
ICAO • OACI • ИКАО
国际民航组织 • ايكاو
INTERNATIONAL
CIVIL AVIATION
ORGANIZATION

AFS to SWIM Transition Task Force (AST TF)

SEVENTH MEETING

AMHS SECURITY WORKSHOP

(Dubrovnik, Croatia, 21-24 April 2026)

Agenda

- ✓ Introduction to the European Aviation Common PKI (EACP)
- ✓ AMHS requirements gathering and analysis
- ✓ Securing AMHS with EACP certificates

Dr Abdel Youssouf

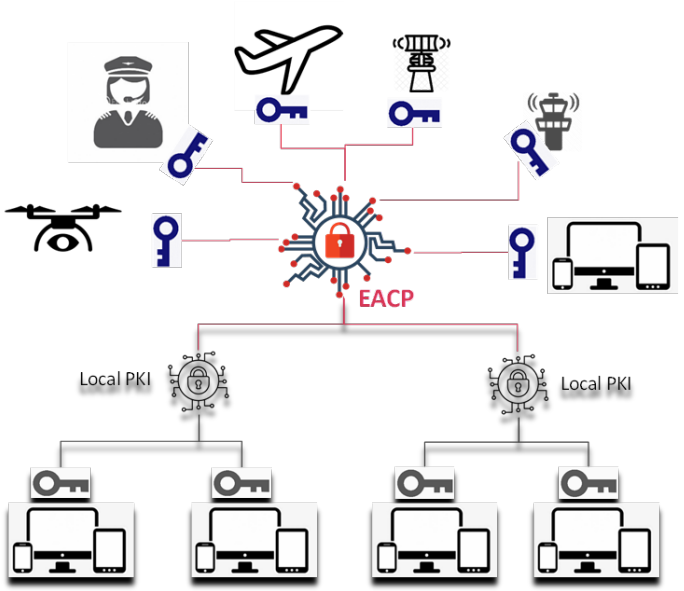
Securing AMHS services with EACP certificates

Agenda

- ✓ Introduction to the European Aviation Common PKI (EACP)
- ✓ AMHS requirements gathering and analysis
- ✓ Securing AMHS with EACP certificates

European Aviation Common PKI

Introduction



Family 5.1.1: Common Backbone for digital certificate

Lifecycle management + Interoperability Tool for Local PKIs.

Family 5.2.1:

- Option A: Use Common Backbone
- Option B: Use eligible local PKIs

Improve security throughout aviation value chain

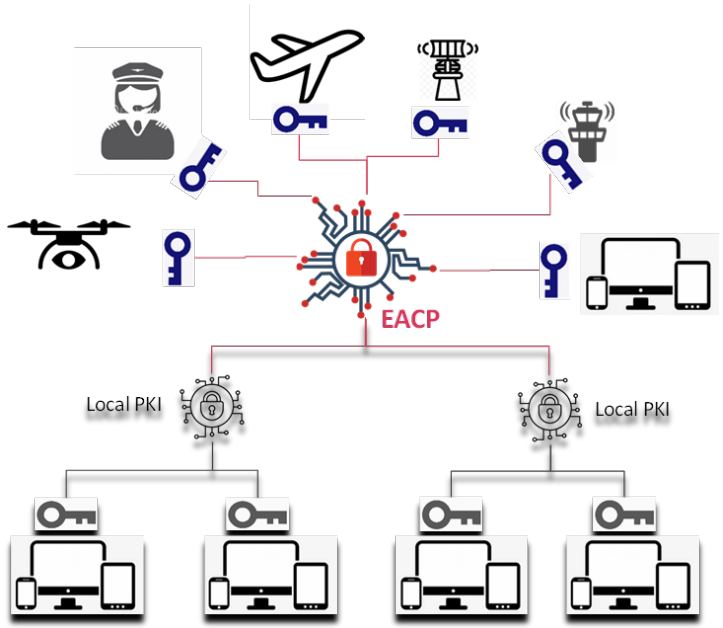
Trust Framework (governance, policies, procedures)

