

Email Security

Kai Bu

kaibu@zju.edu.cn

<http://list.zju.edu.cn/kaibu/netsec2022>

Email?

Electronic Mail

- for exchanging electronic messages



Gmail



Yahoo



GoDaddy

Aol Mail.

Aol Mail



Hotmail



Outlook



Office365



Exchange



iCloud



GMX



Zoho



FastMail

<https://tinyurl.com/yne3hdc7>

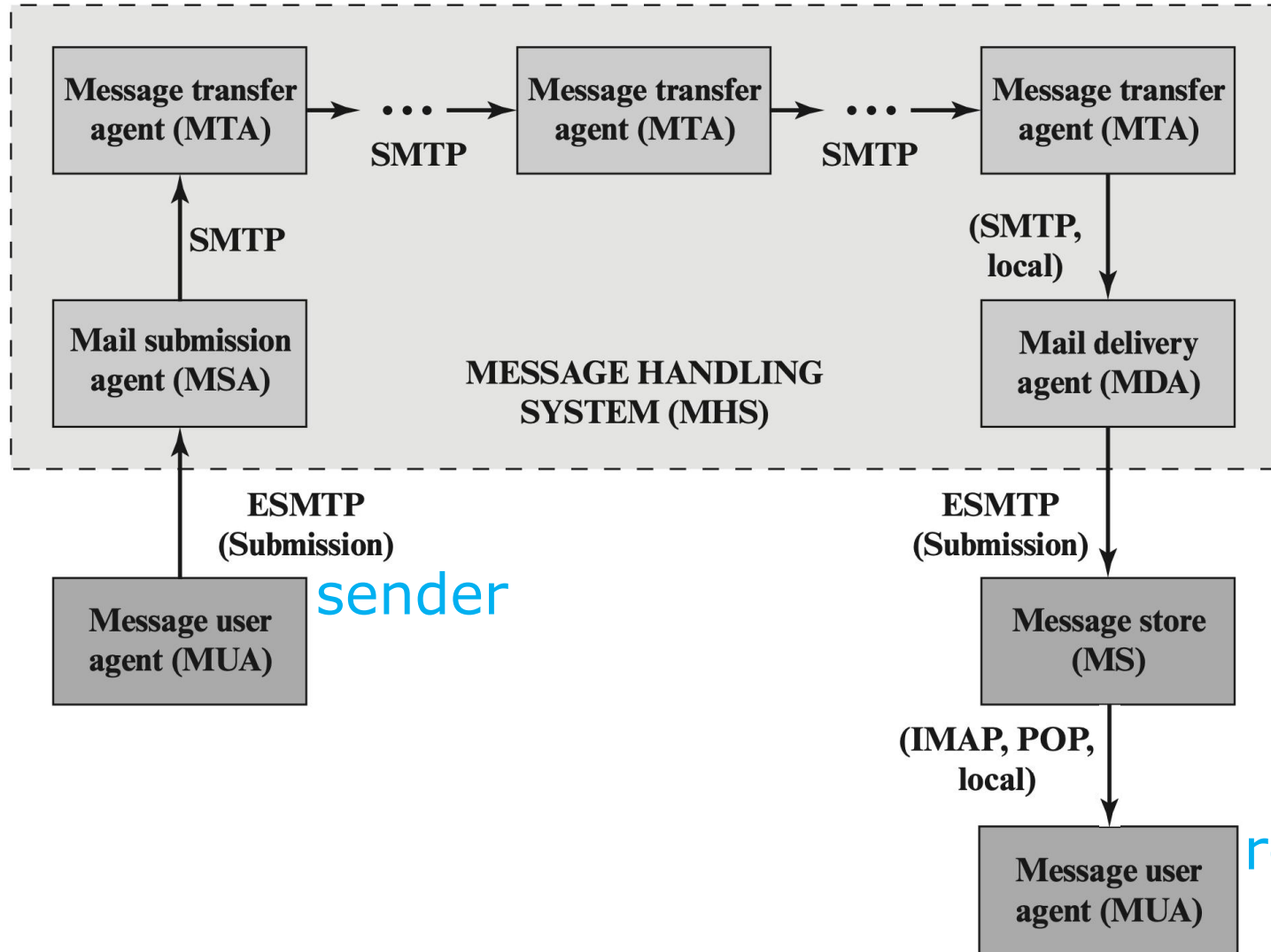
Email Architecture

- **MUA: Message User Agent**
hosted on a client email program or a local network email server;
sender MUA formats a message and performs initial submission into MHS via a MSA (Mail Submission Agent);
recipient MUA processes received email for storage and/or display to the recipient user
- **MHS: Message Handling Service**

