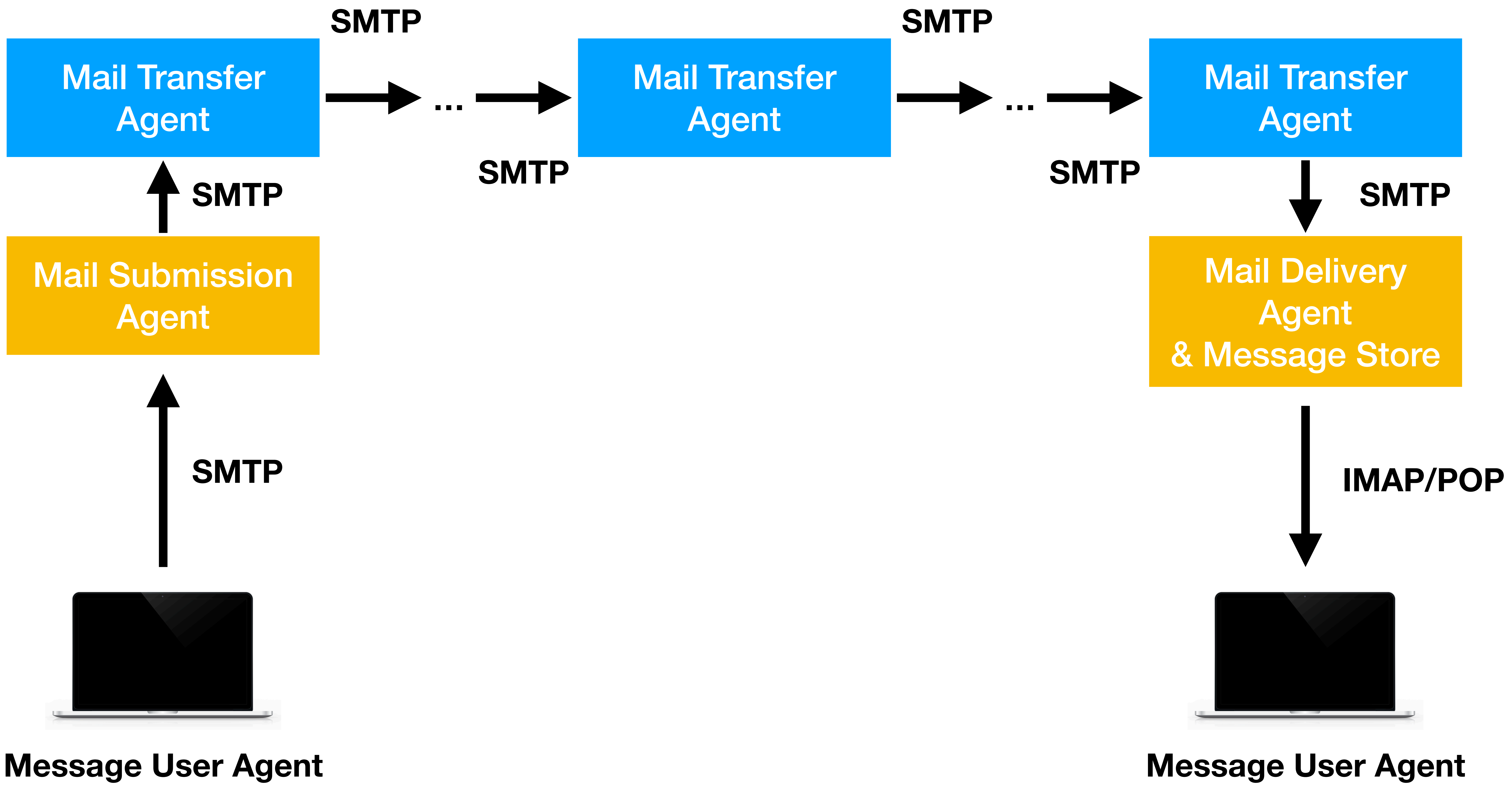
Email Security

Network Security

Email Overview



Mail Transfer Agent

SMTP

...

SMTP

Mail Transfer Agent

SMTP

...

