CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

S/MIME standard

CCERT-PUBDOC-2009-05-263

CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Pitanje sigurne komunikacije na Internetu važno je zbog velike količine osjetljivih informacija koje njime kolaju. Otvorenost Interneta prema korisnicima čini ga iznimno nesigurnim. Budući da Internet u osnovi nije zamišljen (niti ostvaren) kao sigurna mreža, zaštita komunikacije mora se omogućiti nadogradnjom. Zato postoje protokoli na različitim razinama mrežne infrastrukture, od IPsec protokola na mrežnom sloju, SSL/TLS protokola na transportnom sloju pa sve do zaštite na razini aplikacije. S/MIME je jedan od standarda koji pružaju zaštitu upravo na najvišoj - aplikativnoj razini. Riječ je o skupu kriptografskih algoritama i metoda koje su objedinjene u jedinstven model. Primjena ovog standarda omogućuje zaštitu elektroničkih poruka što uključuje očuvanje tajnosti i integriteta poruke te jamstvo autentičnosti njezinog pošiljatelja.

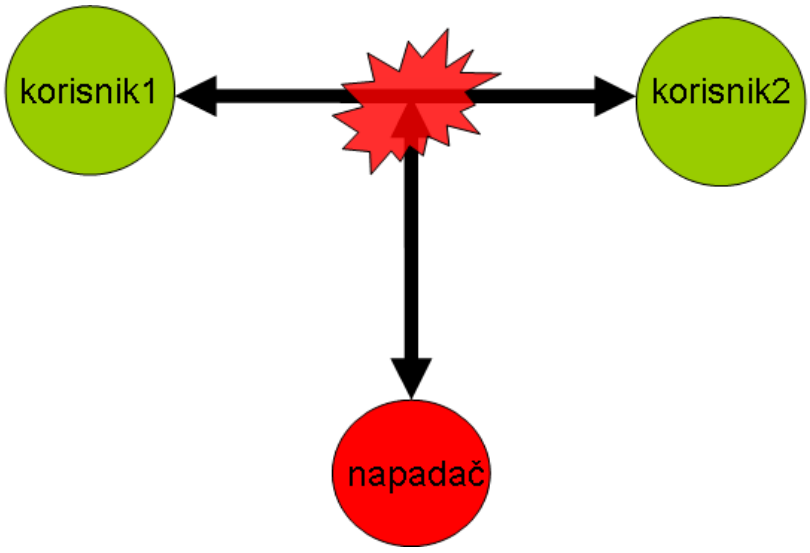
U ovom dokumentu dan je uvod u osnove kriptografskih metoda na kojima se temelji S/MIME i pregled specifikacije samog standarda. Na kraju je dana usporedba S/MIME standarda s OpenPGP standardom, koji mu predstavlja glavnu konkurenciju i alternativu. Budući da jedinstvenog odgovora na pitanje koja je sigurnosna politika najbolja nema, preostaje na korisnicima da se informiraju o dostupnim rješenjima i odaberu ono koje je njima najpovoljnije. Cilj ovog dokumenta je predstaviti jedno takvo rješenje.

2. Sigurnost komunikacije na Internetu

2.1. Vrste sigurnosnih prijetnji

Siguran komunikacijski kanal na Internetu podrazumijeva tajnost podataka koji se njime prenose, stabilnost veze (svi poslani podaci stižu na odredište), sigurnost u identitet pošiljatelja i besprijekornost sadržaja (sadržaj nije mijenjan na putu kroz Internet). S obzirom na svojstva sigurnosti koja ugrožavaju, napadi se mogu podijeliti na sljedećih pet skupina:

1. napadi na raspoloživost – napadač prekida komunikacijsku vezu između pošiljatelja i primatelja,
2. napadi na tajnost – napadač prisluškuje informacije koje prolaze komunikacijskim kanalom,
3. napadi na autentičnost – napadač se lažno predstavlja kao siguran i poznat entitet (osoba ili računalo),
4. napadi na besprijekornost – napadač presreće podatke, mijenja ih i prosljeđuje dalje i
5. napadi na neporecivost – korisnik poriče da je sudjelovao u komunikaciji.



Slika 1. Shema napada na sigurnost komunikacije na Internetu

Većinu navedenih napada moguće je spriječiti uvođenjem kriptografskih metoda koje se opisuju u idućem poglavlju.

2.2. Kriptografija

Kriptografija se smatra granom matematičkih i računarskih znanosti, a uključuje primjenu matematičkih metoda u razvoju algoritama za kriptiranje podataka. Cilj kriptografije je preoblikovati zadani tekst u takav oblik iz kojeg neće biti vidljiv njegov smisao i sadržaj. Kriptirani tekst mora biti moguće vratiti u izvorni oblik, ali samo pomoću tajnog ključa. Taj ključ može biti isti kao i onaj koji je korišten prilikom kriptiranja, ali i ne mora. Najjednostavniji primjer kriptiranja teksta tajnim ključem može se prikazati pomoću XOR (isključivo ili) logičke operacije. Primjer se prikazuje na bitovima jer se svi podaci u Internetu zaista kodiraju na razini bitova (tj. poprimaju vrijednosti 0 i 1). „Isključivo ili“ operacija definirana je za dva ulazna podatka tako da je izlaz 1 ukoliko oni imaju različitu vrijednost, 0 inače.

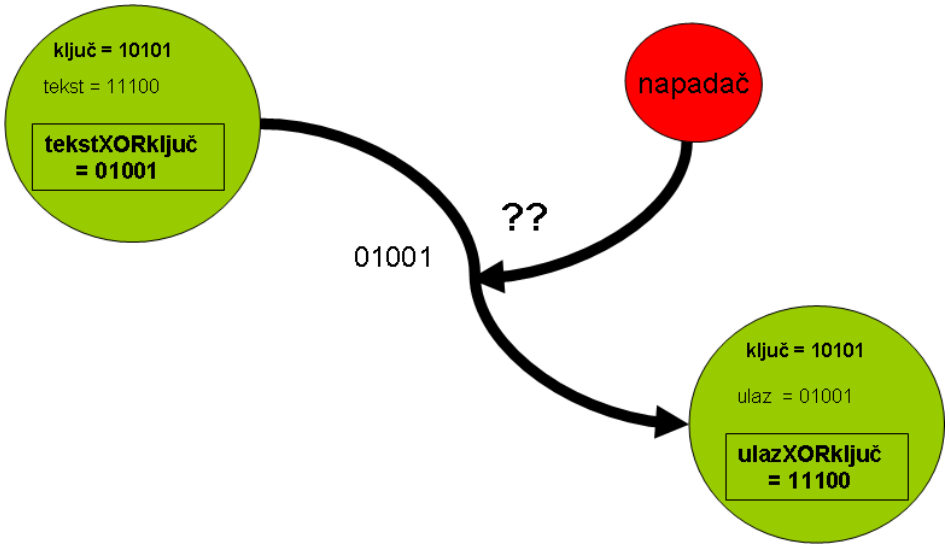
$$XOR(0,1)=1$$
$$XOR(1,0)=1$$
$$XOR(0,0)=0$$
$$XOR(1,1)=0$$

Definicija XOR funkcije

Ako se za nekakav proizvoljan niz bitova (otvoreni tekst) izmisli tajni niz (koji osim pošiljatelja zna samo osoba koja prima poruku), taj se tajni niz može koristiti kao ključ za kriptiranje i dekriptiranje. To je moguće zato što je XOR operacija simetrična, odnosno vrijedi:

$$XOR(tekst, kljuc) = kod \Rightarrow XOR(kod, kljuc) = tekst$$

Postupak kriptiranja XOR funkcijom prikazan je na sljedećoj slici:



Slika 2. Shema komunikacije zaštićene XOR kriptiranjem

Na ovom jednostavnom primjeru prikazan je najosnovniji princip kriptografskih algoritama. On ostavlja puno pitanja otvorenima, a najvažnija su:

- Kako sigurno razmijeniti tajni ključ?
- Koliko dugačak ključ je siguran ključ? Sigurnim se ključem pritom smatra onaj kojeg je nemoguće u razumnom vremenu otkriti tzv. „brute force“ metodama koje ispituju sve moguće vrijednosti ključa.
- Kako prilagođavati duljinu tajnog ključa duljini teksta?