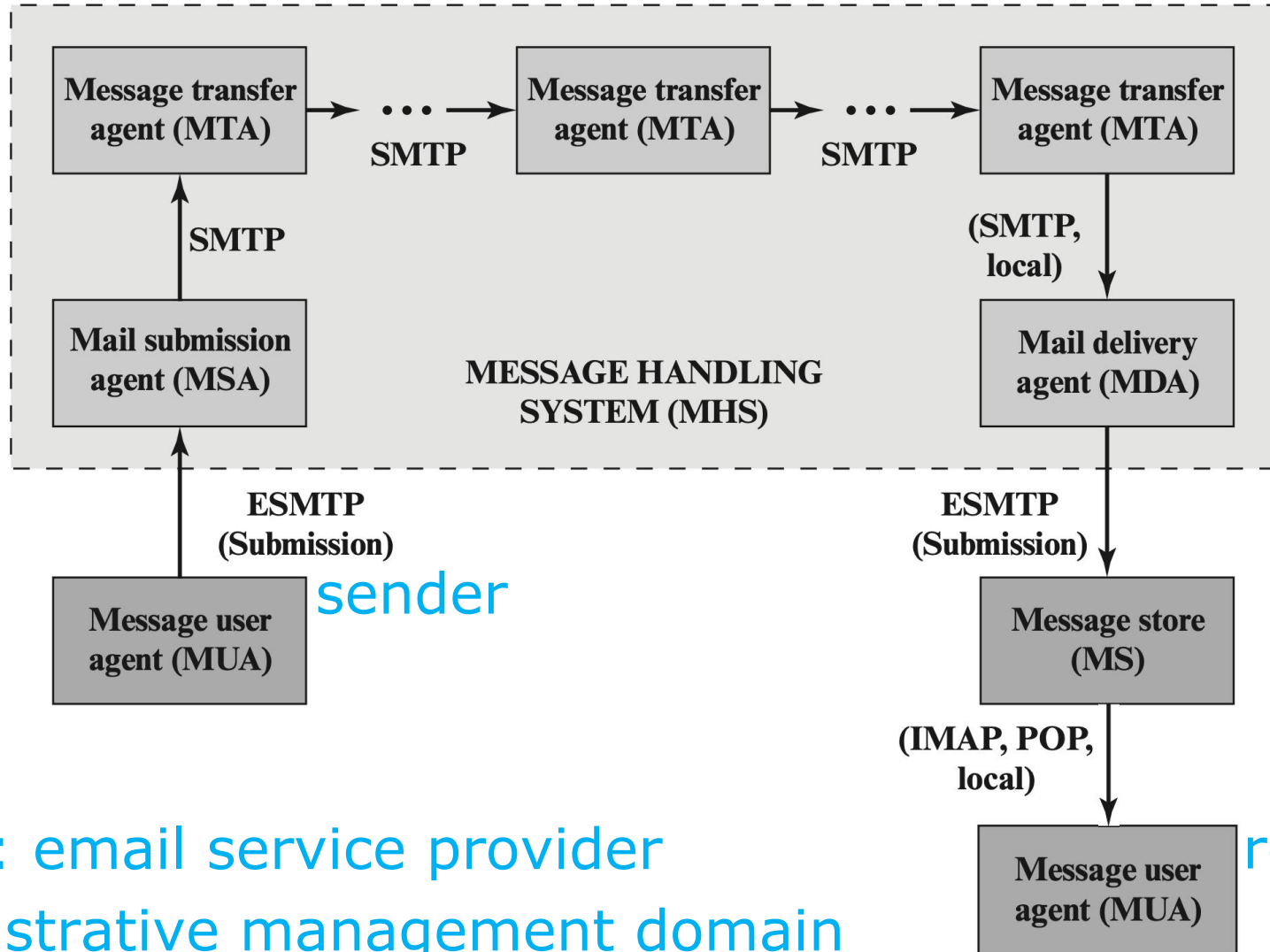
Email Architecture

- **MUA: Message User Agent**
- **MHS: Message Handling Service**
composed of MTAs (Message Transfer Agents);
accepts a message from sender and delivers it to one or more recipients;
creates a virtual MUA-to-MUA environment;

Email Architecture



Email Architecture



ADMD: email service provider
administrative management domain

Email Protocol

- **Type 1: SMTP**

Simple Mail Transfer Protocol
move messages through the Internet
from source to destination;

- **Type 2: IMAP and POP**

Internet Mail Access Protocol;
Post Office Protocol;
transfer messages between mail
servers

Email Format

- **RFC 5322**

view messages as having an envelope and contents;

envelope contains whatever information needed to accomplish transmission and delivery;

contents compose the object to be delivered to the recipient;

Email Format

- **RFC 5322**

view messages as having an envelope and contents;

RFC 5322 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;

Email Format

- **RFC 5322**

header + body

seperated by a blank line in ASCII form

Date: October 8, 2009 2:15:49 PM EDT

From: "William Stallings" <ws@shore.net>

Subject: The Syntax in RFC 5322

To: Smith@Other-host.com

Cc: Jones@Yet-Another-Host.com

Hello. This section begins the actual message body, which is delimited from the message heading by a blank line.

Email Format

- **MIME**

Multipurpose Internet Mail Extensions extend RFC 5322 with enhancements;

Email Format

- **MIME**

- Define five new header fields to provide information about message content
- Standardize representations that support multimedia electronic mail
- Define transfer encodings that enable the conversion of any content format into a form that is protected from alteration by the mail system

MIME Header

- MIME-Version
- Content-Type
- Content-Transfer-Encoding
- Content-ID
- Content-Description

MIME Header

- MIME-Version

parameter value should be 1.0,
indicating that the message conforms
to RFCs 2045 and 2046

MIME Header

- Content-Type

describe the data contained in the body with sufficient detail, so that the recipient agent can pick an appropriate agent or mechanism to represent the data to the recipient or deal with the data in an appropriate manner

MIME Header

- Content-Transfer-Encoding
indicate the type of information used to
represent message body,
should be acceptable for mail transport

MIME Header

- **Content-ID**
identify MIME entities uniquely in multiple contexts
- **Content-Description**
text description of the object with body;
useful when the object is not readable
(e.g., audio data)
- both fields are optional and may be ignored by the recipient implementation

MIME Content Type

Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN μ -law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript format.
	octet-stream	General binary data consisting of 8-bit bytes.

MIME Transfer Encoding

- Provide reliable delivery across the largest range of environments

7 bit	The data are all represented by short lines of ASCII characters.
8 bit	The lines are short, but there may be non-ASCII characters (octets with the high-order bit set).
binary	Not only may non-ASCII characters be present but the lines are not necessarily short enough for SMTP transport.
quoted-printable	Encodes the data in such a way that if the data being encoded are mostly ASCII text, the encoded form of the data remains largely recognizable by humans.
base64	Encodes data by mapping 6-bit blocks of input to 8-bit blocks of output, all of which are printable ASCII characters.
x-token	A named nonstandard encoding.

Email Security?

Email Security Threats

- Authenticity-related Threats
- Integrity-related Threats
- Confidentiality-related Threats
- Availability-related Threats

Email Security Threats

- Authenticity-related Threats
could result in unauthorized access to
an email system

Email Security Threats

- Integrity-related Threats
could result in unauthorized
modification of email content

Email Security Threats

- Confidentiality-related Threats
could result in unauthorized disclosure
of sensitive information

Email Security Threats

- Availability-related Threats
could prevent end users from being able to send or receive email

Threats and Mitigations

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 servers. 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 servers. Use of end-to-end email encryption.
Unsolicited Bulk Email (UBE) (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.