Common service reducing costs & providing:

- Digital certificates
- Interoperability between existing Local PKI

European Aviation Common PKI

Introduction



- EACP: Family 5.1.1
  - EACP - Common PKI Services
    - EACP – Public (Well-Known CA) part.
    - EACP – Private (Non-Well-Known CA) part.
  - EACP – Certificate Trust List (CTL)
- Stakeholders can use:
  - Family 5.2.1 Option A: use EACP – Common Backbone
  - Family 5.2.1 Option B: Use eligible Local PKI from the CTL
  - Both options

European Aviation Common PKI

Introduction

- EACP Interfaces:
  - EACP Production (OPS) Environment: https://cm.harica.gr
  - EACP Staging environment: https://cm-stg.harica.gr
- Provider's CAs:
  - https://repo.harica.gr/rep_dyn.php
- EACP Policy documentation (CP, CPS, PDS, Subscriber Agreement, Data Privacy Statement):
  - https://repo.harica.gr/procedures.php
- Certificate Status:
  - Via OCSP: http://ocsp.harica.gr
  - Via CRLs: http://crl.harica.gr / + reference to the certificate type signed by the issuer
- Guides on how to purchase HARICA digital certificates:
  - https://www.harica.gr/en/Guides and https://guides-stg.harica.gr/docs/Guides/
  - To develop JSON calls (REST API): https://developer.harica.gr

European Aviation Common PKI

EACP Certificate fees

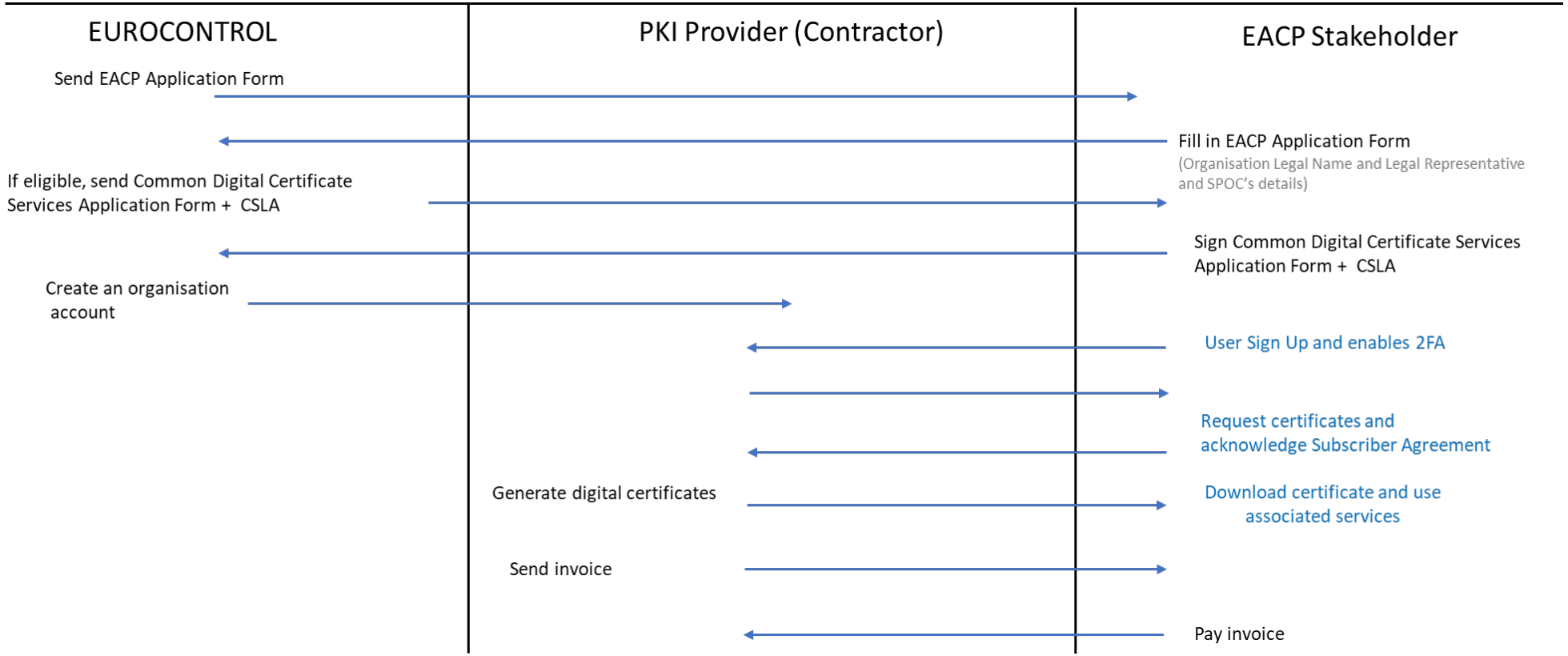
Digital certificate for TLS server (not required to be signed by a Well-known CA) – Type 2

