upotrebom kripitranja polja podataka.

5.1. Formati poruka

Postoje dva formata poruka:

Format 1: Format je nastao prema standardu ISO/IEC 7816-4, poglavlje 5.6. Nad poljem podataka je provedeno BER-TLV kodiranje po pravilima ASN.1/ISO 8825 standardu. To je eksplicitno specificirano u bitovima najniže težine bajta naredbe. To isto implicira da je zaglavlje naredbe uvijek integrirano u izračunavanje MAC-a.

Format 2: Format kod kojeg se ne upotrebljava BER-TLV kodiranje. U ovom slučaju pošiljatelj naredbe mora znati koji podaci se šalju i koje su veličine. Format je ekplicitno definiran u najnižim bitovima naredbe.

5.2. Sigurno slanje poruka u svrhu zaštite inegriteta i autentifikacije

Polje podataka naredbe

FORMAT 1:

Polje podataka naredbe je sastavljeno od slijedećih TLV objekata podataka kako je to prikazano na na slici 3:

Tag 1	Length 1	Value 1	Tag 2	Length 2	Value 2
T	L	Value (L bytes)	'8E'	'04'-'08'	MAC (4-8 bytes)

Slika 3: Format 1 polja podataka naredbe u svrhu zaštite inegriteta i autentifikacije

Ako postoje, podaci o naredbi moraju biti posebno naznačeni.

Ako je polje podataka BER-TLV kodirano, nebi smjelo pripadati specifičnom kontekstu (značka nebi smjela biti u rasponu od "80" do "BF") ili mora imati značku sa neparnom vrijednošću (treba voditi računa da to može biti i složeni object podataka).

Ako polje podataka nije BER-TLV kodirano, značka ima vrijednost "81".

Drugi object podataka je MAC. Zastavica je "8E", a dužina mora biti u rasponu od 4 do 8 bajtova.

FORMAT 2:

Elementi podataka (uključujući i MAC) su sadržana u polju podataka i njihovu duljinu bi morao znati pošiljatelj naredbe. MAC nije BER-TLV kodiran i mora biti uvijek na posljednjem mjestu polja podataka. Njegova duljina mora biti od 4 do 8 bajtova (slika 4).

Value 1	Value 2
Command data (if present)	MAC (4-8 bytes)

Slika 4: Format 2 polja podataka naredbe u svrhu zaštite inegriteta i autentifikacije

Izračunavanje MAC-a

Izračunavanje MAC-a S nad porukom MSG pomoću sjedničkog ključa Ks se izvodi u slijedećim koracima:

1. Dodavanje oznake "80" sa desne strane poruke i tada dodavanje još najmanji broj "00" sa desna tako da je dužina rezultirajuće poruke umnožak broja 8 (bajtova):

MSG := (MSG || '80' || '00' || '00' || . . . || '00').

MSG se tada još dijeli u 8-bajtne blokove X1, X2, …, Xk.

2. MAC sjednički ključ Ks se sastoji samo od krajnje ljevog bloka ključa Ks = Ksl ili konkatenacije krajnje lijevog i krajnje desnog bloka ključa Ks = (Ksl | | Ksr).

3. Izračunavanje kriptograma

Upotrebljavanjem 8-bajtnih blokova X1, X2, …, Xk i krajnje lijevog MAC sjedničkog ključa Ksl izračunava se:

Hi := ALG(Ksl)[Xi ⊕ Hi-1], za i = 1, 2, . . . , k.

Inicijalna vrijednost H0 := (‘00’ || ‘00’ || ‘00’ || ‘00’ || ‘00’ || ‘00’ || ‘00’ || ‘00’).

“ALG” je funkcija kriptiranja.

Izračunavanje 8-bajtnih blokova Hk+1 se obavlja na jednan od slijedećih načina:

- prema standardu ISO/IEC 9797-1 algoritam 1:

  Hk+1 := Hk.

- prema standardu ISO/IEC 9797-1 algoritam 3:

  Hk+1 := ALG(Ksl)[ALG-1(Ksr)[Hk]].

MAC S je onda jednak s (s je prema potrebi od 1 do 8) bajtova najviše težine od Hk+1.

5.3. Sigurno slanje poruka za osiguravanje povjerljivosti

Polje podataka naredbe

FORMAT 1:

Format kriptiranih podataka u polju podataka naredbe je prikazano na slici 5:

Tag	Length	Value
T	L	Cryptogram (enciphered data)

Slika 5: Format 1 kriptiranih objekata podataka u polju podataka naredbe

Ovisno u tekstu koji se kriptira, ISO/IEC 7816-4 specificira značku (Tag) koja že biti dodana rezultirajućem kriptogramu: neparna značka se upotrebljava kada se objekt koristi u izračunavanju MAC-a, a inače se upotrebljava parna značka.