Authenticity and Integrity

DANE = DNS-based Authentication of Named Entities

DKIM = DomainKeys Identified Mail

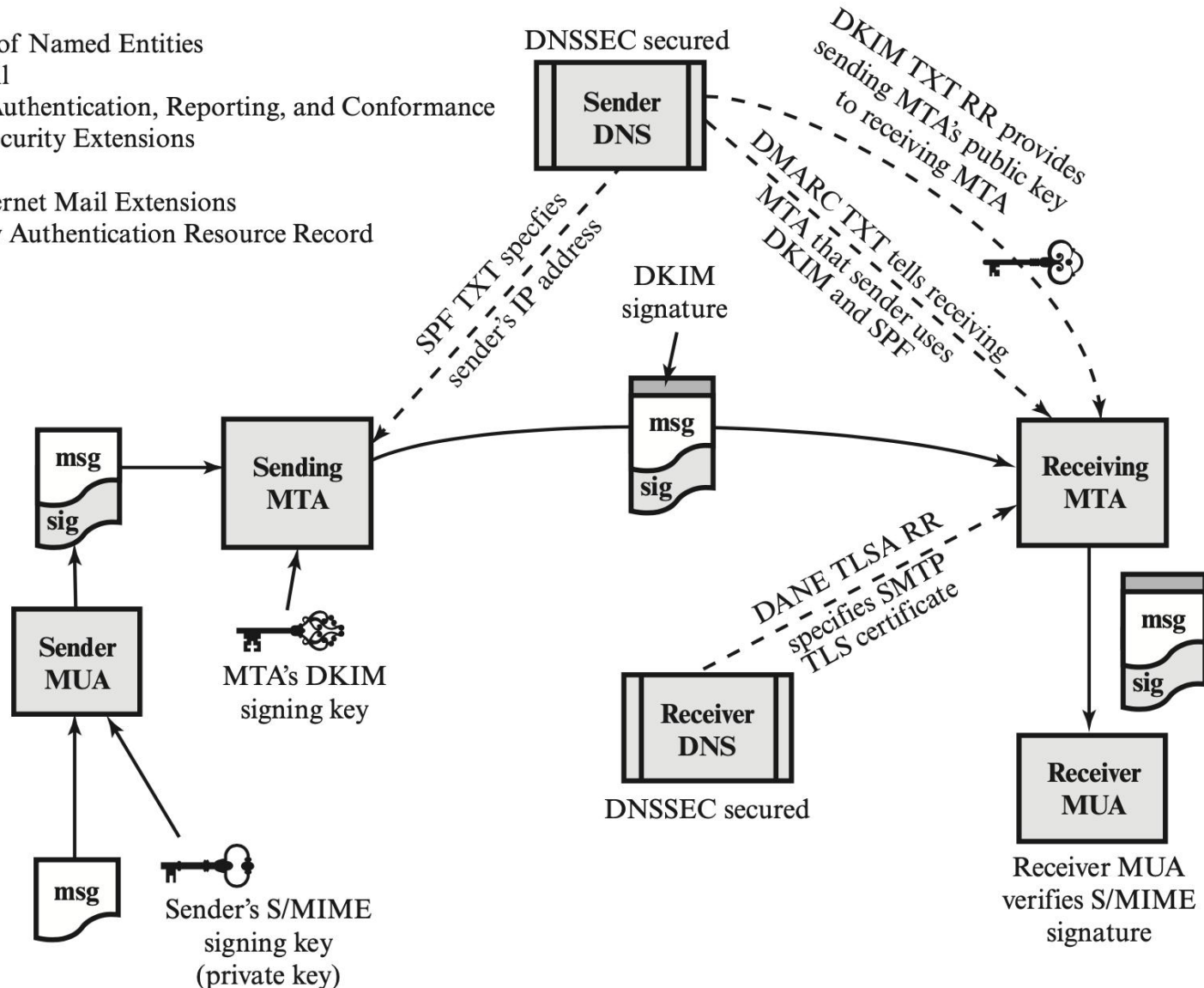
DMARC = Domain-based Message Authentication, Reporting, and Conformance

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



S/MIME

Secure/Multipurpose Internet Mail Extension

S/MIME

- Authentication
- Confidentiality
- Compression
- Email compatability

S/MIME

Function	Typical Algorithm	Typical Action
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 included with the 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.
Email compatibility	Radix-64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

Authentication

- 1. the sender creates a message
- 2. use SHA-256 to generate a 256-bit message digest
- 3. encrypt the message digest with RSA using the sender's private key; append the result as well as the signer's identity to the message
- 4. the receiver uses RSA with the sender's public key to decrypt, recover, and verify the message digest

Confidentiality

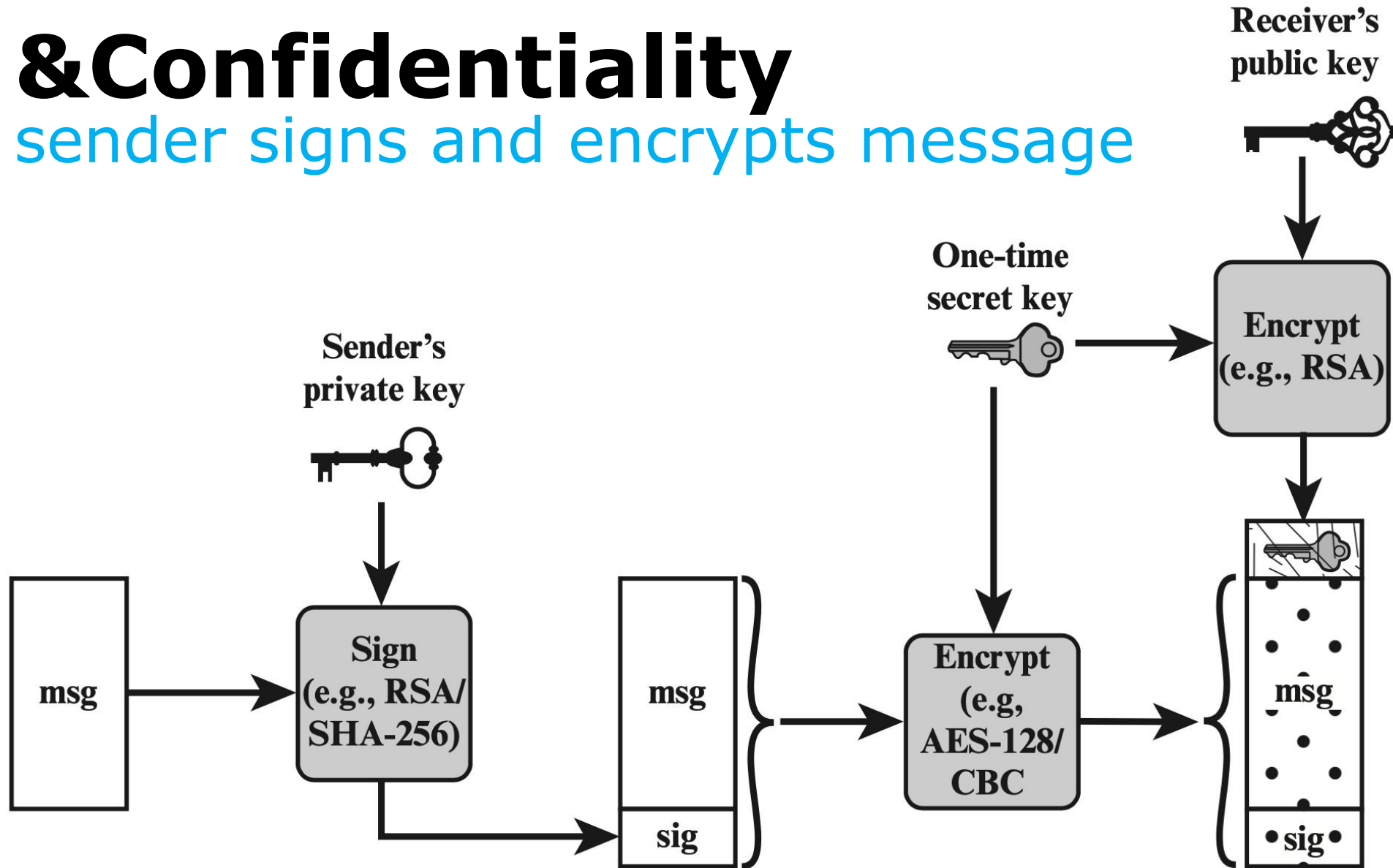
- 1. the sender creates a message and a random 128-bit number as a content-encryption key for this message only
- 2. encrypt the message using the content-encryption key
- 3. encrypt the content-encryption key with RSA using the receiver's public key and append it to the message

