
ICAO • OACI • ИКАО
国际民航组织 • ايكاو
INTERNATIONAL
CIVIL AVIATION
ORGANIZATION

AFS to SWIM Transition Task Force (AST TF)

SEVENTH MEETING

AMHS SECURITY WORKSHOP

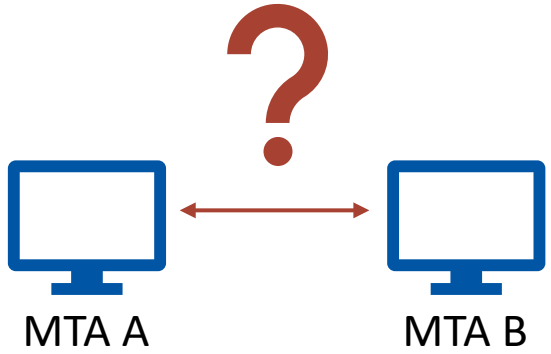
(Dubrovnik, Croatia, 21-24 April 2026)

Ryan Petroschka

IT Security Engineer @ Indra Avitech GmbH

PKI – Foundation of Trust

How systems establish trust in AMHS environments



AMHS supports multiple trust relationships (e.g. Message Transfer Agent (MTA), User Agent (UA), Message Transfer and Control Unit (MTCU)).
For simplicity, this presentation focuses on MTA ↔ MTA communication.

Key Concepts

Simple analogies for PKI concepts

Key Pair
→ Like a special tool:
- one part creates a stamp (Private Key),
- the other verifies it (Public Key)

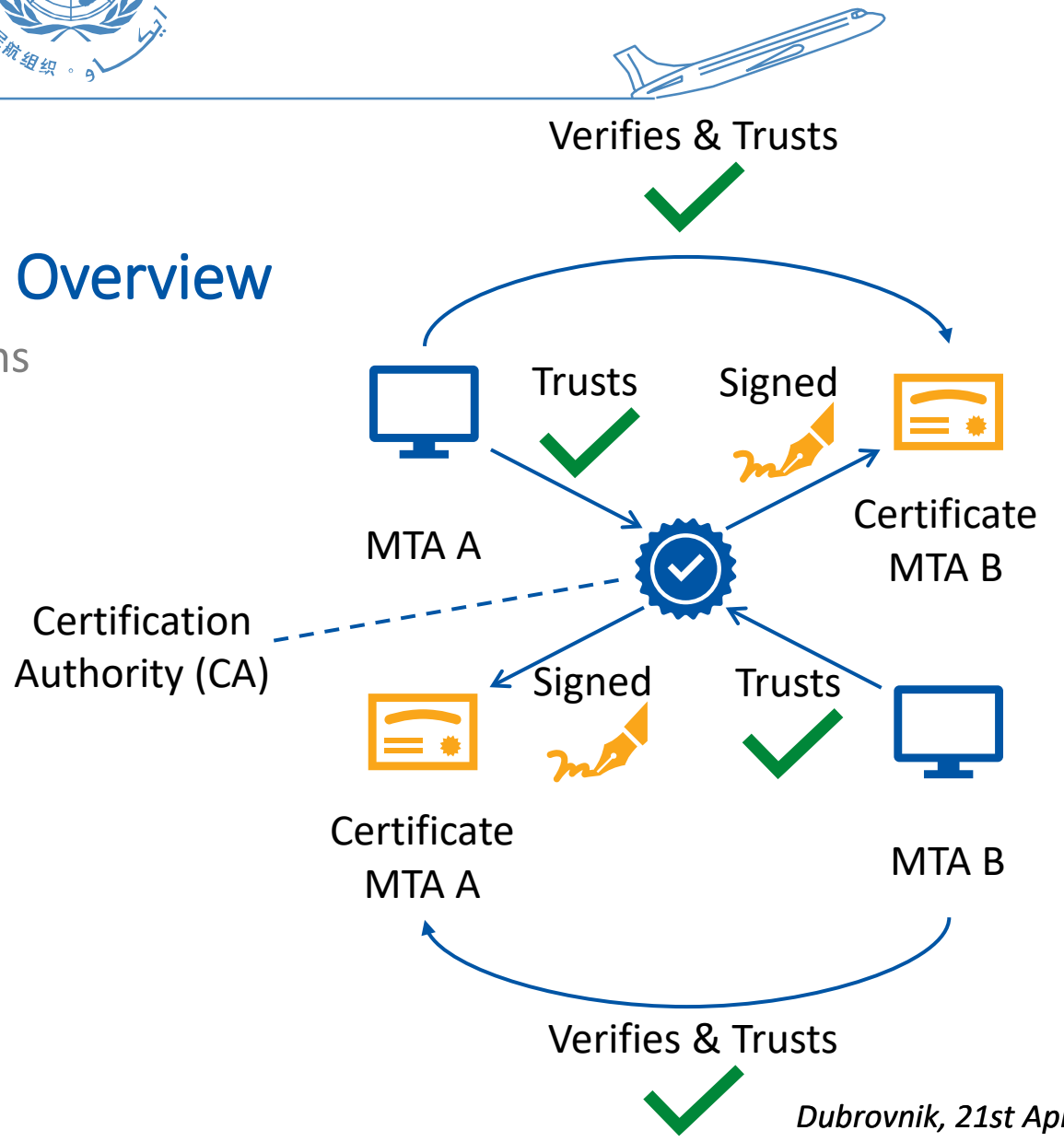
Message Signature
→ Like a stamped proof attached to a message

