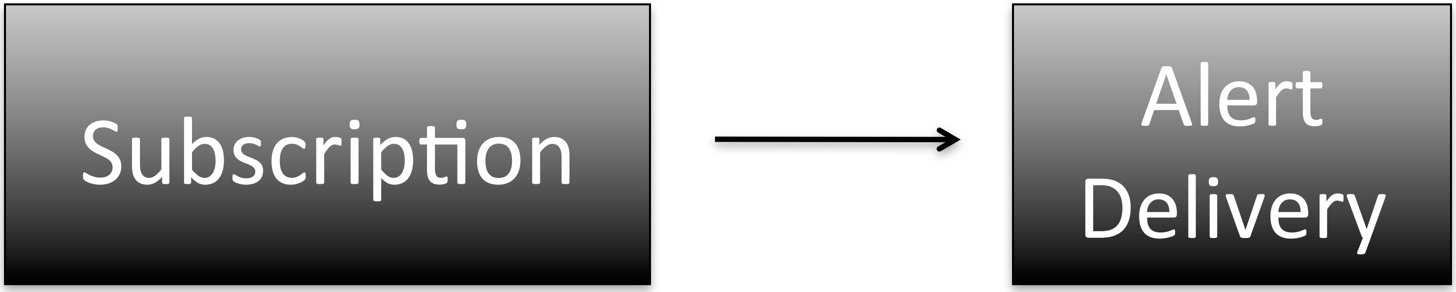
ATOCA & Security

Hannes Tschofenig

Two Phases



Subscription

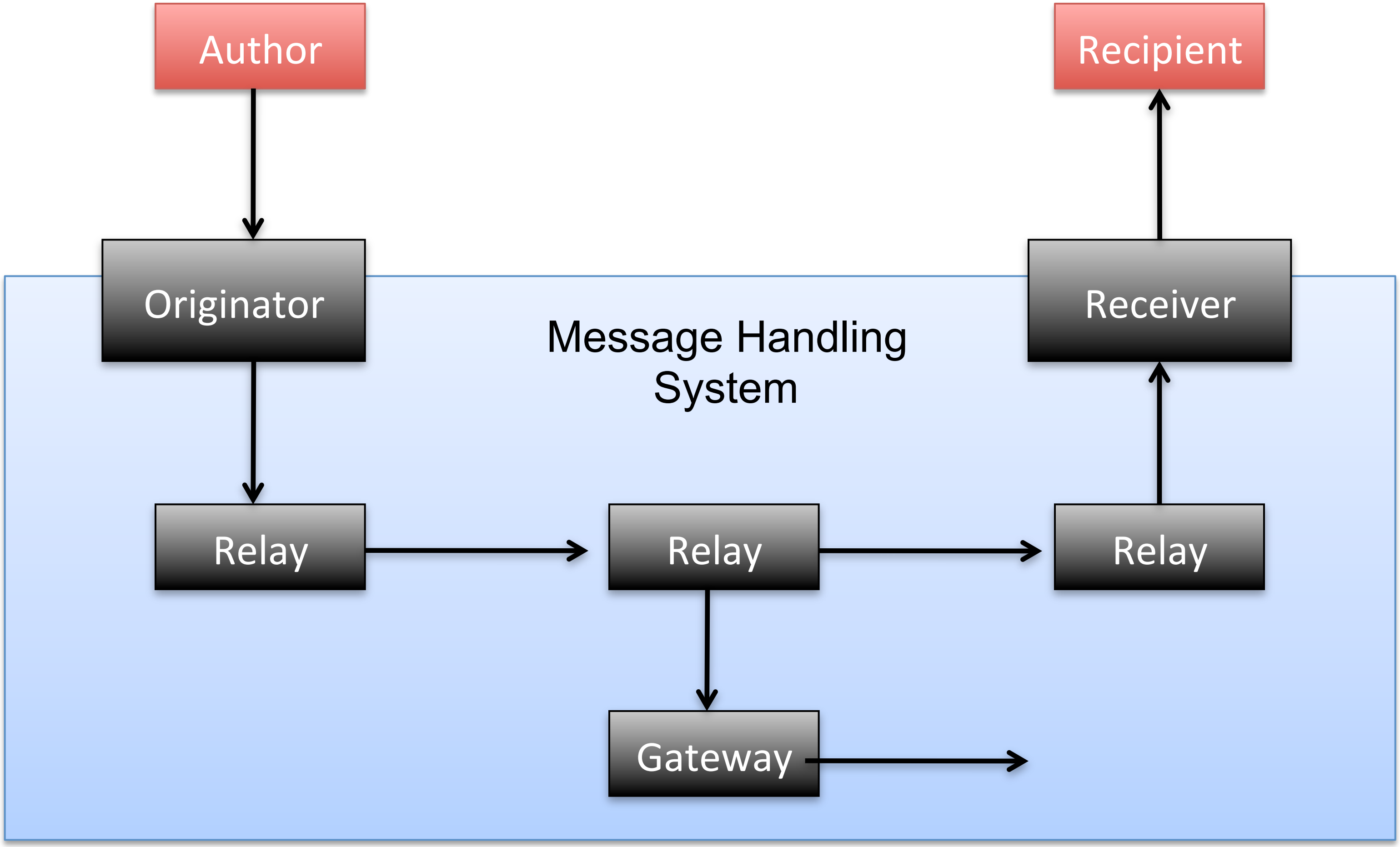
Alert Delivery

Re-use of Common Mechanism.

Subscription

- RFC 3265 talks about:
  - Access Control
  - Denial-of-Service attacks (of server’ s and third parties)
  - Replay Attacks
  - Man-in-the middle attacks
- Event packages may describe additional considerations.
- XEP 60 covers similar aspects.

Message Delivery



```xml
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.1">
  <identifier>KSTO1055887203</identifier>
  <sender>KSTO@NWS.NOAA.GOV</sender>
```

Author

```xml
  <sent>2003-06-17T14:57:00-07:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <info>
    <category>Met</category>
    <event>SEVERE THUNDERSTORM</event>
    <urgency>Severe</urgency>
    <certainty>Likely</certainty>
    <senderName>NATIONAL WEATHER SERVICE SACRAMENTO</senderName>
```

Author

```xml
