FSI

LEI

2025/2026

T9 – Electronic Mail Security

Email Protocols

Two types of protocols are used for transferring email:

- Used to move messages through the Internet from source to destination (mail servers)
  - Simple Mail Transfer Protocol (SMTP)
- Used to access messages stored in mailboxes (in mail servers)
  - IMAP (Internet Message Access Protocol) and POP (Post Office Protocol) are the most commonly used

Internet Mail Architecture

- Defined in RFC 5598
- Message User Agent (**MUA**): client email program, local email server
- Mail Submission Agent (**MSA**): enforces policies and standards
- Message Transfer Agent (**MTA**): relays messages
- Mail Delivery Agent (**MDA**): transfers messages from MHS to the MS
- Message Store (**MS**): same machine as MUA or remote server

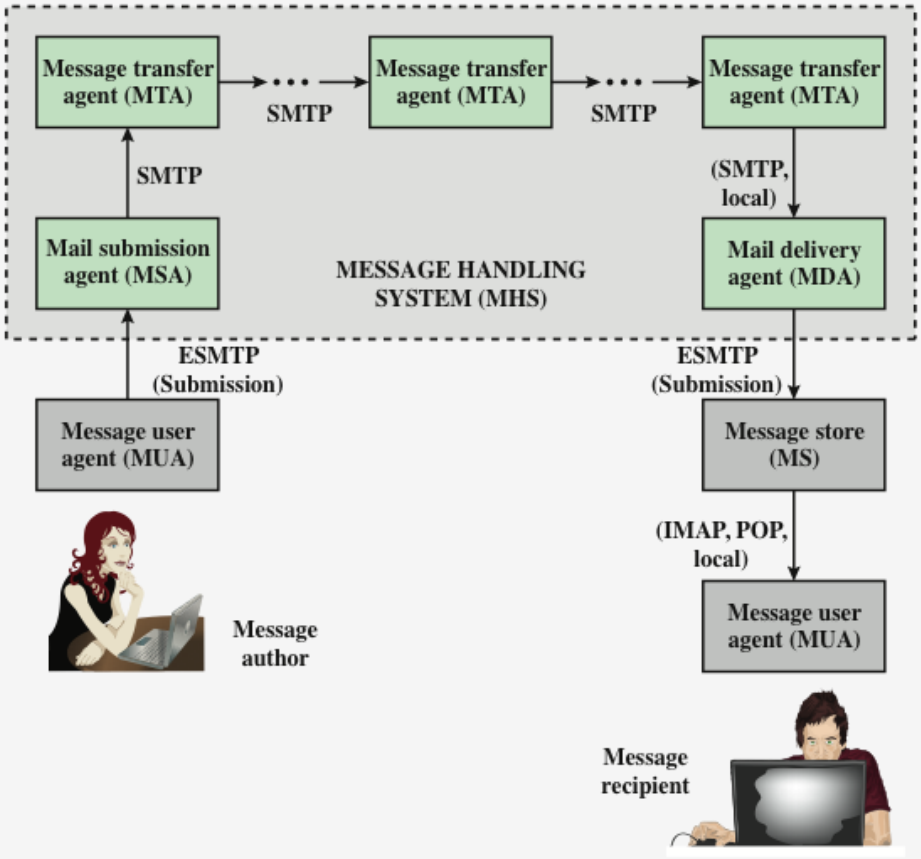


Figure 19.1 Function Modules and Standardized Protocols Used Between Them in the Internet Mail Architecture

SMTP (Simple Message Transfer Protocol)

Simple Mail Transfer Protocol

Encapsulates an email message in an envelope and is used to relay the encapsulated messages from source to destination through multiple MTAs

Is a text-based client-server protocol

Was originally specified in 1982 as RFC 821

The term Extended SMTP (ESMTP) is often used to refer to later versions of SMTP (last revision from 2008, RFC 5321)

Mail Access Protocols

POP3

- Post Office Protocol
- Allows an email client to download an email from an email server (MTA)
- POP3 user agents connect via TCP to the server
- After authorization, the MUA can issue POP3 commands to retrieve and delete mail

IMAP

- Internet Mail Access Protocol
- Enables an email client to access mail on an email server
- Also uses TCP, with server TCP port 143
- Is more complex than POP3
- Provides stronger authentication and provides other functions not supported by POP3

RFC 5322 (Internet Message Format)

Defines a format for text messages that are sent using electronic mail

Messages are viewed as having an **envelope** and **contents**

- The **envelope** contains whatever information is needed to accomplish transmission and delivery
- The **contents** compose the object to be delivered to the recipient
- RFC 5322 standard applies only to the contents

The content standard includes a set of header fields that may be used by the mail system to create the envelope

Example Message

```
Delivered-To: jgranjal@gmail.com
Received: by 10.202.168.7 with SMTP id r7csp406081oie;
       Sat, 10 Feb 2018 07:00:05 -0800 (PST)
X-Received: by 10.223.158.193 with SMTP id b1mr5539498wrf.156.1518274804931;
       Sat, 10 Feb 2018 07:00:04 -0800 (PST)
Return-Path:<me@xpto.com>
Received: from smtp2.dei.uc.pt (smtp.dei.uc.pt. [193.137.203.234])
       by mx.google.com with ESMTPS id e25si984421wmh.124.2018.02.10.07.00.04
       for<jgranjal@gmail.com>
       (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
       Sat, 10 Feb 2018 07:00:04 -0800 (PST)
Received: from eden.dei.uc.pt (eden-out.dei.uc.pt [193.136.212.2]) by smtp2.dei.uc.pt
(8.15.2/8.14.4) with ESMTPS id w1AExuN6020603 (version=TLSv1.2 cipher=DHE-RSA-AES256-GCM-SHA384
bits=256 verify=NO) for<jgranjal@gmail.com>; Sat, 10 Feb 2018 14:59:57 GMT
Received: from smtp.dei.uc.pt (smtp.dei.uc.pt [193.137.203.253]) by eden.dei.uc.pt
(8.14.4/8.14.4) with ESMTP id w1AExu9n018679 for<jgranjal@dei.uc.pt>; Sat, 10 Feb 2018 14:59:56
GMT
Received: from xpto.com (eden-out.dei.uc.pt [193.136.212.2]) by smtp.dei.uc.pt (8.15.2/8.14.4)
with ESMTP id w1AEwBmR005461 for<jgranjal@dei.uc.pt>; Sat, 10 Feb 2018 14:58:33 GMT
Date: Sat, 10 Feb 2018 14:58:11 GMT
From: me@xpto.com
Message-Id:<201802101458.w1AEwBmR005461@smtp.dei.uc.pt>
Subject: A quick test


Hello, this is a simple test on how easy
it is to forge the source address of an
email message.


Best regards,
Xpto person
```

