AMHS To SWIM Transition Task Force (AST TF)

AST TF/07 meeting

21st to 24th 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)

Copperchase AMHS Security Demo
P3 and P7 Strong Authentication

Leonardo de Vida

Copperchase AMHS Security P3 and P7 Strong Authentication Demo

What will this Demo will cover?

- An example of X.400 P3 Strong Authentication between a User Agent and the MTA
- An example of X.400 P7 Strong Authentication between a User Agent and the Message Store
- An example of submission by a User Agent of an AMHS message via P3
- An example of reception by a User Agent of an AMHS message via P7

Copperchase AMHS Security Demo

Software used for the demo

- Isode M-Switch pre-release R19.2 – The X.400 MTA and X.400 Message Store
- Copperchase AMHS Terminal – An AMHS User agent
- Wireshark

Isode M-Switch

- Isode M-Switch is an X.400 MTA
- It can be used as an AMHS server, as it supports X.400 P1 and X.400 P3
- The current version, R19.1, supports the requirements of ICAO Doc 9880 Edition 2
- Previous versions supported ICAO Doc 9880 Edition 2, and X.400 P1 Strong Authentication
- The additional Isode X.400 P7 Message Store software adds support to X.400 P7 users

Isode M-Switch release R19.2

- For this demo, we are using a pre-release version of Isode R19.2
- It has been extended to support all the AMHS Security requirements specified in ICAO Doc 9880 Edition 3
- This new release implements
  - X.400 P3 Strong Authentication
  - X.400 P7 Strong Authentication
  - AMHS message signing according to Doc 9880 Edition 3 by the MTCU

AMHS Terminal

- The AMHS Terminal is an X.400 User Agent that can be used to send and receive AMHS messages
- It supports both X.400 P3 and X.400 P7 to send AMHS messages
- It also supports AFTN to send AFTN messages
- Like most email clients, the AMHS Terminal supports multiple “accounts” running at the same time
- It is possible to have one account connected to an X.400 P3 MTA and another to an X.400 P7 Message Store
- This makes it easy to send and receive messages from the same application
- To avoid having two User Agents, we will use the multiple-account feature for the demo

AMHS Terminal – New AMHS Security Features

- The new version of the AMHS Terminal supports P3 and P7 Strong Authentication and AMHS message signing
- The use of P3 and P7 Strong Authentication is optional, as Simple Authentication is also supported
- To configure Strong Authentication, the AMHS Terminal needs to be provided with at the very least:
  - An PKCS#12 certificate that matches the O/R address of the account to use
  - The passphrase required to use the PKCS#12 certificate
  - A directory in the file system where CA Trust Anchors are stored
  - For P3 accounts, it also requires: The MTA Name and Global Domain Identifier

Certificates

- To configure P3 and P7 Strong Authentication, it was necessary to obtain suitable certificates for the User Agents
- Copperchase does not have, as of today, access to EACP certificates
- For this demo, the required certificates were generated with an Isode tool, called Sodium CA
- To keep this demo simple, for this demo, we will not show the Sodium CA tool or the generation of certificates
- SodiumCA was used to create a self-generated CA certificate and then issue the required user certificates
- The use of these self-generated certificates is suitable for a demonstration like this
- For operational systems in Europe, certificates for MTAs, MTCUs and UAs will be generated by EACP

DEMO

Thank You

ICAO