

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)



European and North Atlantic Office



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)



European and North Atlantic Office



Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	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	P1	256	Bind-Result MTA-CIRN-1
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 established using certificates
- ✓ Configuration required on both MTAs
- ✓ Strong bind declared at peer MTA level

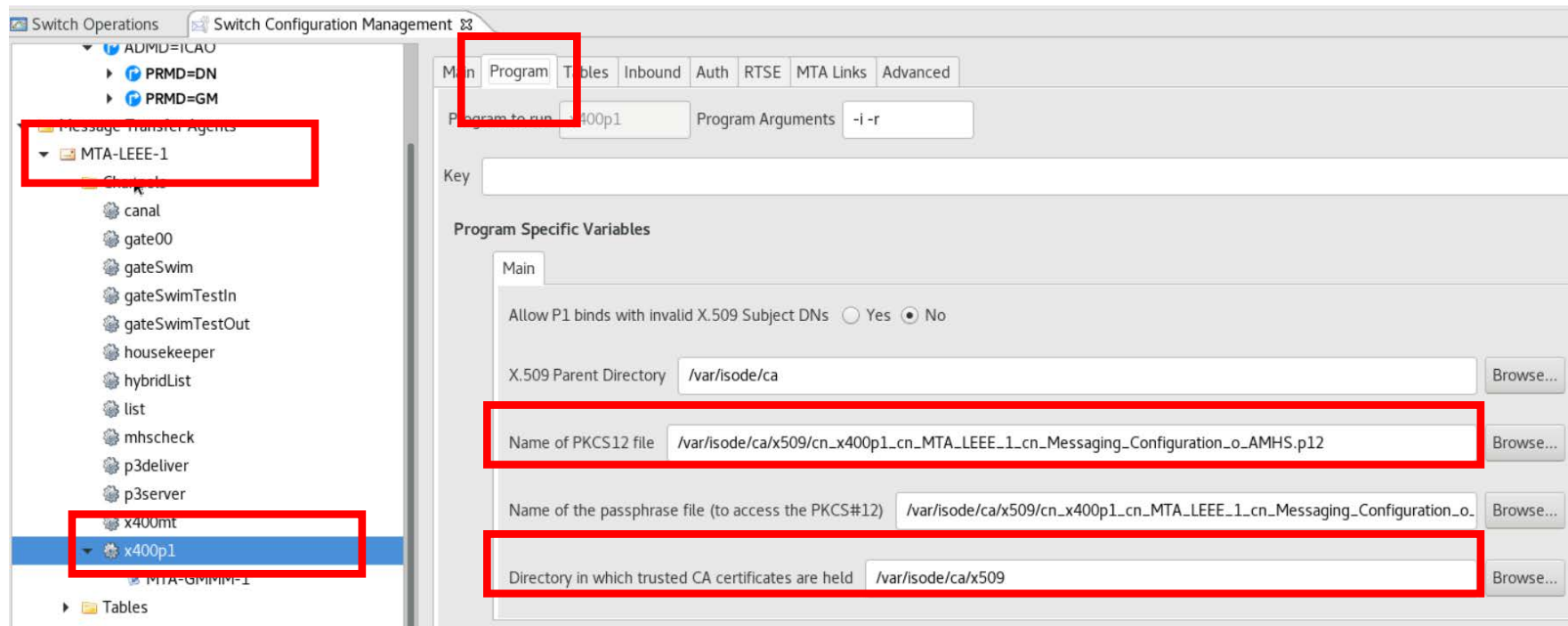


P1 MTA Strong Bind – Certificates configuration (Both)

- ✓ 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)