Type of certificate	Number of certificates	Validity: cost for 1 year validity	cost for 2 year validity	cost for 3 year validity
SSL DV (simple) Cost per validated Domain	1 - 5.000	€ 0,80	€ 1,44	€ 1,92
	5.001 - 10.000	€ 0,72	€ 1,30	€ 1,73
	10.001 - 20.000	€ 0,65	€ 1,17	€ 1,56
	20.001 - 50.000	€ 0,58	€ 1,05	€ 1,40
	50.001 - 100.000	€ 0,52	€ 0,94	€ 1,26
	100.001 - 500.000	€ 0,47	€ 0,85	€ 1,13
	500.001 - 1.000.000	€ 0,43	€ 0,77	€ 1,02

Type of certificate	Number of certificates	Validity: cost for 1 year validity	cost for 2 year validity	cost for 3 year validity
TLS client OV Certificates for client authentication that contain Subject information about the Organization	1 - 5.000	€ 2,00	€ 3,60	€ 4,80
	5.001 - 10.000	€ 1,80	€ 3,24	€ 4,32
	10.001 - 20.000	€ 1,62	€ 2,92	€ 3,89
	20.001 - 50.000	€ 1,46	€ 2,62	€ 3,50
	50.001 - 100.000	€ 1,31	€ 2,36	€ 3,15
	100.001 - 500.000	€ 1,18	€ 2,13	€ 2,83
	500.001 - 1.000.000	€ 1,06	€ 1,91	€ 2,55

European Aviation Common PKI

EACP Onboarding Process



Agenda

- ✓ Introduction to the European Aviation Common PKI (EACP)
- ✓ AMHS requirements gathering and analysis
- ✓ Securing AMHS with EACP certificates

AMHS Requirements gathering and analysis

AMHS - Requirement 1

Use Case 1	
Business Case Description	Certificates for mutual authentication between AMHS MTAs, upon X.400 MTABind.
Description	Authentication by means of X.400 bind-token (including a *bind-token-signed-data*), based on the signature of a random number. The system (MTA) itself, which corresponds to the *subject* of the certificate, is identified by its MTAName, stored in the *subjectAltName*certificate extension taking its *otherName* name form.
ICAO Requirements	ICAO Requirement (ICAO Doc 9880 Part II, paras 3.2.4.7: *An X.509 MTA certificate used in support of the extended ATSMHS shall include a SubjectAltName certificate extension implementing the otherName name form among those offered by the GeneralName syntax.* The type/OID required by the otherName is set to 2.6.5.6.0.