Envelope vs Header FROM

THE ENVELOPE

- Communication between the SMTP Client and Server
- The client and server first greet each other with a HELO command
- Client uses MAIL FROM to represent the sender's address.
- Client sends one or more recipient's email address using the RCPT TO command.
- It is very easy to specify a fake/forged address in the MAIL FROM command

THE HEADER

- An email is divided in at least two parts: Header and Body
- The sender's email address and name is specified in the FROM header
- The sender's email address can be different from the envelope's MAIL FROM
- An email client will only display the FROM header, the user will never know what was the value for the MAIL FROM in the envelope

Example SMTP Transaction Scenario

```
S: 220 foo.com Simple Mail Transfer Service Ready
C: HELO bar.com
S: 250 OK
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: RCPT TO:<Green@foo.com>
S: 550 No such user here
C: RCPT TO:<Brown@foo.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: <CRLF><CRLF>
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel
```

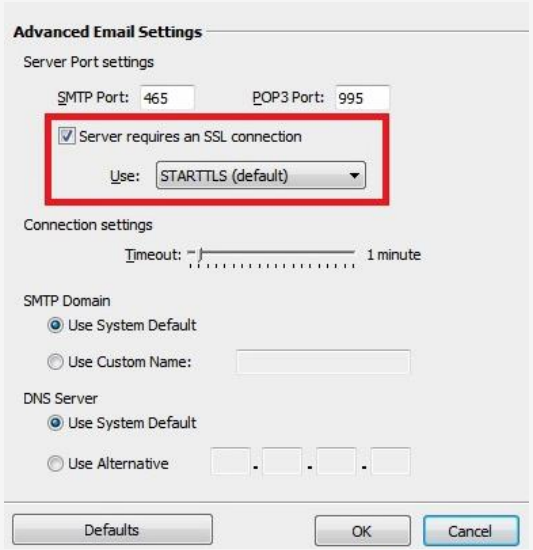
Figure 19.2 Example SMTP Transaction Scenario

Email (in)security (example)

```
jgranjal@eden ~ $ telnet smtp.dei.uc.pt 25
Trying 193.137.203.253...
Connected to smtp.dei.uc.pt.
Escape character is '^]'.
220 smtp.dei.uc.pt ESMTP Sendmail 8.15.2/8.14.4; Sat, 10 Feb 2018 14:58:11 GMT
EHLO xpto.com
250-smtp.dei.uc.pt Hello eden-out.dei.uc.pt [193.136.212.2], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE 60000000
250-DSN
250-STARTTLS
250-DELIVERBY
250 HELP
MAIL FROM:<me@xpto.com>
250 2.1.0 <me@xpto.com>... Sender ok
RCPT TO:<jgranjal@dei.uc.pt>
250 2.1.5 <jgranjal@dei.uc.pt>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: A quick test

Hello, this is a simple test on how easy
it is to forge the source address of an
email message.

Best regards,
Xpto person
.
250 2.0.0 w1AEwBmR005461 Message accepted for delivery
quit
221 2.0.0 smtp.dei.uc.pt closing connection
Connection closed by foreign host.
```

STARTTLS

- A significant security-related extension for SMTP
- Defined in RFC 3207 (*SMTP Service Extension for Secure SMTP over Transport Layer Security,* February 2002)
- Enables the addition of confidentiality and authentication in the exchange between SMTP agents
- This gives SMTP agents the ability to protect some or all of their communication from eavesdroppers and attackers
- Advantage of using STARTTLS is that the server can offer SMTP service on a single port, rather than requiring separate port numbers for secure and cleartext operations
- Similar mechanisms are available for IMAP and POP



Email Security Threats

Authenticity-related threats:

- Could result in unauthorized access to an enterprise's email system

Integrity-related threats:

- Could result in unauthorized modification of email content

Confidentiality-related threats:

- Could result in unauthorized disclosure of sensitive information

Availability-related threats:

- Could prevent end users from being able to send or receive mail

Specific email threats (together with approaches to mitigation) provided in NIST SP 800-177 (*Trustworthy Email*, Sep 2015)

Threat	Impact on Purported Sender	Impact on Receiver	Mitigation
Email sent by unauthorized MTA in enterprise (e.g. malware botnet)	Loss of reputation, valid email from enterprise may be blocked as possible spam/phishing attack.	UBE and/or email containing malicious links may be delivered into user inboxes	Deployment of domain-based authentication techniques. Use of digital signatures over email.
Email message sent using spoofed or unregistered sending domain	Loss of reputation, valid email from enterprise may be blocked as possible spam/phishing attack.	UBE and/or email containing malicious links may be delivered into user inboxes	Deployment of domain-based authentication techniques. Use of digital signatures over email.
Email message sent using forged sending address or email address (i.e. phishing, spear phishing)	Loss of reputation, valid email from enterprise may be blocked as possible spam/phishing attack.	UBE and/or email containing malicious links may be delivered. Users may inadvertently divulge sensitive information or PII.	Deployment of domain-based authentication techniques. Use of digital signatures over email.
Email modified in transit	Leak of sensitive information or PII.	Leak of sensitive information, altered message may contain malicious information	Use of TLS to encrypt email transfer between server. Use of end-to-end email encryption.
Disclosure of sensitive information (e.g. PII) via monitoring and capturing of email traffic	Leak of sensitive information or PII.	Leak of sensitive information, altered message may contain malicious information	Use of TLS to encrypt email transfer between server. Use of end-to-end email encryption.
Unsolicited Bulk Email (i.e. spam)	None, unless purported sender is spoofed.	UBE and/or email containing malicious links may be delivered into user inboxes	Techniques to address UBE.
DoS/DDoS attack against an enterprises' email servers	Inability to send email.	Inability to receive email.	Multiple mail servers, use of cloud-based email providers.