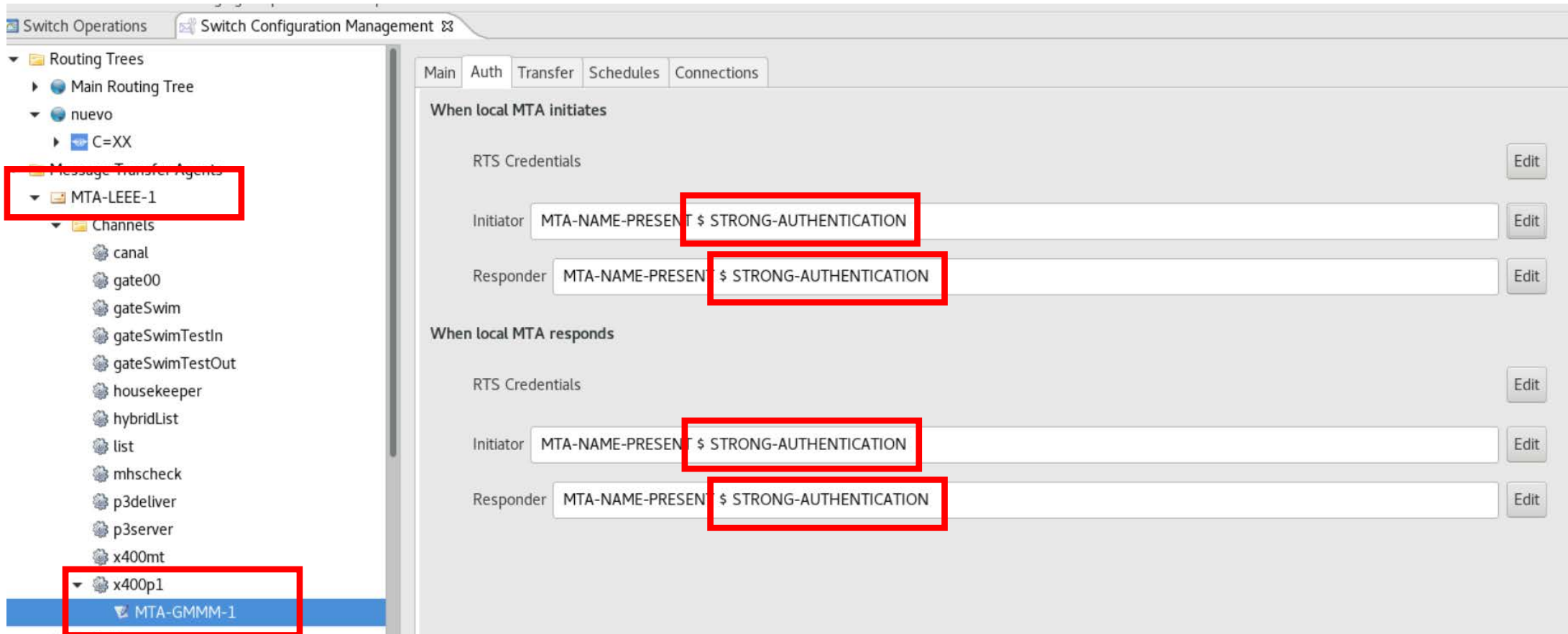
P1 certificates configuration (Both)



The screenshot shows the 'Switch Configuration Management' interface. On the left, a tree view shows the configuration hierarchy: ADMD=ICAO, PRMD=DN, PRMD=GM, Message Transfer Agents, MTA-LEEE-1, and x400p1. The 'Program' tab is selected. The 'Program to run' is 'x400p1' and 'Program Arguments' are '-i -r'. Under 'Program Specific Variables', the 'Main' tab is active. The configuration includes: 'Allow P1 binds with invalid X.509 Subject DNs' set to 'No'; 'X.509 Parent Directory' set to '/var/isode/ca'; 'Name of PKCS12 file' set to '/var/isode/ca/x509/cn_x400p1_cn_MTA_LEEE_1_cn_Messaging_Configuration_o_AMHS.p12'; 'Name of the passphrase file (to access the PKCS#12)' set to '/var/isode/ca/x509/cn_x400p1_cn_MTA_LEEE_1_cn_Messaging_Configuration_o_'; and 'Directory in which trusted CA certificates are held' set to '/var/isode/ca/x509'. Red boxes highlight the 'Program' tab, the 'MTA-LEEE-1' and 'x400p1' nodes in the tree, and the three PKCS12 file and passphrase file configuration fields.



