Bezpečnosť elektronickej pošty

- štandard PGP
- S/MIME
- útoky na elektronickú poštu

Primárny zdroj informácii k dnešnej prednáške:

[1] prof. Ing. Dušan Levický, CSc.
APLIKOVANÁ KRYPTOGRAFIA
od utajenia správ ku kybernetickej bezpečnosti
Elfa, Košice, 2018 (str.335-340)

[2] PGP from: Cryptography and Network Security. Fifth Edition by Wiliam Stallings, Lecture slides by Lawrence Brown. http://www.diag.uniroma1.it/~damore/websec/slides/pgp-smime-stallings.pdf

Bezpečnosť elektronickej pošty

Elektronická pošta je významným prostriedkom na komunikáciu veľkého počtu ľudí, ktorí ju používajú každý deň. Z uvedeného vyplýva, že dôležitým aspektom elektronickej pošty je jej bezpečnosť. **Bezpečnosť elektronickej** pošty zahŕňa najmä dve základné požiadavky. Sú to:

• dôvernosť správ
• autentizácia, resp. pôvod dát.

Dôvernosť správ elektronickej pošty vyjadruje zabezpečenie prenášaných správ z vysielacieho zariadenia elektronickej pošty do jej prijímacieho zariadenia. Je potrebné poznamenať, že počas prenosu správ elektronickej pošty správy prechádzajú cez viaceré prenosové zariadenia, ako sú servery, resp. smerovače, ktoré vytvárajú nezabezpečené komunikačné siete. Preto je dôvernosť správ elektronickej pošty veľmi dôležitá a je realizovaná najmä šifrovaním.

Autentizácia, resp. pôvod prenášaných, dát vyjadruje originálny pôvod prenášaných správ a ochranu proti ich odmietnutiu. Je to najmä preto, lebo protokoly správ elektronickej pošty sú veľmi jednoduché a dobre štruktúrované, čo umožňuje útočníkom realizovať útoky na prenášané správy.

Na zabezpečenie elektronickej pošty existujú hlavne dva štandardy, ktoré sú implementované do aplikácií elektronickej pošty. Sú to tieto štandardy:

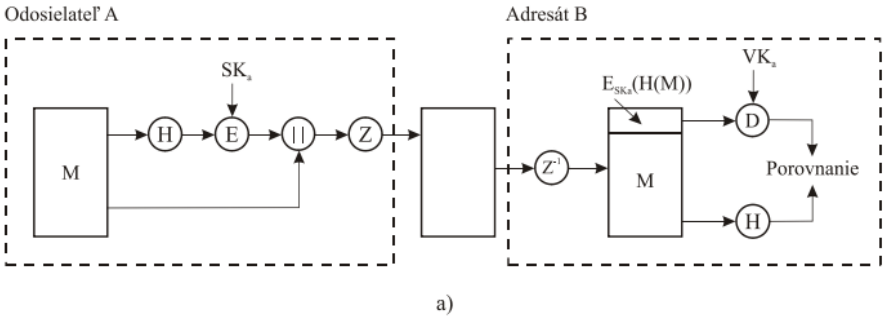
• PGP
• S/MIME.

Štandard PGP

Štandard elektronickej pošty PGP (Pretty Good Privacy), resp. Open PGP realizuje zabezpečenie elektronickej pošty a pozostáva z týchto služieb:

- **autentizácia**
- **dôvernosť**
- **kompresia**
- **kompatibilita elektronickej služby**
- **segmentácia.**

Autentizáciu prenášaných dát v PGP ilustruje *Obr. 16.6a*. Zahŕňa túto postupnosť krokov:



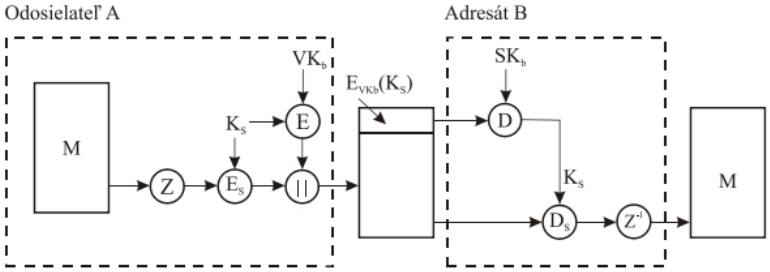
Obr. 16.6 a) autentizácia prenášaných dát v PGP

Autentizáciu prenášaných dát v PGP ilustruje *Obr. 16.6a*. Zahŕňa túto postupnosť krokov:

1. odosielateľ vytvára správu M
2. hašovacia funkcia H, ktorá je typu SHA-1, vygeneruje 160-bitový kód správy M
3. hašovací kód je zašifrovaný algoritmom RSA s využitím súkromného kľúča odosielateľa SK_a a výsledok sa pridá k správe M
4. výsledok, teda $M||(E_{SKa}(H(M)))$, sa komprimuje algoritmom Z, teda algoritmom ZIP
5. na strane adresáta sa aplikuje dekompresný algoritmus Z^{-1}, čím vzniknú položky M a $E_{SKa}(H(M))$
6. adresát dešifruje položku $E_{SKa}(H(M))$ algoritmom RSA s využitím verejného kľúča VK_a (algoritmus D), čím vzniká $H(M)$
7. adresát vytvorí nový hašovací kód $H'(M)$ a porovná ho s dešifrovaným kódom $H(M)$. Zhoda hašovacích kódov znamená, že autentizácia je úspešná.