Email Threats and Mitigations

NIST Special Publication 800-177

Trustworthy Email

Counter Threat Protocols

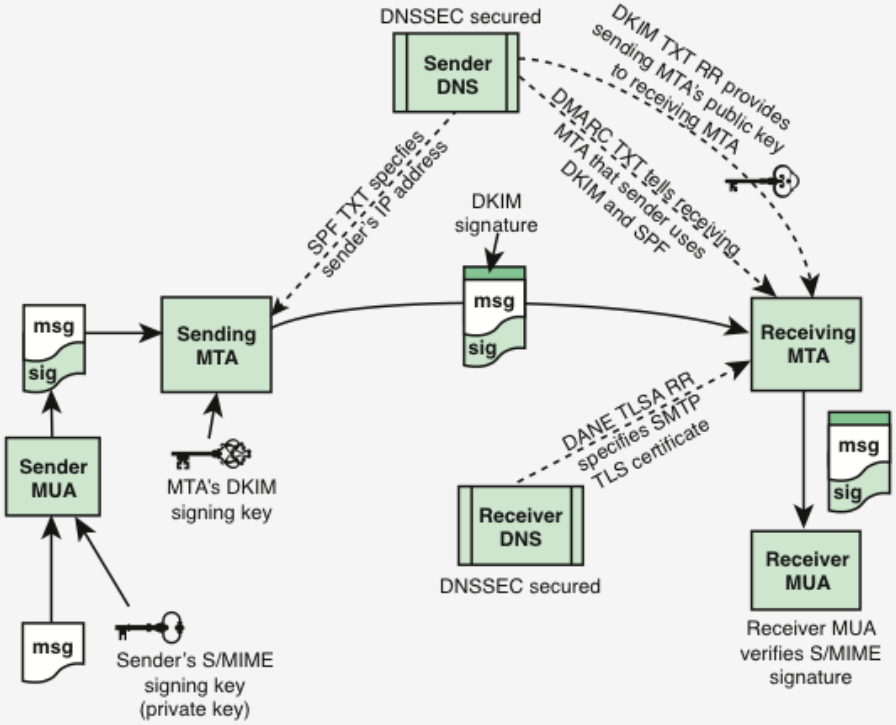
SP800-177 recommends use of a variety of standardized protocols as a means for countering threats:

- **STARTTLS**
  - An SMTP security extension that provides authentication, integrity, non-repudiation and confidentiality for the *entire SMTP message* by running SMTP over TLS
- **S/MIME and PGP**
  - Provides authentication, integrity, non-repudiation and confidentiality of the *message body* carried in SMTP messages
- **DNS Security Extensions (DNSSEC)**
  - Provides *authentication and integrity protection of DNS data*, and is an underlying tool used by various email security protocols
- **DNS-based Authentication of Named Entities (DANE)**
  - Is designed to overcome problems in the certificate authority (CA) system by providing an *alternative channel for authenticating public keys based on DNSSEC*, with the result that the same trust relationships used to certify IP addresses are used to certify servers operating on those addresses

Counter Threat Protocols (cont.)

- **Sender Policy Framework (SPF)**
  - Uses the Domain Name System (DNS) to allow domain owners to create records that associate the domain name with a specific IP address range of *authorized message senders*.
- **DomainKeys Identified Mail (DKIM)**
  - Enables an MTA to *sign selected headers and the body of a message*. This validates the source domain of the mail and provides message body integrity
- **Domain-based Message Authentication, Reporting, and Conformance (DMARC)**
  - Lets senders know the proportionate effectiveness of their SPF and DKIM policies, and signals to receivers what action should be taken in various individual and bulk attack scenarios

Interaction between Counter Threat Protocols



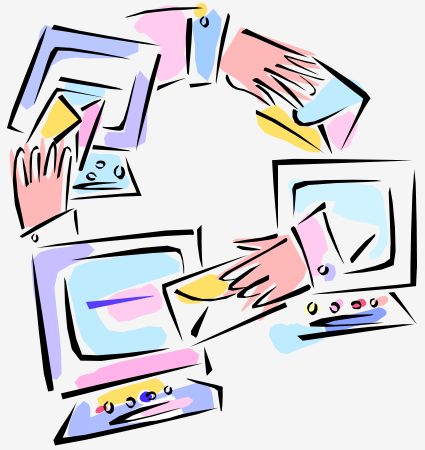
DANE = DNS-based Authentication of Named Entities
DKIM = DomainKeys Identified Mail
DMARC = Domain-based Message Authentication, Reporting, and Conformance
DNSSEC = Domain Name System Security Extensions
SPF = Sender Policy Framework
S/MIME = Secure Multi-Purpose Internet Mail Extensions
TLSA RR = Transport Layer Security Authentication Resource Record

Figure 19.4 The Interrelationship of DNSSEC, SPF, DKIM, DMARC, DANE, and S/MIME for Assuring Message Authenticity and Integrity

Secure/Multipurpose Internet Mail Extension (S/MIME)

A security enhancement to the MIME Internet e-mail format standard based on technology from RSA Data Security

The most important documents relevant to S/MIME include:



- RFC 5750, S/MIME Version 3.2 Certificate Handling
- RFC 5751, S/MIME Version 3.2 Message Specification
- RFC 4134, Examples of S/MIME Messages
- RFC 2634, Enhanced Security Services for S/MIME
- RFC 5652, Cryptographic Message Syntax (CMS)
- RFC 3370, CMS Algorithms
- RFC 5752, Multiple Signatures in CMS
- RFC 1847, Security Multiparts for MIME – Multipart/Signed and Multipart/Encrypted

S/MIME provides **four message-related services**: authentication, confidentiality, compression and email compatibility

Summary of S/MIME Services

Function	Algorithms Used	Description
Digital signature	RSA/SHA-256	A hash code of a message is created using SHA-256. This message digest is encrypted using SHA-256 with the sender's private key and includes with this message.
Message encryption	AES-128 with CBC	A message is encrypted using AES-128 with CBC with a one-time session key generated by the sender. The session key is encrypted using RSA with the recipient's public key and included with the message.
Compression	unspecified	A message may be compressed for storage or transmission.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