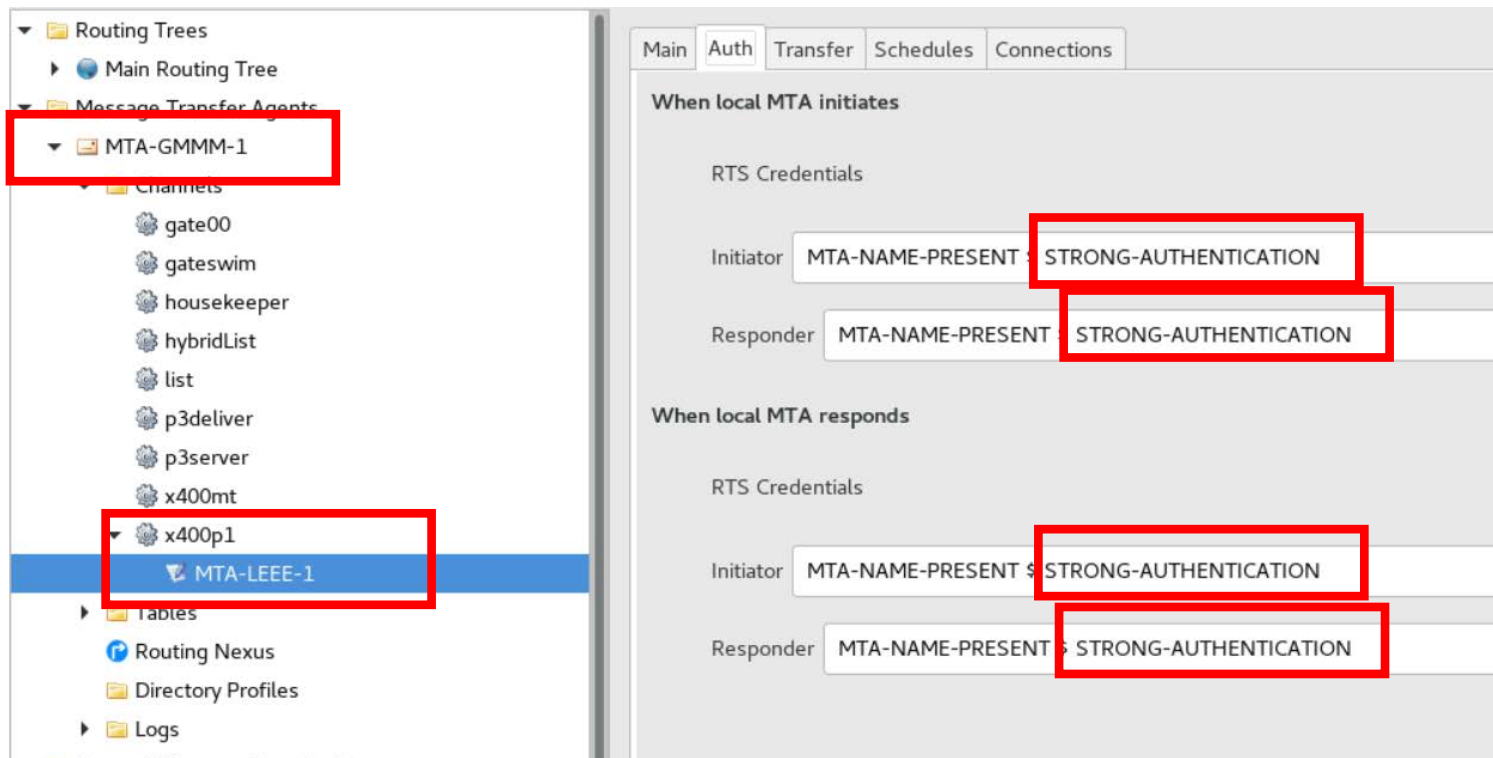
P1 Strong authentication – Configuration (MTA-LEEE-1)