SMTP

Mail Transfer Agent

SMTP

Mail Submission Agent

SMTP

Message User Agent

SMTP

Mail Delivery Agent & Message Store

IMAP/POP

Message User Agent

SMTP

- SMTP is a text-based protocol (client and server exchange ASCII messages)
- When talking about SMTP, we usually refer to ESMTP – an extension of SMTP, allowing for example user authentication
- To send an email to the correct destination, an MTA uses the Domain Name System (DNS) and looks up the MX (mail exchanger) record for the recipient domain (the part after the @). The MX record contains the name of the target MTA.

```
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
```

SMTP – STARTTLS

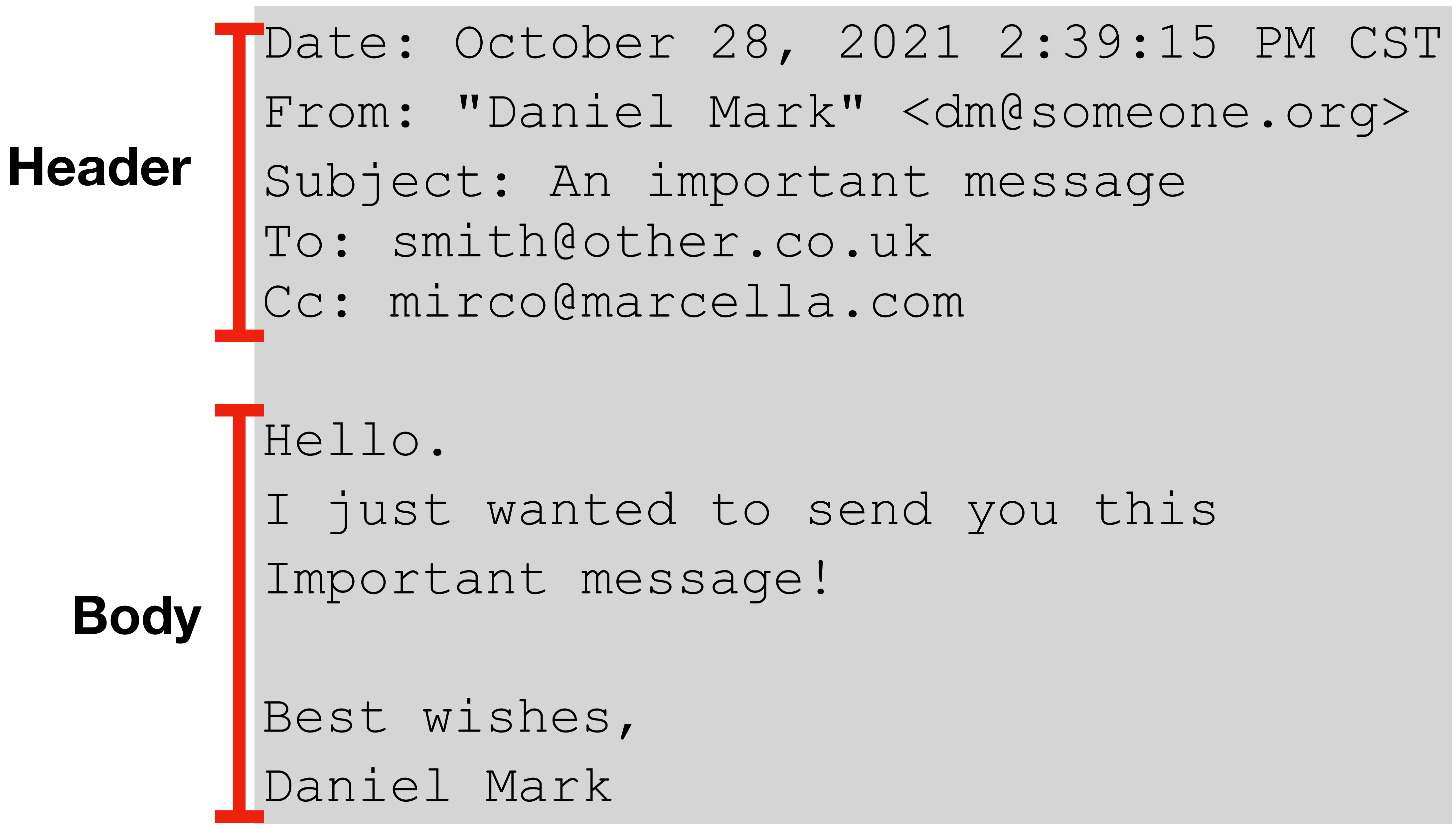
- By default, SMTP traffic is **not encrypted**. However, there is the **STARTTLS** extension, which adds confidentiality and authentication between SMTP agents via TLS.
- Problem: Since TLS is not required, a MITM attacker could strip away the corresponding line!

