Digitalna poštna znamka

Seminar pri predmetu
Kriptografija
in
računalniška varnost

Ludvik Kos

Mentor: prof. dr. Aleksandar Jurišić

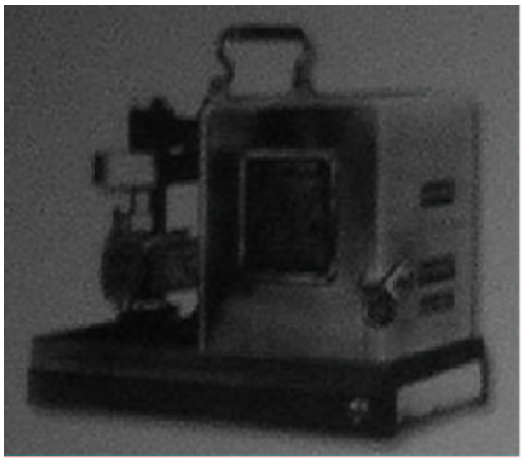
September 2004

Povzetek. Pričujoče delo predstavlja temeljne koncepte digitalne poštne znamke. Najprej so našteti motivi za razvoj takega načina plačevanja poštnih storitev. Sledi prikaz zgradbe digitalne poštne znamke. Opisana je infrastruktura, ki ji sledijo kriptografski temelji z uporabo asimetrične in simetrične kriptografije za generiranje kriptografske kode za preverjanje.

1 Uvod

Ko želimo poslati pismo, moramo na ovojnico prilepiti poštno znamko. Leta je dokaz, da smo poravnali stroške poštnine. Težava nastopi, ko želimo poslati veliko pisem. Lepljenje znamk na nekaj deset ali celo nekaj sto ovojnic bi bilo zamudno.
Če so vse pošiljke podobnega formata in teže, lahko s ponudnikom poštnih storitev sklenemo pogodbo. Vse pošiljke imajo posebno oznako, ki služi za evidentiranje števila poslanih kosov. Take pošiljke so npr. bančni izpiski ali računi.
Če pošiljke niso vse istega formata in mase, lahko podjetja, ki pošiljajo veliko pošte, uporabljajo t.i. *frankirne stroje*. To so elektro-mehanske naprave, ki natisnejo žig, ki nadomešča poštno znamko. Frankirni stroj vsebuje dva registra: prvi je naraščujoči, ki šteje, koliko znamk smo že natisnili; drugi register je padajoči, pove pa, kolikšna je vrednost kredita, ki ga lahko uporabimo za tiskanje znamk. Včasih imamo še tretji register, ki šteje vrednost vseh natisnjenih znamk. Preden začnemo napravo uporabljati, jo moramo odnesti na

pošto, kjer vplačamo kredit. Naprava je narejena tako, da ni nepropustna, vendar je razvidno, če je prišlo do nepooblaščenega posega vanjo (*angl. tamper evident device*). Prvo napravo te vrste lahki vidimo na Sliki 1. Težava pri frankirnem stroju je v tem, da ga je potrebno fizično nositi na pošto[1] ter da je z napredkom v kvaliteti tiskalnikov več možnosti za ponarejanje. V ZDA ocenjujejo, da vsako leto nastane za okoli 100 milijonov dolarjev škode s ponarejanjem natisnjenih poštnih znamk.



Slika 1: prvi frankirni stroj podjetja Pitney Bowes Postage Meter Company (*Vir: Aleksandar Jurišić, fotografija iz muzeja NSA*)

Omenjene težave in posebno še finančni vidik so bili spodbuda, da je ameriška poštna služba pričela s programom za uvajanje *digitalne poštne znamke*. V pričujočem delu bodo najprej predstavljene osnovne lastnosti digitalne poštne znamke. Sledil bo opis infrastrukture, ki jo potrebujemo v ta namen. Predstavljeni bodo tudi kriptografski temelji, ki otežujejo zlorabe.