Današnji kriptografski algoritmi bitno su složeniji od ovog primjera, ali njihova sigurnost uvijek se zasniva na težini otkrivanja tajnog ključa – što dulji ključ to sigurniji algoritam. Ipak, predug ključ može značiti dugotrajno kriptiranje i dekriptiranje pa se zato obično koriste „dovoljno dugački" ključevi. Za različite algoritme te su duljine različite. Simetrični algoritmi rabe veličine ključa od nekoliko stotina bitova (128, 256), a asimetrični do nekoliko tisuća bitova (1024, 2048) što ih čini složenijim (vremenski zahtjevnijim) metodama kriptiranja. U nastavku poglavlja dodatno će se pojasniti pojmovi i primjene kriptografskih algoritama.

2.2.1. Simetrični kriptografski algoritmi

U uvodu je prikazan primjer simetričnog kriptografskog algoritma. To znači da se isti ključ koristi za kriptiranje i za dekriptiranje sadržaja. Simetrični algoritmi u principu se zasnivaju na već navedenoj XOR operaciji, ali uključuju i dodatne složenije funkcije koje ih čine pouzdanima. Budući da su relativno brzi, mogu se koristiti za kriptiranje većih količina podataka. Neki od danas najčešće korištenih simetričnih algoritama su DES, 3DES, DESX, IDEA, Twofish i AES. Njima se kodiraju podaci u blokovima do nekoliko stotina bitova, a duljine ključeva iznose između 128 i 256 bitova. Problem kod simetričnih kriptografskih algoritama je razmjena tajnih ključeva.

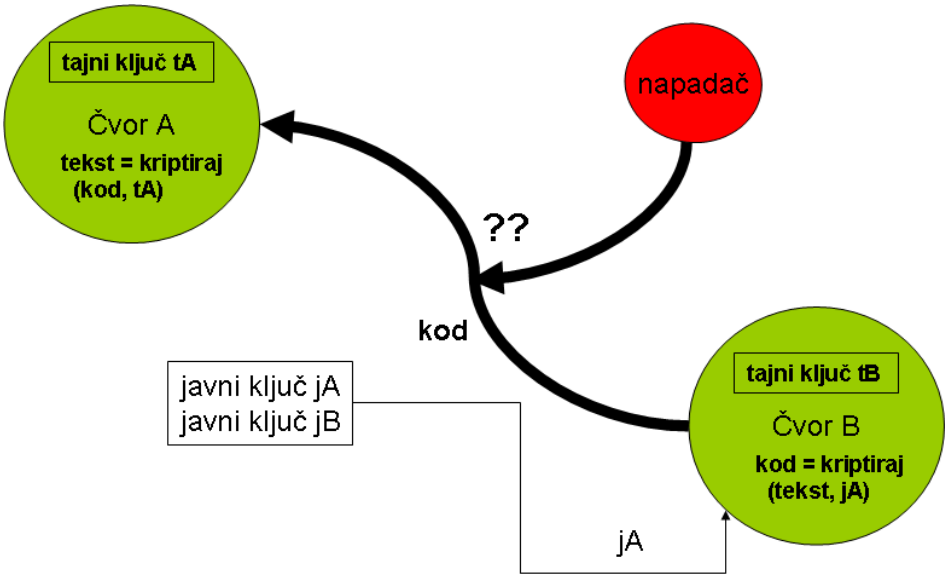
2.2.2. Asimetrični kriptografski algoritmi

Asimetrični kriptografski algoritmi koriste dva ključa – jedan za kriptiranje i jedan za dekriptiranje. Redoslijed operacija kriptiranja pritom nije bitan, ali je bitno da je tekst kriptiran jednim ključem moguće dekriptirati jedino drugim pripadnim ključem. U takvom paru ključeva jedan se odabire kao javni ključ, dok drugi ključ ostaje tajan.

Ovakvi algoritmi zasnivaju se na matematičkim funkcijama kod kojih za neki par ključeva(brojeva) $ključevi = (e, d)$ vrijedi da se tekst može kodirati ključem e na slijedeći način: $f(tekst, e) = kod$. Iz koda je potom izvorni tekst moguće je dobiti jedino pomoću ključa *d*: $f(kod, d) = tekst$. Kod kriptiranja se također mogao koristiti ključ *d*, a kod dekriptiranja ključ *e*.

Najpoznatiji asimetrični algoritam je RSA, a zasniva se na složenosti faktorizacije prostih brojeva. Za otkrivanje tajnog ključa potrebno je faktorizirati veliki broj koji je umnožak dva prosta broja što je izuzetno složen zadatak. Niti RSA kriptiranje nije najjednostavniji problem jer zahtijeva pronalaženje izuzetno velikih prostih brojeva (preko 100 znamenki), ali je izvedivo. Ipak, budući da je postupak dugotrajan, ne koristi se za prenošenje velikih količina podataka. Asimetrični algoritmi koriste se u pravilu za razmjenu tajnih simetričnih ključeva pomoću kojih se onda većom brzinom sigurno razmjenjuju podaci.

Kao što je već navedeno, kod asimetričnih algoritama jedan ključ se objavi i postaje javni ključ (eng. public key), a drugi se zadrži tajnim. Na taj način bilo koji korisnik može javnim ključem primatelja kriptirati podatke i odaslati ih u nesigurnu mrežu. Budući da je jedina osoba koja ima mogućnost dekriptiranja podataka (tajnim ključem) upravo primatelj, osigurana je tajnost podataka u komunikacijskom kanalu.



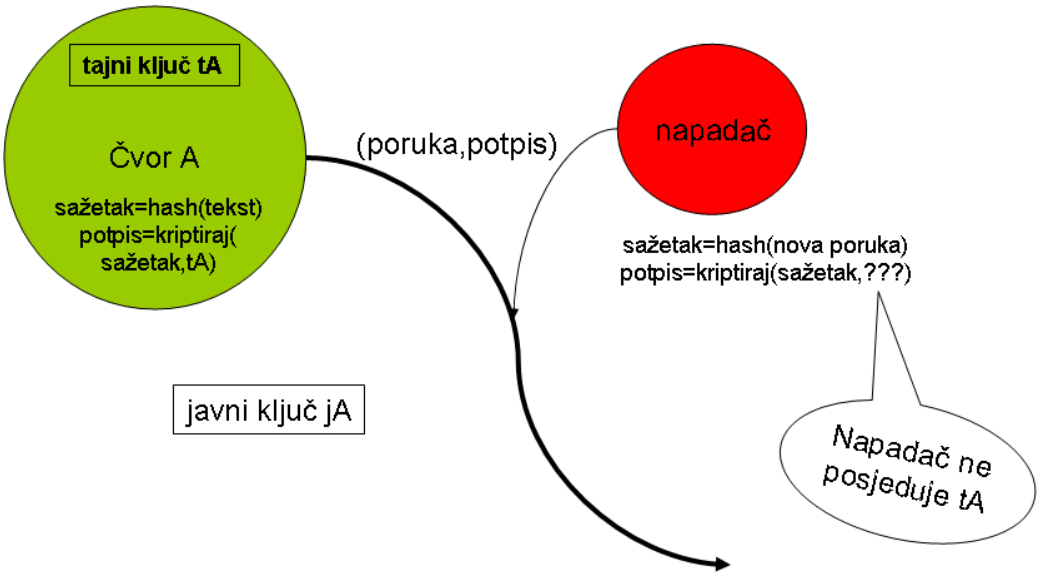
Slika 3. Shema komunikacije zaštićene asimetričnim kriptiranjem

2.2.3. Izračunavanje sažetka

Opisanim algoritmima kriptiranja rješava se problem tajnosti podataka u komunikacijskom kanalu. No ostaju neriješena pitanja besprijekornosti poruka (jer nije moguće utvrditi jesu li mijenjane putem). U najvećem broju slučajeva, ukoliko su poruke mijenjane, dekodirat će se u besmislen tekst. No to ne mora uvijek biti tako i nema nikakvog jamstva da je tekst koji smo primili tekst koji je pošiljatelj poslao. Problem nije samo u mijenjanju poruka, već i u mogućnosti lažnog predstavljanja i slanja poruka u tuđe ime. Primatelj ne može biti siguran je li pošiljatelj doista onaj kojim se predstavlja, što znači da netko drugi može poslati poruku u njegovo ime ili da on sam može poslati poruku i kasnije poreći da ju je poslao.