SMTP – STARTTLS

- Problem: Since TLS is not required, a MITM attacker could strip away the corresponding line!
- **DANE:** Bind X.509 certificates to DNS names using DNSSEC.
  - A corresponding DNS record might indicate that the server supports STARTTLS (prevents stripping away the STARTTLS command).
  - Provides authentication in the case of self-signed certificates.
- Some clients allow forcing TLS and there is SMTPS, a version of SMTP wrapped in TLS from the start.

Email Format

- Emails are text messages. They consist of a **header** (also called envelope) and a **body**.
- The two are separated by a blank line.
- The header consists of key-value-pairs. The keys are separated from the values by a colon.
- By default, only ASCII text is allowed.



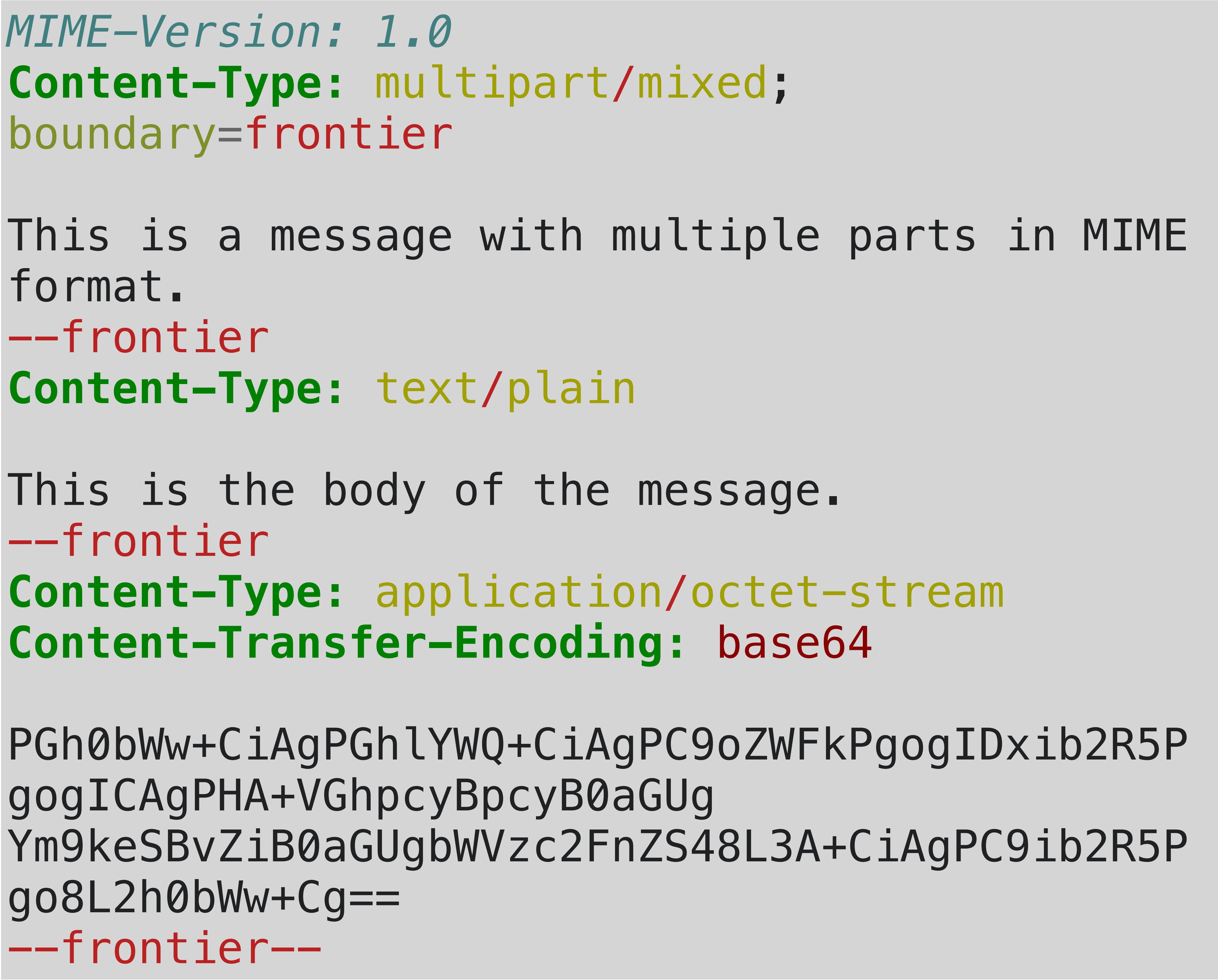
```
Date: October 28, 2021 2:39:15 PM CST
From: "Daniel Mark" <dm@someone.org>
Subject: An important message
To: smith@other.co.uk
Cc: mirco@marcella.com

Hello.
I just wanted to send you this
Important message!

Best wishes,
Daniel Mark
```