FORMAT 2:

Kriptirani podaci se odnose na cijeli tekst bez MAC-a:

Value1	Value2
Cryptogram (enciphered data)	MAC (if present)

Slika 6: Format 2 polja podataka naredbe za sigurno slanje poruka

Kriptogram i MAC se dobivaju na sličan način kako je to navedeno u prethodnom poglavlju.

6. Javni ključ certifikatora

U ovom poglavlju definira okosnicu principa i načina rukovanja sa platnim sistemom koji koristi statičku i dinamičku autentifikaciju podataka.

Principi su koncepti kao osnovica za implementaciju rukovanja javnim ključem certifikatora. Ti principi definiraju postupke koji se koriste u svim platnim sistemima ili su adaptirani u individulanim platnim sistemima. Svaki platni sistem će razviti svoj set procedura za implementaciju.

6.1. Životni ciklus javnog ključa certifikatora

Normalni životni ciklus javnog ključa certifikatora

Životni ciklus javnog ključa certifikatora se u normalnim okolnostima može podijeliti u slijedeće faze:

- planiranje
- generiranje
- distribucija
- upotreba
- poništavanje

PLANIRANJE

Tijekom faze planiranja, platni sistem istražuje zahtjeve za uvođenje novog para ključeva certifikatora u bližoj budućnosti. Ti zahtjevi su vezani uz broj potrebnih ključeva i parametara tih ključeva.

Važan dio faze planiranja je pregled sigurnosti RSA za odlučivanje o duljini života novih i potencijanih ključeva. Primarna funkcija pregleda je u tome da donese odluke o postavkama duljina trajanja valjanosti novih ključeva i datuma isteka valjanosti novih ključeva te potencijalne modifikacije u odnosu na postojeće ključeve i zamjena ključeva.

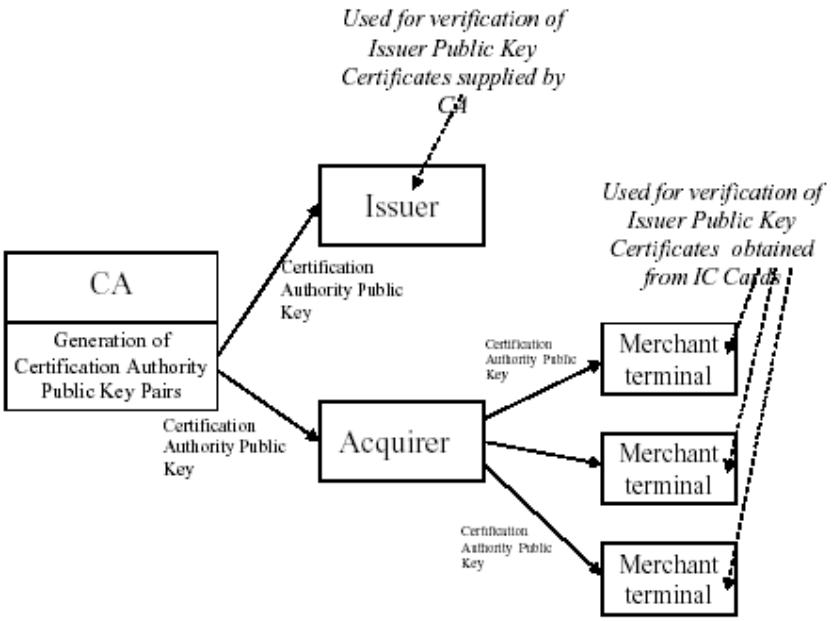
GENERIRANJE

Ako rezultat faze planiranja zahtijeva uvođenje novog para ključeva certifikatora, oni moraju biti generirani od platnog sustava. Preciznije, dio platnog sistema za autorizaciju certifikata (fizička i logička infrastruktura sa visokom razinom sigurnosti upravljanja platnim sistemom) će generirati na siguran način potreban par RSA ključeva za autorizaciju certifikata za buduću upotrebu.

Zato se posebno mora izgraditi podsekvenca koja se brine za tajnost privatnog ključa za autorizaciju certifikata. Također se mora omogućiti integritet privatnih i javnih ključeva.

