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)

Telefonica AMHS Security Demo
AMHS Strong Authentication

Pedro Juan Jimenez Garcia

Demo - P1 MTA Strong Bind

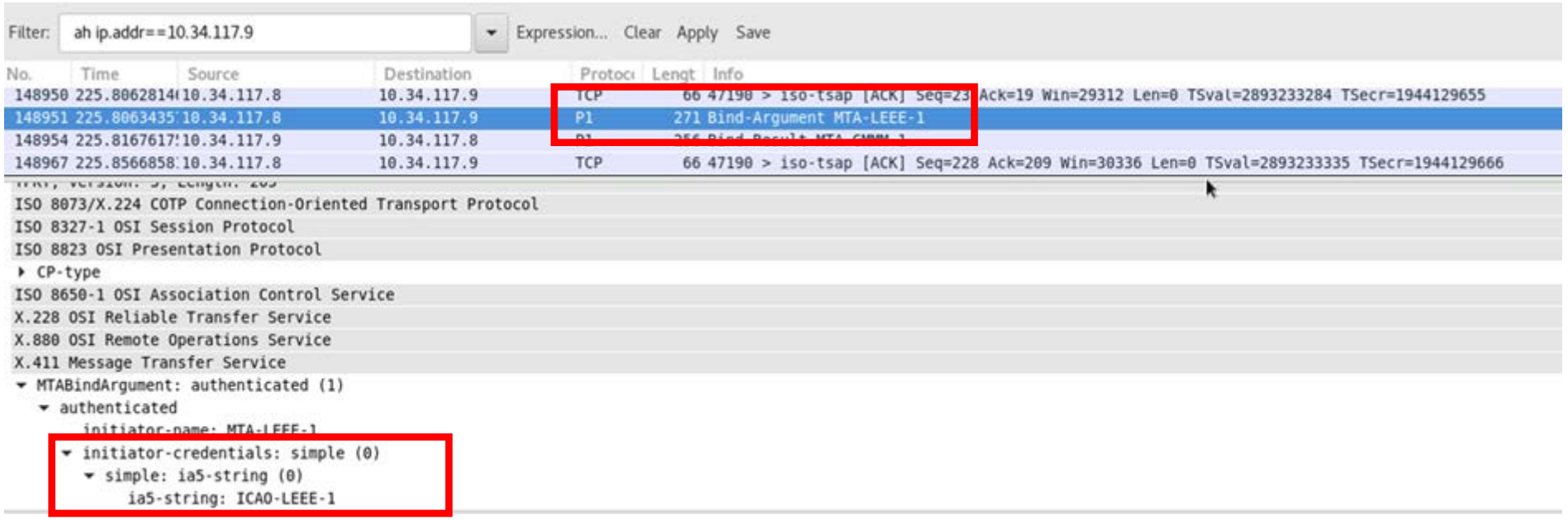
- ✓ Demonstrated using **current version of ENAIRE AMHS System** (development environment)
  - ✓ Based on **Doc 9880 Edition 2** specification **+ optional features (strong bind is only optional in Ed2)**
  - ✓ Slightly different from Doc 9880 Edition 3 specification but with a lot of similarity
    - ✓ **Close enough to be used for the demo in a manner representative of Ed3**

Demo environment

- ✓ **Telefonica development environment** – production mirror (Isode R18.0v22)
- ✓ Two MTAs on two machines - operated with Mconsole Isode tool
- ✓ Use of Wireshark packet analyzer to examine bind operations

X.400 P1 MTA Binds

- ✓ 2 MTAs that uses X.400 P1 connects to the peer MTA using an MTA Bind
  - ✓ MTA-LEEE-1
  - ✓ MTA-GMMM-1
- ✓ The MTA Bind operation can be Simple or Strong (currently all MTAs use Simple binds)