Kombinácia algoritmov RSA a SHA-1 vytvárajú efektívnu realizáciu digitálneho podpisu. Alternatívou je digitálny podpis s využitím DSS/SHA-1.

Ďalšou službou elektronickej pošty je **dôvernosť**, ktorá sa realizuje šifrovaním správ, ktoré sú prenášané alebo uchované. Na zabezpečenie dôvernosti správ sa využívajú algoritmy symetrického šifrovania (napr. CAST-128, 3 DES), ktoré využívajú blokové šifry s veľkosťou bloku 64 bitov a režimom CFB. Ďalším problémom je distribúcia symetrických kľúčov, ktoré majú dĺžku 128 bitov a sú vytvorené náhodne pre každú správu. Tieto kľúče sa označujú ako kľúče relácií K_S (session keys) a sú jednorazové (one-time keys) (*Obr. 16.6b)*).



b)

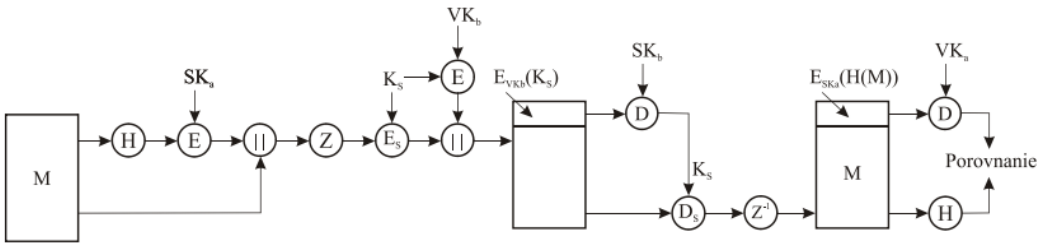
Obr. 16.6 b) zabezpečenie dôvernosti prenášaných dát,

Postupnosť krokov pre dôvernosť zahŕňa:

1. odosielateľ vytvorí správu *M*, ktorú komprimuje algoritmom ZIP (operácia *Z*),
2. odosielateľ vytvorí 128-bitové číslo, označené ako kľúč relácie K_S pre danú správu,
3. zasielaná správa *M* je šifrovaná symetrickým šifrovaním E_S a kľúčom relácie K_S,
4. kľúč relácie K_S je zašifrovaný algoritmom RSA (algoritmus *E*) použitím verejného kľúča VK_b a pripojí sa k zašifrovanej správe,
5. adresát dešifruje algoritmom RSA (algoritmus *D*) s použitím súkromného kľúča SK_b kľúč relácie K_S,
6. kľúč relácie K_S dešifruje symetrickým algoritmom D_S zasielanú správu, ktorá sa dekomprimuje algoritmom ZIP (Z^{-1}).

Ako alternatívu k použitiu RSA, algoritmus PGP poskytuje aj algoritmus Diffie-Hellman, pričom tento algoritmus sa označuje ako El Gamal.

Kombináciou dvoch služieb v PGP je zabezpečenie dôvernosti a autentizácie prenášaných správ (*Obr. 16.6c*).



c)

Obr. 16.6 c) kombinácia autentizácie a dôvernosti prenášaných dát

Kombináciou dvoch služieb v PGP je zabezpečenie dôvernosti a autentizácie prenášaných správ (*Obr. 16.6c*).

V prvej fáze sa realizuje autentizácia prenášaných správ elektronickej pošty s využitím súkromného kľúča odosielateľa. V druhej fáze predstavuje zabezpečenie dôvernosti, ktorá sa realizuje symetrickým šifrovaním prenášaných správ.

Na strane adresáta sa teda zabezpečuje autentizácia aj dôvernosť prenášaných správ elektronickej pošty.

Dôležitým aspektom bezpečnosti elektronickej pošty je **kompresia** prenášaných správ. Kompresia prenášaných správ sa symbolicky označuje blokmi Z a dekompresia sa označuje blokmi Z^{-1}. Je potrebné poznamenať, že bezpečnosť správ elektronickej pošty je po kompresii vyššia ako bez kompresie. Je to preto, lebo prenášané správy majú menšiu redundanciu ako otvorený text a ich kryptoanalýza je takto ťažšia. Na kompresiu prenášaných správ sa v elektronickej pošte používa algoritmus ZIP, resp. podobné algoritmy ako sú PKZIP, gzip atď., ktoré využívajú algoritmus LZ77.