Certificate
→ Like a passport that proves who you are

Trusted Root
→ Like a government whose passports we trust

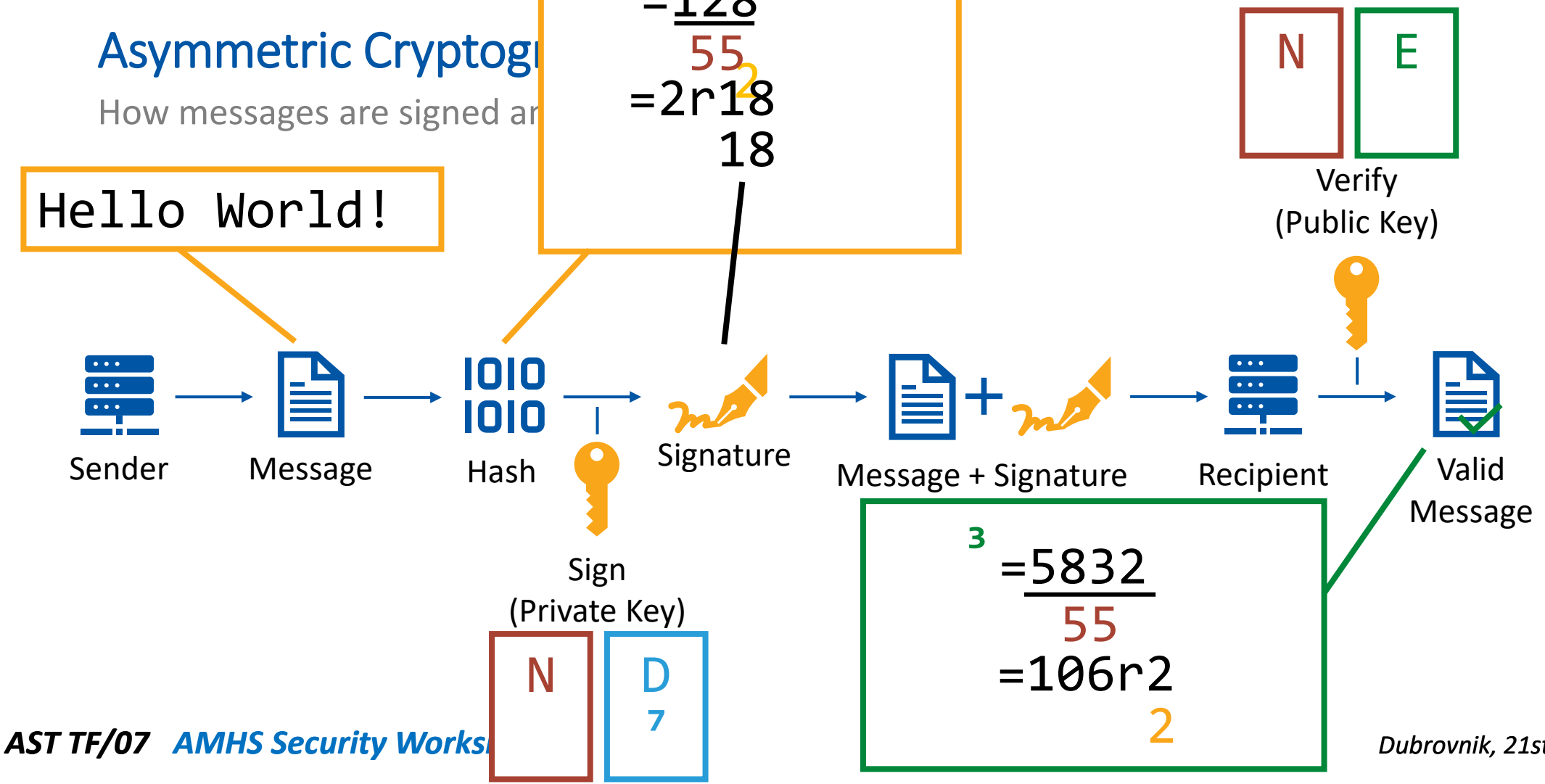
Public Key Infrastructure (PKI) Overview