Filter: ah ip.addr==10.34.117.9
Expression... Clear Apply Save
No. Time Source Destination Protoc Lengt Info
148950 225.8062814 10.34.117.8 10.34.117.9 TCP 66 47190 > iso-tsap [ACK] Seq=23 Ack=19 Win=29312 Len=0 TSval=2893233284 TSecr=1944129655
148951 225.8063435 10.34.117.8 10.34.117.9 P1 271 Bind-Argument MTA-LEEE-1
148954 225.8167617 10.34.117.9 10.34.117.8
148967 225.8566858 10.34.117.8 10.34.117.9 TCP 66 47190 > iso-tsap [ACK] Seq=228 Ack=209 Win=30336 Len=0 TSval=2893233335 TSecr=1944129666
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
ISO 8327-1 OSI Session Protocol
ISO 8823 OSI Presentation Protocol
CP-type
ISO 8650-1 OSI Association Control Service
X.228 OSI Reliable Transfer Service
X.880 OSI Remote Operations Service
X.411 Message Transfer Service
MTABindArgument: authenticated (1)
authenticated
initiator-name: MTA-LEEE-1
initiator-credentials: simple (0)
simple: ia5-string (0)
ia5-string: ICAO-LEEE-1

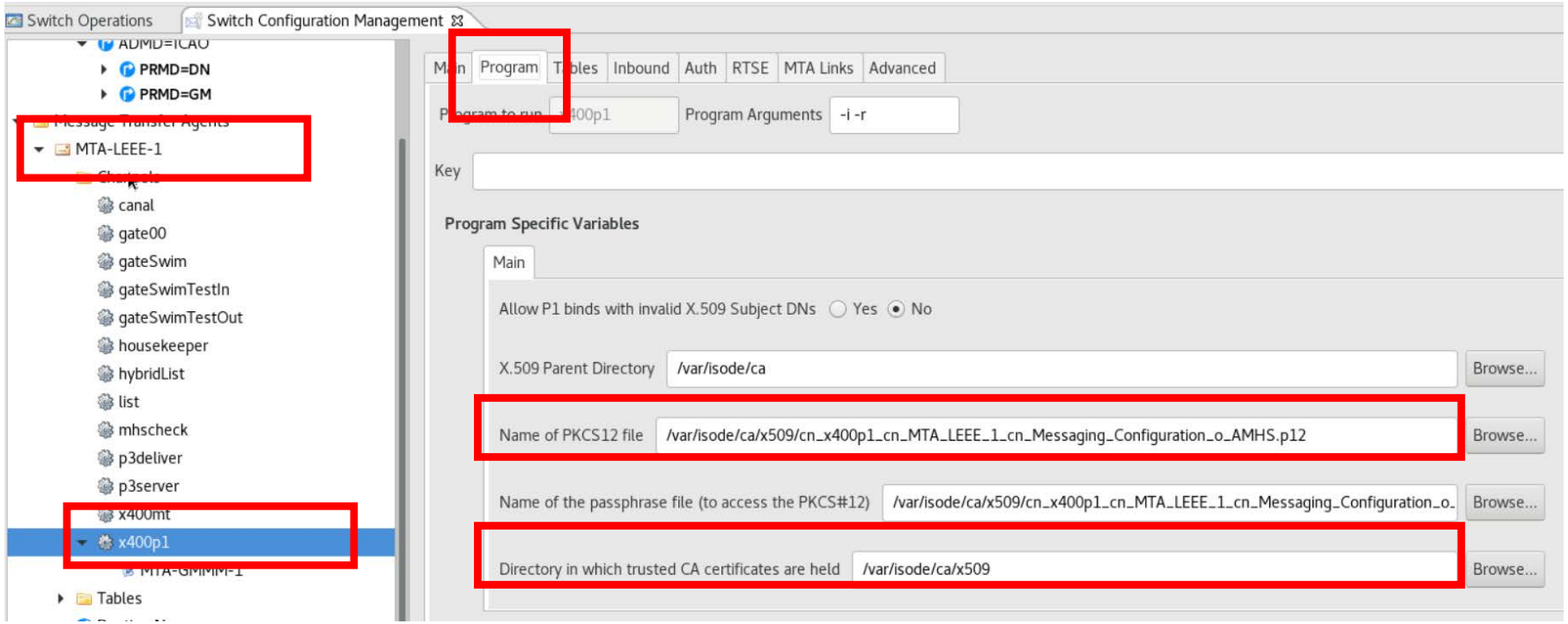
P1 MTA Strong Bind

- ✓ A P1 Strong MTA Bind can be stablished using certificates
- ✓ Configuration required on both MTAs
- ✓ Strong bind declared at peer MTA level