Confidentiality

- 4. The receiver uses RSA with its private key to decrypt and recover the content-encryption key
- 5. use the content-encryption key to decrypt the message

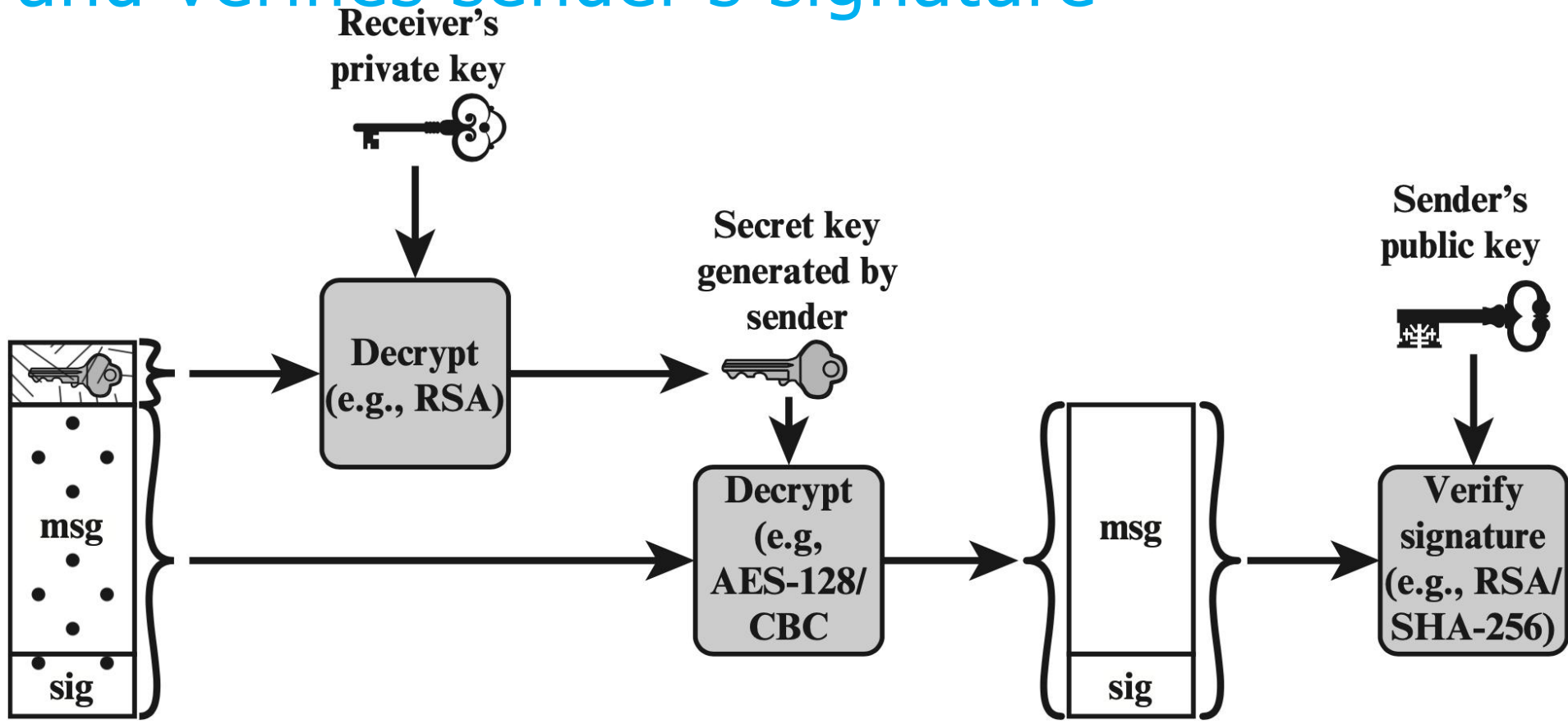
Authentication & Confidentiality

sender signs and encrypts message



Authentication & Confidentiality

receiver decrypts message
and verifies sender's signature



Content Type

- Data

inner MIME-encoded message content;
may be encapsulated in the following
types;

- SignedData
- EnvelopedData
- CompressedData

Content Type

- **Data**
inner MIME-encoded message content;
- **SignedData**
digital signature of a message
- **EnvelopedData**
encrypted data of any type, and
encrypted content-encryption keys for
one or more recipients;
- **CompressedData**
data compression of a message

PGP

Pretty Good Privacy

same functionality as S/MIME

free and popular for personal use

PGP

Differences from S/MIME:

- Key Certification

S/MIME uses X.509 certificates issued by CA or delegated authorities;

OpenPGP allows users to generate their own OpenPGP public and private keys, and then solicit signatures for their public keys from known individuals or organizations

- Key Distribution

PGP

Differences from S/MIME:

- Key Certification
- Key Distribution

OpenPGP does not include the sender's public key with each message; recipient needs to separately obtain that from TLS-protected websites or OpenPGP public key servers; no vetting of OpenPGP keys, users decide whether to trust on their own

PGP

Differences from S/MIME:

- Key Certification
- Key Distribution
- 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

What if CA is compromised?

What if CA is compromised?

steal CA's private key
issue false certificates

DANE!

DNS-based Authentication of Named Entities
allow X.509 certificates to be bound to
DNS names using DNSSEC

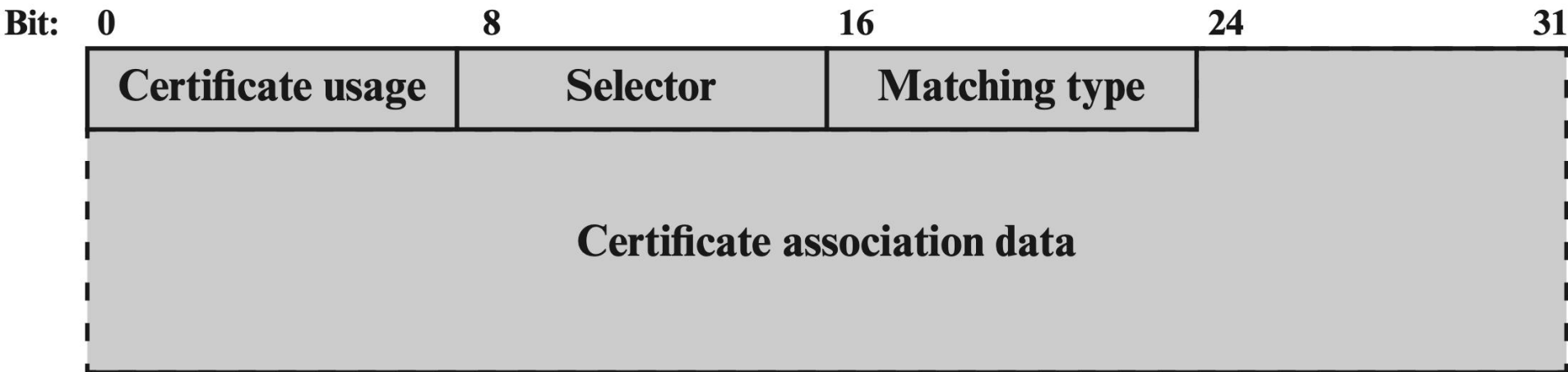
TLSA Record

- TLS Authentication record
- A new DNS record type defined by DANE
- Used for a secure method of authenticating SSL/TLS certificates