AMHS Requirements gathering and analysis

AMHS – Requirement 2

Use Case 2	
Business Case Description	Certificates for mutual authentication between a UA and its Attachment-MTA, upon X.400 MTSBind. The MTA certificates can be identical to those for MTA-MTA authentication.
Description	Authentication by means of X.400 bind-token (including a bind-token-signed-data), based on the signature of a random number. The system (UA) itself, which corresponds to the subject of the certificate, is identified by itsORAddressAndOptionalDirectoryName, which is an X.400 O/R address and is stored in the subjectAltNamecertificate extension taking it in its x400Address name form.
ICAO Requirements	ICAO Requirement (ICAO Doc 9880 Part II, para 3.1.4.3.5: *An AMHS user X.509 certificate used in support of the extended ATSMHS shall include a SubjectAltName certificate extension implementing the x400Address name form among those offered by the GeneralName syntax.*

AMHS Requirements gathering and analysis

AMHS - Requirement 3

Use Case 3	
Business Case Description	Certificates for digital signature of messages generated and sent by a UA, to ensure message origin authentication and message content integrity.
Description	Signature by means of X.400 message-token (including a message-token-signed-data), based on message content signature. The system (UA) itself, which corresponds to the subject of the certificate, is identified by itsORAddressAndOptionalDirectoryName, which is an X.400 O/R address and is stored in the subjectAltNamecertificate extension taking its in its x400Address name form.
ICAO Requirements	ICAO Requirement (ICAO Doc 9880 Part II, para 3.1.4.3.5: *An AMHS user X.509 certificate used in support of the extended ATSMHS shall include a SubjectAltName certificate extension implementing the x400Address name form among those offered by the GeneralName syntax.*

AMHS Requirements gathering and analysis

AMHS - Requirement 4

Use Case 4	
Business Case Description	Certificates for digital signature of messages generated and sent by a MTCU.
Description	Signature by means of X.400 message-token (including a message-token-signed-data), based on message content signature. The system (MTCU) itself, which corresponds to the subject of the certificate, is identified by its MTAName, stored in the subjectAltNamecertificate extension taking its otherName name form.
ICAO Requirements	ICAO Requirement (ICAO Doc 9880 Part II, paras 4.2.3.13: *An X.509 MTA certificate allocated to a message transfer and control unit used to support the extended ATSMHS shall include a SubjectAltName certificate extension implementing the otherName name form among those offered by the GeneralName syntax.*