Kompatibilita elektronickej pošty zabezpečuje konverziu blokov textu, obvykle oktet bitov (8 bitov), na bloky s ASCII znakmi. Systém PGP poskytuje konverziu týchto blokov na ASCII znaky, ktorá sa označuje ako konverzia Radix-64.

Každá skupina troch oktetov binárnych znakov je mapovaná na štyri ASCII znaky. Tento formát zahŕňa aj zabezpečenie s kódmi CRC na detekciu chýb pri prenose.

Segmentácia elektronickej pošty znamená rozdelenie bloku dĺžky správy na menšie úseky. Maximálna dĺžka správy zahŕňa 50 000 oktetov. Všetky väčšie dĺžky sa musia rozdeliť na menšie segmenty pošty, ktoré sú prenášané separátne.

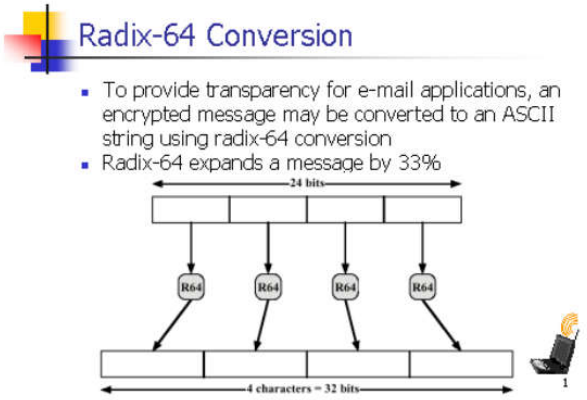
***Radix-64** (v PGP terminológii sa používa termín „**ASCII Armour**“)

Kódovanie Radix-64 (slov. termín Base-64)

Používa sa na kódovanie (binárnych) dát, ktoré je možné reprezentovať pomocou tlačiteľných ASCII znakov. Na kódovanie sa používajú znaky (2^6=**64 znakov** + **vyplňovací znak** „=“) z nasledujúcej tabuľky:

6 bit value	Character encoding	6 bit value	Character encoding	6 bit value	Character encoding	6 bit value	Character encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

Základný princíp konverzie do Radix-64 formátu je znázornený na nasledujúcom obrázku:



Radix-64 Conversion: Example

- Suppose the email message is: new
- ASCII format: 01101110 01100101 01110111
- After encryption: 10010001 10011010 10001000
- The Radix-64 conversion:
  - The 24-bit block: 10010001 10011010 10001000
  - Four 6-bit blocks: 100100 011001 101010 001000
  - Integer version: 36 25 38 8
  - Printable version: k Z m I

Poznáka:
Pokiaľ nie je počet vstupných 8-bitových znakov násobkom čísla 3, je použitý **jeden alebo dva** vyplňovacie znaky „=“. Podrobnejšie informácie o kódovaní Radix-64 vrátane implementácie v jazyku C (https://github.com/DavidCWebs/radix-64-encoding) budú **preberané na cvičení**.

Príklad **on-line** nástroja pre Radix-64 kódovanie:https://www.base64encode.org/

Používané štandardy a programy:

OpenPGP je opísaný v internetovom štandard **RFC 4880**, 2007 - https://tools.ietf.org/html/rfc4880

Aktuálne sú dostupné dve najznámejšie **implementácie OpenPGP**:

• **PGP firmy PGP Inc.** (komerčný product, aktuálne od roku 2010 vo vlastníctve firmy Symantec (https://en.wikipedia.org/wiki/PGP_Corporation), https://www.symantec.com/content/dam/symantec/docs/data-sheets/encryption-solutions-for-email-en.pdf
• **GNU Privacy Guard** (GnuPG alebo GPG - https://www.gnupg.org/), Open-source

Základné informácie o použitých **šifrovacích algoritmoch** v GnuPG a aktuálnych verziách je možné nájsť napr. na stránke:
https://en.wikipedia.org/wiki/GNU_Privacy_Guard

Niektoré informácie z uvedenej stránky:

As of versions 2.0.26 and 1.4.18, GnuPG supports the following algorithms:

Public key
: RSA, ElGamal, DSA

Cipher
: 3DES, IDEA (since versions 1.4.13 and 2.0.20), CAST5, Blowfish, Twofish, AES-128, AES-192, AES-256, Camellia-128, -192 and -256 (since versions 1.4.10 and 2.0.12)