How trust is established between systems



Asymmetric Cryptogr

How messages are signed ar



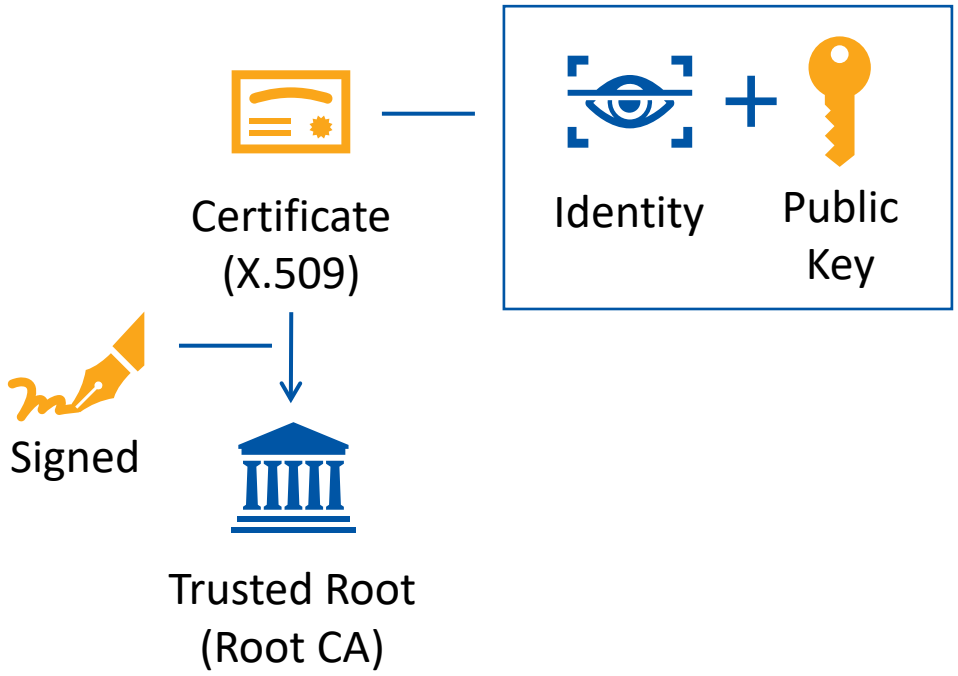
Trusting the Public Key

Why certificates are required for trust

- Public key must be trusted
- Trust comes from certificates signed by a trusted root
- Certificate = Identity + public key + signature

Identity Examples:

- UA (User Agent)
  → e.g. /C=XX/ADMD=ICAO/PRMD=LH/O=AFTN/OU=LHBPABCD/ (user/application identity)
- MTA (Message Transfer Agent)
  → e.g. MTA-LHBP-1 within /C=XX/ADMD=ICAO/PRMD=LH/ (mta identity)
- MTCU (Message Transfer and Control Unit)
  → e.g. MTCU-LHBP-1 within /C=XX/ADMD=ICAO/PRMD=LH/ (mtcu identity)

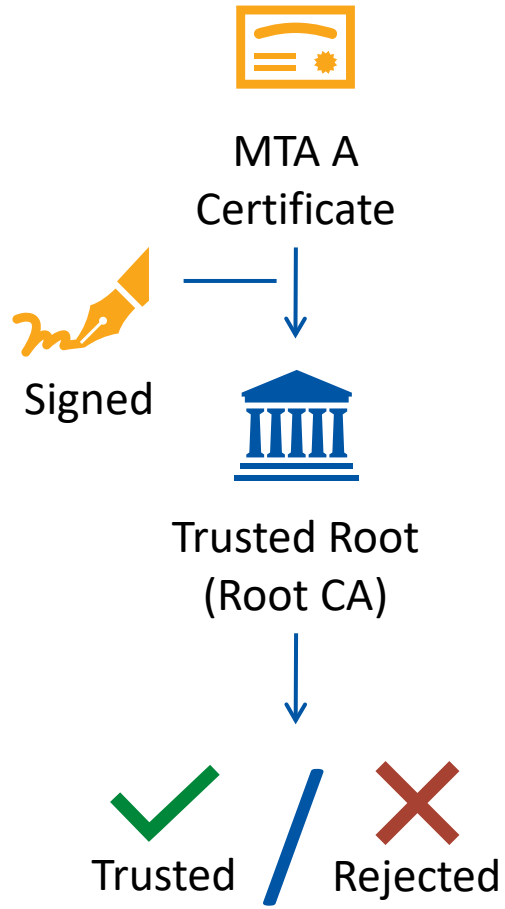


Certificate Validation (Trust Decision)

How trust is verified

- Verify certificate signature
- Verify trusted root
- Validate certificate (time, identity, revocation)

→ Accept or reject



What Can Break Trust?

Validation failures that lead to rejection

- Certificate expired
- Certificate not yet valid
- Certificate revoked (CRL)
- Identity mismatch (wrong MTA / UA)
- Not signed by a trusted root

→ Outcome is determined by policy

Thank You

ICAO