2 Kaj je digitalna poštna znamka?

Digitalna poštna znamka je skupek podatkov, ki so vezani na pošiljatelja in pošiljko ter imajo dodano *kriptografsko kodo za preverjanje* (*angl. Cryptographic Validation Code*, CVC). Povezanost s pošiljateljem omogoča lažje odkrivanje ponarejevalcev ter otežuje anonimno uporabo poštnih storitev (kar je postalo v ZDA bolj aktualno po 11. septembru 2001).
Da dosežemo povezanosti s pošiljko, so običajno vključeni v digitalno poštno znamko naslednji podatki:

[1] To slabost so kasneje odpravili s polnitvami prek telefona.

- primerno zakodiran naslov prejemnika;
- oznaka pošiljatelja;
- znesek poštnine;
- datum pošiljanja;
- zaporedna številka.

Podatkom je dodana kriptografska koda za preverjanje (CVC), ki predstavlja digitalni podpis. S CVC lahko ponudnik poštnih storitev odkrije, če so bili podatki naknadno spremenjeni.

Slika 2: poštna ovojnica z natisnjeno digitalno poštno znamko
(*Vir: Pintsov, Vanstone, Postal Revenue Collection in the Digital Age*)

Podatki, ki sestavljajo digitalno poštno znamko, morajo biti pretvorjeni v obliko, ki je primerna za strojno odčitavanje. V ta namen se uporablja dvorazsežna črtna koda (npr. PDF417, Data Matrix,...). Primer pisemske ovojnice z natisnjeno digitalno poštno znamko lahko vidimo na Sliki 2.

3 Infrastruktura

Za delovanje sistema v praksi potebujemo ustrezno infrastrukturo, ki jo sestavljajo:

- varna naprava za generiranje dig. poštnih znamk (*angl. Postal Security Device, PSD*);
- osebni računalnik s tiskalnikom in omrežno povezavo (internet);
- sistem za preverjanje veljavnosti digitalnih poštnih znamk.

Naprava PSD mora biti nepropustna (*angl. tamper resistant*), kar pomeni, da mora biti vsebina njenega pomnilnika nedostopna zunanjemu svetu. Glavna naloga naprave PSD je generiranje kriptografske kode za preverjanje. Poleg tega mora voditi lastno računovodstvo o stanju dobroimetja, številu izdanih digitalnih poštnih znamk, itd. PSD se lahko nahaja pri ponudniku storitev, lahko pa tudi pri samem uporabniku (za večje stranke). Dobroimetje se zmanjšuje z vsako izdano znamko, poveča pa ga lahko ponudnik storitev na podlagi zahteve uporabnika (na osnovi potrdila o plačilu). Povečanje dobroimetja se izvede z varno transakcijo.
Naprava PSD ima lahko vgrajen tiskalnik, kar pa ni nujno. Uporabnik osebnega računalnika lahko dostopa do naprave PSD prek interneta in si znamko natisne na svojem tiskalniku. Tako postane koncept digitalne poštne znamke sprejemljiv tudi za domačo rabo.
Zaščita pred ponarejanjem in kopiranjem ne deluje, če ne preverjamo znamk. Preverjanje veljavnosti digitalnih poštnih znamk se izvaja pri ponudniku poštnih storitev (t.j. na pošti). Preverjamo pristnost znamke in če je bila le-ta prekopirana (t.j. ponovno uporabljena). Preverjanje digitalnih poštnih znamk predstavlja ozko grlo v sistemu. Če ne moremo preveriti vsake pošilke, jih lahko pregledujemo statistično in s tem vpeljemo t.i. *planiran obseg poštnih zlorab*.
Pristnost ugotovimo razmeroma enostavno: preverimo, če je koda CVC veljavna glede na ostale podatke na znamki. Seveda mora biti narava kode CVC taka, da je mogoče preverjanje v realnem času.
Preverjanje ponovne uporabe (*angl. replay detection*) je težje. V drugem poglavju smo omenili, da je znamka vezana na pošiljko, kar naj bi otežilo kopiranje. Povezava med znamko in pošiljko je izvedena tako, da med podatke vključimo (primerno kodiran) naslov prejemnika. Težava nastopi, če uporabnik pošilja več pošiljk istega dne na isti naslov. Tako bi lahko uporabnik plačal eno znamko ter jo poljubno mnogokrat uporabil za istega naslovnika. Zaplet rešimo z uporabo zaporedne številke znamke: na pošti beležimo zaporedne številke znamk in preverjamo, če ni bila znamka z določeno številko

že kdaj uporabljena. V takem primeru bi rabili ogromno bazo podatkov, v kateri bi morali delati poizvedbe v realnem času. V [3] je predlagana naslednja prostorsko učinkovitejša izvedba take baze: za vsakega uporabnika C hranimo največje število i_C za katero velja, da so vse znamke z zaporedno številko manjšo od i_C že uporabljene ali pa jih je pretekel rok veljavnosti. Poleg tega števila še hranimo stisnjen seznam vseh zaporednih številk, ki so večje od i_C.