S/MIME functional flow

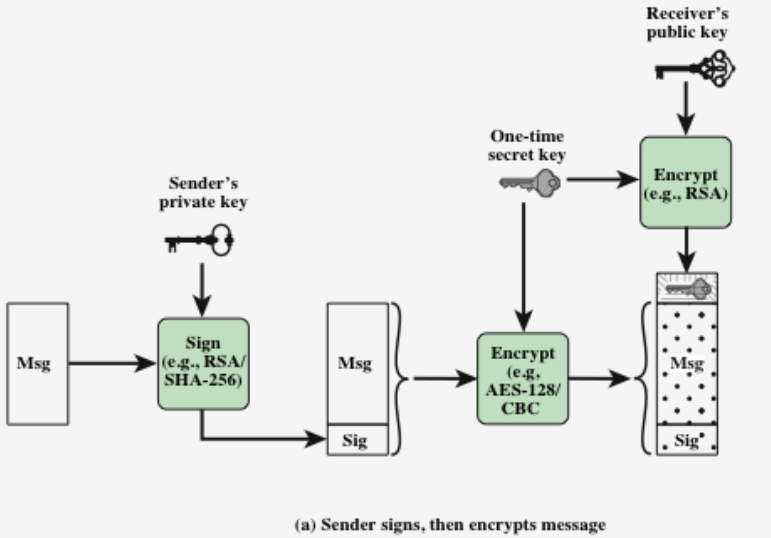
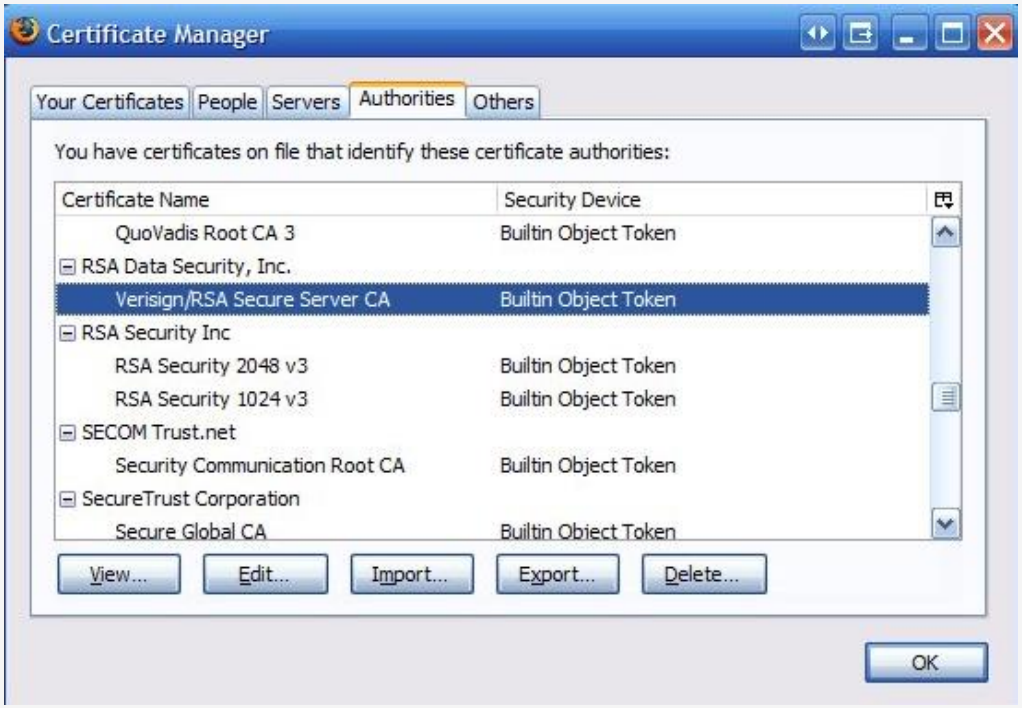


Figure 19.5 Simplified S/MIME Functional Flow

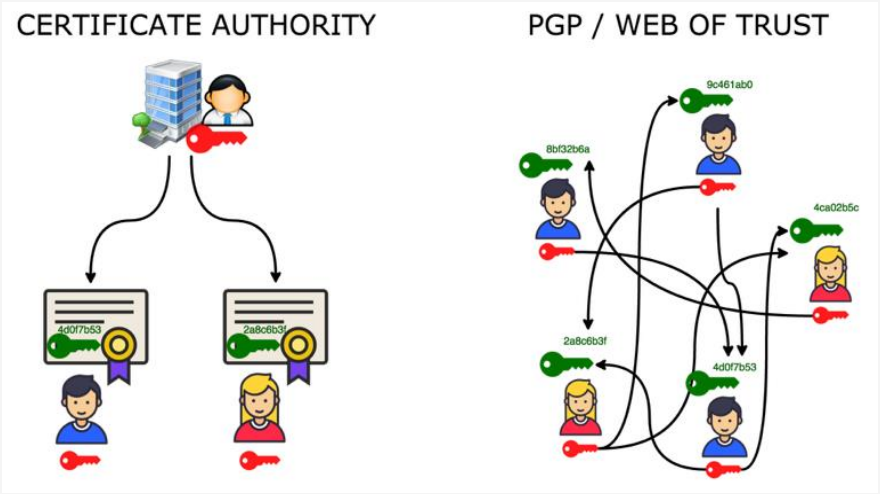
S/MIME and Certification Authorities

- S/MIME uses **X.509 v3 certificates**
- S/MIME clients must be configured with **trusted keys, certificates and revocation lists**



Web of Trust versus PKI (Certification Authorities)

- The user decide whom trust and whom not
- It is thus a cumulative trust model
- When any user signs another's key, he or she becomes an introducer of that key.
- As this process goes on, it establishes a web of trust