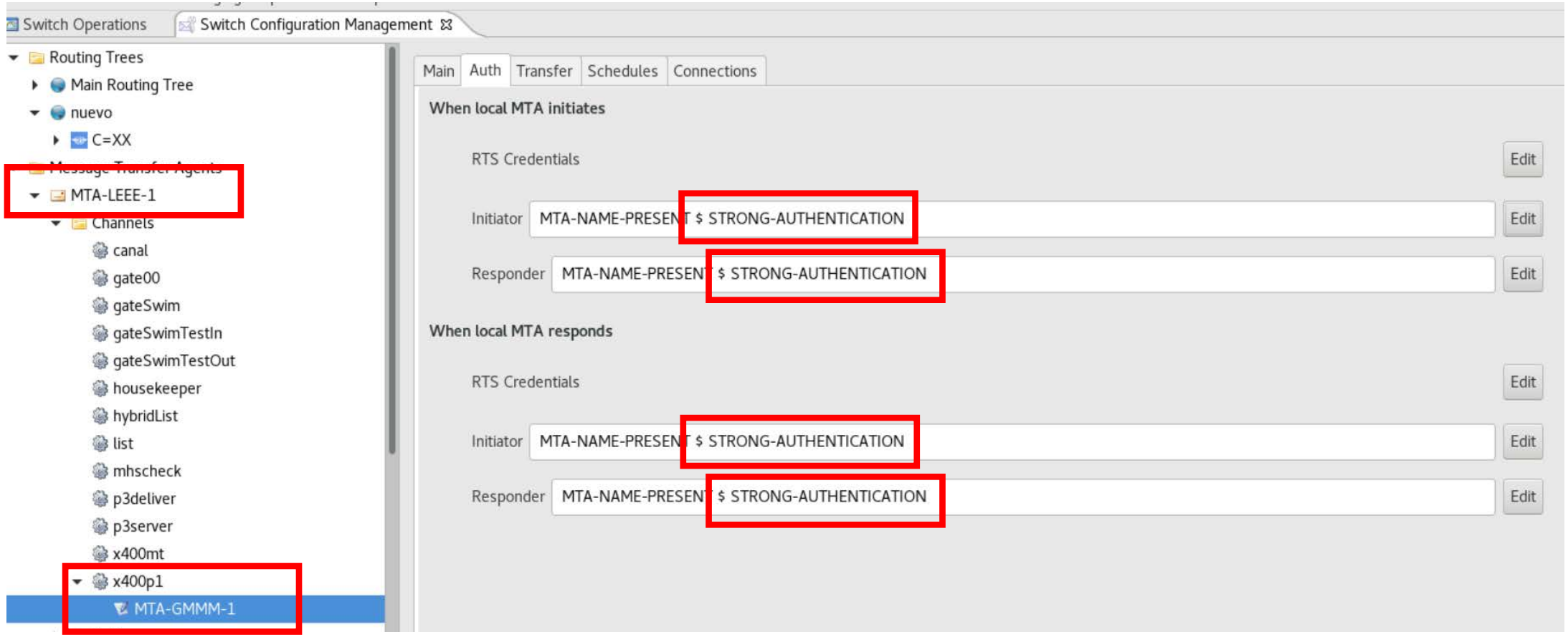
P1 MTA Strong Bind – Certificates configuration (Both)

- ✓ Required certificates were generated Isode CA tool
- ✓ Certificates issued for the X.400 P1 functionality, the local MTA
- ✓ Configuration implemented for the demo:
  - ✓ Certificate of local MTA in PKCS 12 format
  - ✓ Directory in which trusted CA certificates are held (including peer MTA certificates)