Hash
: MD5, SHA-1, RIPEMD-160, SHA-256, SHA-384, SHA-512, SHA-224

Compression
: Uncompressed, ZIP, ZLIB, BZIP2

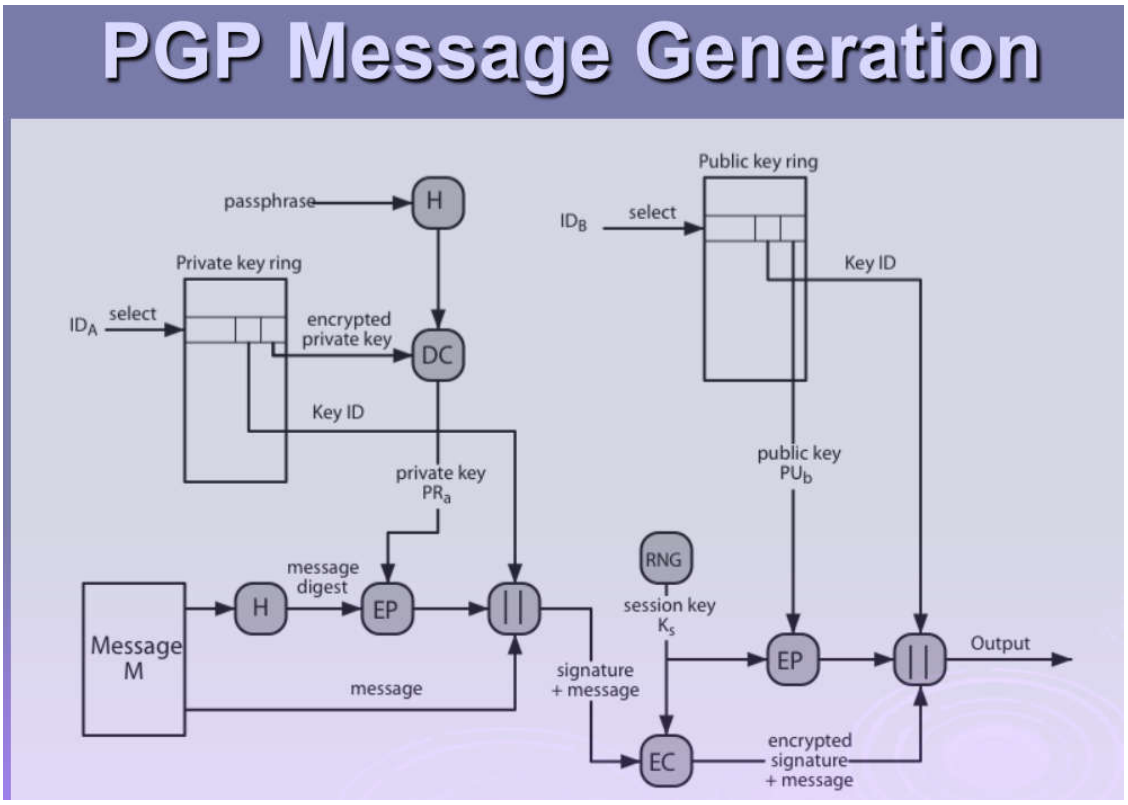
More recent releases of GnuPG 2.x ("modern" and the now deprecated "stable" series) expose most cryptographic functions and algorithms Libgcrypt (its cryptography library) provides, including support for elliptic curve cryptography (ECDSA, ECDH and EdDSA)[9] in the "modern" series (i.e. since GnuPG 2.1).

Na cvičeniach bude nainštalovaná **“modern”verzia** z rady **2.3.x**

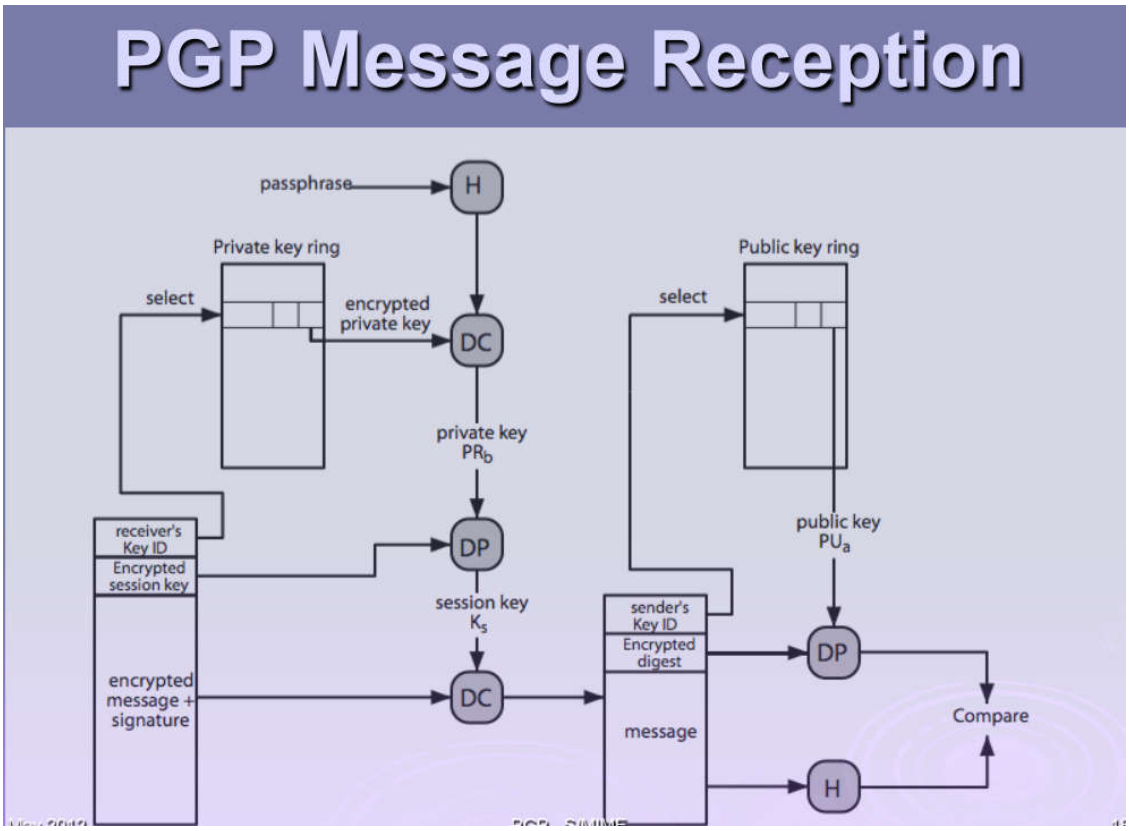
Konecept kľúčeniek (Private key ring, Public key ring) v programe GnuPG [2, str.17-18]