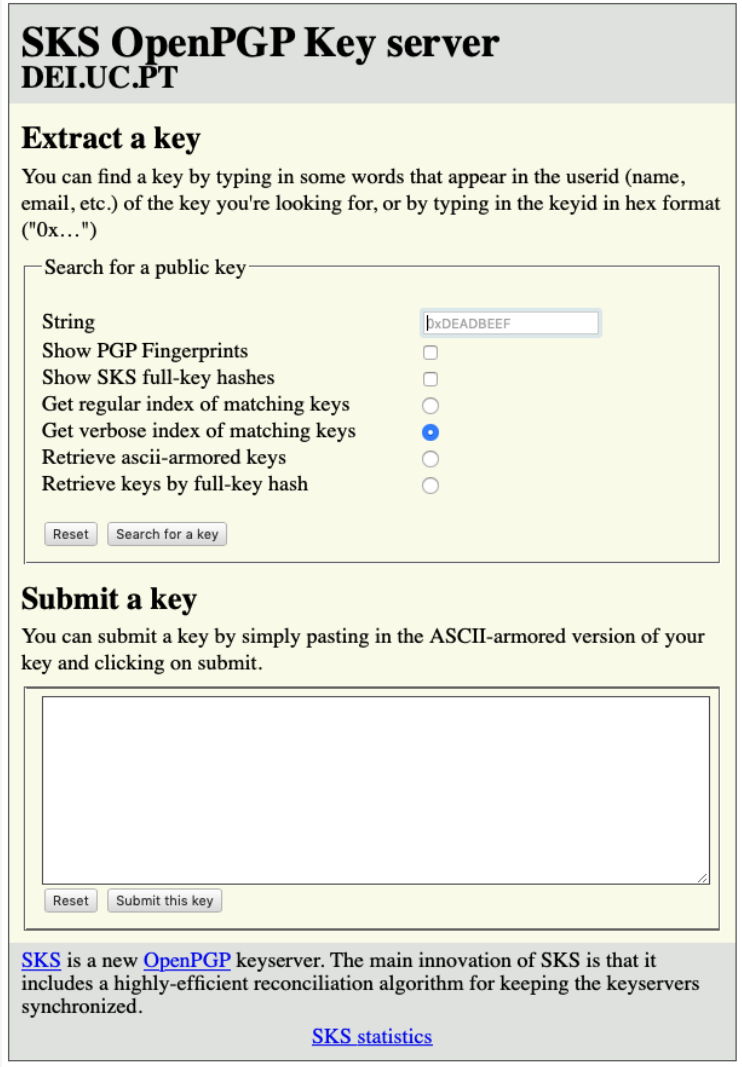


Pretty Good Privacy (PGP)

- Alternative email security protocol which has essentially the same functionality as S/MIME
- PGP was created by Phil Zimmerman and implemented as a product first released in 1991
- It was made available free of charge and became popular for personal use
- The initial protocol was proprietary and used some encryption algorithms with intellectual property restrictions

- OpenPGP was developed as a new standard protocol based on PGP version 5.x
- OpenPGP is defined in RFC 4880 and RFC 3156
- There are two significant differences between S/MIME and OpenPGP:
  - Key Certification (X.509 in S/MIME, versus *web of trust* with OpenPGP public keys)
  - Key Distribution (Certification Authorities versus OpenPGP *public key servers*)
- NIST 800-177 recommends the use of S/MIME rather than PGP because of the greater confidence in the CA system of verifying public keys

PGP Public Key servers



Domain Name System (DNS)

- A directory lookup service that provides a mapping between the name of a host on the Internet and its numeric IP address
- Is essential to the functioning of the Internet
- Is used by MUAs and MTAs to find the address of the next hop server for mail delivery (MTAs query DNS for MX Resource Records of the recipient's domain)
- Is comprised of four elements:
  - ✓Domain name space
  - ✓DNS database
  - ✓Name servers
  - ✓Resolvers

DNSSEC (DNS Security Extensions)

- Provides **end-to-end protection** through the use of digital signatures that are created by responding zone administrators and verified by a recipient's resolver software
- Avoids the need to trust intermediate name servers and resolvers that cache or route the DNS records originating from the responding zone administrator before they reach the source of the query
- Consists of a set of **new resource record types** and **modifications to the existing DNS protocol**
- Defined in these documents:
  - RFC 4033, DNS Security Introduction and Requirements
  - RFC 4034, Resource Records for the DNS Security Extensions
  - RFC 4035, Protocol Modifications for the DNS Security Extensions

DNSSEC Operation

- In essence, DNSSEC is designed to protect DNS clients from accepting forged or altered DNS resource records
- It does this by using digital signatures to provide:
  - **Data origin authentication**: ensures that data has originated from the correct source
  - **Data integrity verification**: ensures that the content of a RR has not been modified
- The DNS zone administrator digitally signs every RR set (RRset) in the zone, and publishes this collection of digital signatures, along with the public key, in DNS itself
- Trust in the public key of the source is established by starting from a trusted zone and establishing the chain of trust down to the current source of response through successive verifications of signature of the public key of a child by its parent
  - The public key of the trusted zone is called the *trust anchor*

DANE

DNS-Based Authentication of Named Entities

Is a protocol to allow X.509 certificates, commonly used for Transport Layer Security (TLS) to be bound to DNS names using DNSSEC

It is proposed in RFC 6698 as a way to authenticate TLS client and server entities without a certificate authority (CA)

The purpose of DANE is to **replace reliance on the security of the CA system with reliance on the security provided by DNSSEC**

Sender Policy Framework (SPF)

- SPF is the standardized way for a sending domain to **identify and assert the mail senders for a given domain**
- SPF addresses a problem with the current email infrastructure: any host can use any domain name for various identifiers in the mail header (a major cause of *spam*).
- It provides a protocol by which admins can authorize hosts to use their domain names in the "MAIL FROM" or "HELLO" identities
- SPF works by checking a sender's IP address against the policy encoded in any SPF record found at the sending domain
- This means that SPF checks can be applied before the message content is received from the sender

SPF mechanisms and modifiers

Table 19.7 Common SPF Mechanisms and Modifiers

(a) SPF Mechanisms

Tag	Description
ip4	Specifies an IPv4 address or range of addresses that are authorized senders for a domain.
ip6	Specifies an IPv6 address or range of addresses that are authorized senders for a domain.
mx	Asserts that the listed hosts for the Mail Exchange RRs are also valid senders for the domain.
include	Lists another domain where the receiver should look for an SPF RR for further senders. This can be useful for large organizations with many domains or sub-domains that have a single set of shared senders. The include mechanism is recursive, in that the SPF check in the record found is tested in its entirety before proceeding. It is not simply a concatenation of the checks.
all	Matches every IP address that has not otherwise been matched.

(b) SPF Mechanism Modifiers

Modifier	Description
+	The given mechanism check must pass. This is the default mechanism and does not need to be explicitly listed.
–	The given mechanism is not allowed to send email on behalf of the domain.
~	The given mechanism is in transition and if an email is seen from the listed host/IP address, that it should be accepted but marked for closer inspection.
?	The SPF RR explicitly states nothing about the mechanism. In this case, the default behavior is to accept the email. (This makes it equivalent to '+' unless some sort of discrete or aggregate message review is conducted).