    <headline>SEVERE THUNDERSTORM WARNING</headline>
    <description> SEVERE  THUNDERSTORM OVER SOUTH CENTRAL ALPINE COUNTY…</description>
    <instruction> TAKE COVER IN A SUBSTANTIAL SHELTER UNTIL THE STORM PASSES </instruction>
    <contact>BARUFFALDI/JUSKIE</contact>
    <area>
      <areaDesc> EXTREME NORTH CENTRAL TUOLUMNE COUNTY
        IN CALIFORNIA, EXTREME NORTHEASTERN
        CALAVERAS COUNTY IN CALIFORNIA, SOUTHWESTERN
        ALPINE COUNTY IN CALIFORNIA </areaDesc>
      <polygon> 38.47,-120.14 38.34,-119.95 38.52,-119.74
        38.62,-119.89 38.47,-120.14 </polygon>
    </area>
  </info>
 </alert>
```

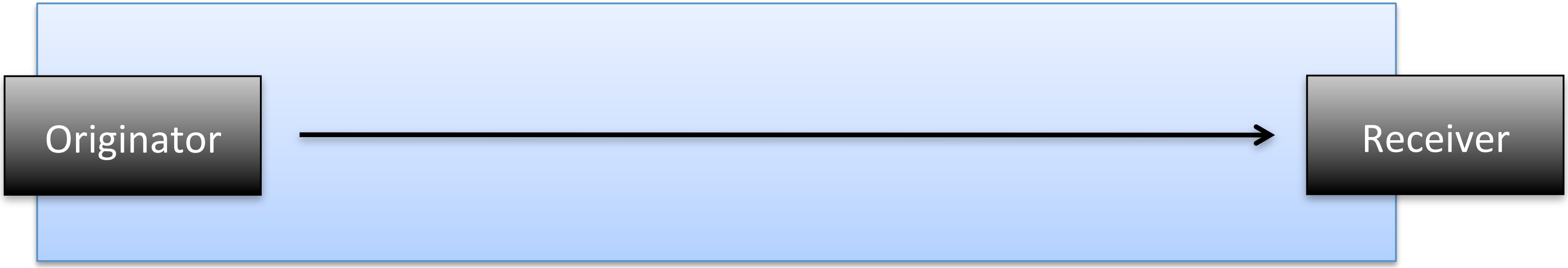
```
MESSAGE sip:aggregator@domain.com SIP/2.0
  Via: SIP/2.0/TCP relay.domain.com;branch=z9hG4bK776sgdkse
  Max-Forwards: 70
  From: sip:dean@school.example.edu;tag=49583
  To: sip:tony@foobar.com
  Call-ID: asd88asd77a@1.2.3.4
  CSeq: 1 MESSAGE
  Content-Type: common-alerting-protocol+xml
  Content-Length: ...
   ……
```