4 Kriptografski temelji

Kriptografska koda za preverjanje (CVC) predstavlja stičišče digitalne poštne znamke s kriptografijo. Opravlja nalogo digitalnega podpisa podatkov v digitalni poštni znamki:

- zagotavlja, da je znamko generirala pooblaščena naprava;
- zagotavlja celovitost podatkov, ki sestavljajo digitalno poštno znamko.

Koda CVC mora biti zasnovana tako, da je njena fizična predstavitev dovolj majhna (ne smemo pozabiti, da smo omejeni z velikostjo pisemske ovojnice) ter da hkrati zagotavlja primerno stopnjo varnosti. Pomembna lastnost je tudi to, da je možna računsko učinkovita izvedba operacij generiranja in preverjanja kode CVC.
Koda CVC je lahko zasnovana na podlagi asimetrične ali pa simetrične kriptografije. V naslednjih podrazdelkih sta opisana oba primera.

4.1 CVC z uporabo asimetrične kriptografije

Digitalni podpis nam lahko služi kot koda CVC. Uporabimo lahko npr. algoritem RSA.

Generiranje kode CVC poteka takole:

1. zberemo podatke, ki bodo sestavljali dig. poštno znamko (glej drugo poglavje);
2. izračunamo zgostitev podatkov z ustrezno zgoščevalno funkcijo (npr. SHA-1);
3. zašifriramo zgostitev s tajnim ključem naprave PSD - dobimo digitalni podpis.

Preverjanje kode CVC poteka takole:

1. pridobimo veljaven javni ključ naprave PSD;
2. zberemo podatke, ki sestavljajo dig. poštno znamko;
3. izračunamo zgostitev z ustrezno zgoščevalno funkcijo;
4. odšifriramo digitalni podpis in primerjamo zgostitvi.

Pri preverjanju je problematična prva točka, ki zadeva pridobitev veljavnega javnega ključa naprave, ki je generirala digitalno poštno znamko. Pomagamo si z digitalnim certifikatom, ki ni nič drugega, kot javni ključ naprave PSD s pridruženim podatkom o identiteti naprave. Vse to pa je digitalno podpisano s strani zaupanja vredne agencije, ki je v našem primeru lahko poštna organizacija.
Pojavi se še vprašanje, od kod pridobimo certifikat, ko preverjamo posamezno digitalno poštno znamko. En način je, da vzdržujemo centralno bazo certifikatov za vse naprave PSD. Celotna baza - lahko je velika, če je število naprav PSD veliko - mora biti neprestano dostopna vsem enotam poštne organizacije, kar lahko predstavlja performančno težavo, če je veliko enot. Če predpišemo, da se pošiljke, ki so frankirane z digitalno poštno znamko lahko oddajajo samo v kraju/regiji, kjer je naprava PSD registrirana, omenjene težave omilimo. Sedaj potrebujejo posamezne enote seznam certifikatov samo tistih naprav, ki so v danem kraju/regiji.
Izberemo lahko tudi drugačen pristop: sama digitalna poštna znamka vsebuje certifikat. V tem primeru dosežemo določeno samozadostnost pri preverjanju veljavnosti. Potrebujemo samo javni ključ poštne organizacije, s katerim preverimo veljavnost certifikata. Slabost tega načina je, da z vključitvijo certifikata velikost poštne znamke precej naraste. Primerjavo velikosti digitalnih poštnih znam pridobljenih z različnimi metodami vidimo v tabeli na Sliki 6. Z uporabo *kriptografije eliptičnih krivulj* (bralec lahko najde osnove recimo v [6] ali [7]) se velikost digitalnega podpisa precej zmanjša in tako postane ideja o vključitvi certifikata sprejemljivejša.
Pintsov in Vanstone v [5] opisujeta uporabo *optimalnega poštnega certifikata* v kombinaciji z *digitalnim podpisom z delnim povračilom sporočila*, kar še dodatno pripomore k zmanjšanju velikosti digitalne poštne znamke (glej tudi tabelo na Sliki 6). Ta pristop bo opisan v nadaljevanju.