Pod kľúčenkou rozumieme súbory v operačnom systéme, kde program ukladá a chráni uložené kľúče. Program ukladá **súkromné kľúče** do "súkromnej kľúčenky (private key ring)" a chráni uložené kľúče s **použitím frázy** (passphrase). **Verejné kľúče** sú uložené do "verejnej kľúčenky (public key ring)".

Využitie kľúčeniek pri **vytváraní správy** (**podpise a šifrovaní**) je znázornené na nasledujúcom obrázku:



Využitie kľúčeniek pri **príjme správy** (**dešifrovaní a overení podpisu**) je znázornené na nasledujúcom obrázku:



Generovanie a manažment kľúčov

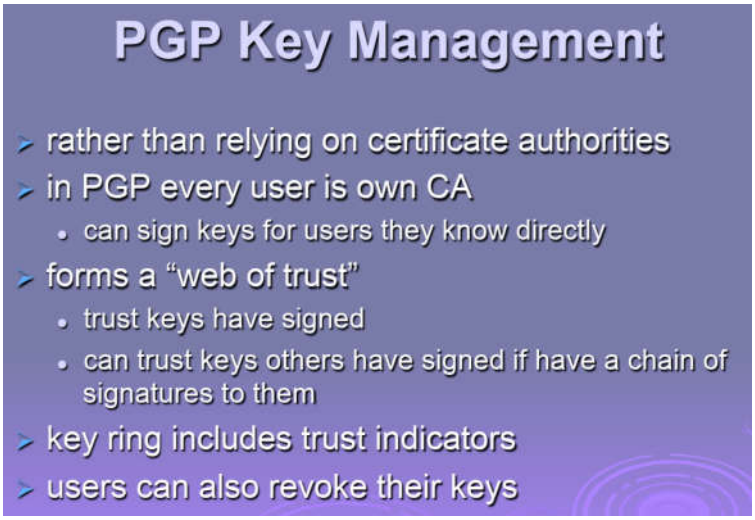
Program GnuPG umožňuje pomocou vhodných príkazov užívateľovi generovať pár kľúčov (verejný a súkromný) s požadovanými vlastnosťami. Vygenerované alebo získané kľúče je možné pomocou príkazov umiestniť na príslušne kľúčenky. Podrobnejšie informácie o základných príkazoch programu GnuPG budú preberané na cvičeni.

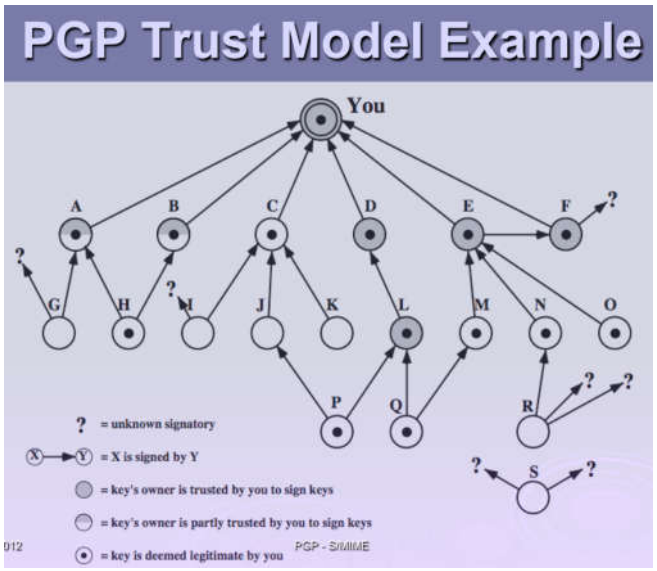
Verejné kľúče môžu užívatelia **zverejniť** napr. aj pomocou na to určených serverov, napr.:
https://pgp.key-server.io/
http://keys.gnupg.net/
https://pgp.circl.lu/

Napr. verejný kľúč prednášajúceho, ktorý budú študenti využívať pri odovzdávaní zadaní je na serveroch dostupný s nasledujúcimi identifikátormi:

„Web of trust“

Aj keď PGP kľúče môžu byť uložené na špecializovaných PGP serveroch, koncepcia manažovania kľúčov v programoch PGP **nevyužíva certifikačné autority**. Verejné kľúče na server môže nahrať prakticky hocikto a autentizácia užívateľov je minimálna. Programy PGP podporujú zdieľanie dôvery medzi užívateľmi, pričom úroveň dôvery k jednotlivým verejným kľúčom si určuje samotný užívateľ. V tomto procese môže užívateľ A využívať aj **informácie** od iných **užívateľov ktorým dôveruje** a ktorí podpísali kľúče ďalších užívateľov, ktoré užívateľ A nemá možnosť inak overiť. Vytvára sa tak „web of trust“.





V kódovaní Radix-64 sú často reprezentované aj šifrovacie kľúče a certifikáty, napr. **PEM formát** žiadosti o certifikát (https://support.quovadisglobal.com/kb/a37/what-is-pem-format.aspx):

What is PEM Format?

Root > SSL Certificates > SSL General Topics

Problem

What is PEM Format?

Resolution

PEM or Privacy Enhanced Mail is a Base64 encoded DER certificate. PEM certificates are frequently used for web servers as they can easily be translated into readable data using a simple text editor. Generally when a PEM encoded file is opened in a text editor, it contains very distinct headers and footers. Below are some examples of different files in PEM format.

-----BEGIN CERTIFICATE REQUEST-----
MIIB9TCCAWACAQAwgbgxGTAXBgNVBAoMEFF1b1ZhZGlzIExpbWl0ZWQxHDAaBgNV
BAsME0RvY3VtZW50IERlcGFydG1lbnQxOTA3BgNVBAMMMFdoeSBhcmUgeW91IGRl
Y29kaW5nIG1lPyAgVGhpcyBpcyBvbmx5IGEgdGVzdCEhITERMA8GA1UEBwwISGFt
aWx0b24xETAPBgNVBAgMCFBlbWJyb2tlMQswCQYDVQQGEwJCTTEPMA0GCSqGSIb3
DQEJARYAMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCJ9WRanG/fUvcfKiGl
EL4aRLjGt537mZ28UU9/3eiJeJeznNSOuNLnF+hmabAu7H0LT4K7EdqfF+XUZW/2j
RKRYcvOUDGF9A7OjW7UfKk1In3+6QDCi7X34RE161jqoaJjrm/T18TOKcgkkhRzE
apQnIDm0Ea/HVzX/PiSOGuertwIDAQABMAsGCSqGSIb3DQEBBQOBgQBzMJdAV4QP
Awel8LzGx5uMOshezF/KfP67wJ93UW+N7zXY6AwPgoLj4Kjw+WtU684JL8Dtr9FX
ozakE+8p06BpxegR4BR3FMHf6p+0jQxUEAkAyb/mVgm66TyghDGC6/YkiKoZptXQ
98TwDIK/39WEB/V607As+KoYazQG8drorw==
-----END CERTIFICATE REQUEST-----

Above is the example of a CSR (certificate signing request) in PEM format. You can see that PEM has the characteristics of containing a header, the body (which consists mainly of code) and footer.

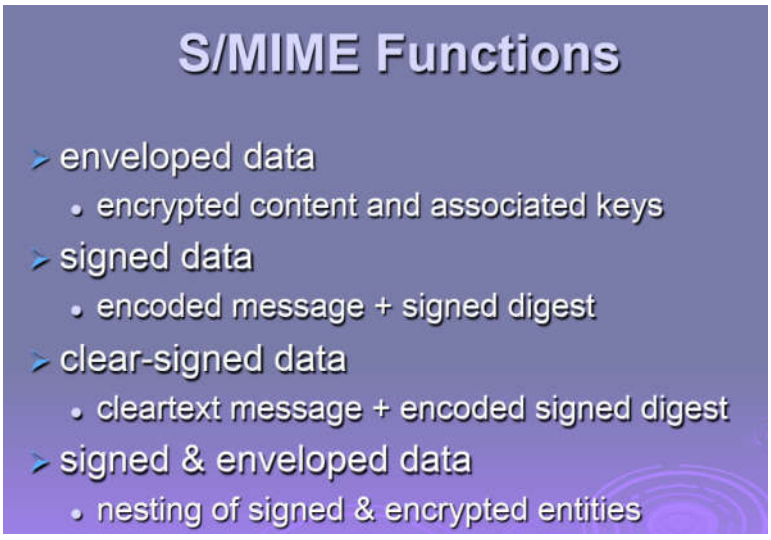
The header and footer is what identifies the type of file, however be aware that not all PEM files necessarily need them.

-----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- show a CSR in PEM format.
-----BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY----- show a private key in PEM format.
-----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- show a certificate file in PEM format.