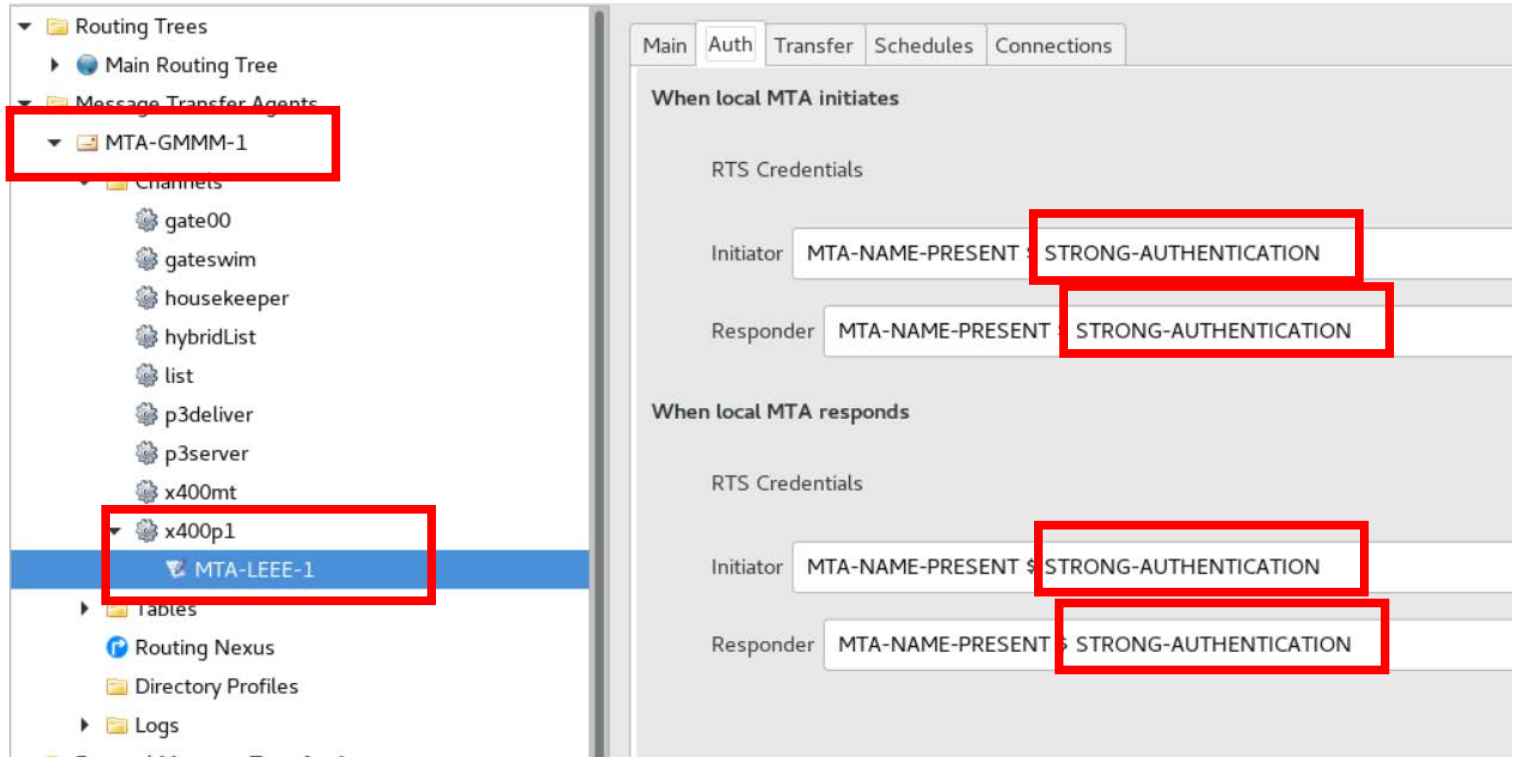
P1 certificates configuration (Both)