TLSA Record

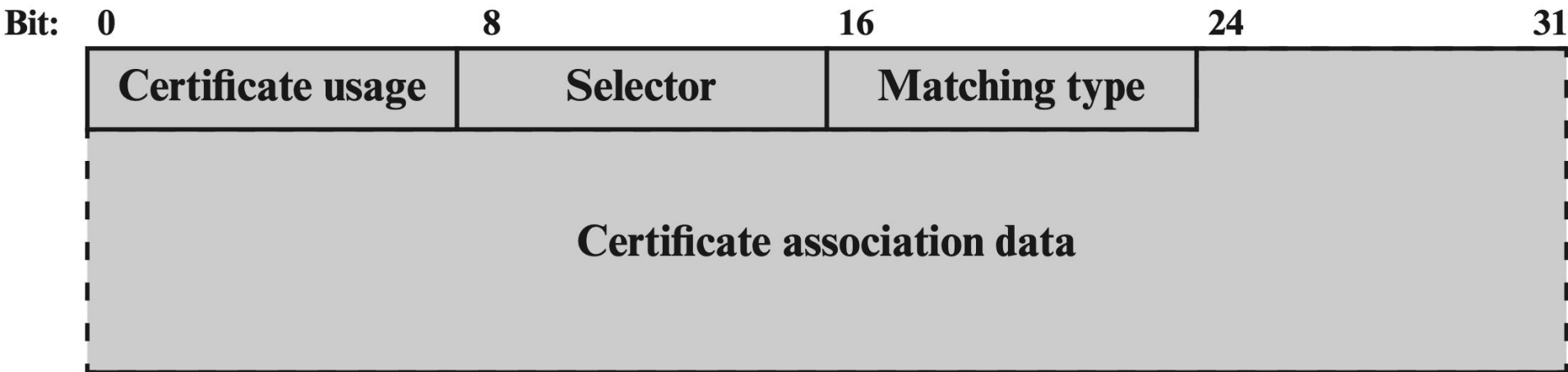
- Specify constraints on which CA can vouch for a certificate, or which specific PKIX [Public Key Infrastructure (X.509)] end-entity certificate is valid
- Specify that a service certificate or a CA can be directly authenticated in the DNS itself

TLSA Record



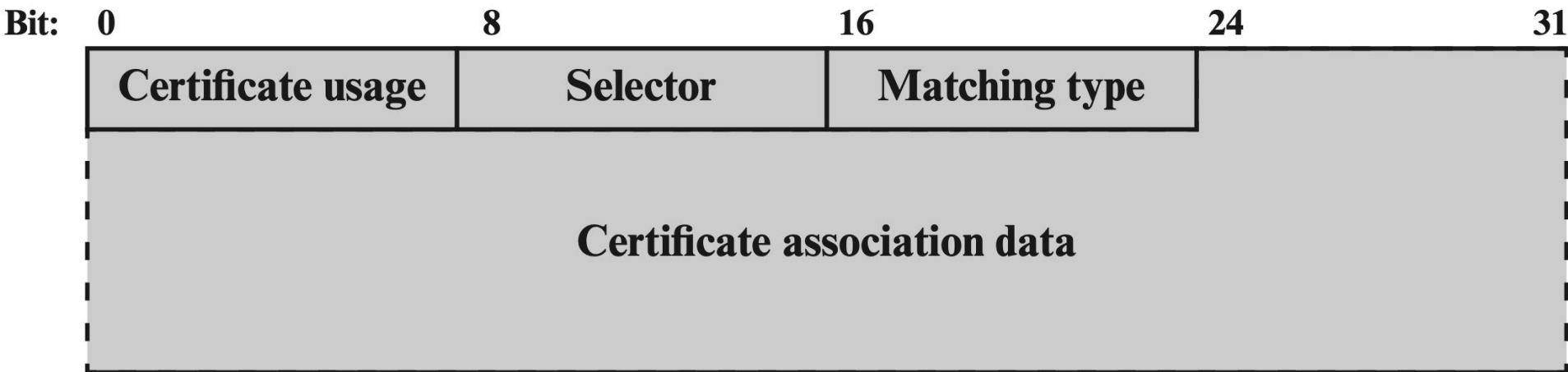
- format of TLSA as it is transmitted to a requesting entity

TLSA Record



- **Certificate Usage**
define four different usage models,
to accommodate users who require
different forms of authentication

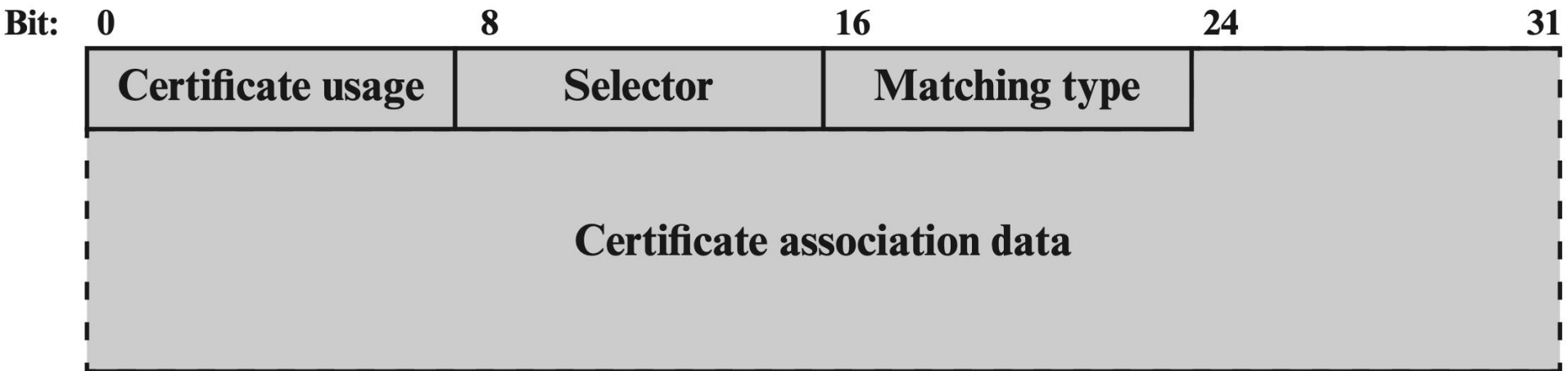
TLSA Record



- **Certificate Usage**

PKIX-TA (CA constraint): Specifies which CA should be trusted to authenticate the certificate for the service