Originator

Receiver

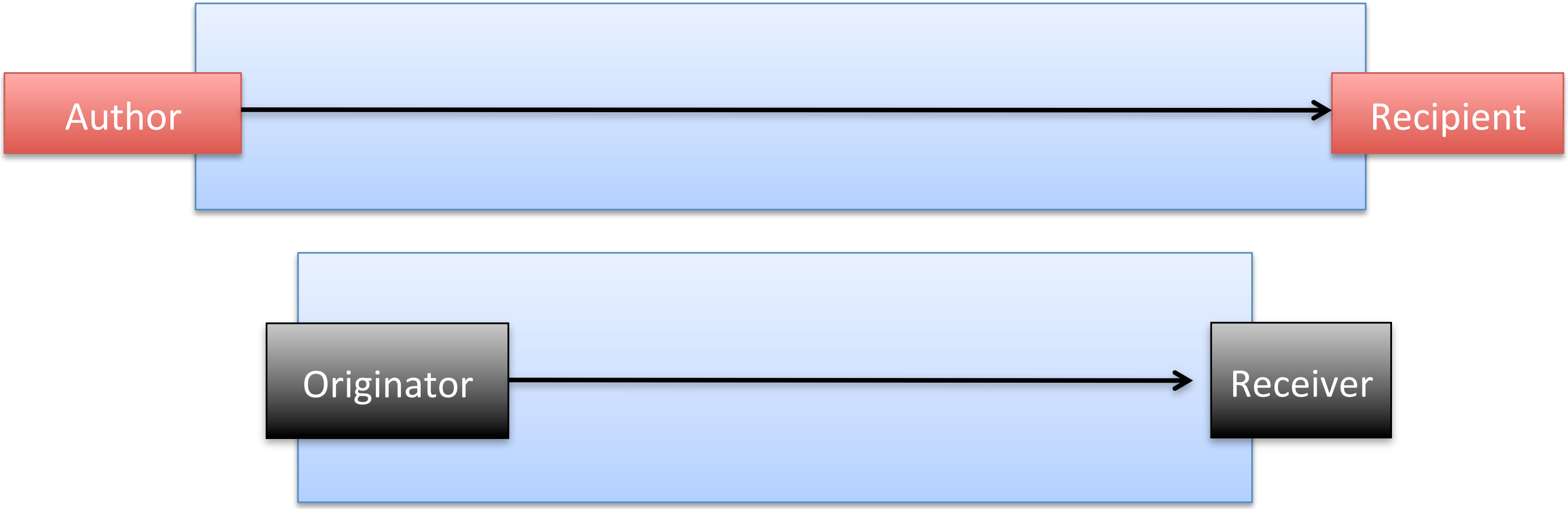
Message Delivery: Communication Security

- SIP/XMPP End-to-End Security Mechanisms
  - Authentication of originator
  - Integrity protection
  - Confidentiality protection
- Example mechanisms:
  - S/MIME
  - SIP Identity, PAI