DISTRIBUCIJA

U fazi distribucije ključa, dio platnog sistema za autorizaciju certifikata će distribuirati novo-generirane javne ključeve za autorizaciju certifikata traženom izdavačima (Issuer) i korisnicima (Acquirer) za slijedeće svrhe (slika 7):



Slika 7: Distribucija javnog ključa za autorizaciju certifikata

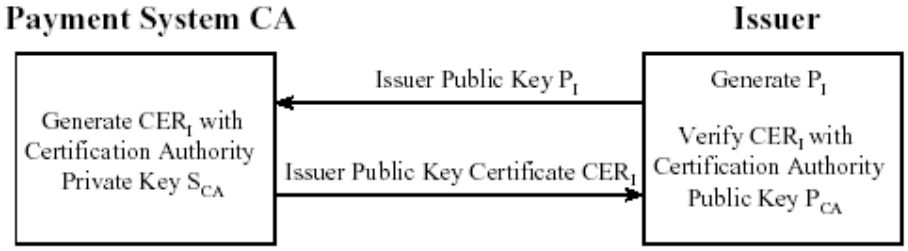
- Izdavač verificira javni ključ certifikatora izdanog od platnog sistema tijekom faze korištenja ključa
- Korisnici za siguran prijenos javnih ključeva za autorizaciju certifikata do terminala trgovca

Da bi se spriječilo uvođenje lažnih javnih ključeva za autorizaciju certifikata, sučelja između platnog sistema, izdavača i korisnika moraju osigurati integritet distribucije javnih ključeva.

UPOTREBA

Javni ključ certifikatora se upotrebljava u terminalima trgovaca da bi se mogla provoditi statička ili dinamička autorizacija podataka.

Privatni ključ certifikatora je upotrebljen u dijelu platnog sistema za autorizaciju certifikata za generiranje certifikata javnog ključa izdavača. Preciznije, događaju se slijedeće interakcije (slika 8):



Slika 8: Distribucija javnog ključa izdavača

- Izdavač generira svoj javni ključ izdavača i šalje ga platnom sustavu
- Platni sistem označi javni ključ izdavača sa privatnim ključem certifikatora da bi dobio certifikat javnog ključa izdavača i vraća ga izdavaču

- Sa javnim ključem certifikatora, izdavač provjerava ispravnost primljenog certifikata javnog ključa izdavača. Ako je u redu, izdavač može tada uključiti svoj dio podataka za otkrivanje identiteta sa kartičinim podacima

Da bi se spriječilo uvođenje lažnih javnih ključeva izdavača, sučelje između izdavača i platnog sistema moraju osigurati integritet javnog ključa izdavača koji je izdan za certifikaciju.

PONIŠTAVANJE

Kad par ključeva ispuni svoj radni vijek tijekom faze planiranja, mora se odstraniti iz usluge. U praksi, to znači slijedeće:

- Kad im istekne radni vijek, certifikat javnog ključa izdavača zajedno sa privatnim ključem certifikatora prestaju biti važeći. Izdavač zato mora osigurati da kartice personalizirane sa tim certifikatom javnog ključa izdavača onda kada i zadani par ključeva.
- Određeno vrijeme prije istjeka valjanosti, platni sistem će prestati označavati javne ključeve izdavača sa korespondiranim privatnim ključem certifikatora
- Kad isteknu, korisnici moraju moći lakoćom odstraniti javne ključeve za autorizaciju certifikata iz usluge u terminalu

Kompromis para javnih ključeva za autorizaciju certifikata

U slučaju kompromisa (probijanje tajnosti ili sigurnosti) para javnih ključeva certifikatora, mora se pokrenuti hitni postupak koji može na kraju rezultirati ubrzanim poništavanjem para javnih ključeva certifikatora prije njihovog istjeka radnog vijeka. U ovom slučaju postoje slijedeće faze životnog ciklusa ključa:

- detektiranje
- procjena
- odluka
- poništavanje (ubrzano)

DETEKTIRANJE

Kompromis para javnih ključeva certifikatora može biti aktualni kompromis, na primjer potvrđeni sigurnosni prekid u platnom sistemu, ili potvrđeno probijanje ključa kriptoanalizom. Nadalje, kompromis može biti:

- Očekivani: praćenje sistema ili član transakcije i vlasnik kartice zapaža provođenje lažnih transakcija koje mogu biti zbog kompromisa ključa, ali nije potvrđeno, ili
- Potencijalni: kriptoanalitičkim tehnikama, na primjer faktorizacijom, se razvila duljina ključa koji može biti kompromisni, ali nema dokaza da je to istina

Detektitanje kompromisnog ključa može nastati zbog aktualnog fizičkog provaljivanja u platni sistem. To se može zapaziti preko izvještaja lažnih off-line transakcija između platnog sistema i članova transakcija. Probijanje se izvodi inteligentnim unaprijeđenim faktoriziranjem otkrivene od strane kriptografske zajednice.