SPF records (example for domain *dei.uc.pt*)

```
jgranjal$ nslookup
> set query=txt
> dei.uc.pt
Server:10.0.1.254
Address:10.0.1.254#53

Non-authoritative answer:
dei.uc.pt text = "v=spf1 ip4:193.137.203.253 ip4:193.137.203.234 mx ?all"
dei.uc.pt text = "U.C. Dep. Eng. Informatica"
dei.uc.pt text = "MS=ms12952510"

>
```

SPF operation

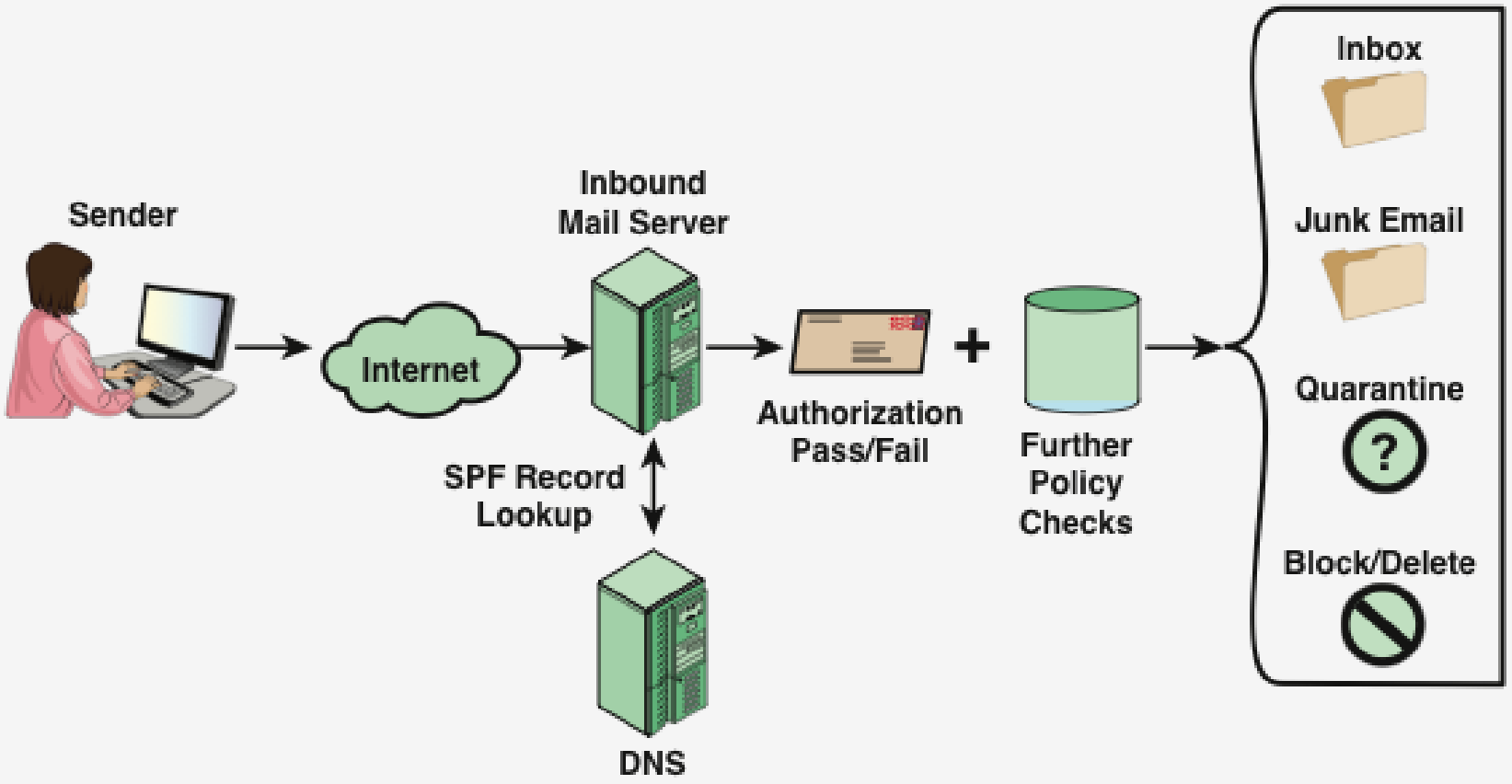
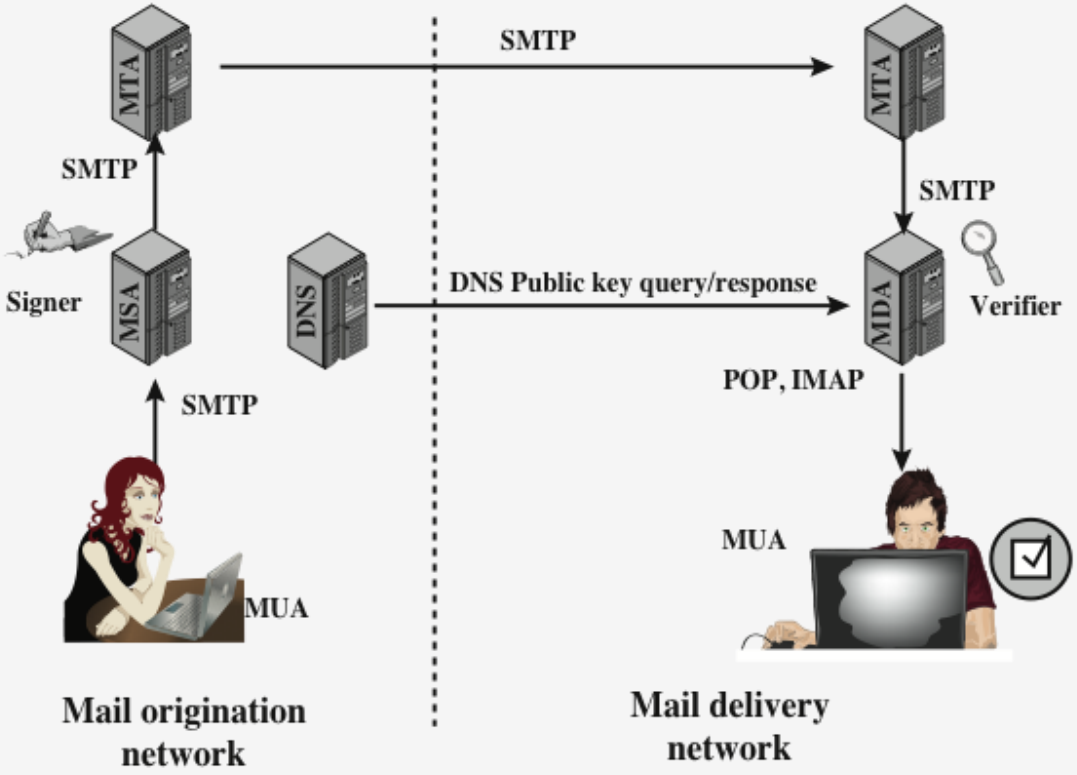