AMHS Digital Certificate Specifications

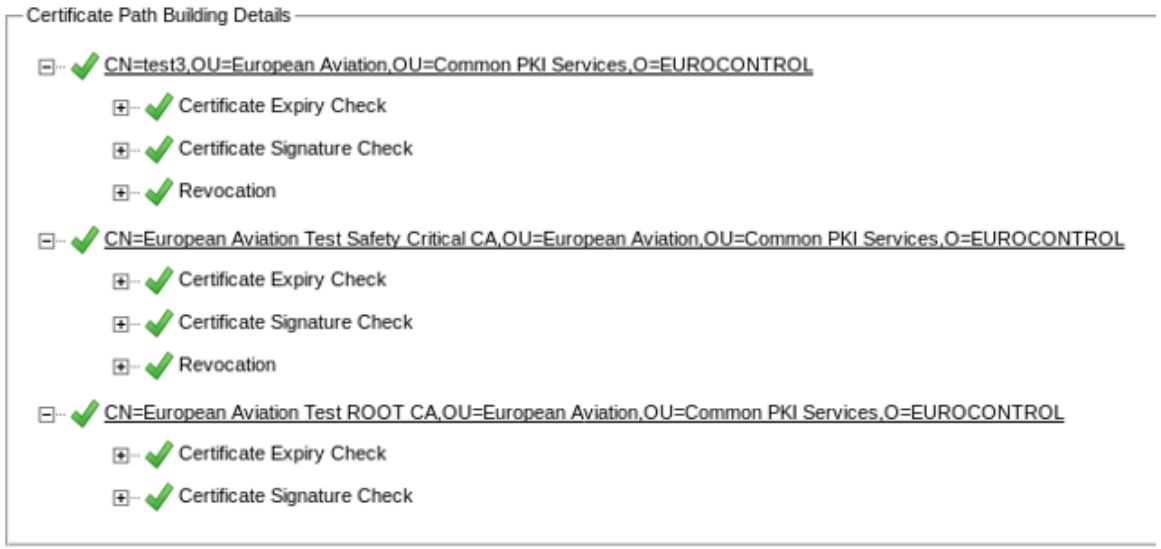
AMHS Digital Certificate analysis

- Digital Certificate Type and Purpose:
  - Type 1 certificate: MTA to MTA (requirement 1)
    - → Authentication certificate with SAN having Othername with OID= 2.6.5.6.0 and MTA-name
  - Type 2 certificate: UA to MTA (requirement 2 & requirement 3)
    - → Authentication and Message Signing certificate having SAN with X400AddressName
  - Type 3 certificate MTCU (requirement 4)
    - → Message Signing certificate with SAN having Othername with OID= 2.6.5.6.0 and MTA-name

AMHS Digital Certificate Specifications

Digital Certificate Validation: Basic validation

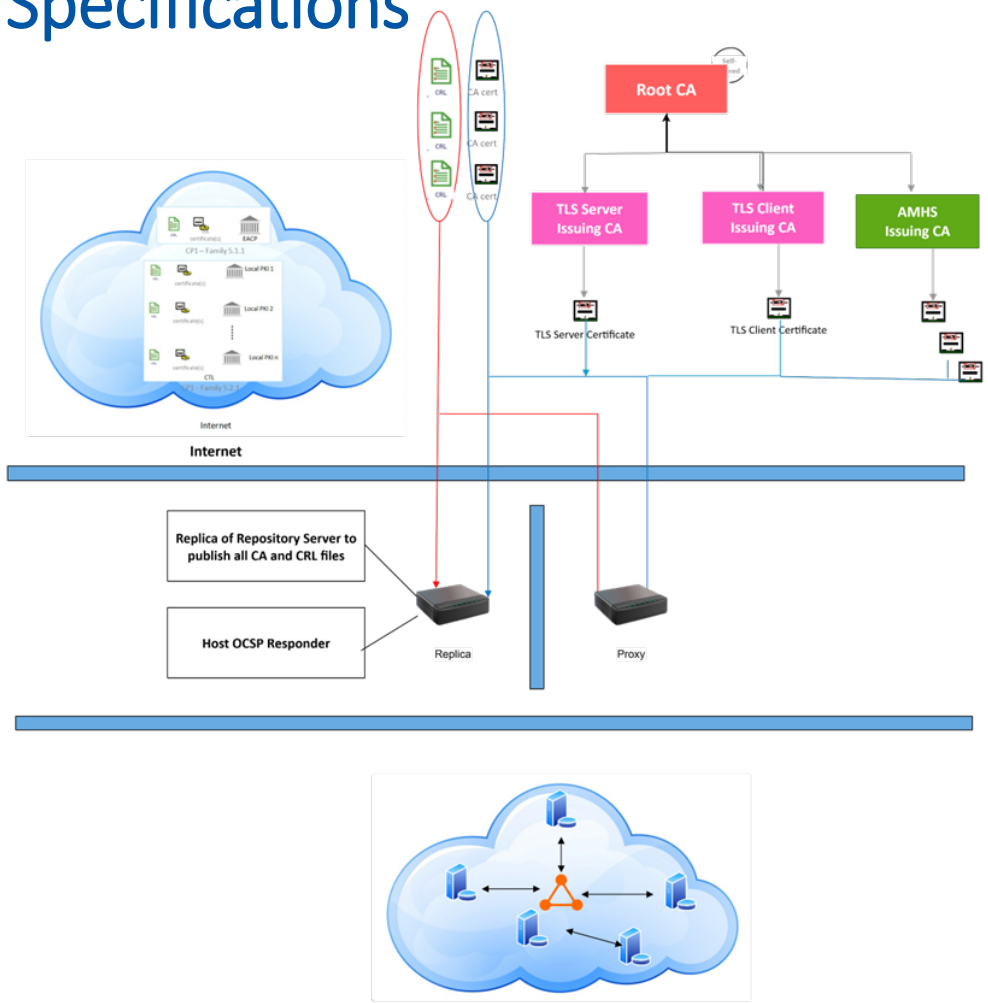
- Path validation. At every layer, validate the following items up to a trusted Anchor:
  - Validity period
  - Digital signature
  - Revocation