Ovi problemi u komunikaciji ne mogu se riješiti kriptiranjem podataka, ali mogu se riješiti pomoću tzv. „hash" funkcija, odnosno funkcija za izračunavanje sažetaka poruke. Osobitost idealne funkcije za izračunavanje sažetka jest to da je iz sažetka nemoguće izračunati originalnu poruku, a svi sažeci su iste duljine. Sažetak je kraći od izvorne poruke, a može se koristiti za provjeru besprijekornosti poruke. Primjerice, ako je poznata funkcija sažimanja, pošiljatelj uz poruku šalje i njezin sažetak. Primatelj poruke tada može na temelju dobivene poruke izračunati sažetak. Ako izračunati sažetak odgovara onom poslanom uz poruku, primatelj može biti siguran da je poruka primljena u istom obliku u kojem ju je pošiljatelj poslao. Ukoliko se sažetak šalje u otvorenom obliku, bilo tko ga može presresti skupa s porukom te promijeniti poruku i poslati novi odgovarajući sažetak. Ovaj se problem rješava asimetrično kriptiranje sažetka i to privatnim ključem pošiljatelja. Što se ovim putem postiže? Budući da tajni ključ zna jedino njegov vlasnik, onemogućuje se presretanje sažetka i njegova izmjena (jer bi ponovno kriptiranje zahtijevalo poznavanje tajnog ključa izvornog pošiljatelja). Bilo tko pritom može dekriptirati sažetak javnim ključem pošiljatelja i provjeriti odgovara li taj sažetak onom koji se dobije sažimanjem dobivene poruke. To znači da bilo tko može provjeriti je li izvorna poruka od navedenog pošiljatelja, ali izmjena sažetka i poruke nije izvediva jer:

- izmjena poruke dovesti će do neslaganja sa sažetkom,
- ne postoji način da se nakon dekriptiranja sažetka on ponovno kriptira tajnim ključem pravog pošiljatelja.



Slika 4. Shema uporabe digitalnog potpisa

Time kriptiranje sažetka istovremeno osigurava autentičnost pošiljatelja i besprijekornost sadržaja. Zbog toga se ovakve metode nazivaju i digitalni potpisi. Korištenje kriptiranja sadržaja i funkcija za izračunavanje sažetaka osigurava tajnost, autentičnost, neporecivost i besprijekornost komunikacije u računalnoj mreži.

2.3. Infrastruktura javnih ključeva

Infrastruktura javnih ključeva definira način na koji se javni ključevi dodjeljuju korisnicima i način na koji se oni objavljuju drugim korisnicima. Iako su to javni ključevi, važno je biti siguran da je objavljeni javni ključ doista javni ključ onog entiteta čijim se predstavlja. Ukoliko ne postoji nikakva kontrola, bilo tko može objaviti javni ključ u ime nekog drugog korisnika. Za to je potrebna posebna infrastruktura koja se naziva infrastruktura javnih ključeva (eng. PKI Public Key Infrastrucutre). Općenito, takva struktura obuhvaća korisnike koji komuniciraju i jednu pouzdanu upraviteljsku jedinicu koja čuva sve javne ključeve i preko koje se uspostavlja sigurna komunikacija bilo koja dva korisnika u mreži. Takva se jedinica nazva PKM (eng. Public Key Manager) upravitelj. Sustav s jednim PKM centrom pogodan je za manje mreže, no u slučaju većih otvorenih sustava pogodnije je rješenje uvođenje digitalnih certifikata.

2.3.1. Digitalni certifikati

Digitalni certifikat je skup podataka koji uključuje identifikacijsku oznaku korisnika i njegov javni ključ. Osim toga sadrži i potpis, odnosno sažetak poruke (javnog ključa i identifikacijske oznake korisnika) kriptiran javnim ključem certifikacijskog centra. Na taj način jamči se povezanost javnog ključa i korisnika navedenog u certifikatu, a jamstvo je pouzdanost certifikacijskog centra koji je izdao certifikat. To znači da se provjera certifikata mora uvijek obaviti u centru u kojem je sudionik prijavljen. Osim toga, javlja se pitanje opozivanja certifikata koji se nalaze na različitim dijelovima mreže. Taj se problem u različitim sustavima rješava na različite načine.

Certifikacijski centri (eng. Certificate Authorities) su pouzdana javna tijela koja izdaju digitalne certifikate. Postoji više takvih centara, a među najprisutnijima su VeriSign, GeoTrust, Thawte i Comodo.

Slika 5. Primjer digitalnog certifikata

3. S/MIME standard

S/MIME (eng. Secure / Multipurpose Internet Mail Extensions) je standard za zaštitu komunikacije elektroničkim porukama, a uključuje enkripciju javnog ključa i digitalno potpisivanje poruka elektroničke pošte. Na taj način osigurava se autentičnost, neporecivost, besprijekornost i naravno tajnost komunikacije. S/MIME sigurnosne usluge ostvaruju se u okviru MIME formata elektroničkih poruka koji će biti objašnjen u nastavku poglavlja. Kriptirane i potpisane digitalne poruke omataju se posebnim MIME digitalnim tipom formata i kao takve se mogu umetnuti u novu MIME poruku i sigurno slati kroz mrežu. U ovom poglavlju daje se uvod u povijest razvoja S/MIME standarda i njegove glavne odrednice.

3.1. Povijest razvoja standarda

Prvu inačicu S/MIME standarda razvila je korporacija RSA Data Security 1995. godine. U to vrijeme nije postojao jedinstveni standard za sigurnu komunikaciju elektroničkim porukama, već je postojalo nekoliko različitih prijedloga. PGP (eng. Pretty Good Privacy) i S/MIME su primjeri predloženih specifikacija. Druga inačica S/MIME standarda objavljena je 1998 godine i IETF (eng. Internet Engineering Task Force) ju je uveo u listu RFC (eng. Request for Comments) standarda i to dokumentima RFC 2311 (standard za rukovanje porukama) i RFC 2312 (standard za rukovanje certifikatima). Na ovaj način je stvorena službena specifikacija S/MIME standarda prema kojoj su različiti proizvođači mogli oblikovati sigurnosne usluge svojih proizvoda za razmjenu elektroničke pošte. Zahvaljujući jedinstvenom standardu te su usluge između različitih klijenata postale programski prepoznatljive.

1999. godine izlazi S/MIME v3, treća inačica S/MIME standarda koja je opisana u IETF dokumentima RFC 2632, 2311, 2633, 2312 i 2634. Njome su povećane mogućnosti i učinkovitost S/MIME sigurnosnih usluga, Uvedena je mogućnost RSA enkripcije kod slanja poruke, ne samo kod provjere potpisa, a dodane su i nove usluge poput zaštićene potvrde primitka, sigurnosnih oznaka poruka i trostrukog omatanja (višestruka zaštita iste poruke). S/MIME v3 je do danas ostao široko prihvaćen i primjenjivan standard, a trenutno je u uporabi njegova inačica 3.1.

3.2. Formati i algoritmi

U ovom poglavlju opisuju se formati poruka i dijelova poruka te algoritmi korišteni u ostvarenju S/MIME sigurnosnih usluga.

3.2.1. MIME

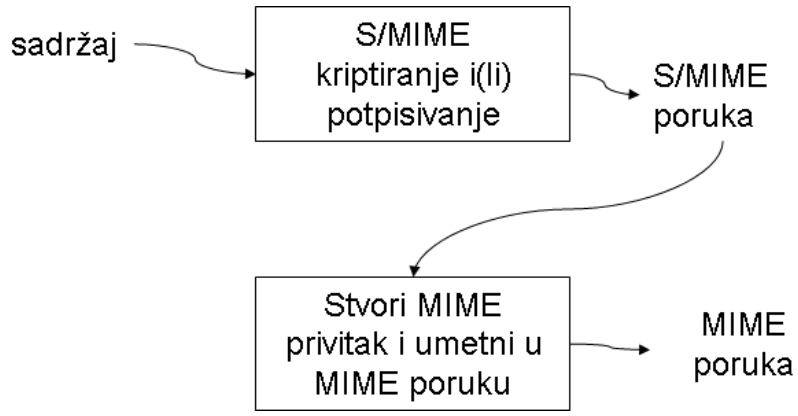
MIME je standardni format za strukturirano oblikovanje tijela elektroničke poruke. Osim tijela poruke definira i neke mogućnosti oblikovanja zaglavlja poruke, ali one u okviru ove teme nisu bitne. Općenit oblik MIME poruke sastoji se od dva dijela:

- **zaglavlje** – sadrži informacije bitne za programsku obradu poruke, tj. njezino slanje kroz mrežu. Sastoji se od polja i vrijednosti pridruženih tim poljima. Ona uključuju pošiljatelja, primatelja, datum, ID poruke, tip sadržaja u poruci, uključujući i postojanje privitaka i sl.
- **tijelo** – sadrži podatke koje je pošiljatelj namijenio primatelju.

