AFS To SWIM Transition Task Force (AST TF)

AST TF/07 meeting

Dubrovnik, Croatia, 21-24 April 2026

Hosted by Croatia Control

INTERNATIONAL CIVIL AVIATION ORGANIZATION

AFS to SWIM Transition Task Force (AST TF)

SEVENTH MEETING

(Dubrovnik, Croatia, 21-24 April 2026)

AMHS SECURITY WORKSHOP

(Dubrovnik, 21 April 2026)

AMHS Strong Authentication

Jean-Marc VACHER

Supporting DSNA, France

AMHS Strong Authentication

01 Main characteristics

02 Technical Principles

03 Offered benefits

04 Infrastructure, organization and prerequisites

05 Possible failures and mitigation approaches

06 Summary

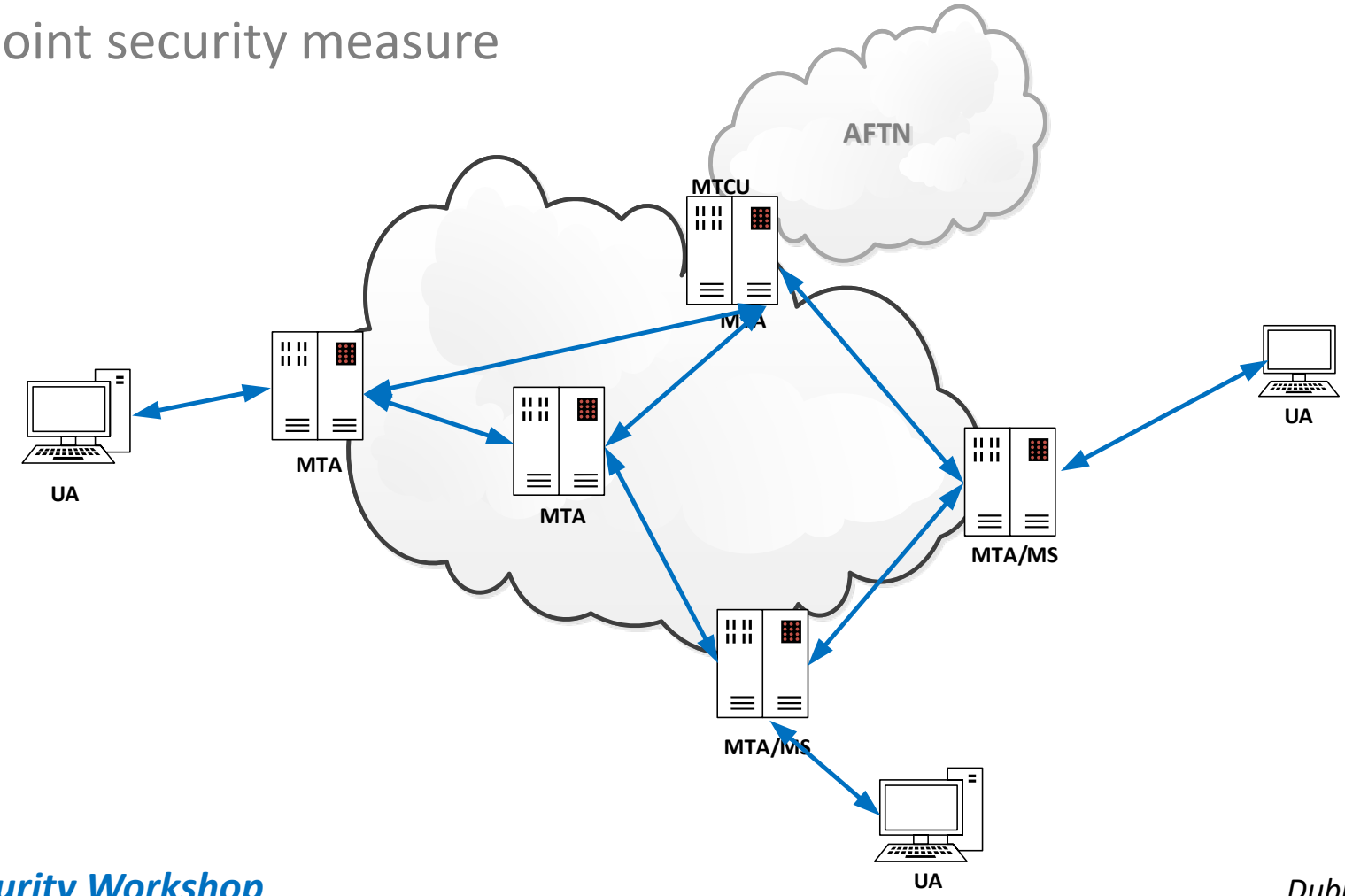
AMHS strong authentication: main characteristics