PROCJENA

Procjena potencijalnog kompromisa para ključeva će uključiti tehničke, rizične, lažne, i, najvažnije, udare na poslovnu sigurnost između platnog sistema i članova transakcija. Rezultat procjene uključuje potvrđivanje kompromisa, određivanje mogućih smjerova akcija protiv troškova i rizika kompromisa, i prezentiranje rezultata procjene za donošenje odluke.

ODLUKA

Na osnovi rezultata faze procjene, platni sistem odlučuje o akciji koja će biti poduzeti u svezi kompromisa ključa. U najgorem slučaju, ova odluka povlači dotični ključ iz upotrebe prije njegovog isteka radnog vijeka.

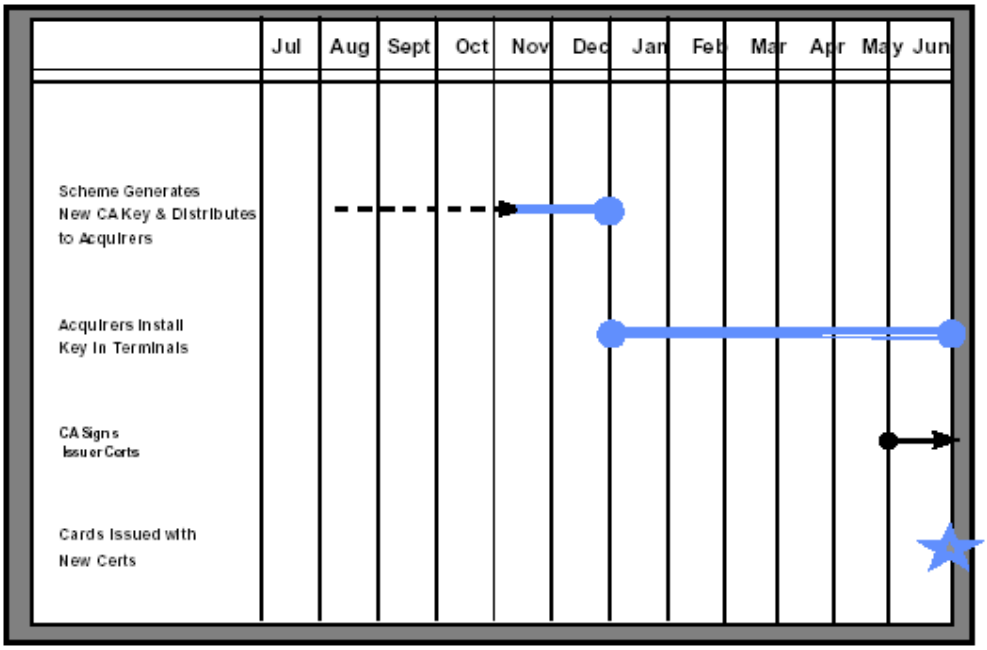
PONIŠTAVANJE (UBRZANO)

Poništavanje dotičnog ključa vodi do određivanja trajanja novog radnog vijeka tog ključa. Postupak je isti kao što je opisan u prethodnom odjeljku.

6.2. Vremenski odnosi

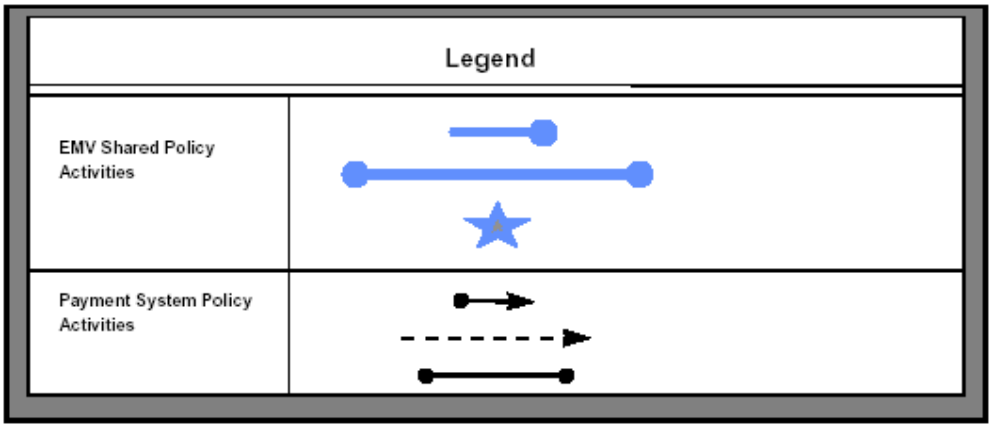
Slijedeći dijagrami prikazuju vremenske odnose za poništavanje i uvođenje javnih ključeva certifikatora. Svaka vremenska linija predstavlja raspored uvođenja ili ukidanja ključa. U slučaju ubrzanog uvođenja ili ukidanja ključa, vremena ostaju ista, ali za mjesece uvođenja i ukidanja ključa brine platni sistem.