Figure 19.9 Sender Policy Framework Operation

DomainKeys Identified Mail (DKIM)

- A specification for cryptographically signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream
- Message recipients can verify the signature by querying the signer's domain directly to retrieve the appropriate public key and can thereby confirm that the message was attested to by a party in possession of the private key for the signing domain
- Proposed Internet Standard RFC 6376
- Has been widely adopted by a range of e-mail providers and Internet Service Providers (ISPs)

DKIM deployment example



DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent

Figure 19.10 Simple Example of DKIM Deployment

DMARC (Domain-Based Message Authentication, Reporting and Conformance)

- Allows email senders to specify **policy** on **how their mail should be handled**, the types of reports that receivers can send back, and the frequency those reports should be sent
- DMARC tells receivers if SPF or DKIM are in use at the sender domain, standardizes how receivers perform email authentication using SPF and DKIM
- It is defined in RFC 7489 (*Domain-based Message Authentication, Reporting, and Conformance,* March 2015)
- DMARC reporting provides the sender's feedback on their SPF and DKIM anti-spam policies and enable senders to advice receivers, via DNS, whether mail purporting to come from the sender should be delivered, flagged or discarded
- May also state that the From: address needs to be aligned with an Authenticated Identifier from DKIM (signing domain) or SPF (authenticated domain/envelope information)
- Two type of reports are sent: **aggregate reports** and **forensic reports**

DMARC (example report)

no-reply@master.cleanmx.pt

Tue, Feb 7, 10:34 AM (8 days ago) to postmaster

A message claiming to be from you has failed the published DMARC policy for your domain.

Sender Domain: example.com

Sender IP Address: 139.59.190.159

Received date: Tue, 07 Feb 2023 10:34:16 +0000

SPF Alignment: no

DKIM Alignment: no

DMARC Results: None, Accept

------ This is a copy of the headers that were received before the error was detected.

X-DKIM-Failure: bodyhash_mismatch

DMARC functional flow

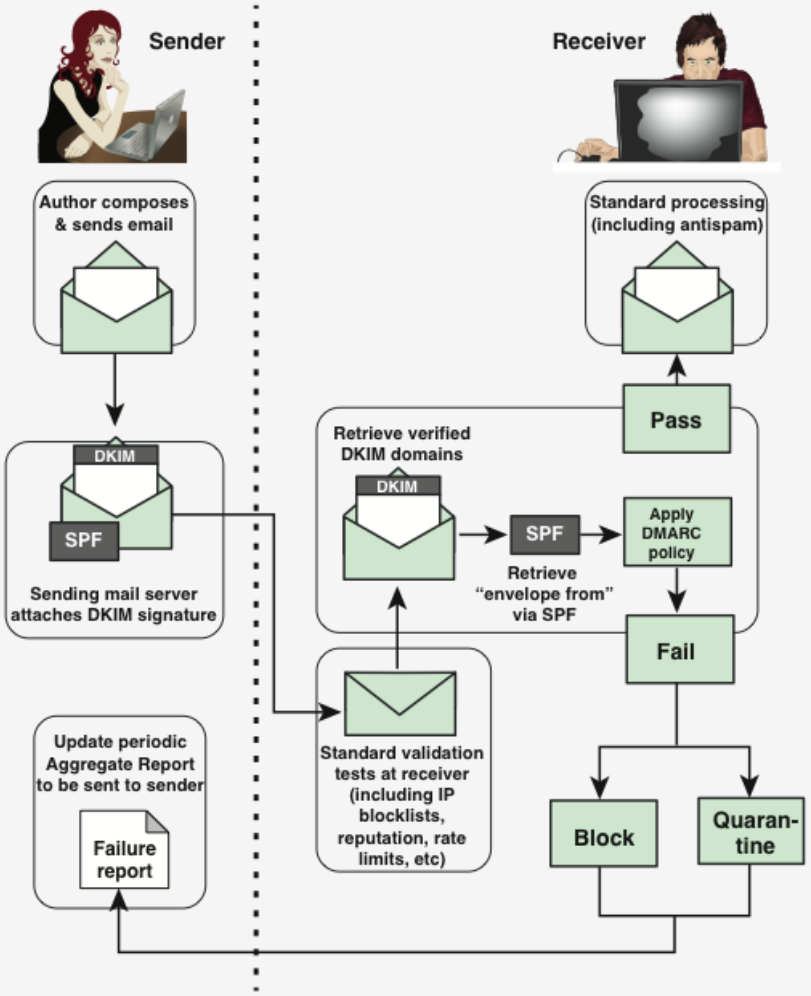


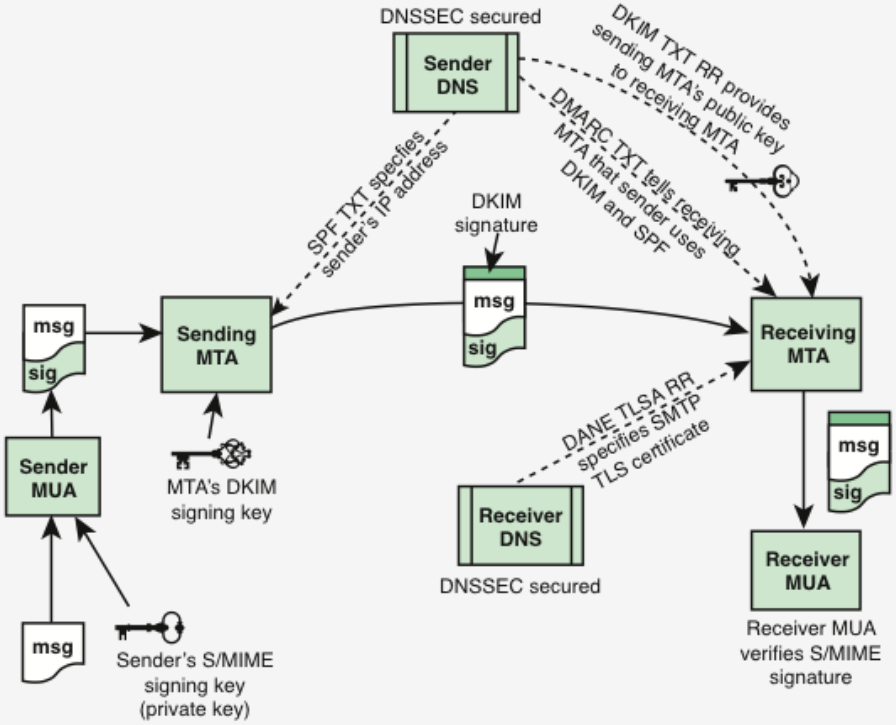
Figure 19.12 DMARC Functional Flow

Using SPF, DKIM and DMARC (Example from Google Mail)