A point-to-point security measure

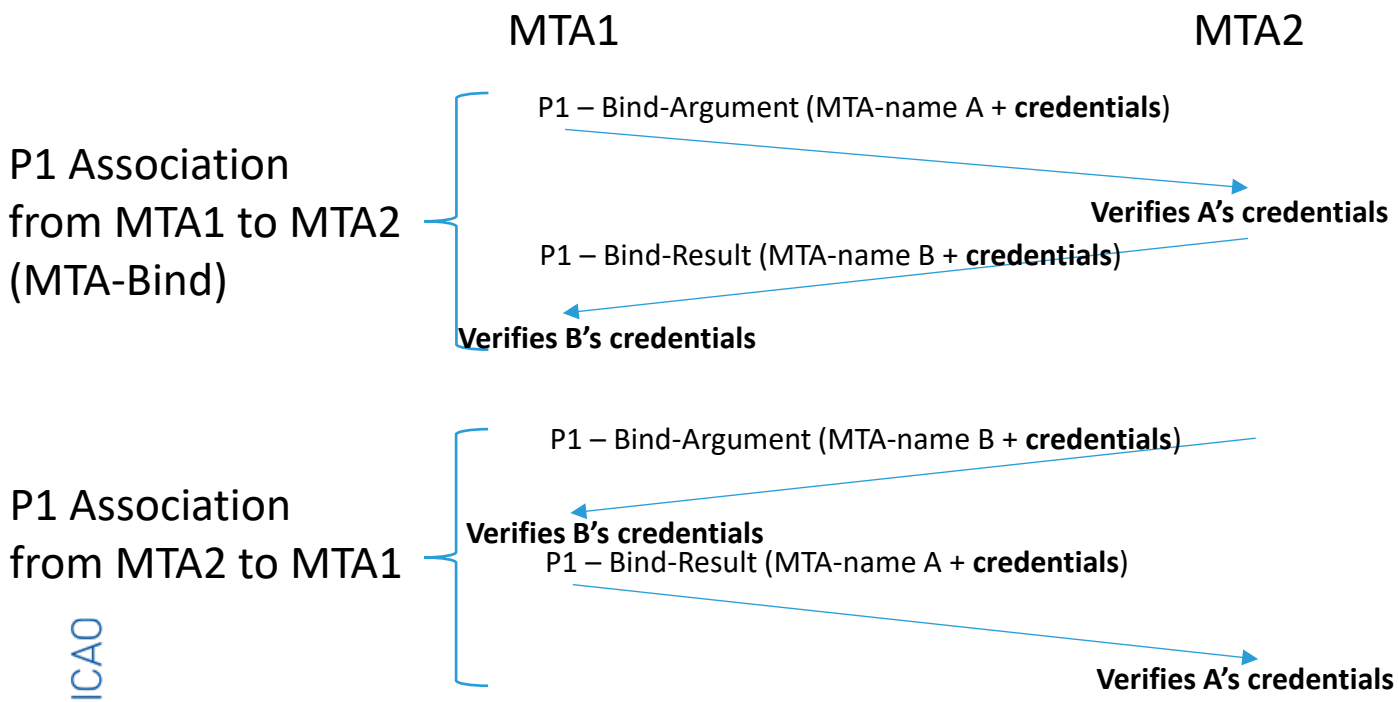
- As in Doc 9880 Edition 3, AMHS Security / Extended ATS Message Handling Service
- Based on X.400 / ISO/IEC 10021 built-in security mechanisms
- Using X.509 public key certificates and public key infrastructure (PKI)
- Aims at replacing the current simple authentication
- From MTA to MTA and between UA and MS/MTA
- Performed at the start of each AMHS association (MTA Bind or MS/MTS Bind)