Tijelo poruke je samo po sebi nestrukturirano, zbog čega je nemoguće umetati dodatne sadržaje (osim običnog teksta) u poruku ako nije određen način na koji će se ti sadržaji rastumačiti na odredištu. MIME standard upravo definira način na koji se tijelo poruke oblikuje, što omogućuje umetanje dodatno oblikovanog teksta, grafičkih i audio datoteka te drugih sadržaja. MIME ne uključuje sigurnosne usluge, samo jedinstven način oblikovanja tijela elektroničkih poruka. Početno polje zaglavlja svake MIME poruke određuje inačicu MIME standarda. Primjer MIME dijelova poruke:

```
MIME-Version: 1.0
…
Content-Type: multipart/mixed; boundary=001636c5b2c45ca8620468c66a87

--001636c5b2c45ca8620468c66a87
Content-Type: multipart/alternative; boundary=001636c5b2c45ca85b0468c66a85

--001636c5b2c45ca85b0468c66a85
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit

Ovo je sadrzaj koji je upisao korisnik.

--001636c5b2c45ca85b0468c66a85
Content-Type: text/plain; charset=US-ASCII; name="dodana_datoteka.txt"
Content-Disposition: attachment; filename="dodana_datoteka.txt"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_fu5jnml81

aHR0cDovL2ltYWdlcy5nb29nbGUuaHIvaW1ncmVzP2ltZ3VybD1odHRwOi8vd3d3Lm15c2VjdXJl
Y3liZXJzcGFjZS5jb20vZW5jeWNsb3BlZGlhL2luZGV4L2RpZ2l0YWxjZXJ0aWZpY2F0ZS5waWMx
LmpwZWcmaW1ncmVmdXJsPWh0dHA6Ly93d3cubXlzZWN1cmVjeWJlcnNwYWNlLmNvbS9lbmN5Y2xv
cGVkaWEvaW5kZXgvZGlnaXRhbC1jZXJ0aWZpY2F0ZXMuaHRtbCZ1c2c9X191OVRBeVBraUVza24w
eVBTZy0yRWtOQmpjeDA9Jmg9NDc1Jnc9NDA4JnN6PTMwJmhsPWVuJnN0YXJ0PTEmc2lnMj1hNC1V
MVBxWXJtWUkwX3c0Y3FKSk13JnVtPTEmdGJuaWQ9NWNHYlFCOFVSZ0ltbE06JnRibmg9MTI5JnRi
bnc9MTExJnByZXY9L2ltYWdlcyUzRnElM0RkaWdpdGFsJTJCY2VydGlmaWNhdGUlMjZobCUzRGVu
JTI2cmx6JTNEMUIzR0dHTF9lbkhSMjc2SFIyNzYlMjZzYSUzRE4lMjZ1bSUzRDEmZWk9R3JMNVNl
cXVENDZIc0FiczNkVERCQQ==
--001636c5b2c45ca8620468c66a87
```

U ovom primjeru osim teksta koji je upisan u tijelo poruke (svaki znak kodiran u 7 bita), dodana je i datoteka „dodana_datoteka.txt“. Ona je zapisana u base64 formatu koji je posebno pogodan jer omogućuje prikaz bilo kakvih binarnih datoteka (grafički, video, audio i drugi sadržaji) u tekstualnom obliku. U ovom formatu se prenose svi dodatni sadržaji u MIME poruci, uključujući i S/MIME sadržaj.



Slika 6. Shema omatanja S/MIME poruke MIME formatom

3.2.2. CMS format poruke

Format S/MIME poruka temelji se na binarnom CMS formatu. CMS (eng. Cryptographic Message Syntax) je standard za kriptiranje, autentifikaciju, sažimanje i potpisivanje bilo kojeg dijela poruke. CMS zapravo opisuje sintaksu za zaštitu sadržaja elektroničkih poruka, a omogućuje ugnježđivanje takvih sadržaja (primjerice višestruko potpisivanje istog sadržaja). Format je razvijen na temelju PKCS7# formata koji je nastao unutar iste korporacije koja je razvila prvobitnu inačicu S/MIME standarda. CMS prepoznaje šest osnovnih tipova podataka:

1. data,
2. signed-data,
3. enveloped-data,
4. digested-data,
5. encrypted-data i
6. authenticated-data.

Sintaksa definira način na koji se u poruci zapisuje sadržaj te ostale bitne informacije za njegovo razumijevanje i njegovu obradu – primjerice tip sadržaja, korištene kriptografske algoritme, parametre tih algoritama, podatke o certifikatu pošiljatelju i sl. Zapis u poruci ostvaruje se pomoću tipova podataka i različitih pripadnih atributa. Detaljan opis CMS sintakse moguće je pronaći u dokumentu RFC 3852.

3.2.3. S/MIME certifikati

S/MIME standard zahtijeva X.509v3 format digitalnih certifikata. X.509 je model PKI infrastrukture uspostavljen u okviru Međunarodne telekomunikacijske unije (eng. ITU International Telecommunication Union), a čini osnovu za ostvarenje većine današnjih PKI sustava. Digitalni certifikati definirani unutar ovog modela sadrže:

1. javni ključ,
2. ime i identifikacijsku oznaku korisnika,
3. verziju X.509 preporuke,
4. serijski broj certifikata,
5. naziv certifikacijskog centra koji izdaje certifikat,
6. primijenjeni algoritam sažimanja i potpisivanja,
7. primijenjeni kriptografski algoritam i parametre,
8. razdoblje valjanosti certifikata (početni i završni dan) i
9. digitalni potpis certifikacijskog centra.

Primjer X.509v3 certfikata:

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                   68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                   85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                   6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                   6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                   29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                   6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                   5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
       4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
       8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
        70:47
```

3.2.4. Simetrična enkripcija

Rečeno je već na početku ovog dokumenta da se kod prenošenja velikih količina kriptiranih podataka preporuča primjena simetričnih kriptografskih algoritama jer su oni bitno brži od asimetričnih. Pritom se jedino simetrični tajni ključ koristen u komunikaciji razmijeni korištenjem asimetričnog kriptografskog algoritma.

S/MIME standard zahtijeva primjenu 3DES algoritma za simetričnu enkripciju. Radi se o metodi koja se temelji na DES kriptografskom algoritmu. Budući da je izvorni DES moguće razbiti zbog relativno male duljine ključa koja iznosi 56 bitova, uvedena je nova inačica DES-a koja se ostvaruje uzastopnim izvođenjem DES algoritma tri puta, svaki put s drukčijim tajnim ključem. Ukupna duljina ključa koji se treba otkriti tada iznosi 168 bitova što je nemoguće otkriti u razumnom vremenu. To se lako objašnjava time što broj mogućih 168-bitnih ključeva iznosi 2^{168} ($\sim 10^{50}$). Ukoliko bi računalo u sekundi moglo provjeriti milijardu mogućih ključeva ($\sim 10^{9}$) trebalo bi mu 10^{41} sekundi da provjeri sve ključeve, odnosno otprilike 10^{33} godina što je daleko više i od starosti Svemira.

3DES kriptiranje može se opisati u slijedećim koracima:

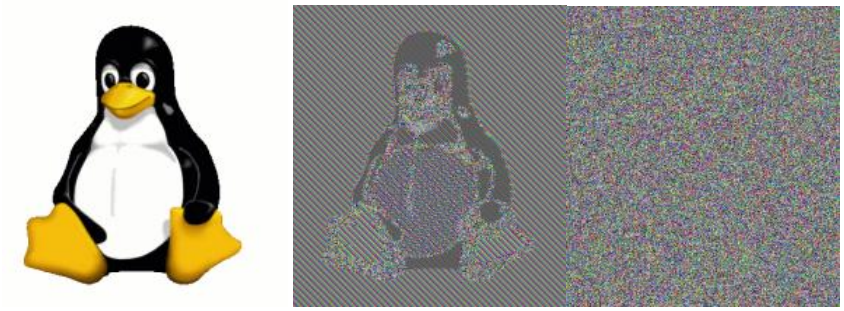
1. kriptiraj tekst prvim tajnim ključem,
2. dekriptiraj rezultat iz koraka 1 drugim tajnim ključem,
3. kriptiraj rezultat koraka iz 2 trećim tajnim ključem.

3DES dekriptiranje izmjenjuje redoslijed DES kriptiranja i dekriptiranja te izgleda ovako:

1. dekriptiraj tekst prvim tajnim ključem,
2. kriptiraj rezultat iz koraka 1 drugim tajnim ključem,
3. dekriptiraj rezultat koraka iz 2 trećim tajnim ključem.

Možda je na prvi pogled zbunjujuće istovremeno korištenje kriptiranja i dekriptiranja u oba procesa, no kriptiranje i dekriptiranje u DES algoritmu su praktički identični postupci, a jedina je razlika u redoslijedu korištenja pomoćnih ključeva koji se stvaraju prilikom izvođenja algoritma. Jednostavno se ta razlika može objasniti i tako da se prvi i treći ključ gledaju od prve pozicije prema zadnjoj, a drugi od zadnje prema prvoj. Npr. ako cijeli 3DES ključ je izgleda ovako: 123 456 789, prvi ključ kod kriptiranja biti će 123, drugi 654, a treći 789. Kako bi dekriptiranje bilo uspješno potrebno je taj redoslijed zamijeniti u 321 456 987.

Također, zahtijeva se tzv. CBC (eng. Cipher Block Chaining) način izvođenja koji ulančava kriptiranje. Radi se o tome da kriptiranje malih blokova kod nekih vrsta sadržaja, primjerice slikovnih, može ostaviti globalnu strukturu prepoznatljivom. Zato se uvodi ulančano kriptiranje u kojem se u rezultat kriptiranja svakog idućeg bloka uzima u obzir rezultat kriptiranja prošlog bloka. Takvo kriptiranje onemogućuje pojavu istih globalnih pravilnosti u izvornom i kriptiranom sadržaju. Primjer razlike u rezultatu CBC kriptiranja i običnog kriptiranja po blokovima (eng. ECB Electronic CodeBook) dan je na slijedećim slikama:



Originalna slika ECB kriptirani sadržaj CBC kriptirani sadržaj

Slika 7. Primjer rezultata ECB i CBC kriptiranja slike

Izvor: Wikipedia

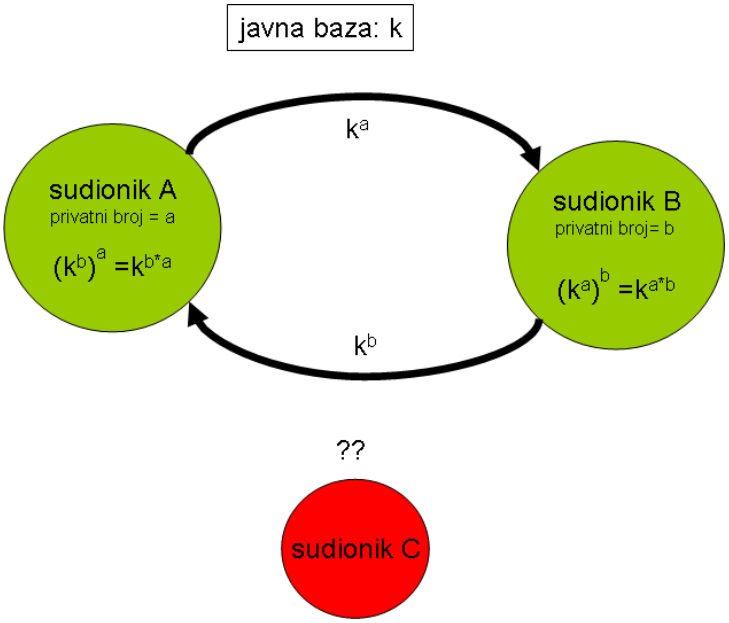
3.2.5. Digitalno potpisivanje

Digitalno potpisivanje unutar S/MIME standarda ostvaruje se Diffie-Hellman postupkom uz DSS ili RSA enkripciju. Diffie-Hellman procedura koristi se za razmjenu tajnog ključa, a temelji se na teškoći izračunavanja diskretnog logaritma u odnosu na diskretno potenciranje. Princip rada ovog algoritma jednostavan je za objasniti:

Cilj Diffie-Hellman algoritma je razmijeniti neku tajnu vrijednost između sudionika komunikacije tako da drugi sudionici ne znaju o kojoj se vrijednosti radi (tajni ključ). To se može učiniti na slijedeći način:

1. objavi se pred svim sudionicima jedan broj (baza računanja),
2. korisnici koji žele razmijeniti tajni ključ tu bazu potenciraju na neki svoj tajni broj koji jedino oni znaju i objave rezultat javno,
3. nakon što korisnik primi rezultat od sudionika s kojim želi komunicirati, taj rezultat potencira na svoj tajni broj i dobiveni rezultat je tajni ključ.

Ista stvar opisana je na idućoj slici:



Slika 8. Shema Diffie-Hellman protokola

Sigurnost i učinkovitost ove metode temelji se na dvije činjenice:

- komutativnost množenja – nije bitno kojim će se redoslijedom broj potencirati, rezultat je isti u oba slučaja
- teškoća otkrivanja eksponenta iz rezultata (logaritmiranje) –primijetimo da je treći sudionik dobio samo gotove rezultate potenciranja brojeva, a da bi saznao na koji je broj baza potencirana morao bi znati izračunati logaritam. Za vrlo velike brojeve kakvi se koriste u kriptografiji, takvo izračunavanje je izuzetno teško zbog čega napadač nikako neće moći otkriti tajni ključ.

Ipak ova procedura ne štiti od lažnog predstavljanja. Napadač se uvijek može ubaciti u komunikaciju i lažno predstaviti te razmijeniti svoj tajni broj sa oba sudionika i na taj način saznati sve podatke koje oni razmjenjuju misleći da komuniciraju sigurnim kanalom. Ta se vrsta napada naziva „man in the middle" napad, a može se izbjeći uvođenjem provjere autentičnosti u komunikaciju, odnosno provjerom identiteta krajnjeg korisnika. Zato se uz Diffie-Hellman proceduru ovdje rabe i digitalni potpisi koji se temelje na DSA ili RSA metodama. Radi s o različitim asimetričnim kriptografskim metodama pomoću kojih se autentičnost provjerava na temelju poznavanja privatnog ključa. Opisano je već u poglavlju o digitalnim potpisima da pošiljatelj kriptira podatak svojim privatnim ključem što znači da će informacija biti ispravno dekriptirana njegovim javnim ključem jedino ukoliko je netaknuta prošla kroz komunikacijski kanal (time je onemogućen „man in the middle" napad).

Osim toga digitalni potpisi uključuju izračunavanje sažetaka čime se osigurava besprijekornost poruke. S/MIME zahtijeva korištenje SHA-1 algoritma sažimanja u tu svrhu.

3.2.6. S/MIME omotavanje podataka

S/MIME razlikuje digitalno omotavanje potpisanih podataka (osiguranje autentičnosti pošiljatelja i besprijekornosti poruke) i kriptiranih podataka (osiguranje tajnosti podataka). Omotavanje potpisanih podataka obavlja se u CMS formatu ili u MIME *multipart/signed* formatu. MIME *multipart* definira odvajanje različitih dijelova u MIME poruci, primjerice ukoliko dodajemo više slikovnih datoteka u elektronički poruku svaka će biti predstavljena kao jedan „*multipart*" element. *Signed* je poseban podtip *multipart* strukture koji omogućuje umetanje digitalnih potpisa u MIME poruku. Ovaj format opisan je u dokumentu RFC 1847, a primjer *multipart/signed* elementa u MIME poruci izgleda ovako:

```
Content-Type: multipart/signed; protocol="tip_protkola/podtip";
            micalg="algoritam_sazimanja"; boundary="Signed Boundary"

    --Signed Boundary
    Content-Type: text/plain; charset="us-ascii"

    Primjer potpisanog teksta, iako može biti bilo kakav tip podataka.