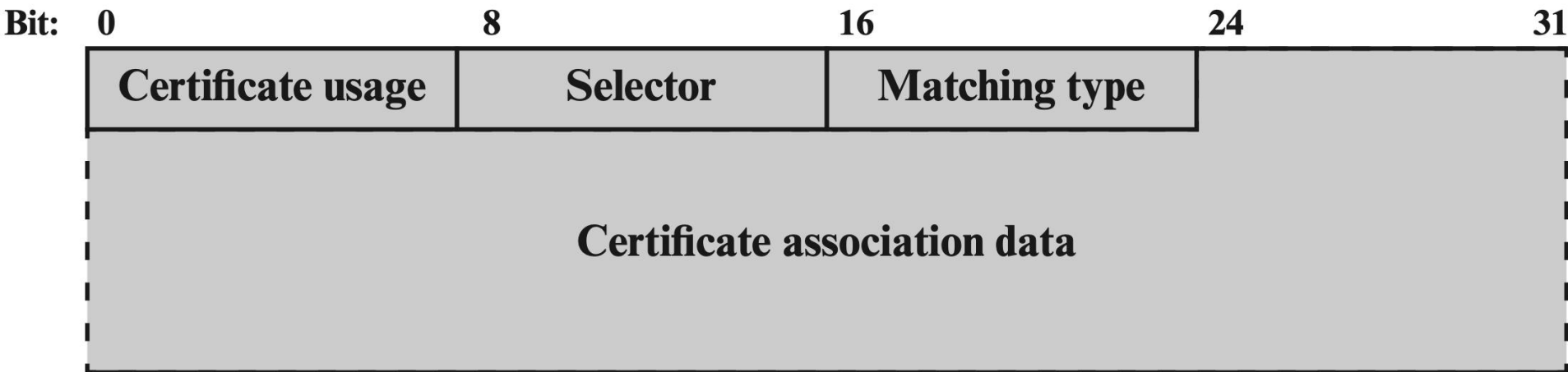
TLSA Record



- **Certificate Usage**

PKIX-EE (service certificate constraint):
Defines which specific end entity service certificate should be trusted for the service

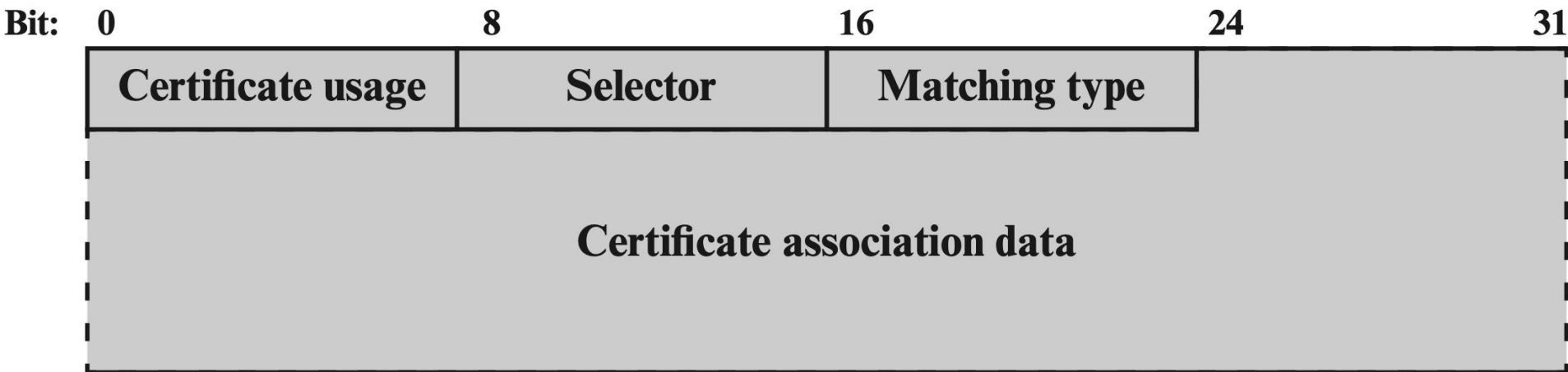
TLSA Record



- **Certificate Usage**

DANE-TA (trust anchor assertion):
Specifies a domain-operated CA to be used as a trust anchor

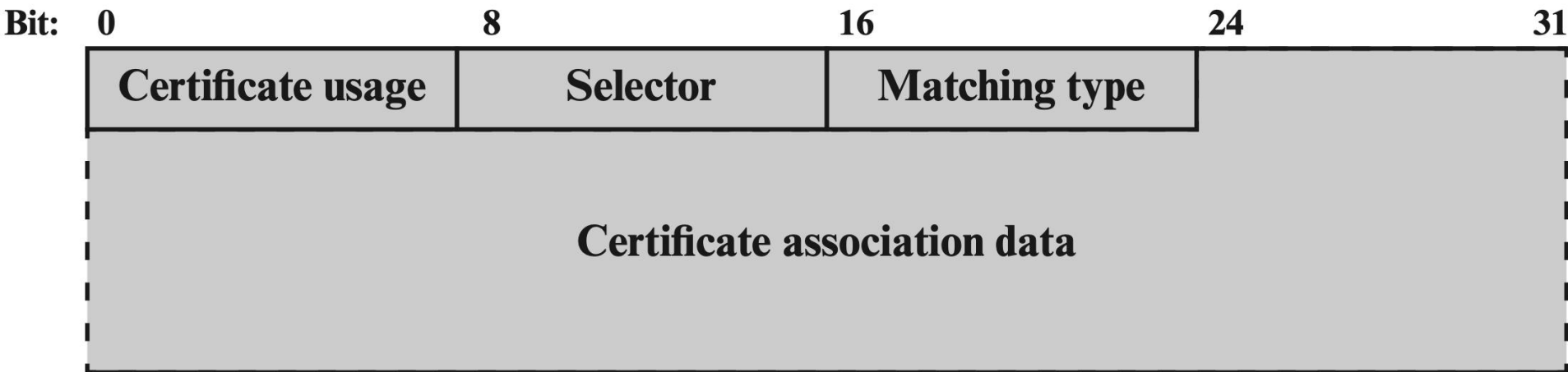
TLSA Record



- **Certificate Usage**

DANE-EE (domain-issued certificate):
Specifies a domain-operated CA to be
used as a trust anchor