4.1.1 Optimalni poštni certifikat

Običajni (*eksplicitni*) certifikat, je sestavljen iz javnega ključa, identifikacije lastnika ter iz podpisa agencije. Slednji ni nič drugega, kot podpisana zgostitev javnega ključa in identifikacije s tajnim ključem agencije. Veljavnost podpisa preverimo z javnim ključem agencije. Velikost takega certifikata je enaka vsoti velikosti javnega ključa lastnika, velikosti identifikacijskih podatkov ter velikosti podpisa agencije (enaka velikosti tajnega ključa agencije). Javni ključ avtenticiramo (t.j. preverimo, da res pripada določenemu uporabniku) tako, da njegov lastnik dokaže poznavanje pripadajočega tajnega ključa.
Implicitni certifikat je vrednost, s pomočjo katere ob uporabi javnega ključa agencije izračunamo uporabnikov javni ključ. Velikost takega certifikata je precej manjša in zato primerna za sisteme z omejeno pasovno širino, kamor spadajo brezžična omrežja in seveda tudi digitalna poštna znamka. Avtentikacija je podobna, kot pri klasičnem certifikatu.
Optimalni poštni certifikat je realizacija implicitnega certifikata s pomočjo kriptografije eliptičnih krivulj. Matematično nezahtevni uvod v kriptografijo eliptičnih krivulj lahko bralec najde v [6] ali v [7]. Podrobnosti najdemo v eni od Menezesovih knjig (npr. v *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993) oz. v *Dr. Dobbs Journal*-u (A. Jurišić, A. Menezes, *Elliptic Curves and Cryptography*, april 1997).

V nadaljevanju uporabljamo naslednjo notacijo:
G - generator grupe eliptične krivulje (definirana nad obsegom $GF(2^n)$, $130 \leq n \leq 200$);
c - tajni ključ poštne agencije;
B - javni ključ poštne agencije (izračunan kot $B = cG$).
I_A - identifikacijska oznaka naprave PSD;
$H(\cdot)$ - zgoščevalna funkcija;
$\|$ - operator stika dveh nizov;

Protokol za izračun optimalnega poštnega certifikata je prikazan na Sliki 3. Vidimo, da lahko uporabnikov javni ključ izračunamo s pomočjo certifikata na dva načina. Če poznamo uporabnikov tajni ključ: $Q_A = aG$, kar je enako $(m_A + k_A)G = (cf + c_A + k_A)G$. Če člene malo preuredimo ter upoštevamo definiciji javnega ključa agencije ter optimalnega poštnega certifikata, dobimo: $fcG + (c_A G + k_A G) = fB + \gamma_A = H(\gamma_A \parallel I_A) \cdot B + \gamma_A$. Dobljeni rezultat predstavlja drugi način izračuna javnega ključa (brez poznavanja tajnega ključa uporabnika).
Tajni ključ lahko izračunamo na en sam način in to samo s poznavanjem

tajne vrednosti k_A. Varnost metode temelji na težavnosti *problema diskretnega logaritma* eliptične krivulje: čeprav poznamo vrednost produkta k_AG (to vrednost lahko prestrežemo), ne moremo iz njega v razumnem času dobiti tajne vrednosti k_A. Le-ta bi nam pomagala pri izračunu tajnega ključa a.

protokol: generiranje optimalnega poštnega certifikata γ_A
izvajalca: poštna agencija (A), naprava PSD (B)

1. B generira naključno tajno število k_A
2. B pošlje A vrednost k_AG
3. A generira naključno tajno število c_A
4. A izračuna $\gamma_A := k_AG + c_AG$
5. A izračuna $f := H(\gamma_A \parallel I_A)$
6. A izračuna $m_A := cf + c_A$
7. A pošlje B naslednje podatke: $\gamma_A,\ m_A,\ I_A$
8. B izračuna svoj tajni ključ: $a := m_A + k_A$
9. B izračuna svoj javni ključ: $Q_A := aG$

Slika 3: protokol za generiranje optimalnega poštnega certifikata

Dokaz o varnosti implicitnih certifikatov lahko najdemo v [1].