    --Signed Boundary
    Content-Type: tip_protokola/podtip

    Kontrolne informacije za protokol

    --Signed Boundary--
```

Omatanje kriptiranih podataka obavlja se u application/pkcs7-mime formatu, opisanom u RFC 2311 dokumentu. Podaci koji se prenose ovim formatom prikazuju se najčešće u base64 kodiranju, a datoteke koje ih sadrže trebaju imati „.p7m“ nastavak. Primjer omotanih kriptiranih podataka u MIME poruci izgleda ovako:

```
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
            name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
0GhIGfHfQbnj756YT64V
```

3.2.7. Primjer S/MIME sigurne komunikacije

Uloga svih S/MIME sastavnica u sigurnoj komunikaciji pokazuje se kroz sljedeće korake:

- Prvi korak u ostvarenju sigurne komunikacije je certifikacija vlastite adrese kod nekog od provjerenih CA tijela (Thawte, Comodo i dr.). Pritom se odabire X.509v3 format certifikata.
- Zatim je potrebno instalirati klijent elektroničke pošte koji sadrži S/MIME podršku i uvesti (instalirati) svoj certifikat u klijentu kako bi se mogao koristiti za sigurnu komunikaciju.
- Potom korisnik S/MIME komunikaciju ostvaruje jednostavno odabirom na dostupne mogućnosti kriptiranja i potpisivanja poruka u klijentu elektroničke pošte, a sve druge sigurnosne radnje preuzima S/MIME podrška u klijentu.
- Certifikati se razmjenjuju s korisnikom s kojim se želi komunicirati i provjeravaju se kod CA tijela koja su ih izdala.
- Ukoliko je korisnik odabrao zaštitu poruke kriptiranjem i digitalnim potpisom obavljaju se slijedeći koraci:
    1. generira se nasumični simetrični ključ kojim se kriptira sadržaj kojeg je korisnik unio i odabrao za zaštitu kriptiranjem,
    2. simetrični ključ kriptira se javnim ključem primatelja (koji se saznaje iz certifikata korisnika) – na ovaj način simetrični ključ može saznati jedino korisnik koji posjeduje svoj tajni ključ potreban za dekripciju simetričnog ključa,
    3. podaci se zapisuju u CMS formatu i umeću u MIME poruku kao S/MIME „enveloped-data“ tip u application/pkcs7-mime privitku,
    4. izračunava se sažetak poruke propisanim algoritmom (SHA-1) i kriptira vlastitim tajnim ključem – digitalni potpis,
    5. potpis se oblikuje prema CMS formatu i zapisuje u application/x-pkcs7-signature MIME privitak, a potpisani podaci umeću se u MIME poruku kao multipart/signed tip,
    6. MIME poruka šalje se putem elektroničke pošte odabranom korisniku.

Po primitku poruke klijent elektroničke pošte obraditi će podatke i prikazati sadržaj korisniku skupa s eventualnim upozorenjima, npr. o neispravnosti ili nemogućnosti provjere potpisa. Obrada podataka uključuje:

1. analizu sadržaja prema MIME i CMS formatima,
2. dekripciju simetričnog ključa vlastitim tajnim ključem,
3. dekripciju kriptiranog teksta simetričnim ključem i
4. provjeru digitalnog potpisa što uključuje: dekripciju sažetka javnim ključem pošiljatelja, izračun sažetka potpisanog teksta i usporedbu dobivenih sažetaka – ako su isti zaključuje se da je potpis valjan.

4. Primjene S/MIME standarda

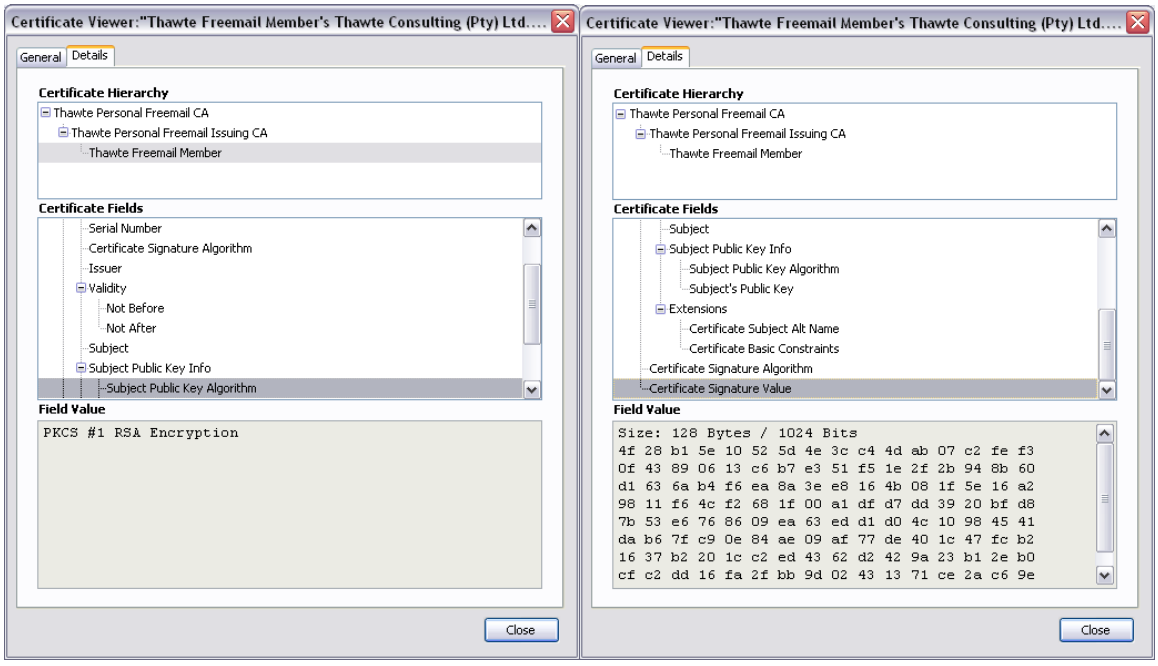
S/MIME je široko prihvaćen standard za ostvarenje sigurnog prijenosa elektroničke pošte putem Interneta. Podržavaju ga brojni klijenti elektroničke pošte za različite operacijske sustave: od Windowsa preko Unix/Linux sustava do Mac OS-a. Ipak postoje određeni problemi u primjeni standarda. Oni su uglavnom praktične prirode, a njihov kratak pregled nalazi se u trećem dijelu ovog poglavlja.

4.1. Klijenti E-pošte sa S/MIME podrškom

Klijenti elektroničke pošte koji podržavaju S/MIME su:

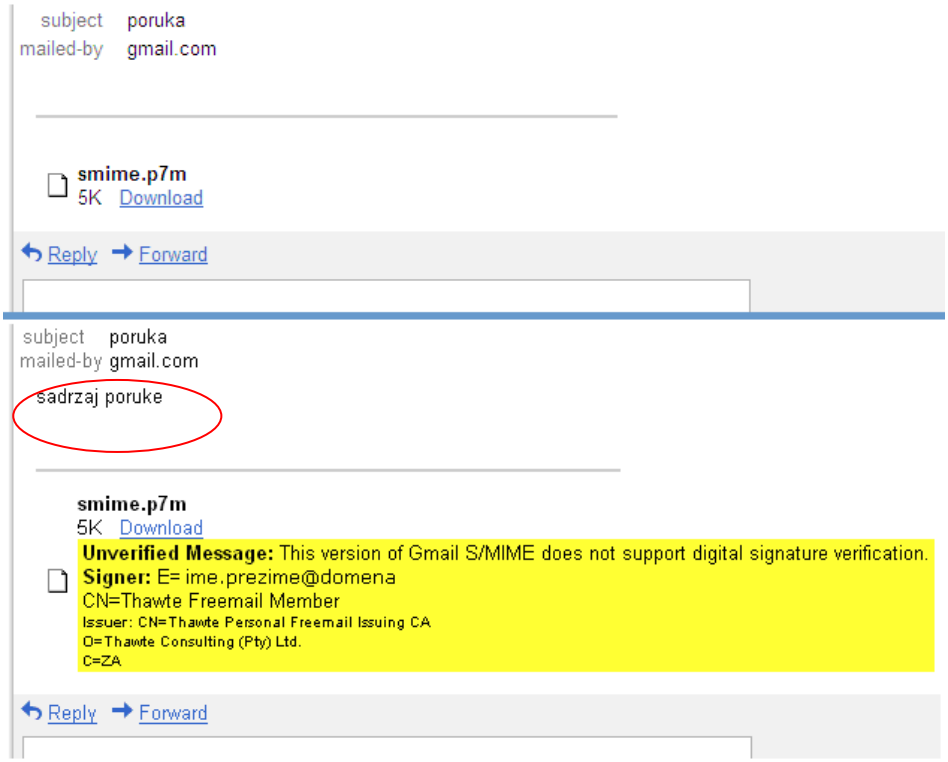
- OpenSSL (Linux)
- Mozilla Thunderbird (Linux, Windows)
- Mulberry (Linux, Windows, Mac OS)
- Outlook (Windows),
- Outlook Express (Windows),
- Netscape Communicator (Windows, Linux)
- Mail (Mac OS)
- Lotus Notes (Windows, Mac OS, Linux) i
- Evolution 2 (Linux).

Korištenje S/MIME digitalnih potpisa ili enkripcije poruka zahtijeva posjedovanje digitalnog certifikata. Njega je moguće nabaviti besplatno za osobne adrese elektroničke pošte (Thawte CA, Comodo CA). CA poslužitelj vodi korisnika kroz proces izdavanja digitalnog certifikata. Pritom se mora odabrati odgovarajući oblik certifikata za S/MIME standard (X.509v3) koji se na kraju sprema na korisnikom računalu. Primjer izdanog Thawte certifikata za klijent elektroničke pošte Mozilla Thunderbird dan je na sljedećoj slici:



Slika 9. Digitalni cerifikat i informacije dostupne u njemu

Nakon što je digitalni certifikat instaliran u postavkama klijenta elektroničke pošte moguće je odabrati uvoz digitalnog certifikata, enkripciju poruke i/ili digitalno potpisivanje poruke. Ove mogućnosti se u programu Mozilla Thunderbird nalaze u *Tools -> Account Setting -> Security* izborniku. Na različitim klijentima odabir sigurnosnih usluga obavlja se na različite načine, no uglavnom je vezan uz *Tools*, *Account Settings* i *Security* mogućnosti. Ukoliko se S/MIME poruka primi u klijentu elektroničke pošte koji ne podržava S/MIME standard ona će ostati u „.p7s“ formatu i time nerazumljiva korisniku.



Slika 10. Primjer S/MIME poruke na gmail sučelju bez S/MIME podrške i s ograničenom S/MIME podrškom

Primjerice, popularni poslužitelj elektroničke pošte GMail u osnovom obliku ne podržava S/MIME, no može se besplatno nadograditi. Pritom još uvijek nije omogućena verifikacija potpisa, no poruka će biti prikazana dekriptirana, jasnog sadržaja. S/MIME privitci u MIME formatu izgledaju ovako:

```
Content-Type: application/x-pkcs7-mime; name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: S/MIME Encrypted Message

MIAGCSqGSIb3DQEHA6CAMIACAQAxggERMIIBDQIBADB2MGIxCzAJBgNVBAYTAlpBMSUwIwYD
VQQKExxUaGF3dGUgQ29uc3VsdGluZyAoUHR5KSBMdGQuMSwwKgYDVQQDEyNUaGF3dGUgUGVy
c29uYWwgRnJlZW1haWwgSXNzdWluZyBDQQIQVLl3gIyRoet/8/m8rKh/3zANBgkqhkiG9w0B
AQEFAASBgCxfN1UjsUNe8hwfeYxlc6C0QXdp8tZSS5b5JU3Pr2sbaPqFpAV6JrvtkRPdvMqF
H77VACHMOShKncrBnZACCBAiAr7yW/MZZCerGXYDCuSGcv5Tf+sWTolOmBo5IZooGywin1QA
```

Neki od klijenata elektroničke pošte koji ne podržavaju S/MIME su:

- QuickMail Pro (Windows, Mac OS),
- Sylpheed (Linux, Mac OS, Windows) i
- Eudora (Windows, Mac OS) - postoji programski dodatak koji omogućuje korištenje S/MIME usluga.

4.2. Programske biblioteke

Za različite programske jezike dostupne su biblioteke za primjenu S/MIME sigurnosnih standarda pri razvoju usluga koje uključuju razmjenu elektroničkih poruka. Chilkat MIME biblioteke koje omogućuju rad s MIME i S/MIME porukama dostupne su za sljedeće programske jezike:

- Java,
- Python,
- Perl,

- Ruby i
- .NET okruženje.

Riječ je o *„shareware“* izdanjima za koja se plaća licenca (100 - 150 USD).

Tvrtka IP*Works! nudi komercijalne S/MIME biblioteke za programske jezike:

- C++,
- .NET okruženje i
- Java.

Njihove cijene iznose oko 1.000 USD.

Osim komercijalnih izdanja, dostupne su i različite besplatne programske biblioteke koje omogućuju rad sa S/MIME porukama. Neke od poznatijih su:

- BouncyCastle S/MIME (Java),
- Me2Crypto (Python),
- NetToolWorks.NET S/MIME (.NET) i dr.

4.3. Problemi u primjeni standarda

Problemi u primjeni S/MIME standarda vezani su uz to što je S/MIME oblikovan kao tzv. *„end to end“* standard, odnosno što se (de)kriptiranje i potpisivanje obavlja na razini aplikacije. To znači da će zlonamjerni sadržaj u kriptiranoj poruci izbjeći sigurnosne provjere na ulazu u mrežu. Problem se može riješiti tako da se poruka dekriptira i provjeri prije ulaska u mrežu. Ipak, to narušava razinu sigurnosti jer znači da tajni ključevi moraju biti dostupni na poslužitelju koji kontrolira promet prema sigurnoj mreži i od nje. Idealno rješenje što se tiče pohranjivanja ključeva bilo bi pohraniti ih tako da budu dostupni jedino korisniku, no to nije moguće u ovom tipu tehnologije jer pregledniku mora biti dostupan tajni ključ kako bi proizveo digitalni potpis.

Drugi način bio bi provjera sadržaja nakon dekripcije, što je u većim lokalnim mrežama nepraktično za izvedbu jer se opterećuju pojedinačna korisnička računala.

Osim toga, S/MIME ne podržavaju svi klijenti elektroničke pošte što znači da se zaštićena komunikacija može izvoditi samo unutar skupa korisnika koji su sinkronizirani po pitanju sigurnosne politike (koriste iste sigurnosne standarde i protokole).

5. Usporedba s OpenPGP-om i budućnost standarda

OpenPGP je alternativna mogućnost zaštite elektroničkih poruka. Riječ je standardu koji se zasniva na potpuno različitom modelu razmjene javnih ključeva od S/MIME modela te su zbog toga potpuno nekompatibilni. Što se sigurnosti i kriptografskih algoritama tiče, oba su standarda vrlo sigurna. U ovom poglavlju razmotrit će se OpenPGP kao alternativa S/MIME standardu te njihove sličnosti i razlike.

5.1. OpenPGP

OpenPGP standard zasniva se na PGP (eng. *Pretty Good Privacy*) sustavu za enkripciju i digitalno potpisivanje poruka osmišljenom 1991. godine. OpenPGP ponuđen je kao IETF standard 1997. godine, a njegova se specifikacija nalazi u dokumentu RFC 4880.

PGP sustav zasniva se na modelu mreže povjerenja (eng. *web of trust*). Smisao ove mreže je decentralizirana razmjena javnih ključeva. S/MIME PKI sustav zasniva se na centraliziranom hijerarhijskom modelu CA tijela u koja svi sudionici komunikacije imaju povjerenje i koja potvrđuju vezu između javnog ključa i identifikacijske oznake korisnika. S druge strane, u PGP sustavu ne postoje CA tijela, a vezu između javnog ključa i korisnika potvrđuje neki korisnik u mreži. Budući da korisnici međusobno uvode nove članove u mreži i potvrđuju njihovu autentičnost, pretpostavka je da će se s vremenom razviti mreža u kojoj svaki korisnik preko relativno malog broja drugih korisnika može potvrditi autentičnost bilo kojeg korisnika. Pritom se korisnik kreće „putovima povjerenja“, počevši od osoba kojima on vjeruje, preko osoba kojima one vjeruju pa do osobe čija je autentičnost bila upitna.

PGP sustav razlikuje četiri razine sigurnosti ključa:

1. **nepouzdani ključevi** – certifikati potpisani ključevima ove razine pouzdanosti smatraju se nevaljalima
2. **granični ključevi** – bilo koji ključ mora biti potpisan barem s dva granična ključa kako bi se smatrao valjanim. Riječ je o stupnju povjerenja koje označava djelomičnu pouzdanost. Može se koristiti recimo za zaštitu od pogreške - ako jedan granični ključ pogreškom potpiše nevaljali, taj potpis sam ne znači mnogo, ali vjerojatnost da će dva korisnika učiniti pogrešku je mala pa se na dva potpisa korisnik može osloniti.
3. **pouzdani ključevi** – ključ potpisan jednim pouzdanim ključem smatra se valjanim, dakle ovo je stupanj potpunog povjerenja drugom korisniku.
4. **potpuno pouzdan** – onaj ključ za kojeg se posjeduje tajni ključ (korisnikov ključ). Bilo koji ključ potpisan ovim ključem smatra se valjanim.

Ove razine sigurnosti zapravo definiraju razinu povjerenju koju korisnik može pridati nekom ključu kada ga potpisuje (potvrđuje) kao autentičnog.

Prednosti ovog sustava leže u decentraliziranosti, koja ga čini fleksibilnim u tehničkom smislu i otpornim na promjene u CA hijerarhiji jer se autentičnost potvrđuje preko korisnika. Problem kod ovakvog sustava je težina ulaska u mrežu za nove korisnike koji trebaju čekati neko vrijeme dok ne steknu dovoljnu razinu povjerenja u mreži da mogu učinkovito komunicirati sa svim drugim korisnicima.

5.2. Usporedba OpenPGP i S/MIME standarda