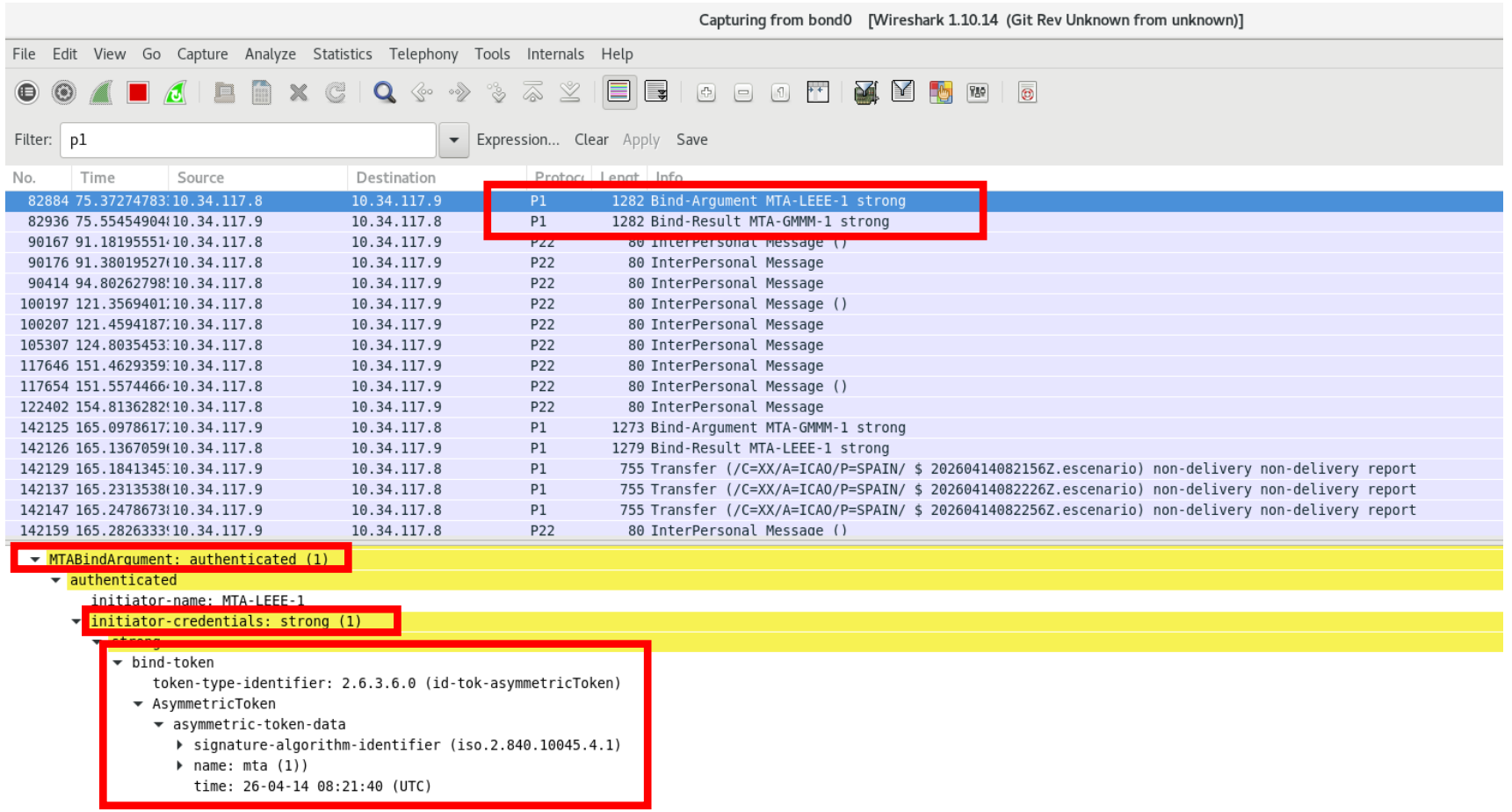
P1 Strong authentication – Configuration (MTA-LEEE-1)



P1 MTA Bind Strong - Configuration (MTA-GMMM-1)



P1 Strong Authentication Result



MTA Strong Bind – **Current situation**

- ✓ X.400 P1 bind operations
- ✓ If both MTAs implement it, P1 Strong Bind can be configured.
- ✓ If generic CA root doesn't exist, an agreement on CAs is required

MTA Strong Bind – **Target situation**

- ✓ Based on **Doc 9880 Edition 3 for all MTA implementations**
- ✓ As soon as both MTAs implement it, P1 Strong Bind should be configured.
- ✓ **European Aviation Common PKI** to be used as Common CA

Thank You

ICAO