MIME

- MIME extends the format of emails to support more than just ASCII messages.
- Also allows attachments of binary form (via encoding).
- Is an extension of the ASCII based email standard.
    - Some more header fields, content types, and content transfer encodings.



```
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary=frontier

This is a message with multiple parts in MIME
format.
--frontier
Content-Type: text/plain

This is the body of the message.
--frontier
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64

PGh0bWw+CiAgPGhlYWQ+CiAgPC9oZWFkPgogIDxib2R5P
gogICAgPHA+VGhpcyBpcyB0aGUg
Ym9keSBvZiB0aGUgbWVzc2FnZS48L3A+CiAgPC9ib2R5P
go8L2h0bWw+Cg==
--frontier--
```

Source: Wikipedia

Email Threats

- **Confidentiality:** unauthorised disclosure of email contents
- **Integrity:** unauthorised modification of email contents
- **Availability:** preventing users from sending emails
  - Solutions rely on infrastructure: multiple, redundant mail servers etc.
- **Authenticity:** email spoofing
- **Accountability:** denying having sent a message

Email Threats

- **Confidentiality:** unauthorised disclosure of email contents
- **Integrity:** unauthorised modification of email contents
- **Authenticity:** email spoofing
- **Accountability:** denying having sent a message

S/MIME

- Security enhancement to MIME, providing authentication, integrity, and confidentiality.
  - **Confidentiality:** encryption
  - **Integrity:** digital signatures
  - **Authenticity:** digital signatures
  - **Accountability:** *non-repudiation of origin* via digital signatures

S/MIME

- Identities are established using X.509 certificates sent along the emails (certificates are signed by CAs).
    - Class 1 certificates only bind public keys to email addresses.
    - Class 2 certificates include an identity verification of the person.

S/MIME

- Encryption is done via **symmetric encryption** (typically AES-128 CBC) and a one-time session key. The one-time key is encrypted via asymmetric encryption using the recipient's public key from the certificate.

