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 Message Signature

Hans-Jörg MERKLE

Subject Matter Expert

Frequentis Comsoft GmbH, Germany

AMHS Message Signature

01 Introduction

02 Technical Principles

03 Benefits

04 Prerequisites

05 Potential Issues and Mitigation Approaches

06 Summary

AMHS Message Signature – Introduction

An end-to-end security measure

Overall target: Protect AMHS information exchanges at an end-to-end level

- Between User Agents and between User Agent and MTCU

Specification in ICAO Doc 9880, 3rd Edition, Part II

- Element of the AMHS Security Functional Group (AMHS SEC)
- Based on X.400 / ISO/IEC 10021 built-in security mechanisms
- Using well-known asymmetric cryptography

Additional service element

- Component of every AMHS message

Prerequisites: X.509 Public Key Infrastructure (PKI) providing certificates for public keys

AMHS Message Signature – Introduction

Threats – Potential attack vectors

Message-oriented threats in end-to-end information exchanges

- Masquerade
- Modification
- Leakage (loss of confidentiality, anonymity, ...)
- Sequencing (delay, replay, ...)
- ...

MHS in general

Global AMHS security policy:

- Masquerade (originator)
- Modification (content)
- Sequencing (replay)

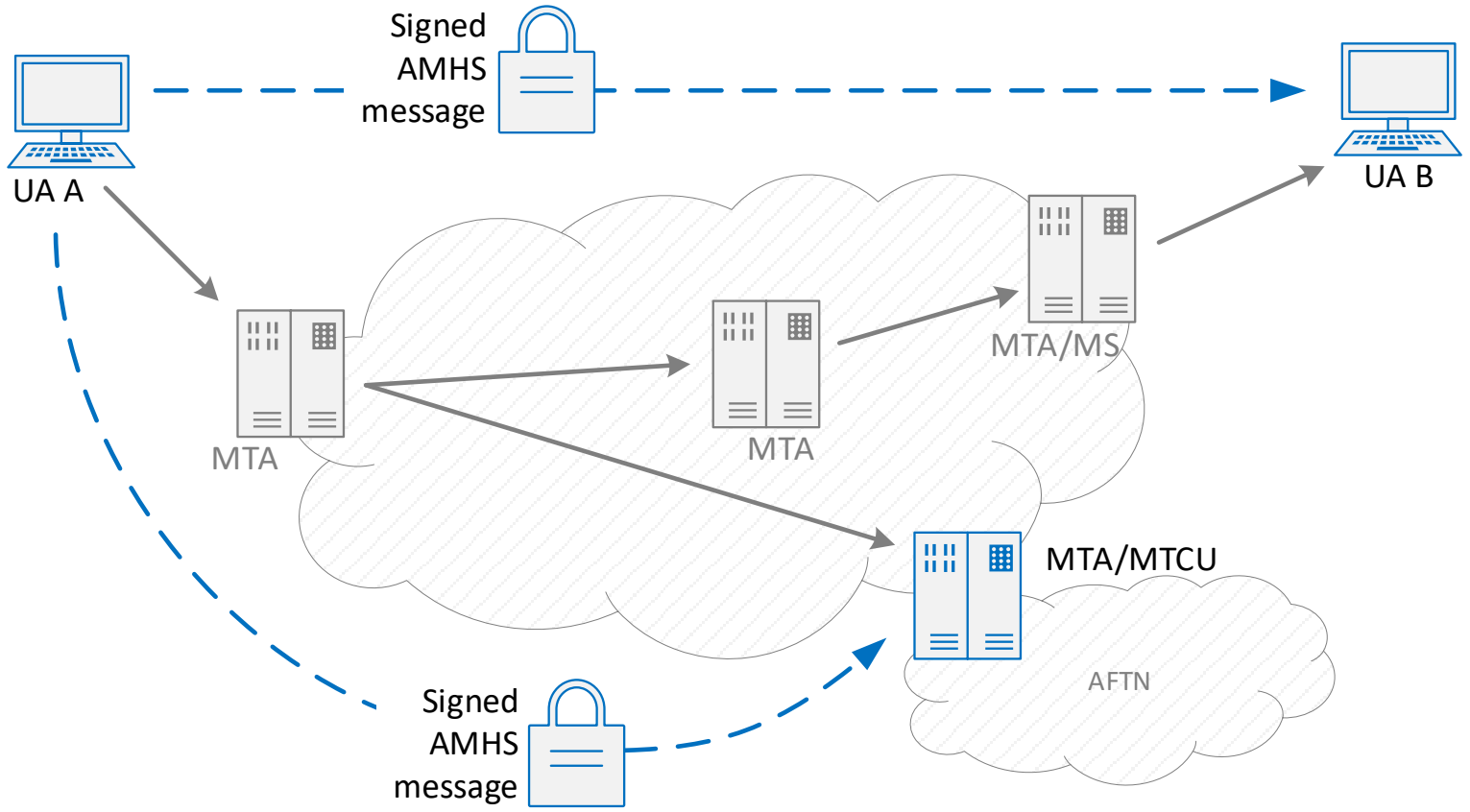
Addressed by AMHS

AMHS Message Signature – Technical Principles

Overview

Scenario

UA A sends
an AMHS message
to UA B and
to an AFTN user
via MTA/MTCU

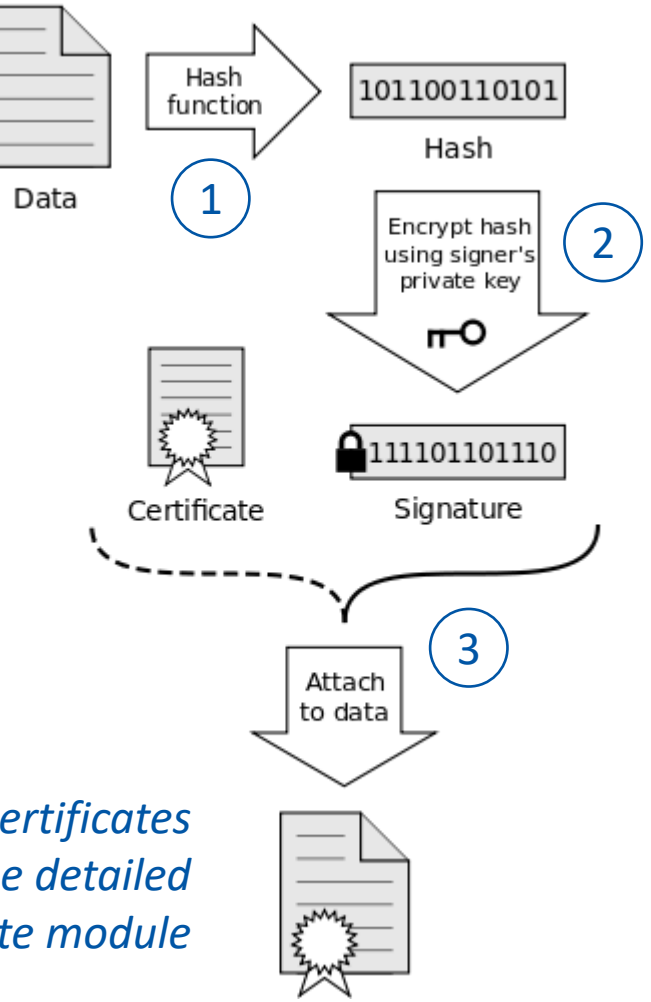


AMHS Message Signature – Technical Principles

How message signing works?

Sender creates AMHS message with additional components

1. Calculate hash value from message content
2. Encipher hash value using own private key
3. Enclose additionally in the envelope
   a. Encrypted hash value and time of generation
      Included in the message-token of the per-recipient-fields
   b. Originator certificate providing the public key
      Included in the message extensions



Asymmetric cryptography, certificates and signing principles will be detailed by a separate module

AMHS Message Signature – Technical Principles

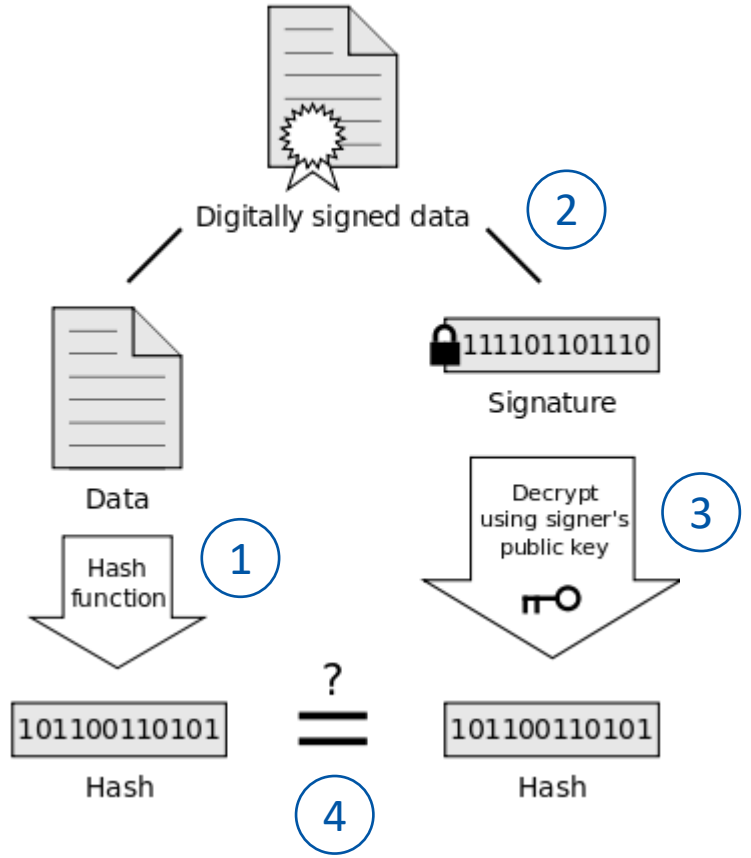
How does the signature protect?