AMHS Digital Certificate Specifications

Digital Certificate Validation: Basic validation

- AMHS servers and associated services may be provided in dedicated network (e.g. PENS/NewPENS) while the PKI services are (may be) running on the Internet.
- Need to access at least Validation inputs (CRLs/OCSP + CA Certificates)
- EUROCONTROL is studying the possibility to provide Replica/Proxy
- In the meantime: use the CRL and CA certificate **caching**



Agenda

- ✓ Introduction to the European Aviation Common PKI (EACP)
- ✓ AMHS requirements gathering and analysis
- ✓ Securing AMHS with EACP certificates

AMHS Digital Certificate Lifecycle Management

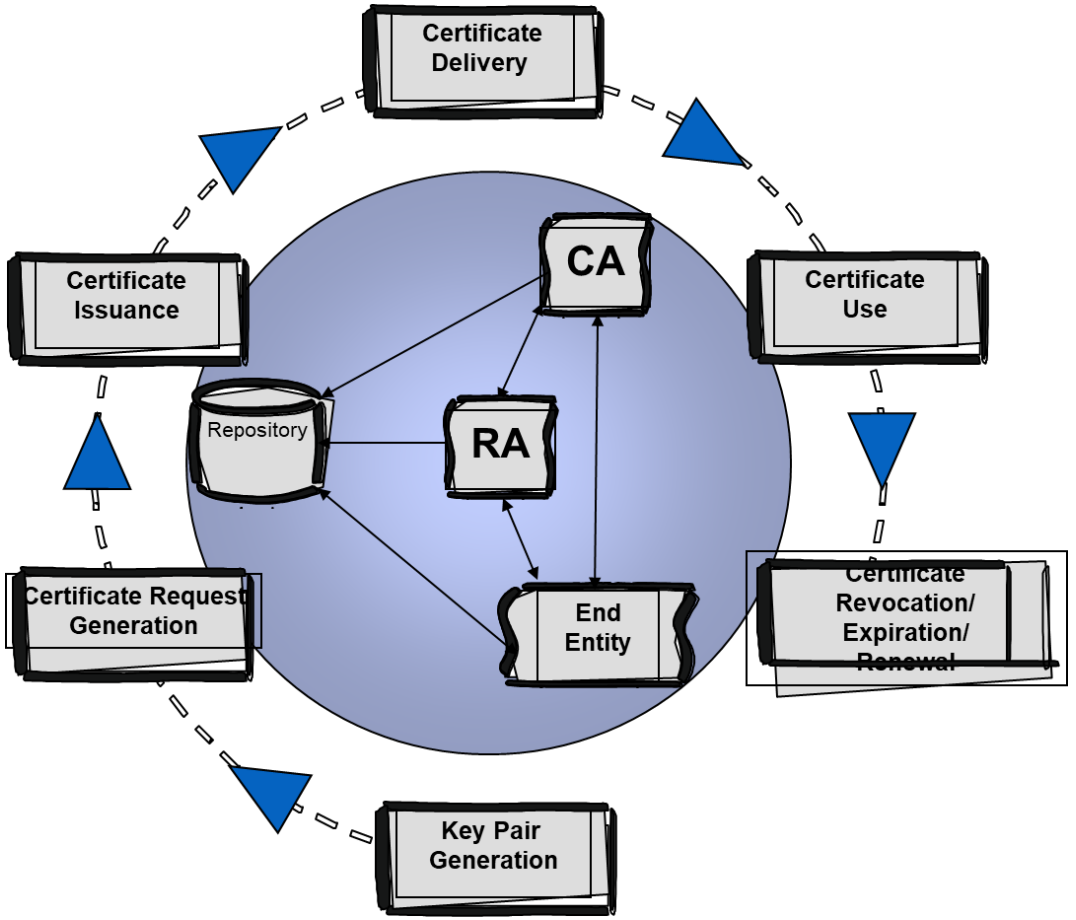
Certificate lifecycle management phases

- Key-pair generation
- Certificate Request

- Request Verification