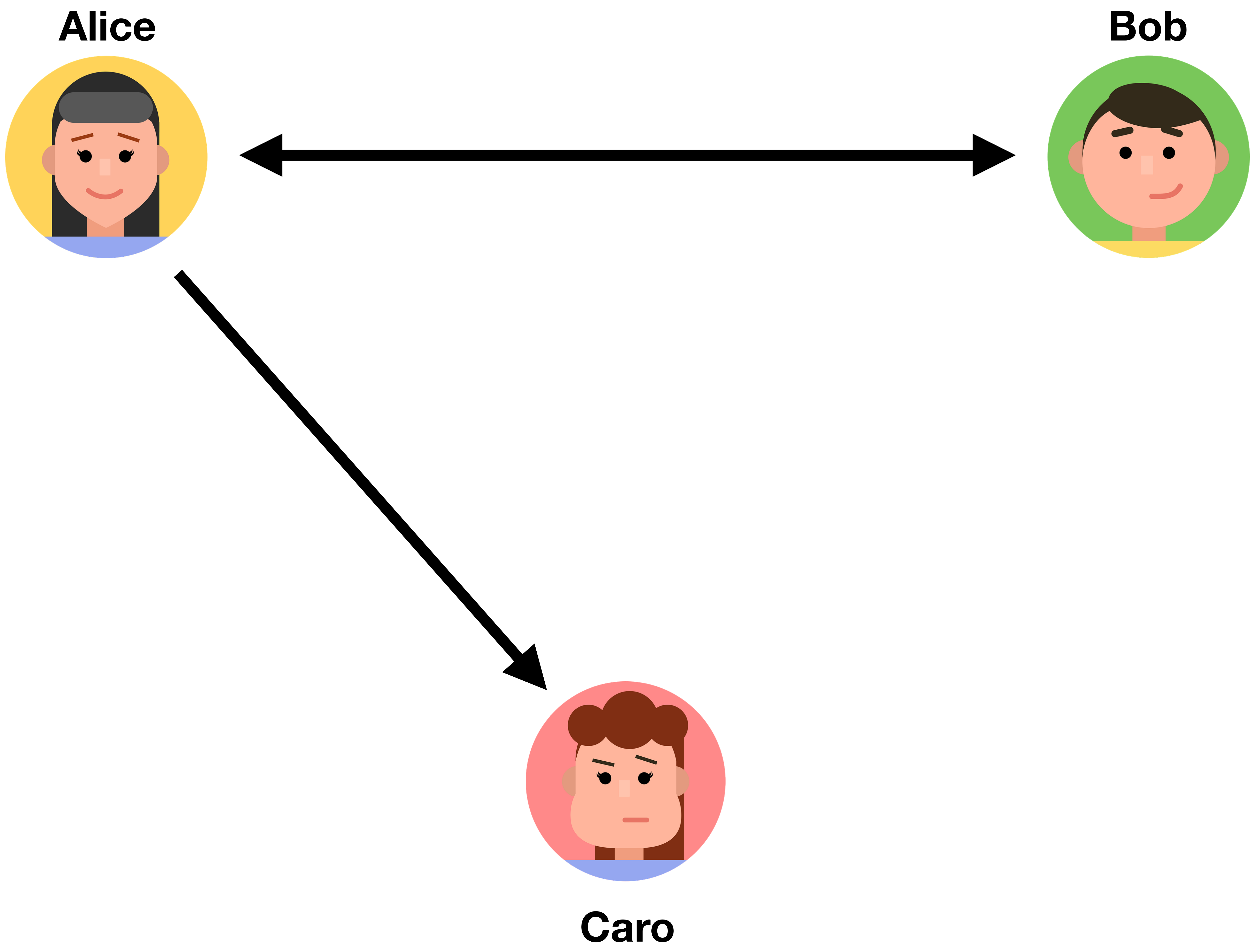
- Signing is done by **hashing** (typically SHA-256) and **encrypting** (via RSA) the hash using the sender's private key. The recipient can decrypt and check the hash.

- It is possible to use only signing, only encryption, or both (in either order).

PGP

- Pretty Good Privacy (PGP) is an alternative to S/MIME. The main difference is the **key certification** and **distribution**.
    - S/MIME relies on X.509 certificates issued in a hierarchical system by CAs. Certificates are sent along email messages.
    - PGP relies on a **Web-of-Trust**: Users generate their own key pairs. Users can sign other users' public keys – email address relationships.
      A user trusts another public key, if it is signed by someone (s)he trusts. → **transitive notion of trust**
    - Public keys must be obtained from different channels (i.e., webpages or PGP public key servers).