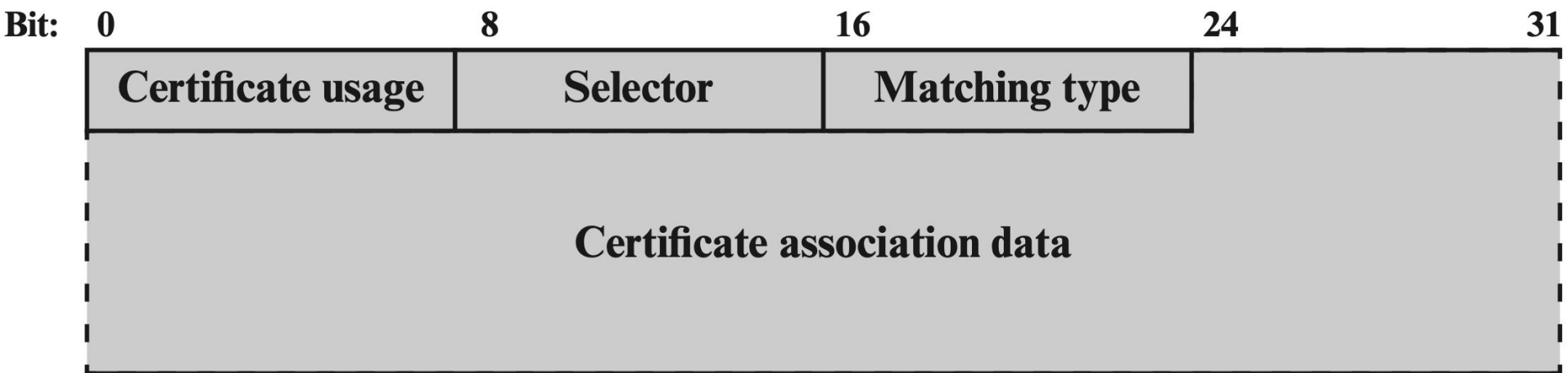
TLSA Record



- **Selector**

indicate whether the full certificate will be matched or just the value of the public key

TLSA Record

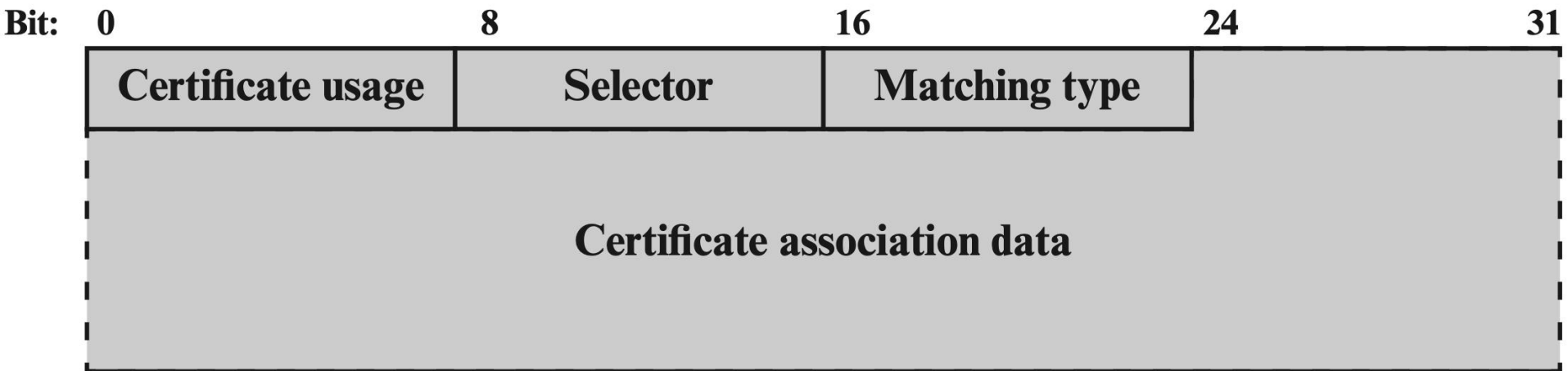


- Matching Type

indicate how the match of the certificate is made:

exact match, SHA-256 hash match, or SHA-512 hash match

TLSA Record



- **Certificate Association Data**
represent the raw certificate data in hex format

DANE for SMTP

- Targeted vulnerabilities:
attackers can strip away the TLS capability advertisement and downgrade the connection to not use TLS;
TLS connections are often unauthenticated (e.g., the use of self-signed certificates as well as mismatched certificates is common)

DANE for SMTP

- A domain can use the presence of TLSA as an indicator that encryption must be performed, thus preventing malicious downgrade
- A domain can authenticate the certificate used in the TLS connection setup using a DNSSEC-signed TLSA

DANE for S/MIME

- Introduce a SMIMEA DNS record to associate certificates with DNS domain names
- Help MUAs to deal with domain names as specified in email addresses in the message body (rather than domain names specified in the outer SMTP envelope – purpose of TLSA)

Remember IP spoofing?

a host can use any domain name in header,
not just the domain name where the host
is located

SPF

- Sender Policy Framework

ADMDs (Administrative Management Domains) publish SPF records in DNS specifying which hosts/IP-addresses are permitted to use their names; receivers use the published SPF records to test the authorization of sending Mail Transfer Agents (MTAs) using a given “HELO” or “MAIL FROM” identity during a mail transaction;

DKIM

- DomainKeys Identified Mail

sign email message by a private key of the administrative domain from which the email originates;
at the receiving end, the MDA can access the corresponding public key via a DNS and verify the signature, thus authenticating that the message comes from the claimed administrative domain