4.1.2 Digitalni podpis z delnim povračilom sporočila

Pintsov in Vanstone v [5] opisujeta uporabo posebne tehnike digitalnega podpisa, iz katerega je mogoče restavrirati (krajši) del sporočila. Ta lastnost je posebno ugodna, ko želimo minimizirati porabo prostora.
Pred nadaljevanjem razlage je potrebno definirati nekatere pojme. Privzemimo, da podatke na digitalni poštni znamki delimo na *odprte* (označimo jih z V) in *zakrite* (označimo jih z P). Ta delitev je realizirana zaradi varovanja zasebnih podatkov (npr. številka pošiljke, oznaka pošiljatelja, ...). Del P, je tisti, ki ga bomo rekonstruirali iz podpisa. Dodaten pogoj je, da so podatki v P dovolj redundantni, da ugotovimo, kdaj so smiselni. To dosežemo tako, da predpišemo, kako obliko morajo imeti podatki v P.
Funkcija $Tr_R(C)$ je bijektivna preslikava s parametrom R, ki zakrije regularnosti v C. V ta namen se lahko uporabi kakšna simetrična šifra ali pa funkcija *ekskluzivni-ali*(XOR)[2].
Z uporabo optimalnega poštnega certifikata (opis v prejšnjem razdelku) in s

[2]V tem primeru mora biti R iste dolžine kot C.

postopek: generiranje kode CVC
izvajalec: naprava PSD
vhod: P, V, I_A, a, G
izhod: CVC

1. generiraj naključno število k
2. $R := kG$
2. $e := Tr_R(P)$ (zakrijemo podatke)
3. $d := H(e \parallel I_A \parallel V)$;
4. $s := ad + k \pmod n$ (ta korak lahko naredi očitno samo naprava PSD, ker je uporabljen njen tajni ključ)
5. $CVC := (s, e)$

Slika 4: postopek za generiranje kode CVC

pomočjo podpisovalne sheme *z delnim povračilom sporočila* generiramo kriptografsko kodo s postopkom, ki je prikazan na Sliki 4.

Veljavnost kode CVC preverimo s postopkom, ki je prikazan na Sliki 5. Naslednja izpeljava nas prepriča, da imamo veljavno digitalno poštno znamko: s poznavanjem javnega ključa agencije ter z identifikacijo uporabnika (dejansko je to naprava PSD) izračunamo iz certifikata uporabnikov javni ključ $Q_A = H(\gamma_A \parallel I_A) + \gamma_A$. Iz kode CVC (t.j. iz para (s, e)), javnih podatkov iz znamke (V) ter iz identifikacije naprave PSD (I_A) izračunamo $d = H(e \parallel I_A \parallel V)$. Želimo razkriti podatke P iz e, zato potrebujemo R. V 2. točki postopka na sliki 4 smo ga definirali kot $R := kG$. Tajno vrednost k dobimo iz formule $s := ad+k \ (mod\ n)$ (ista slika, 4. korak): $k = s-ad$. Tako lahko R izrazimo kot: $(s - ad)G = sG - daG = sG - dQ_A$. Ker poznamo ustrezne podatke, ni težav z izračunom. Sedaj odšifriramo e: $Tr_R^{-1}(Tr_R(P))$ in dobimo P.
V primeru, da je znamka ponarejena, ne dobimo pravilne vrednosti za R. Da to opazimo, moramo definirati ustrezno sintakso ter semantiko za P (s tem uvedemo v P določeno redundantnost). Napačno vrednost R zaznamo tako, da ne dobimo smiselnega niza, ko odšifriramo e.