Original Message

Message ID	<20210219124947.192047sja69pg3qj@mail.dei.uc.pt>
Created at:	Fri, Feb 19, 2021 at 12:49 PM (Delivered after 2 seconds)
From:	Jorge Granjal <jgranjal@dei.uc.pt>
To:	jgranjal@gmail.com
Subject:	Mensagem de teste
DKIM:	'PASS' with domain dei.uc.pt Learn more

Interaction between Counter Threat Protocols



DANE = DNS-based Authentication of Named Entities
DKIM = DomainKeys Identified Mail
DMARC = Domain-based Message Authentication, Reporting, and Conformance
DNSSEC = Domain Name System Security Extensions
SPF = Sender Policy Framework
S/MIME = Secure Multi-Purpose Internet Mail Extensions
TLSA RR = Transport Layer Security Authentication Resource Record

Figure 19.4 The Interrelationship of DNSSEC, SPF, DKIM, DMARC, DANE, and S/MIME for Assuring Message Authenticity and Integrity

Review Questions

What are the four principle services provided by S/MIME?

S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, and provides authentication, confidentiality, compression and email compatibility

What is the basic difference between X.509 and PGP in terms of key hierarchies and key trust?

In X.509 there is a hierarchy of Certificate Authorities. Another difference is that in X.509 users will only trust Certificate Authorities while in PGP users can trust other users.

Summary

Internet mail architecture

✓ Email components

✓ Email protocols

Email formats

✓ RFC 5322

✓ Multipurpose internet mail extensions

Email threats and comprehensive email security

Pretty good privacy

DNSSEC

✓ Domain name system

✓ DNS security extensions

S/MIME

✓ Operational description

✓ S/MIME message content types

✓ Cryptographic algorithms

✓ Certificate processing

Enhanced security services

✓ DNS-based authentication of named entities

✓ SPF

✓ DomainKeys Identified mail

- Email threats
- DKIM strategy
- Functional flow

PGP in the movies..

A subject of controversy, Snowden has been variously called a hero, a whistleblower, a dissident, a traitor, and a patriot. His disclosures have fueled debates over mass surveillance, government secrecy, and the balance between national security and information privacy.

https://www.wired.com/2014/10/laura-poitras-crypto-tools-made-snowden-film-possible/

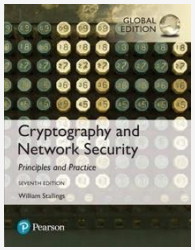
ANDY GREENBERG SECURITY 10.15.14 06:30 AM

LAURA POITRAS ON THE CRYPTO TOOLS THAT MADE HER SNOWDEN FILM POSSIBLE

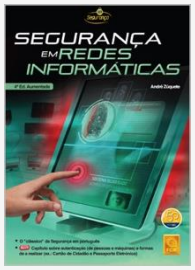
```
SUNDAY Nov 1 2014 (RELEASE)
citizenfour@barbican.UK:~$ cat message.asc

-----BEGIN PGP MESSAGE-----
Version: GnuPg v1

hQIMA9fS04ftZGAQ/6AuxLCM1z81scsvTJWEVjuY1wd0o9SoQfo2N7/Dh4ld1nSP
vfw3Naqpl9EmV7p2J6A+9jLG405Kp46GS3fgD63Y3cDUzwawe@mGBnWvMfbN
og+xzlBGC729QqwUWUP5L2eMbjaa5eNOqYDTP6113Xnve1GQil6NY64UtOn7b
RW6ZY4KQQurEDWARDSNOWDENc005i3IyyznUsRSUTscW79973HMSAdUmjRp
Li6uDFXzrYeCR7zy18b+FX51NMVovpN+vrOpu7RPVY3rx6Q5NH43Cs9GNEXqfhy
VsTz8x46WZbkvuxPGAyJlhMeCITIZENFOURizL1HNLHGhBd4hMTYwIV50qGa
3cznaSNr3HvGSCa18b+t9BCtLvnbpAtell2xo3bErfWByQNVlYMWrxXCEzNCF9NE
FM5iExMCFEL5uXZHZTTD10uy/ii3m/aLAURAPOITRASfilmJAhMzQhG4YzRYwjU
QeViiteG/pgsfnFXtsQTD2FgG7nbpAtell2xo3bErfWi4VK6sG35uEQbogZzwc04aS
EyIXhXfmoxoSU2ITEyIUg08FrMITEzlUo6NNLQ0ZXZUBlemnaQv7TpkqZ98yo2ITE
EXtyByvNb0HCEzNCHJJofFObSb66fvHhAuaTGYZR7VPftmMJpuvfxnEsOe2Wm7
kOgZtTZHKVrwMC3giOQd92EhMTEhFiS4wKKl+dChGtlVZCghMTIhID7tEbTWKX
nz/IflCYkuSN1AF/5A6k7nTA4eKlGnwm/2LQk5Te+/UD/NOeKk2+uGV5AghMTMS
3miExMCEWHBuJ2fA4b7RtRCExMiF+giEwlSiug/DOxh4CL4Xa/2tliSExMSFYapxoT
9yExMCHLXvw2COlkOJeTRa3FRSExMCEhMzMhcBh6H8jvHCsRbriYmiYr5d+dic3
/5twBuHJ3qkQ/pUWHel2Z5/ql3YT2oyExMSGjMgTU==3rvp

-----END PGP MESSAGE-----

citizenfour@barbican.UK:~$ gpg --decrypt message.asc
```

Bibliography

Cryptography and network security, Stallings, Pearson, 2017, Chapter 16: Electronic Mail Security



Segurança em Redes Informáticas, Capítulo 3: Gestão de Chaves Públicas



Segurança Prática em Sistemas e Redes com Linux, Capítulo 2: Segurança em Correio Eletrónico