DKIM

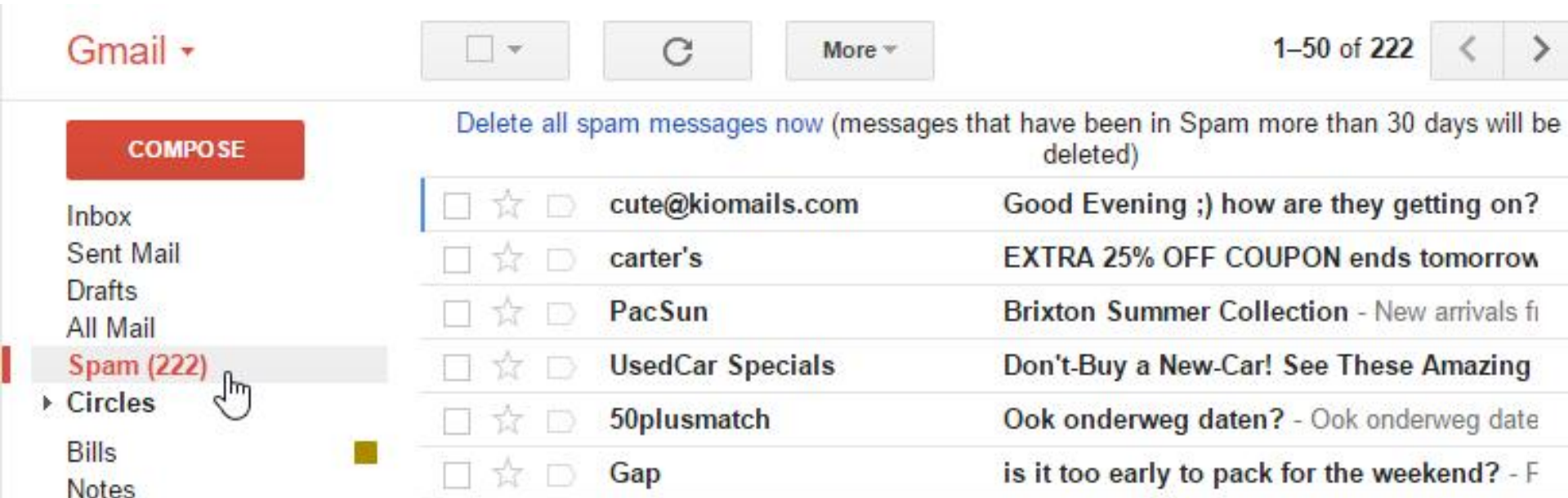
- Difference from S/MIME and PGP
S/MIME and PGP use the sender's private key to sign the content of the message;
DKIM uses the private key of the domain where the sender locates;

Email protected per se

What if Email is exploited?

Spam

- Unwanted email advertisements



The screenshot shows a Gmail interface. On the left, the navigation sidebar includes 'COMPOSE' (red button), 'Inbox', 'Sent Mail', 'Drafts', 'All Mail', 'Spam (222)' (highlighted with a mouse cursor), 'Circles', 'Bills', and 'Notes'. The main area displays a list of spam messages. At the top of the list, there is a link that says 'Delete all spam messages now (messages that have been in Spam more than 30 days will be deleted)'. The messages listed are:

Checkbox	Star	Dropdown	From	Subject
<input type="checkbox"/>	☆	▾	cute@kiomails.com	Good Evening ;) how are they getting on?
<input type="checkbox"/>	☆	▾	carter's	EXTRA 25% OFF COUPON ends tomorrow
<input type="checkbox"/>	☆	▾	PacSun	Brixton Summer Collection - New arrivals fi
<input type="checkbox"/>	☆	▾	UsedCar Specials	Don't-Buy a New-Car! See These Amazing
<input type="checkbox"/>	☆	▾	50plusmatch	Ook onderweg daten? - Ook onderweg date
<input type="checkbox"/>	☆	▾	Gap	is it too early to pack for the weekend? - F

From: "Bank of America" customerservice@bankofamerica.com

To: "Jane Smith" jane-smith12@gmail.com

Date: Wed, May 26, 2010

Subject: Fraud Alert – Action Required

Phishing



use deceptive email addresses;
trick receivers into providing sensitive information;

Dear Customer,

At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com.


If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, [sign up now](#). New online members will automatically be enrolled in the Advanced Online Security program.

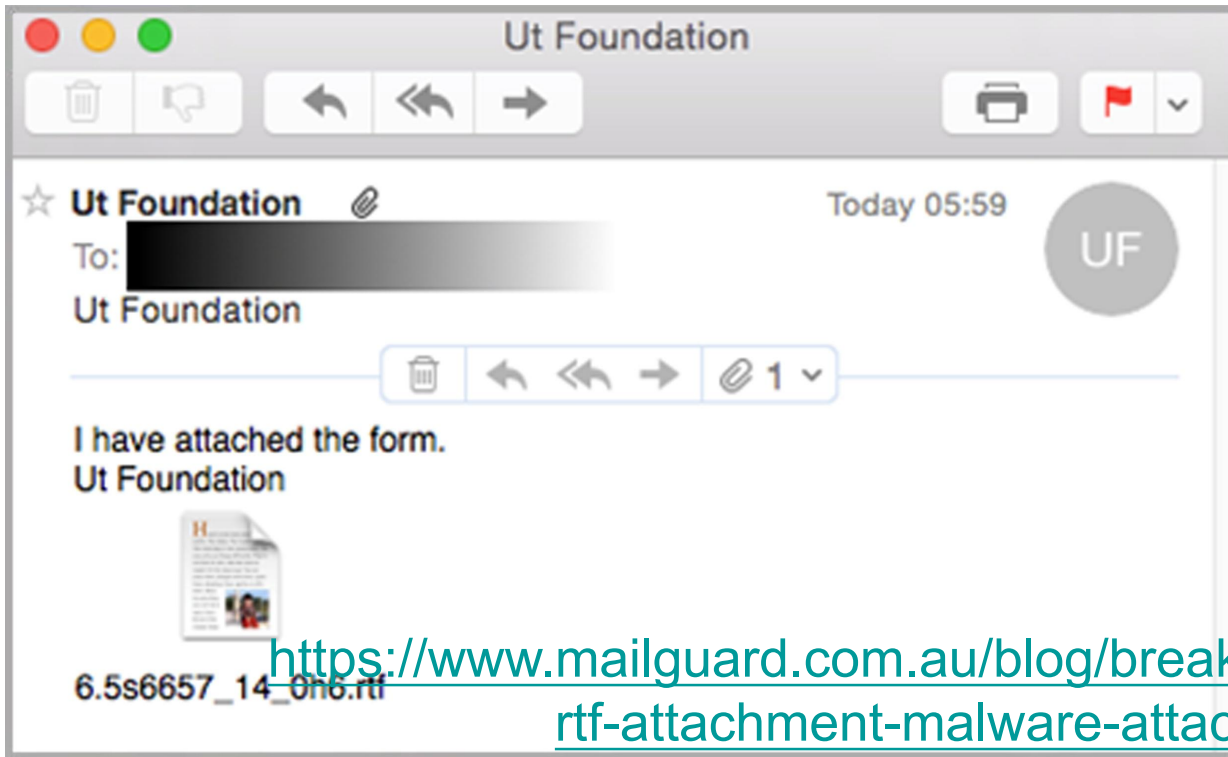
Sincerely,

<https://edu.gcfglobal.org/en/internetsafety/avoiding-spam-and-phishing/1/>

Bank of America Online Security Department 

Malware

- Spread via malicious email attachments
- Commonly suspicious file types:
.bat, .exe, .vbs, .com, .ade, .rtf, etc.



<https://www.mailguard.com.au/blog/breaking-unprecedented-rtf-attachment-malware-attack-impacting-millions>



Readings

- [Cryptography and Network Security: Principles and Practice](#)
by William Stallings
Chapter 19: Electronic Mail Security
- [Avoiding Spam and Phishing](#)
by LearnFree.org

Thank You