Recipient checks signature

1. Calculate hash value from message content
2. Retrieve enclosed encrypted hash value from message envelope (message-token of recipient-extensions)
3. Decipher encrypted hash value using public key of sender included in its certificate
4. Compare calculated with decrypted hash value to prove validity of signature (originator, content)

Recipient checks for duplicates (replay)

5. Compare time of generation and IPM identifier with those of previously received message



AMHS Message Signature – Technical Principles

Encryption versus Signature

Encryption

- Protection against leakage and modification
- Payload is enciphered in its entirety
- Payload requires decipherment to become visible again

Message
(encrypted)

Signature

- Protection against modification
- Hash value (checksum) is encrypted
- Payload remains visible

Message

Hash
(encrypted)

AMHS Message Signature – Benefits

Improving security of messaging

Assurance by message signature that message

- Has been sent by indicated user or MTCU
- Has not been tampered during its conveyance over the AMHS (end-to-end)
- Has not been replayed

Compliance

- 3rd Edition of ICAO Doc 9880, Part II (AMHS SEC FG)
- Contribution to EU NIS2 Directive and its national legal implementations

AMHS Message Signature – Benefits

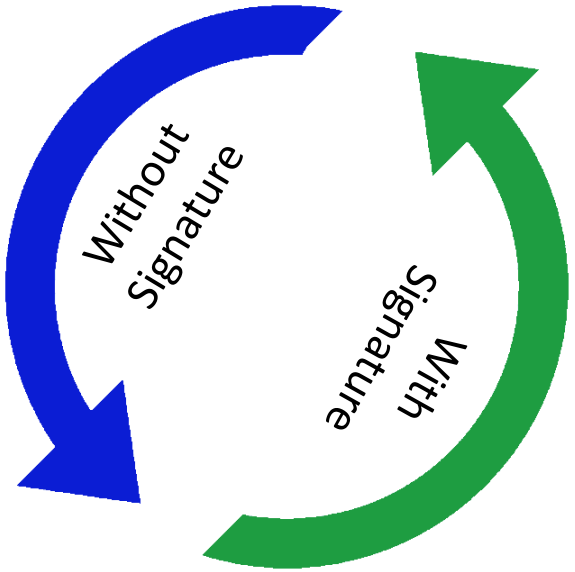
Interoperability

Payload (FPL, MET, NOTAM, ...) remains visible at any point in time because the message content is signed but not encrypted, even if

- AMHS SEC is not supported by recipient implementation
- AMHS message signature check fails

Additional service element

- Not supported by originator
  Recipient receives an unsigned AMHS message
- Not supported by the recipient
  Recipient disregards signature



Full backwards compatibility
Systems (not) implementing AMHS message signature are fully interoperable!

AMHS Message Signature – Prerequisites

What is needed from a technical perspective?

To sign a message ... *upon origination*

- Private key used for message signature → Generation of key pair
- Certificate proving identity (public key) → Issuance of certificate by CA

To validate a signature ... *upon reception*

- Sender certificate → Component of the signed AMHS message
- CA certificates → Pre-installed or part of message
- Certificate Revocation List (CRL) → Provision by the CA issuing certificate

Implementation supporting AMHS message signature

AMHS Message Signature – Prerequisites

What is needed from an organisational perspective?

Internal security organisation

- Procedures Key pair generation, request/renewal of certificates, security errors, ...
- Roles Assignment of related tasks / authorisation by organisation, ...

Internal training for

- Operators (enablement)
- End users (raising awareness)

Joining a Public Key Infrastructure (PKI) establishing trust

- Issuance of certifications by Certification Authority (CA)

Partial conformance, interoperability and pre-operational tests

- Test specifications of ICAO EUR Doc 020 improvements (extensions)

Very similar to AMHS strong authentication

AMHS Message Signature – Potential Issues and Mitigation Approaches

What could go wrong?

- AMHS Security is not implemented — *upon origination or reception*
- Certificate is ... not available — *upon reception*
  - expired
  - revoked (found on certificate revocation list)
- Validation of signature is unsuccessful
  - Originator/certificate mismatch
  - Parameters different from the specification
  - Deviating hash value
  - ...
- Replay identified

AMHS Message Signature – Potential Issues and Mitigation Approaches

How to manage potential issues?

1. Logging of security error

2. Processing in accordance with the local security policy
    a. Make the AMHS message available to the user and indicate a security error
    b. Withhold the AMHS message from the user and indicate a security error
    c. Silently withhold the AMHS message from the user
    d. Another set of actions defined by the local security policy

AMHS Message Signature – Summary

Your key take-aways

- Additional application security element on top of other security features (e.g. network)
- Specification by ICAO Doc 9880, 3rd Edition, Part II – element of Extended ATSMHS
  - Based on X.400 built-in features not specific to AMHS
  - Use of state-of the-art asymmetric cryptography
- End-to-end security by signing every message (originator, content, replay)
- High level of security in combination with AMHS strong authentication
  - Significant reduction of attack surface
- Backwards compatible with implementations w/o AMHS Security
  - Visible content of signed AMHS messages (FPL, MET, NOTAM, ...)
- Public Key Infrastructure (PKI)

Thank You

ICAO