Omeniti je še potrebno navidezno nasprotje med zahtevo, da so podatki P zasebni in dejstvom, da jih lahko razberemo z uporabo javnega ključa ponudnika poštnih storitev. Čeprav ključu B dajemo prilastek *javni*, nikjer ni rečeno, da je znan zunaj poštne organizacije. Tako imamo poseben način rabe kriptografije z javnimi ključi in sicer tak, da sta oba ključa tajna.

postopek: preverjanje veljavnosti kode CVC
izvajalec: ponudnik poštnih storitev
vhod: $B,\ I_A,\ CVC = (s, e),\ V,\ \gamma_A,\ G$
izhod: koda CVC veljavna/neveljavna

1. $f := H(\gamma_A \parallel I_A)$
2. $Q_A := fB + \gamma_A$ (javni ključ naprave PSD)
3. $d := H(e \parallel I_A \parallel V)$
4. $R := sG - dQ_A$
5. $X := Tr_R^{-1}(e)$
6. **če** ima X predpisano obliko ter pomen, je koda CVC veljavna, **sicer** je neveljavna

Slika 5: postopek za preverjanje veljavnosti kode CVC

	RSA	*DSA*	*ECDSA*	*EC z MR*	*EC z MR in OMC*
podatki	20 bajtov	20 bajtov	20 bajtov	20 bajtov	20 bajtov
CVC	128 bajtov	40 bajtov	40 bajtov	20 bajtov	20 bajtov
certifikat	256 bajtov	168 bajtov	60 bajtov	60 bajtov	20 bajtov
skupaj	404 bajte	228 bajtov	120 bajtov	100 bajtov	60 bajtov

Slika 6: velikost poštnih znamk pridobljenih z različnimi metodami (*Vir: Pintsov, Vanstone, Postal Revenue Collection in the Digital Age*)

4.2 CVC z uporabo simetrične kriptografije

Če uporabimo pristop s simetrično kriptografijo, si naprava PSD in ponudnik poštnih storitev delita tajni ključ SK_C. Tajni ključ ponudnik izračuna iz svojega tajnega ključa in iz identifikacije naprave PSD (ID_C). Velja omeniti, da mora biti naprava PSD nepropustna (ni mogoče iz nje pridobiti tajni ključ SK_C), da onemogočimo nepooblaščeno izdajanje digitalnih poštnih znamk. V [3] priporočajo uporabo pametnih kartic.
Naprava PSD vsebuje dva notranja števca z_1 in z_2, ki sta prav tako kot ključ nedosegljiva od zunaj. Števec z_1 vsebuje vrednost kredita, števec z_2 pa šteje število zahtev za polnitev.

protokol: polnjenje dobropisa
izvajlci: uporabnik (A), naprava PSD (B), ponudnik poštnih storitev (C)

1. A pošlje B ukaz $GEN\_REQUEST$ in znesek polnitve x
2. B poveča števec z_2 za ena
3. B pošlje A niz: $Y := F_{SK_C}(REQUEST, z_2, x)$
4. A pošlje C niz: (Y, ID_C)
5. ko C prejme plačilo, izračuna tajni ključ SK_C ter odšifrira Y
6. C pošlje A ukaz $CHARGE$: $Z := F_{SK_C}(CHARGE, z2, x)$
7. A pošlje B niz Z
8 **če** je $F^{-1}_{SK_C}(Z)$ veljaven ukaz za polnjenje,
potem B poveča števec: $z_1 = z_1 + x$

Slika 7: protokol za polnjenje dobropisa v napravi PSD

protokol: generiranje digitalne poštne znamke
izvajalca: uporabnik (A), naprava PSD (B)

1. A določi potrebno poštnino y in zbere podatke D
2. A izračuna $v := h(D)$
3. A pošlje B ukaz $(STAMP, v, y)$
4. **če** je znesek y v mejah kredita,
potem B zmanjša števec $z_1 = z_1 - y$ ter pošlje A niz $X := F_{SK_C}(v, y)$
5. A uporabi (D, X) kot digitalno poštno znamko

Slika 8: protokol za generiranje digitalne poštne znamke

V formulah tega poglavja uporabljamo naslednjo notacijo:
$F_{SK_C}(\cdot)$ - simetrična šifra s ključem SK_C;
$F^{-1}_{SK_C}(\cdot)$ - funkcija za odšifriranje s ključem SK_C;
ID_C - identifikacijska oznaka naprave PSD;
$h(\cdot)$ - zgoščevalna funkcija;
D - podatki, ki so vezani na pošiljko.
Da lahko izdajamo znamke, moramo najprej napolniti kredit. To naredimo po protokolu na Sliki 7.