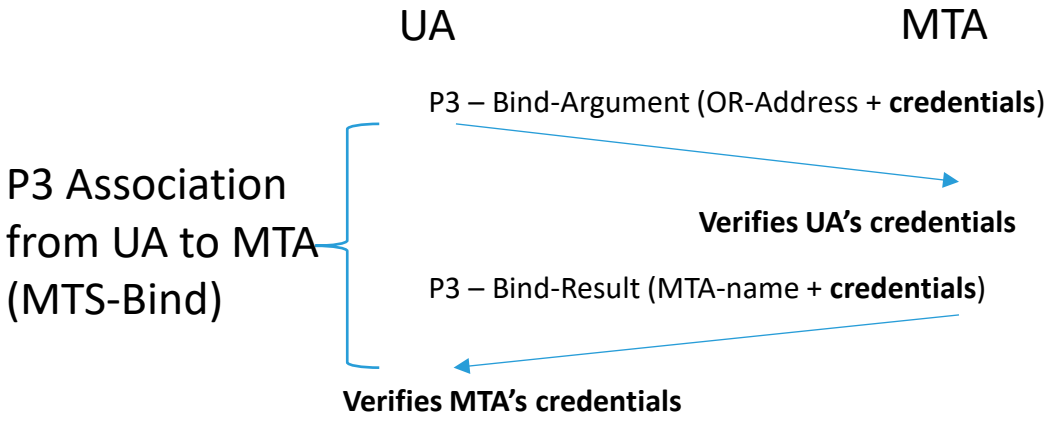
AMHS strong authentication: technical principles (1)

A point-to-point security measure



AMHS authentication : technical principles (2)





Similar patterns for P3 MS to MTA Bind (MTS-Bind) and P7 Association from UA to MS (MS-Bind)

=> Bidirectional "AMHS connection" established

Technical principles (3): two options for authentication credentials

Simple credentials: pre-defined password previously exchanged off-line between MTA administrators

Three problems:

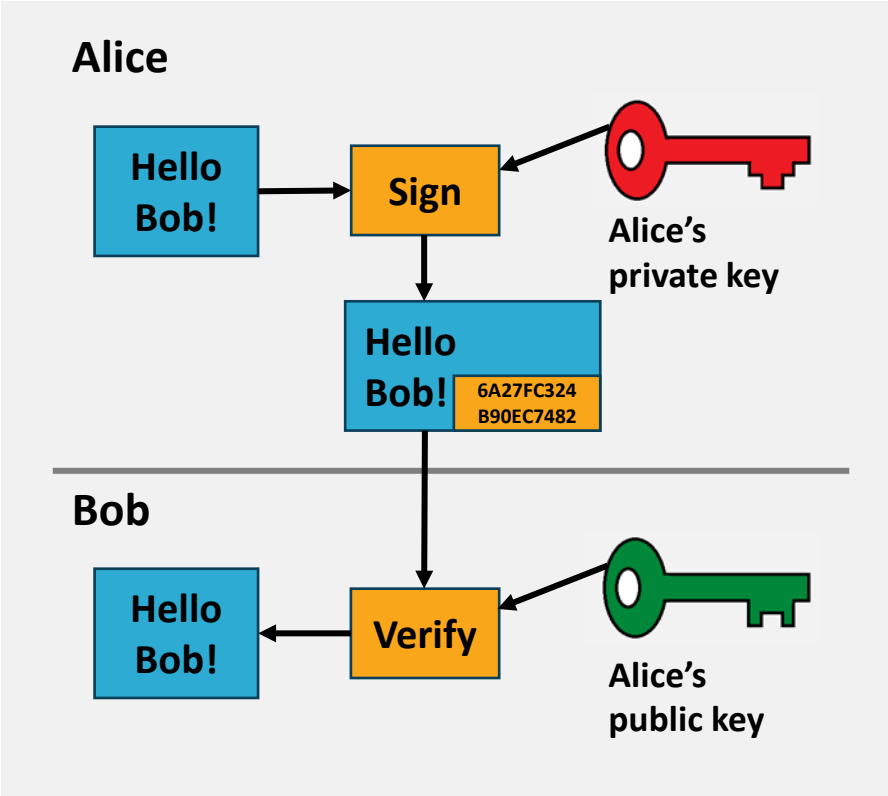
- Well-known MTA passwords in the EUR Region and beyond
- MTA passwords conveyed in clear in application layer data exchanges
- Simple authentication identical for all occurrences of MTA-Bind between two given MTAs