The screenshot displays the 'Switch Configuration Management' interface. On the left, a tree view shows the configuration structure: 'Routing Trees' > 'Main Routing Tree' > 'nuevo' > 'C=XX' > 'Message Transfer Agents' > 'MTA-LEEE-1' (highlighted with a red box). Under 'MTA-LEEE-1', there is a 'Channels' folder containing various channels like 'canal', 'gate00', etc., and 'x400p1' (highlighted with a red box). Below 'x400p1' is 'MTA-GMMM-1' (highlighted with a red box). The main panel shows the configuration for 'When local MTA initiates' and 'When local MTA responds'. Each section has 'RTS Credentials' and 'Initiator' fields. The 'Initiator' fields contain the text 'MTA-NAME-PRESENT \$ STRONG-AUTHENTICATION' and are highlighted with red boxes. 'Responder' fields are also present but not highlighted. Each field has an 'Edit' button to its right.



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



The screenshot shows a configuration interface for Message Transfer Agents (MTAs). On the left, a tree view shows the hierarchy: Routing Trees > Main Routing Tree > Message Transfer Agents > MTA-GMMM-1 > Channels > x400p1 > MTA-LEEE-1. The 'MTA-GMMM-1' and 'MTA-LEEE-1' nodes are highlighted with red boxes. On the right, the 'Auth' tab is active, showing configuration for 'When local MTA initiates' and 'When local MTA responds'. Both sections have 'Initiator' and 'Responder' fields set to 'MTA-NAME-PRESENT' and 'STRONG-AUTHENTICATION', with these values highlighted by red boxes.



P1 Strong Authentication Result

Capturing from bond0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: p1 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
82884	75.37274783	10.34.117.8	10.34.117.9	P1	1282	Bind-Argument MTA-LEEE-1 strong
82936	75.55454904	10.34.117.9	10.34.117.8	P1	1282	Bind-Result MTA-GMMM-1 strong
90167	91.18195551	10.34.117.8	10.34.117.9	P22	80	InterPersonal Message ()
90176	91.38019527	10.34.117.8	10.34.117.9	P22	80	InterPersonal Message
90414	94.80262798	10.34.117.8	10.34.117.9	P22	80	InterPersonal Message
100197	121.3569401	10.34.117.8	10.34.117.9	P22	80	InterPersonal Message ()
100207	121.4594187	10.34.117.8	10.34.117.9	P22	80	InterPersonal Message
105307	124.8035453	10.34.117.8	10.34.117.9	P22	80	InterPersonal Message
117646	151.4629359	10.34.117.8	10.34.117.9	P22	80	InterPersonal Message
117654	151.5574466	10.34.117.8	10.34.117.9	P22	80	InterPersonal Message ()
122402	154.8136282	10.34.117.8	10.34.117.9	P22	80	InterPersonal Message
142125	165.0978617	10.34.117.9	10.34.117.8	P1	1273	Bind-Argument MTA-GMMM-1 strong
142126	165.1367059	10.34.117.8	10.34.117.9	P1	1279	Bind-Result MTA-LEEE-1 strong
142129	165.1841345	10.34.117.9	10.34.117.8	P1	755	Transfer (/C=XX/A=ICAO/P=SPAIN/ \$ 20260414082156Z.escenario) non-delivery non-delivery report
142137	165.2313538	10.34.117.9	10.34.117.8	P1	755	Transfer (/C=XX/A=ICAO/P=SPAIN/ \$ 20260414082226Z.escenario) non-delivery non-delivery report
142147	165.2478673	10.34.117.9	10.34.117.8	P1	755	Transfer (/C=XX/A=ICAO/P=SPAIN/ \$ 20260414082256Z.escenario) non-delivery non-delivery report
142159	165.2826333	10.34.117.9	10.34.117.8	P22	80	InterPersonal Message ()

▾ MTABindArgument: authenticated (1)
 ▾ authenticated
 initiator-name: MTA-LEEE-1
 ▾ initiator-credentials: strong (1)
 ▾ bind-token
 token-type-identifier: 2.6.3.6.0 (id-tok-asymmetricToken)
 ▾ AsymmetricToken
 ▾ asymmetric-token-data
 ▸ signature-algorithm-identifier (iso.2.840.10045.4.1)
 ▸ name: mta (1)
 time: 26-04-14 08:21:40 (UTC)



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