UVOĐENJE KLJUČA



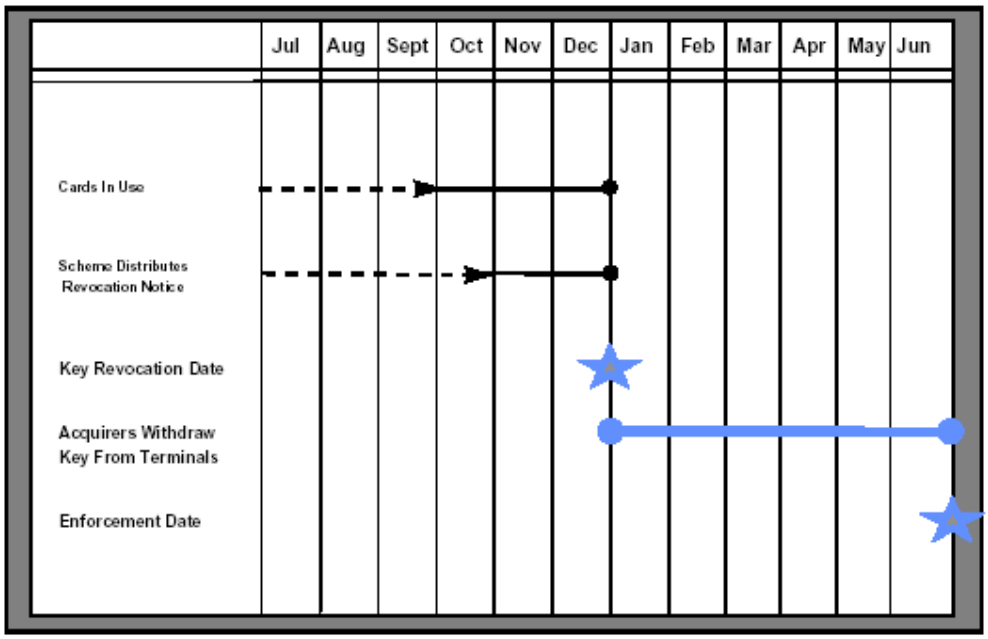
Slika 9: Dijagram uvođenja ključa

Legenda značenja pojedinih oznaka se nalazi na slijedećoj slici:



Slika 10: Legenda oznaka dijagrama

UKIDANJE KLJUČA



Slika 11: Dijagram ukidanja ključa

7. Sigurnost terminala i zahtjevi za rukovanje ključevima

Ovo poglavlje opisuje generalne zahtjeve terminala za rukovanje osjetljivim podacima, kao što su tekst identifikacijskog broja (PIN) ili kriptografski ključevi. Preciznije, imenuje zahtjeve za sigurnost tipkovnice za unošenje identifikacijskog broja i zahtjeve za rukovanje javnim ključevima za autorizaciju certifikata.

7.1 Sigurnosni zahtjevi

Sigurni uređaji (Tamper-Evident Devices)

Sigurni uređaji moraju u normalnom radnom okruženju osigurati da uređaj ili njegovo sučelje ne otkriva ili mijenja osjetljive podatke koji ulaze ili izlaze iz uređaja, ili koji su spremljeni ili se obrađuju u uređaju.

Kada siguran uređaj radi u sigurnosno-kontroliranom okruženju, zahtjevi za karakteristike uređaja su reducirani jer se zaštita provodi sigurnosno-kontroliranim okruženjem i rukovanjem uređaja.

FIZIČKA SIGURNOST

Siguran uređaj mora biti dizajniran tako da onemogućuje fizički pristup interno-spremljenim osjetljivim podacima i da odvraća krađu, neautoriziranu upotrebu ili neautoriziranu modofikaciju opreme. Navedeni ciljevi zahtijevaju otpornost, detekciju ili mehanizme zaštite kao što su vizualni ili zvučni alarmi.