Strong credentials: bind-token + X.509 certificate

- A **bind-token** is a unique X.400 data structure created for a one-time MTA Bind between two MTAs
- The bind-token includes a **digital signature** made with the **private key** of the sending MTA
- The **X.509 certificate** of the sending MTA includes the **public key** enabling to verify the digital signature

AMHS strong authentication: technical principles (4)

What are digital signatures and asymmetric cryptography?



Technical principles (5): what is exactly a bind-token?

A set of parameters including:

- The MTA-name and domain identifier of the remote MTA
- Time of creation
- A random number
- The signature-algorithm-identifier

Transmitted:

- “In clear” (not encrypted)
- In combination with a digital signature of the above set of parameters
- The signature is made with the private key of the sending MTA

Technical principles (6)

How is a bind-token generated?

While creating the Bind request, the MTA software uses

- its configuration parameters (remote MTA name and domain-identifier)
- its locally stored private key

to generate the bind-token and build the MTA Bind Argument, including its own MTA name and certificate

How is a bind-token verified?

Upon reception of the Bind request, the receiving MTA software verifies the signature using

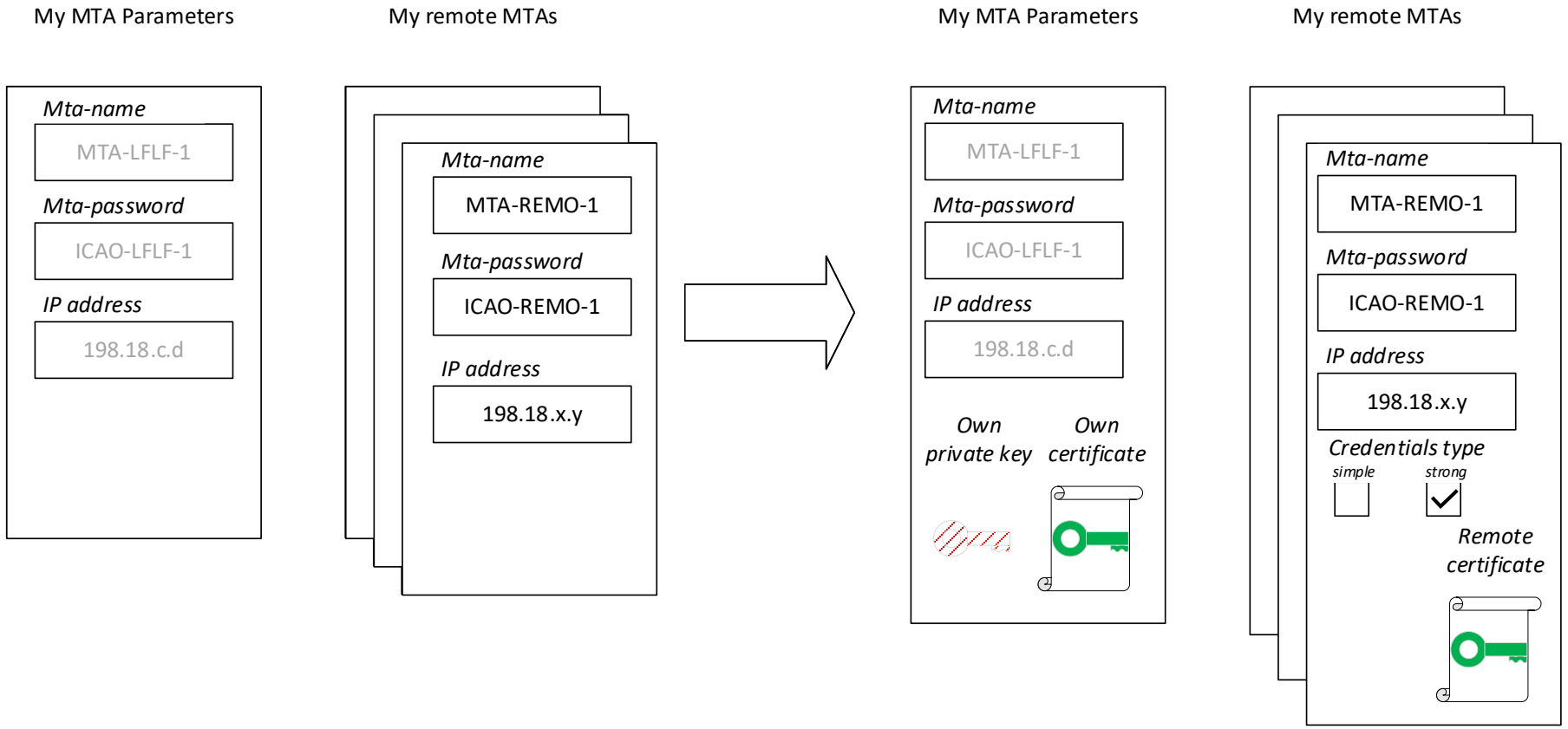
- the received parameters (initiator MTA name and domain-identifier, time, random number)
- the initiator MTA's public key received in the initiator MTA certificate