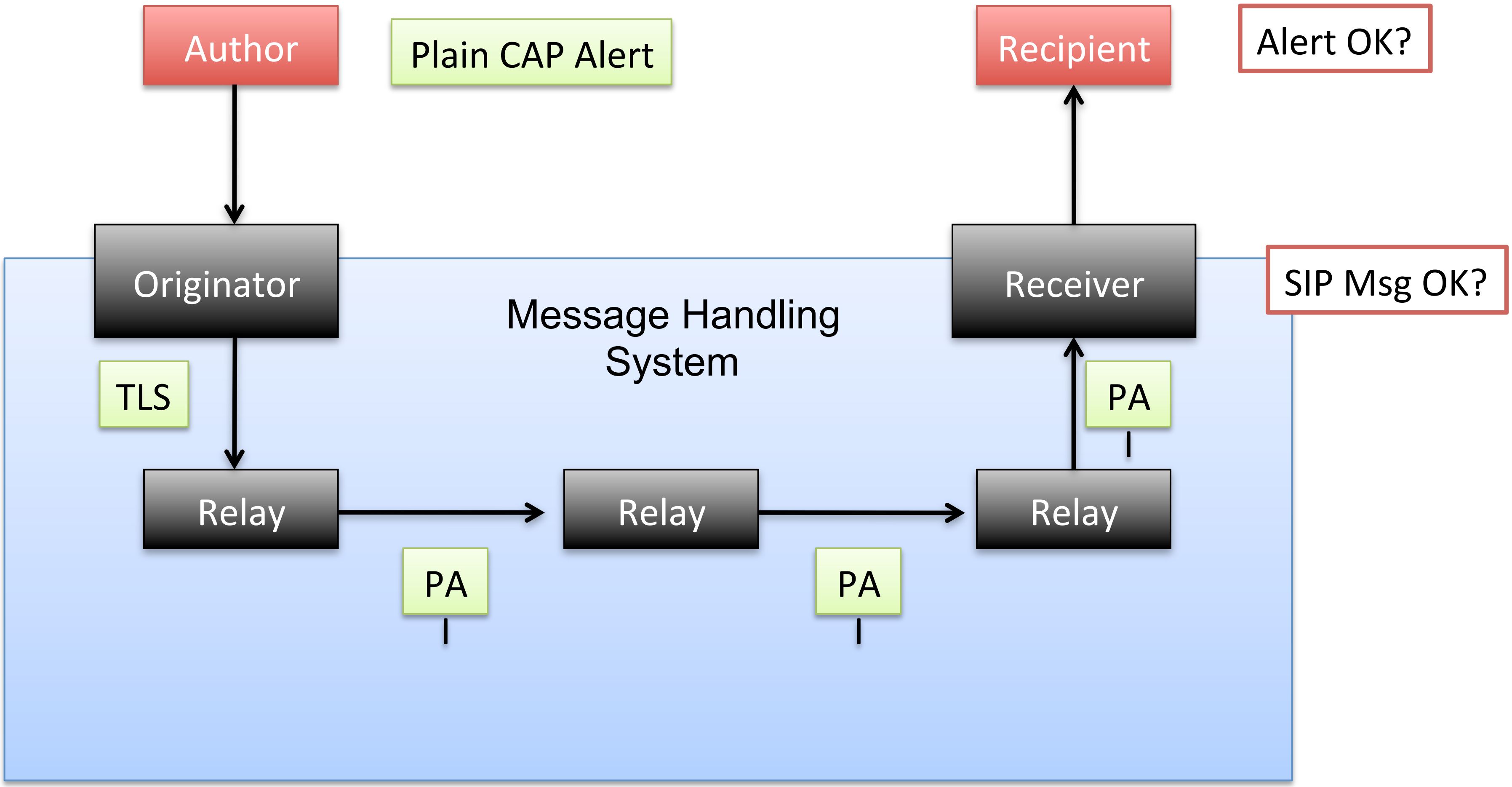


Message Delivery: Alert Security

- CAP security
  - Authentication and integrity protection
- Uses XML Digital Signatures



Example


Author
Plain CAP Alert
Recipient
Alert OK?
Originator
Message Handling System
Receiver
SIP Msg OK?
TLS
PA
Relay
Relay
Relay
PA
PA

Authorization

- Alert delivery:
  - Where do the root certs come from?
  - Once digital signature is verified what check is supposed to be performed to the author's identity?
- More likely that underlying SIP/XMPP communication architecture will be utilized!?
  - Fewer problems where prior subscription step is performed. E.g. School case
  - Originator's identity is asserted via SIP mechanisms.
  - How to deal with messages from unknown authors/ originators that appear out of the blue?