Siguran uređaj, kada ne obavlja nikakve operacije, nebi smio sadržavati nikakve kriptografske ključeve ili druge osjetljive podatke (na primjer PIN-ove) koji su korišteni u nekoj od prethodnih transakcija. Probijanje u sistem može biti bez gubljenja sigurnosti tj. ne detektira ih uređaj, zato se takva probijanja moraju detektirati prije uređaja i prije nego što se kriptografski ključevi i osjetljivi podaci opet stave u operacijski sustav. Ako je uređaj dizajniran tako da je omogućen interni pristup, moraju se odmah osjetljivi podaci obrisati, čim dođe do probijanja u sistem. Sigurni uređaj je ovisan o fizičkoj sigurnosti što se tiče detekcije napada. Zato mora biti dizajniran tako da ima svojstva koja odmah vlasnika kartice ili trgovca upućuju na zločin.

Uređaj mora biti dizajniran i sastavljen tako da se:

- Ne može izvesti probijanje u uređaj u smislu izvođenja nekim promjena, dodataka ili zamjena sklopovske i programske opreme uređaja; ili promjene osjetljivih podataka i naknadno reinstaliranje uređaja bez upotrebne posebnih vještina i uređaja koji nisu generalno dostupni, i bez oštećivanja uređaja tako da se nebi moglo detektirati oštećivanje.
- Svaki neautorizirani pristup ili izmjena osjetljivih podataka, koji se unose, spremaju ili obrađuju, se pripisuje samo aktualnom probijanju uređaja.
- Nije omogućeno na bilo kakav način krivotvorenje i izrađivanje sličnih komponenti od kojih je uređaj sastavljen.
- Kvar na bilo kojem dijelu uređaja ne smije prouzročiti oštećivanje tajnih i osjetljivih podataka.
- Ako je uređaj dizajniran tako da dijelovi mogu biti fizički odvojeni od uređaja, svako obrađivanje podataka između vlasnika kartice i tih odvojenih dijelova mora imati istu razinu sigurnosti kao što je ima i cijeli, nerastavljeni uređaj.
- Integriranje drugačijih dijelova uređaja u kućište sigurnog uređaja je nužan uvjet za izmjenu osjetljivih podataka kao što je PIN.

LOGIČKA SIGURNOST

Siguran uređaj mora biti dizajniran tako da nijedna funkcija ili kombinacija funkcija ne prouzročava otkrivanje osjetljivih podataka, osim ako je to eksplicitno dozvoljeno od strane sigurnost implementirane u terminalu. Logička zaštita mora uvijek štititi osjetljive podatke, pa i ako su samo upotrebljene legitimne funkcije. To svojstvo se može postići internim praćenjem statistike ili mjerenjem minimalnog vremena između poziva osjetljivih funkcija.

Ako terminal može doći u osjetljivo stanje (stanje u kojem se mogu pozivati funkcije koje nisu omogućene u normalnom načinu rada, na primjer, korisničko rukovanje kriptografskim ključevima), takav prijenos mora biti dodatno nadgledan od dviju ili više povjerljivih strana. Ako je lozinka ili drugi tekstualni podaci upotrebljena kod kontrole prijenosa u osjetljivom stanju, unos te lozinke ili tekstualnih podataka mora biti zaštićen na način kao i ostali osjetljivi podaci.

Za minimiziranje rizika koji rezultira neautoriziranom upotrebom osjetljivih finkcija, osjetljivo stanje mora biti postignuto sa ograničenim brojem poziva funkcija (gdje je to prikladno) i vremenskim ograničenjem. Ako je neko od tih ograničenja postignuto, uređaj se mora vratiti u normalno stanje.

Siguran uređaj mora automatski isprazniti svoje unutrašnje spremnike (buffers) na kraju svake transakcije ili u time-out situaciji.

Tipkovnica za unos identifikacijskog broja (PIN Pad)

Tipkovnica za unos identifikacijskog broja mora biti siguran uređaj. Mora podržavati unos 4-12 znamenkastog identifikacijskog broja. Ako je priložen i ispis uz tipkovnicu (display), indikacija unošenja pojedinog broja mora biti ispisana. No, stvarne vrijednosti brojeva se ne smiju vidjeti, već se smiju vidjeti samo oznake (vizualne ili zvučne) da su brojevi unešeni.

Kad terminal podržava off-line verifikaciju PIN-a, IFD (Interface Device) i tipkovnica za unos PIN-a moraju biti intergrirane u jedan uređaj ili IFD i tipkovnica moraju biti dva posebno odvojena uređaja.

Ako su IFD i tipkovnica integrirani i offline PIN se šalje kartici u obliku teksta, tipkovnica ne kriptira offline PIN kada je tekstualni PIN poslan od tipkovnice do IFD-a.