This ensures that the sender was indeed the MTA identified by initiator-name in the MTA Bind Argument

The receiving MTA software also checks the validity of the received initiator certificate

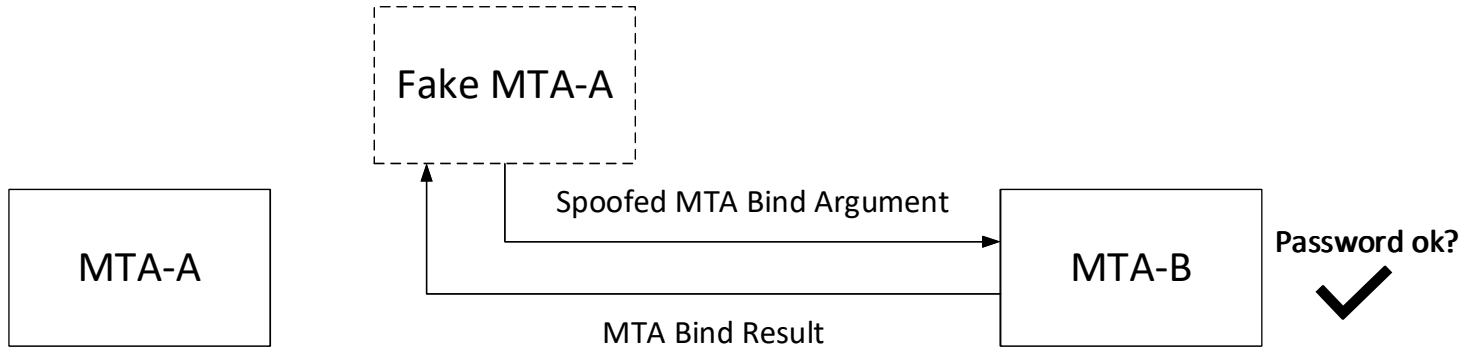
Technical principles (7)