Article ID: 37, Created: April 27, 2009 at 12:00 AM, Modified: July 9, 2013 at 12:23 PM

Štandard S/MIME

Štandard S/MIME (**Secure/Multipurpose Internet Mail Extention**) zabezpečuje bezpečnosť elektronickej pošty na báze technológie RSA Data Security.
Oba štandardy PGP a S/MIME sú založené na odporúčaniach IETF, ale **štandard S/MIME** je využívaný skôr na **priemyselné a organizačné účely**. Štandard PGP je orientovaný skôr na osobnú bezpečnosť klientov elektronickej pošty. Nasledujúce informácie sú z [2]:



S/MIME Cryptographic Algorithms

- digital signatures: DSS & RSA
- hash functions: SHA-1 & MD5
- session key encryption: ElGamal & RSA
- message encryption: AES, Triple-DES, RC2/40 and others
- MAC: HMAC with SHA-1
- have process to decide which algs to use

S/MIME Messages

- S/MIME secures a MIME entity with a signature, encryption, or both
- forming a MIME wrapped PKCS object
- have a range of content-types:
  - enveloped data
  - signed data
  - clear-signed data
  - registration request
  - certificate only message

S/MIME Certificate Processing

- S/MIME uses X.509 v3 certificates
- managed using a hybrid of a strict X.509 CA hierarchy & PGP's web of trust
- each client has a list of trusted CA's certs
- and own public/private key pairs & certs
- certificates must be signed by trusted CA's

Útoky na elektronickú poštu

Elektronická pošta používa **štandardné protokoly**, ktoré sú univerzálne a často zaužívané. Preto sú cieľom viacerých **útokov**, ktoré rozdeľujeme do **dvoch základných skupín**. Sú to:

• odkrývanie prenášaných dát
• prenášanie a realizácia škodlivého softvéru.

Útok na **odkrývanie prenášaných dát** (Attacks on Disclosed Data) je modifikáciou správ elektronickej pošty, ktorá odkrýva citlivé informácie, resp. prenášané správy elektronickej pošty. **Škodlivý softvér** (**Malware**) je program určený na poškodenie alebo na vniknutie do počítačového systému. Je to súhrnné označenie, ktoré zahŕňa **vírusy**, **červy**, **trojské kone**, **špehovací softvér** (spyware) a **reklamný softvér** (adware).

Útok na odkrývanie prenášaných správ

V začiatkoch elektronickej pošty boli využívané najmä protokoly ako **POP3** (**Post Office Protocol**) a protokol **SMTP** (**Simple Mail Transfer Protocol**), ktoré prenášali správy elektronickej pošty **v otvorenom texte**.

Vylepšenia elektronickej pošty a nové protokoly priniesli, ale **aj útoky na odkrývanie prenášaných správ**, ktoré sú najmä:

• **útok zo stredu**
• **útok opakovaním**
• **útok na heslá**.

Útok zo stredu (**Man-in-the-middle Attack**) na elektronickú poštu spočíva v tom, že útočník musí **mať kontrolu** nad jedným z niekoľkých **smerovačov**, **brán firewall** alebo **brán**, cez ktoré sa prenášajú správy elektronickej pošty.

Pomocou existujúcich **softvérových prostriedkov**, ako sú napr. **ARP spoofing** (Address Resolution Protocol spoofing) môže **útočník modifikovať všetky správy** elektronickej pošty **idúce z**, resp. **do sieťových prostriedkov** (smerovače, brány) a môže kontrolovať dve miesta prenosovej cesty.

Existujú štyri možné miesta prenosovej cesty na tento druh útoku. Sú to:

• komunikácia medzi elektronickou poštou typu **klient/server**, pretože majú spoločný segment LAN,
• komunikácia medzi elektronickou poštou typu **klient/brána**,
• komunikácia **medzi dvoma bránami**,
• komunikácia medzi elektronickou poštou typu **brána/server**.

Útoky zo stredu možno **eliminovať** najmä **šifrovaním** a **digitálnymi podpismi** na prenášané správy elektronickej pošty. Účinné šifrovanie zabezpečuje ochranu pred dešifrovaním prenášanej správy útočníkom. Digitálne podpisy zabezpečujú integritu, resp. modifikáciu tela prenášaných správ s využitím hašovacích kódov prenášaných správ.

Útok opakovaním je druh útoku na prenos dát v počítačových sieťach, kde inak platné (originálne) dáta sú zopakované alebo pozdržané s cieľom ich odkrývania. Útočník môže tieto dáta pri prenose **zachytiť a neskôr zopakovať**, resp. pozmeniť priamo pri prechode sieťovým zariadením, napr. smerovačom. **Eliminácia** tohto útoku spočíva najmä **v používaní časových značiek** (**time stamps**) a v požiadavke, aby oba uzly zabezpečenej komunikácie **používali, čo najpresnejší čas**.

Phishing (lov hesiel) je druh útoku, pri ktorom sa útočník snaží vylákať od používateľov rôzne heslá, napr. heslá k bankovému účtu. Útok prebieha tak, že sa v prvej fáze založí webstránka, ktorá vyzerá ako existujúca dôveryhodná stránka. V druhej fáze táto webstránka ponúka rôzne výhody po prihlásení a láka rôzne heslá od používateľov. Cez posielané maily obvykle útočník môže oznámiť používateľom zmenu čísla účtu alebo ich obnovenie a tak vyláka od nich ich heslá.