Ako su IFD i tipkovnica integrirani i offline PIN se šalje kartici u obliku teksta, ali offline PIN tekst nije poslan direktno od tipkovnice do IFD-a, tada tipkovnica mora kriptirati offline PIN za prijenos do IFD-a. U tom slučaju IFD dekriptira offline PIN za prijenos u tekstu do kartice.

Ako IFD i tipkovnica nisu integrirani zajedno, a offline PIN se mora poslati kartici u tekstualnom obliku, tipkovnica mora kriptirati offline PIN za prijenos do IFD-a. U tom slučaju IFD dekriptira offline PIN za prijenos u tekstu do kartice.

Ako se offline PIN šalje kartici u kriptiranom obliku, kriptiranje se provodi na:

- tipkovnici samog uređaja
- sigurnoj komponenti terminala

Ako terminal podržava on-line verifikaciju PIN-a, kada je PIN unesen mora biti zaštićen kriptiranjem unutar terminala i terminal mora slati kriptirani PIN u skladu s pravilima sustava plaćanja.

Ispis prompt-a za unos PIN-a mora biti generiran od same tipkovnice. To znači da se mogu ispisivati sve vrste poruka koje su autorizirane od strane tipkovnice, a ne samo koje su u vezi PIN-a. Tipkovnica mora odbiti ispis bilo kakve neautorizirane poruke.

Za praćene terminale, unos iznosa mora biti separiran od unosa PIN-a da bi se izbjeglo nesretno ispisivanje PIN-a na terminalu. Ako se PIN i iznos unose sa iste tipkovnice, iznos mora biti provjeren od vlasnika kartice prije nego što se unosi PIN.

Tipkovnica mora biti dizajnirana tako da štiti privatnost i tajnost, tako da u normalnoj upotrebi samo vlasnik može vidjeti informacije ispisane na zaslonu terminala. Tipkovnica mora biti tako ugrađena da vlasnik kartice može unijeti PIN sa minimalnim rizikom da su taj unos vidjeli drugi.

Tipkovnica mora isprazniti svoje unutrašnje spremnike u slijedećim uvjetima:

- pri završetku transakcije
- u time-out situaciji, uključujući neodređeni period vremena otkako je unesen PIN

7.2. Zahtjevi za rukovanje ključem

Ovo poglavlje specificira zahtjeve za korisničko rukovanje javnim ključevima certifikatora u terminalu. Zahtjevi pokrivaju slijedeće faze:

- uvođenje javnih ključeva certifikatora u terminal
- spremanje javnih ključeva certifikatora u terminal
- upotreba javnih ključeva certifikatora u terminalu
- ukidanje javnih ključeva certifikatora iz terminala

Uvođenje javnih ključeva certifikatora u terminal

Kada platni sistem donese odluku o uvođenju javnih ključeva certifikatora u terminal, proces je izvršen tako da osigurava distribuciju novog ključa od platnog sistema do korisnika. Od tog trenutka je odgovornost na korisniku da se brine o prijenosu novog javnog ključa certifikatora i podataka vezanih za njega do terminala.

Uvaženi su slijedeći principi kod uvođenja javnog ključa certifikatora od korisnika do terminala:

- Terminal mora moći verificirati da je javni ključ certifikatora primljen bez greške od korisnika
- Terminal mora moći verificirati da je primljen javni ključ certifikatora originalan od legitimnog korisnika
- Korisnik mora moći potvrditi da je javni ključ certifikatora u potpunosti ispravno uveden u terminal

Spremanje javnih ključeva certifikatora u terminal

Terminal koji podržava statičku i/ili dinamičku autentifikaciju podataka mora podržavati šest javnih ključeva certifikatora preko RID-a za kreditne kartice Mastercarda, Vise i Europaya bazirane na EMV standardu.

Svaki javni ključ certifikatora je jednoznačno određen 5-bajtnim RID-om koji identificira platni sistemm i 1-bajtni indeks javnog ključa certifikatora, jednoznačnog za RID dodijeljen od platnog sistema da bude djelomični javni ključ certifikatora.