Sample MTA configuration interface changes

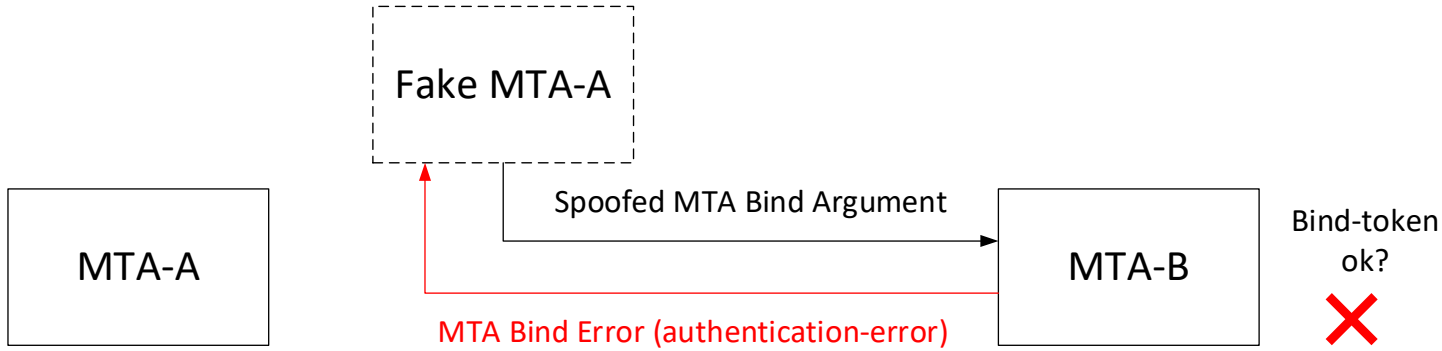


Offered benefits (1): technical view

Simple authentication



Strong authentication



Offered benefits (2):

Practical:

- With strong authentication, MTA B is sure to be truly exchanging data with MTA A
- Dissuasion to potential attackers in search of “weak points”

Institutional / Regulatory:

- Compliance with ICAO Doc 9880 Edition 3, Extended Service / AMHS security
- Contributes to means of conformance to NIS 2 Directive and its national transpositions
- Best security practice to be demonstrated in cybersecurity audits

Infrastructure, prerequisites and organization (1)

As a COM Centre Manager / MTA administrator, what do I need?

To generate a Bind-Token:

- My own private key and public key (**key pair**)
- A means to certify that the public key is mine => a public **certificate** created by the **certification authority (CA)** of a **public key infrastructure (PKI)** such as the **European Aviation Common PKI (EACP)**
- A **software upgrade** (and system configuration) for my ATS Message Server / MTA

To verify a Bind-Token:

- The public key of the communication partner's MTA: included in its **certificate**
- A means to ensure that the key is valid, i.e. **certificate validation**:
  - Not expired
  - Not revoked => **certificate revocation lists (CRLs)**
- A **software upgrade** (and system configuration) for my ATS Message Server / MTA

Needs are similar for a UA owner

In summary: **key pairs – certificates – CRLs – CA/PKI – upgraded software**

Infrastructure, prerequisites and organization (2)

Regarding organization:

- Internal security policy and organization
  - Procedures → Generation of key pair, requesting and renewal of certificates, ...
  - Roles → Assignment of related tasks / authorisation by internal policy
- Internal technical training
- Partial conformance tests
- Internal operational training
- Knowledge of the adjacent COM Centres' status regarding authentication
- A common agreement/date with each adjacent COM Centre individually to use strong authentication
- Partial Interoperability tests (IOT) and pre-operational tests (POT)
- Internal and bilateral procedures (operational & technical) in case something goes wrong

In summary: **security policy/organization**, **coordination, tests, training and procedures**

What could go wrong?

MTA-Bind-error, authentication-error and possible approaches to mitigate potential failures

Event	Details	Likelihood	Comments
Receipt of simple instead of expected strong credentials (or vice-versa)		Very low	Misconfiguration
Signature verification failure		Extremely low	May result from cybersecurity attack
Certificate verification failure	Certificate expired	Low	May happen if not renewed in due time
	Certificate revoked	Extremely low	Private key lost or compromised
	Wrong certificate	Very low	May happen after certificate renewal

What could go wrong? Possible approaches to mitigate potential failures

Authentication failed => No connection is established

Coordinate with adjacent COM Centres:

- In case of key pair / certificate renewal
- Always needed in case of authentication failure

Possible approaches to resume traffic **after due coordination**:

- Rollback to simple authentication
- Re-routing through alternate MTA
- In case of expired certificate, ignore temporarily expiration date

AMHS strong authentication: summary

A point-to-point security measure

- As in Doc 9880 Edition 3, AMHS Security / Extended ATS Message Handling Service
- Ensures identity of peer system (UA, MS, MTA)
- Using functionalities embedded in MHS/X.400 standards
- Using concepts shared with end-to-end security (asymmetric cryptography, digital signatures, certificates)
- Leverages short-term availability of European Aviation Common PKI (EACP) and Certification Authority
- Relieves AMHS from current security weaknesses
- Provides security directly integrated in the application systems rather than relying purely on network security

Thank You

ICAO