Eliminácia tohto útoku spočíva najmä v tom, že používatelia by nemali dôverovať takýmto webstránkam a zverovať žiadne heslá, ktoré od nich žiadajú, pretože legálne stránky nikdy heslá takýmto spôsobom nežiadajú. Zároveň sa odporúča **nepoužívať rovnaké prihlasovacie údaje** do rôznych služieb. Existuje aj **phishing filter**, ktorý preverí to, či existujúca webstránka je legitímna.

Phishing je príkladom techniky **sociálneho inžinierstva**, ktorá je zameraná na oklamanie používateľov a na využitie slabých miest, resp. zraniteľnosti bezpečnostných technológií.

Spam sa definuje ako nevyžiadaná a hromadne rozosielaná správa prakticky rovnakého obsahu. Ide o zneužívanie elektronickej komunikácie, najmä e-mailu.

Rozlišujeme dva druhy spamu podľa adresáta spamu. Prvý druh je poslanie správy do množstva diskusných skupín, ktorá je určená na propagáciu určitých produktov, resp. iných morálne poškodzujúcich materiálov. Je zameraný na ľudí, ktorí často správy čítajú, ale neposkytujú svoje e-mailové adresy.

Druhý typ spamu je e-mailový spam, zaslaný konkrétnemu adresátovi na jeho e-mailovú adresu, ktorý sa získa prehľadaním webstránok, resp. diskusných skupín. E-mailové adresy možno získať aj rôznymi softvérovými produktami automaticky. Ľudia, ktorí rozosielajú spam sa označujú ako **spameri**.

Medzi útoky na elektronickú poštu sa zaraďuje najmä útok typu **Spam DoS**, ktorý zabraňuje štandardnému využitiu elektronickej pošty pomocou nevyžiadaných e-mailov. Ochrana proti spamu je veľmi komplikovaná. Problém spočíva v tom, že ostrá hranica medzi spamom a užitočnými e-mailmi neexistuje. Neexistujú taktiež príznaky, ktoré by jednoznačne indikovali to, že ide o spam. Existujú však celkom jednoduché opatrenia, ktoré minimalizujú množstvo spamov v poštovej schránke. Ide najmä o tieto opatrenia:

- čierna listina e-mailových adries
- filtre spamov.

Čierna listina e-mailových adries (Black list) je databáza IP adries používaných spamermi. Email, prichádzajúci z tejto adresy antispamový program neprepustí. Tvorcovia spamov však o čiernej listine vedia a adresu, z ktorej svoje spamy odosielajú, často menia.

Okrem čiernej listiny e-mailových adries existuje aj **biela listina e-mailových adries** (White list), do ktorej sa zapisujú overené adresy. E-maily prichádzajúce z tejto listiny antispamový program prepustí.

V súčasných softvérových prostriedkoch sa vytvárajú **pokročilé antispamové programy**, ktoré zdokonaľujú filtráciu spamov a využívajú slovné spojenia, podľa ktorých sa dá usúdiť, že ide o spam.

Filtre spamov sú softvérové prostriedky, ktoré identifikujú spam na základe slov, ktoré sa často nachádzajú v spamoch. Pri detekcii týchto slov sa spamy odfiltrujú. Veľmi často sa však správna správa (non-spam) označí ako spam. Na filtráciu spamov je založená napr. metóda jednoduchých Bayesových klasifikátoroch (naive Bayes classifier). Je potrebné však poznamenať, že filtre spamov sa stále zdokonaľujú.

Škodlivý softvér na elektronickú poštu

Škodlivý softvér so zameraním na elektronickú poštu zahŕňa širokú škálu aspektov, ktorá obsahuje zraniteľnosť počítačových systémov a jeho dopady. Zraniteľnosť počítačov vyplýva najmä z:

• homogenity použitých operačných systémov,
• chýb systémov, pretože väčšina počítačových systémov obsahuje chyby v softvérových prostriedkoch, ktoré škodlivý softvér využíva.

Existuje veľa stratégií na ochranu pred škodlivým softvérom, pričom platí, že škodlivý softvér nie je aktívny bez prenášania správ v elektronickej pošte, resp. bez prenášania ich príloh. Medzi niektoré zásady na ochranu proti škodlivému softvéru v elektronickej pošte patria najmä tieto:

• vyhýbať sa útokom proti škodlivému softvéru použitím elektronickej pošty,
• zachovať súkromie pri adrese v elektronickej pošte,
• vytvárať viaceré adresy pre elektronickú poštu,
• vytvárať rôzne kontá pre rôzne organizácie v elektronickej pošte,
• neotvárať žiadne e-maily, ktoré nie sú známe,
• neotvárať žiadne prílohy od neznámych adresátov,
• neotvárať žiadne prílohy, ktoré nie sú absolútne potrebné a žiadané.