Minimalni set elemenata podataka vezanih za javni ključ certifikatora koji se spremaju u terminal je dan u slijedećoj tablici 2:

Name	Length	Description	Format
Registered Application Provider Identifier (RID)	5	Identifies the payment system to which the Certification Authority Public Key is associated	b
Certification Authority Public Key Index	1	Identifies the Certification Authority Public Key in conjunction with the RID	b
Certification Authority Hash algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme	b
Certification Authority Public Key Algorithm Indicator	1	Identifies the digital signature algorithm to be used with the Certification Authority Public Key	b
Certification Authority Public Key Modulus	Var. (max 248)	Value of the modulus part of the Certification Authority Public Key	b
Certification Authority Public Key Exponent	1 or 3	Value of the exponent part of the Certification Authority Public Key, equal to 3 or $2^{16}+1$	b
Certification Authority Public Key Check Sum[10]	20	A check value calculated on the concatenation of all parts of the certification Authority Public Key (RID, Certification Authority Public Key Index, Certification Authority Public Key Modulus, Certification Authority Public Key Exponent) using SHA-1	b

Tablica 2: Minimalni set elemenata podataka vezanih za javni ključ za autorizaciju certifikata koji se spremaju u terminal

RID i indeks javnog ključa certifikatora su jednoznačni za svaki javni ključ certifikatora i jednoznačno povezani sa platnim sistemom.

Indikator algoritma za javni ključ certifikatora identificira algoritam digitalnog potpisa koji se upotrebljava sa korenspondirajućim javnim ključem certifikatora. Jedino prihvatljiva vrijednost u tom slučaju je heksadecimalno “01”, koja označava upotrebu RSA algoritma kod digitalnog potpisa. Indikator hash algoritma specificira hash algoritam koji se koristi kod digitalnog potpisa. Jedino prihvatljiva vrijednost je u tom slučaju heksadecimalno “01”, koja označava da se radi o SHA-1 hash algoritmu.

Suma provjere javnog ključa certifikatora služi za ispitivanje ispravnosti transfera javnog ključa certifikatora na odredište. Terminal može koristiti taj podatak za naknadno re-verificiranje javnog ključa za autorizaciju certifikata i podatke vezane uz njega. Osim tog, terminal može koristiti i druga sredstva za provjeravanje integriteta tih podataka.

Integritet spremljenih podataka bi trebao biti svakog određenog vremenskog intervala.

Ukidanje javnog ključa certifikatora

Kad platni sistem odluči povući neki javni ključ certifikatora iz upotrebe, korisnik mora osigurati da se taj ključ više neće koristiti u terminalima za statičku ili dinamičku autentifikaciju podataka nakon trenutka ukidanja.

Slijedeći principi su uvaženi kod korisničkog ukidanja valjanosti javnog ključa certifikatora u terminalu:

- Terminal mora moću utvrditi ispravnost informacije o ukidanju ključa dobivene od korisnika
- Terminal mora moći utvrditi originalnost informacije o ukidanju ključa od legitimnog korisnika
- Korisnik mora moći potvrditi da je zaista zatražio ukidanje specifičnog javnog ključa certifikatora u terminalu

8. Zaključak

Ova verzija EMV standarda je tek početak i standard prolazi kroz "rano djetinstvo". Organizacije članice postavile su ultimatum svim bankama članicama za prijelaz na EMV standarde do 2005. godine, a one koje to ne ispune same će morati snositi odgovornost i štetu nastalu kompromitiranim transakcijama. EMV je već implementiran u nekim zemljama kao što su Velika Britanija, Brazil, Italija i Francuska.

U skorijoj budućnosti očekuje se ekspanzija EMV pametnih kartica i prihvatnih uređaja s poboljšanim karakteristikama i poboljšanim servisima. Za te se servise očekuje da će biti prilagodljivi jednistvenim potrebama svakog korisnika, a moći će se koristitii u mobilnim uređajima. Za nadogradnju podataka i usluga neće biti potrebno izdavanje nove kartice, već će se moći downloadirati nove aplikacije i parametri.

Također se očekuje ekspanzija stolnih aplikacija zasnovanih na pametnim karticama, koje će omogućiti sigurnu on-line kupovinu. Ona će tada biti jednostavnija i višestruko sigurnija. Nedavno je bilo u tijeku ispitivanje procesa unaprijeđenja level 1 i level 2 testova prema EMV 2000 v.4.0 sprecifikacijama. U tijeku je izrada i dopune za podršku beskontaktnih karticama te karticama i terminalima s manjim radnim naponom, u suradnji sa ISO/IEC odborom. Svake dvije godine očekuje se revizija postojećih verzija EMV-a i izdavanje novih.

Sadržaj

Literatura:

1. VIDI kompjutorski časopis broj 73 (Travanj 2002.)
2. www.emvco.com (datum pristupanja stranici 15.12.2002.) - web stranica na kojoj se nalaze primjerci knjiga EMV 4.0 standarda u pdf formatu