S/MIME i OpenPGP su sigurnosni standardi koji pružaju iste ciljne usluge – autentičnost, besprijekornost i tajnost komunikacije elektroničkim porukama putem nesigurne mreže - Interneta. Ostvarenje tih usluga zasniva se na sličnim kriptografskim algoritmima i metodama. Ono po čemu se ova dva standarda razlikuju je sustav za verifikaciju veze između javnog ključa i korisnika, odnosno provjeru pripadnosti javnog ključa određenom korisniku. S/MIME se zasniva na hijerarhijskom modelu pouzdanih CA tijela. To su sudionici komunikacije koje svi korisnici smatraju pouzdanima i preko njih se provjeravaju drugi nepouzdani korisnici. Za razliku od centraliziranog S/MIME PKI sustava, OpenPGP zasniva se na PGP modelu opisanom u prethodnom poglavlju. Riječ je o decentraliziranoj mreži korisnika u kojoj se preko veza između korisnika koji si međusobno vjeruju može uspostaviti put povjerenja do bilo kojeg drugog korisnika.

Zbog bitnih razlika u načinu provjere certifikata, S/MIME i OpenPGP sigurnosni modeli ne mogu se povezati. Zbog toga poruke zaštićene prema jednom standardu neće biti prepoznatljive u sustavu čija sigurnosna politika uključuje primjenu drugog standarda.

Specifikacija	S/MIMEv3	OpenPGP
Format poruke	Binarni, na temelju CMS specifikacije	Binarni na temelju PGP specifikacije
Format certifikata	Binarni, na temelju X.509v3 specifikacije	Binarni na temelju PGP specifikacije
Simetrični kriptografski algoritam	3DES (DES EDE3 CBC)	3DES (DES EDE3 CFB)
Algoritam za izradu i provjeru digitalnog potpisa	Diffie-Hellman (X9.42) s DSS ili RSA algoritmom	ElGamal s DSS algoritmom
Algoritam za izračunavanje i provjeru sažetka	SHA-1	SHA-1
MIME omotavanje potpisanih podataka	multipart/signed ili CMS format	multipart/signed s ASCII omotom
MIME omotavanje kriptiranih podataka	application/pkcs7-mime	multipart/encrypted

Tablica 1. Usporedba S/MIME i OpenPGP algoritama

Izvor: Internet Mail Consortium

5.3. Budućnost standarda

Postojanje dvaju različitih, široko prihvaćenih, ali bitno različitih standarda posljedica je toga što za pitanje učinkovite razmjene javnih ključeva ne postoji jedno nesumnjivo najbolje rješenje. U takvim uvjetima otvoren je prostor za predlaganje različitih ideja, a ona koja će u konačnici biti opće prihvaćena ne moraju nužno biti bolja od ostalih. Po pitanju sigurnosti komunikacije elektroničkim porukama S/MIME i OpenPGP su dva standarda koja su se izdigla nad drugim predloženim rješenjima i prešla u opću upotrebu. Problem se javlja zbog toga što ne podržavaju svi klijenti elektroničke pošte oba standarda, niti je praktično i dobro rješenje raditi jednu te istu stvar na više načina. Hoće li jedan od ova dva standarda u budućnosti preuzeti dominaciju i koji će to biti teško je reći.

Važno je pritom naglasiti da je Internet oblikovan kao nesigurna mreža što zahtijeva nadogradnju sigurnosti na višim razinama sustava. Zaštita elektroničke pošte ostvaruje se na razini aplikacije i time je najviša moguća razina tehničke zaštite na Internetu. U sigurno oblikovanim mrežama potreba za ovom vrstom zaštite se gubi jer su paketi koji njima putuju zaštićeni na nižim infrastrukturnim slojevima što je zapravo učinkovitiji i bolji izbor.

Još dosta vremena nesavršenosti sigurnosti na Internetu ostavljat će potrebu za primjenom dodatnih sigurnosnih standarda, pa tako i S/MIME standarda.

Zaključak

S/MIME je standard koji omogućuje sigurnu komunikaciju elektroničkim porukama u Internetu, a ostvaren je na razini aplikacije. To znači da se sigurnom okolinom (onom gdje se poruka može prikazati u otvorenom obliku i gdje nema opasnosti od neovlaštenog mijenjanja) smatra tek klijent elektroničke pošte. S/MIME sigurnost uključuje kriptiranje sadržaja poruka čime se osigurava tajnost podataka dok prolaze kroz Internet. Osim toga, u poruke se može uključiti i digitalni potpis koji jamči da je pošiljatelj poruke upravo onaj korisnik koji je potpisan i da je poruka stigla do odredišta u onom obliku u kojem je poslana. Budući da se u ostvarenju ovih usluga koriste vrlo sigurni kriptografski algoritmi, jednom kada se korisnik odluči na primjenu S/MIME standarda, nema razloga sumnjati u njegovu pouzdanost.

Pitanja koja se nameću prilikom odabira sigurnosne politike su praktične prirode. Naime, S/MIME je široko ali ne i opće prihvaćen standard. To znači da ga podržavaju mnogi programi, ali ne svi. Osim toga S/MIME nije jedini korišteni standard za sigurnu komunikaciju elektroničkim porukama. OpenPGP je alternativno rješenje koji je po razini sigurnosti otprilike jednako S/MIME-u, ali drukčije ostvaruje verifikaciju javnih ključeva. S/MIME se temelji na centraliziranoj verifikaciji u CA centrima, dok se OpenPGP temelji na razvoju sigurne mreže korisnika. Iako je OpenPGP prilagodljiviji i samoodrživiji model, zahtijeva veći angažman korisnika u funkcioniranju mreže. Kod S/MIME standarda svaki se korisnik u potpunosti oslanja na CA tijela koja osiguravaju pouzdanost komunikacije.

Na pitanje koji je standard bolji nema jedinstvenog odgovora kao niti na pitanje hoće li neki od njih u budućnosti preuzeti dominaciju, ili će nestati uopće potreba za tom vrstom zaštite (primjerice, ukoliko se odgovarajuća zaštita u potpunosti ostvari na nižim razinama mrežne infrastrukture). Svaki korisnik između ponuđenih rješenja treba odabrati ono koje mu najbolje odgovara. Kako bi ta odluka bila što kvalitetnija, prvenstveno je bitno informirati se o postojećim sigurnosnim problemima i dostupnim rješenjima.

6. Reference

1. S/MIME and OpenPGP, http://www.imc.org/smime-pgpmime.html, svibanj 2009.
2. S/MIME, http://en.wikipedia.org/wiki/Smime, svibanj 2009.
3. Pretty Good Privacy, http://en.wikipedia.org/wiki/Pretty_Good_Privacy, svibanj 2009.
4. MIME, http://en.wikipedia.org/wiki/MIME, svibanj 2009.
5. Cryptographic Message Syntax (CMS), http://tools.ietf.org/html/rfc3852, svibanj 2009.
6. X.509, http://en.wikipedia.org/wiki/X.509, svibanj 2009.
7. Block cipher modes of operation, http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation, svibanj 2009.