Digitalne poštne znamke generiramo po protokolu, ki je prikazan na Sliki 8.

Preverjanje veljavnosti digitalne poštne znamke izvedemo po postopku na Sliki 9. Utemeljitev je naslednja: ponudnik poštnih storitev in naprava PSD si delita isti simetrični ključ in velja, da je $F^{-1}_{SK_C}(F_{SK_C}(h(D), y) = (h(D), y)$.

postopek: preverjanje veljavnosti digitalne poštne znamke
izvajalec: ponudnik poštnih storitev
vhod: (D, X)
izhod: digitalna poštna znamka veljavna/neveljavna

1. iz D izloči identiteto naprave PSD - ID_C
2. s pomočjo ID_C izračunaj SK_C
3. $(v, y) := F^{-1}_{SK_C}(X)$
4. $v' := h(D)$
5. **če** je $v' = v$ in znesek y zadosten,

potem je digitalna poštna znamka veljavna,
sicer je neveljavna

Slika 9: postopek za preverjanje veljavnosti digitalne poštne znamke

V primeru, da bi bila znamka ponarejena, bi se izračunana zgostitev $h(D)$ ne ujemala z dejansko.

Varnost opisane metode temelji na težavnosti razbitja simetrične šifre, ki jo uporabimo v postopkih na slikah 7, 8 in 9 ter na nepropustnosti naprave PSD.
Če primerjamo uporabo asimetrične kriptografije z uporabo simetrične, ugotovimo, da dobimo v zadnjem primeru manjše digitalne poštne znamke (v [3] navajajo, da je dolžina kode CVC 16 bajtov) ter računsko učinkovitejše generiranje/preverjanje kode CVC, saj so simetrične šifre navadno računsko manj zahtevne kot asimetrične pri primerljivi dolžini ključa.
Slabost pa je v tem, da če pride do kompromitiranja ponudnikovega tajnega ključa, moramo zamenjati vse naprave PSD, katerih tajni ključi so generirani iz omenjenega ponudnikovega tajnega ključa.

Literatura

[1] D. R. L. Brown, R. Gallant, S. A. Vanstone, *Provably secure implicit certificate schemes*, Proceedings of the 5th International Conference on Financial Cryptography, strani 156-165, 2002 (http://www.cacr.math.uwaterloo.ca/techreports/2000/corr2000-55.ps)

[2] M. Girault, *Self-certified public keys*, Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of Cryptographic Techniques, strani 490-497, 1991 (http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/E91/490.PDF)

[3] D. Huehnlein, J. Merkle, *Secure and cost efficient electronic stamps*, Proceedings of the International Exhibition and Congress on Secure Networking - CQRE (Secure) '99, strani 94-100, 1999 (http://www.informatik.tu-darmstadt.de/ftp/pub/TI/TR/TI-99-17.stampend.ps.gz)

[4] M. Mikac, *Evidenca poštnih plačil v digitalni dobi*, diplomsko delo, Fakulteta za matematiko in fiziko, Ljubljana 2001

[5] L. A. Pintsov, S. A. Vanstone, *Postal revenue collection in the digital age*, Proceedings of the 4th International Conference on Financial Cryptography, strani 105-120, 2000 (http://www.certicom.com/download/aid-303/Certicom%20WP-DPM.pdf)

[6] W. Stallings, *Cryptography and network security: principles and practices*, tretja izdaja, Prentice Hall, 2003, ISBN 0-13-111502-2

[7] D. R. Stinson, *Cryptography: theory and practise*, druga izdaja, Chapman & Hall/CRC, 2002, ISBN 1-58488-206-9

[8] J. D. Tygar, B. S. Yee, N. Heintze, *Cryptographic postage indicia*, Asian Computing Science Conference, strani 378-391, 1996 (http://www.bennetyee.org/ucsd-pages/pub/asian-96.ps)