PGP / Web-of-Trust



Alice

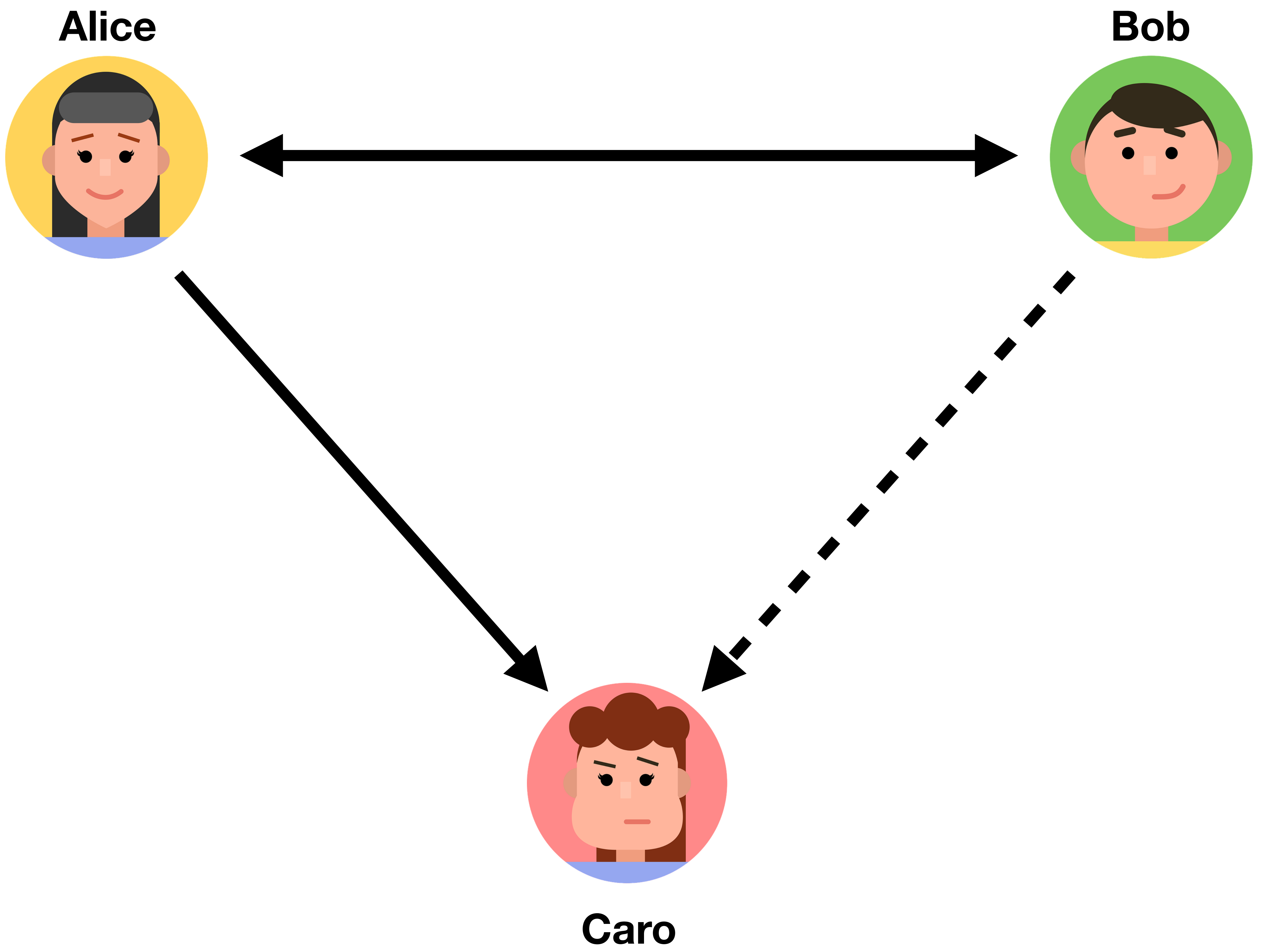
Bob

Caro

Alice signs Bob’s
and Caro’s public key

Bob signs
Alice’s public key

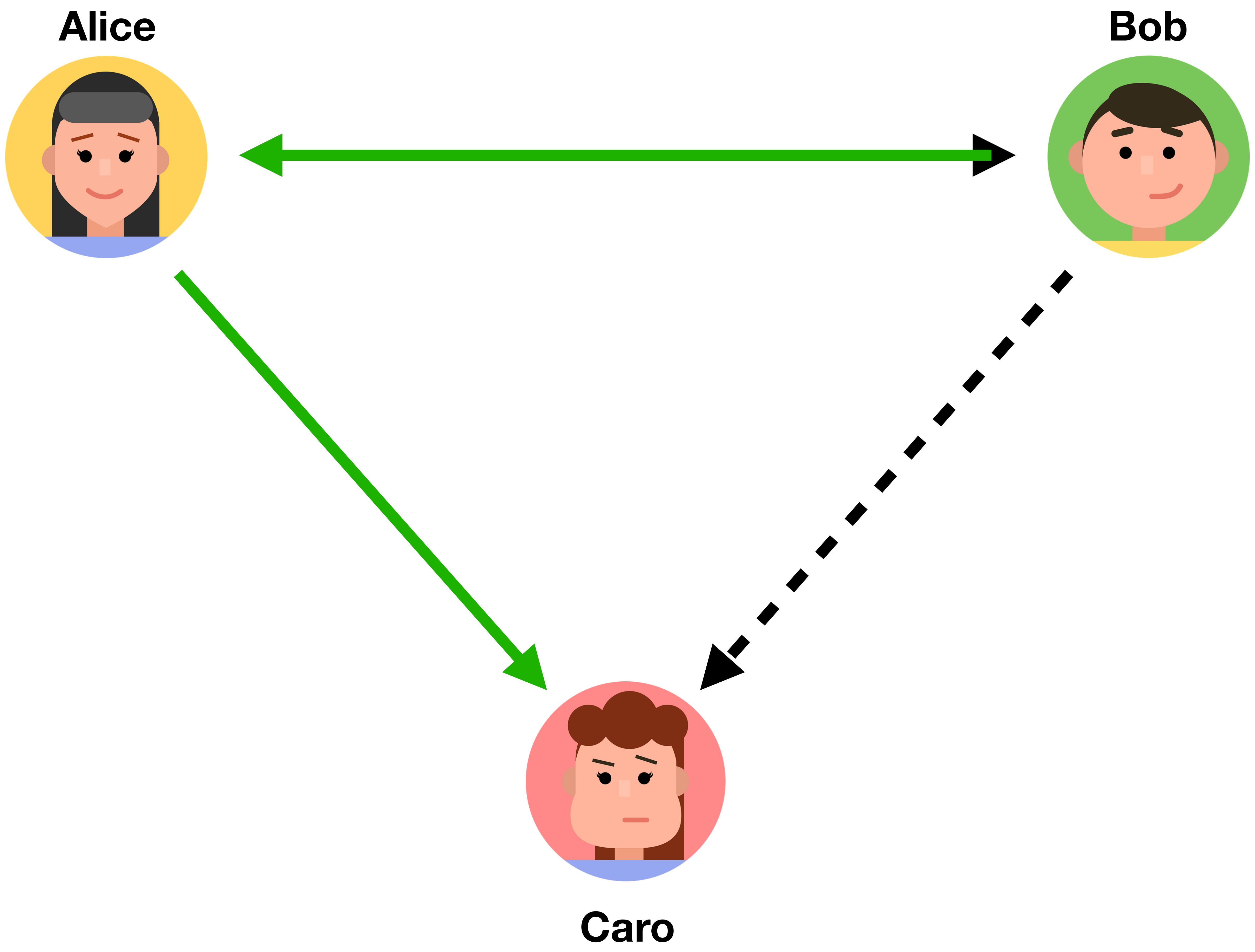
PGP / Web-of-Trust



Alice signs Bob’s
and Caro’s public key

Bob signs
Alice’s public key

PGP / Web-of-Trust



Alice signs Bob’s
and Caro’s public key

Bob signs
Alice’s public key

Email Threats

- **Confidentiality:** unauthorised disclosure of email contents
- **Integrity:** unauthorised modification of email contents
- **Authenticity:** email spoofing
  - What if I receive an unsigned message? Is it spoofed?
- **Accountability:** denying having sent a message

Authenticity

- There are a couple of authenticity related standards that all rely on DNS.
- **SPF – Sender Policy Framework:**
  Allows a sender domain to specify which mail transfer agents are allowed to send from this domain (“MAIL FROM”/“HELO”).
- **DKIM – Domainkeys Identified Mail:**
  Allows a sender domain (or the respective MTA) to sign outgoing messages for authenticity. The corresponding public key is provided to the receiver via DNS.
- **DMARC – Domain-based Message Authentication, Reporting, and Conformance:**
  Allows to specify a policy which of SPF and DKIM is used and how receivers should handle invalid emails. It also includes a feedback mechanism.

Summary

- SMTP
  - SMTP is a text-based protocol used to transfer emails
  - STARTTLS is an extension of it allowing encrypted traffic
  - The STARTTLS command is prone to be stripped away
- MIME
  - An extensible email format that allows other encodings, binary attachments etc.
- S/MIME
  - Enables confidentiality, integrity, authenticity, and accountability through encryption and signing
  - Is based on X.509 certificates
- PGP
  - Same properties as S/MIME but based on a web-of-trust approach
- Authenticity
  - SPF, DKIM, DMARC can be used together to achieve authenticity of origin on a domain level