- Certificate Issuance
- Certificate Publication

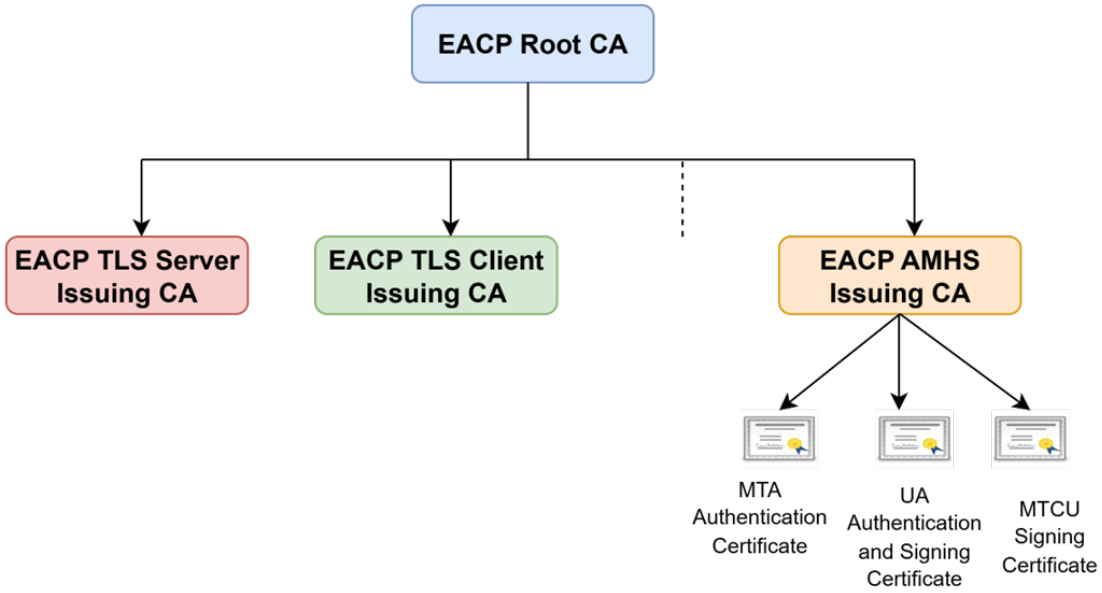
- Certificate Use ...

- Expiration / Revocation
- Renewal/Rekeying



AMHS Digital Certificate Specifications

AMHS Hierarchy of Certification under EACP Private PKI



AMHS Digital Certificate Lifecycle Management

Key Pair Creation and Certificate Request creation

- Example of Key Pair Generation using openssl

Administrator: Command Prompt

```
c:\>openssl ecparam -genkey -name secp384r1 -out myMTA.key
```

- Parsing the Key using openssl

```
c:\>openssl pkey -in myMTA.key -text -noout
Private-Key: (384 bit)
priv:
    b4:66:f5:ec:91:91:6a:30:03:84:bf:5b:b6:96:7d:
    50:4c:43:59:13:0d:ec:99:de:5b:39:f4:ea:22:82:
    17:b1:61:ed:f9:9f:06:e3:86:58:63:6b:1d:2a:7e:
    37:ed:b7
pub:
    04:32:df:5c:af:95:9c:45:77:22:61:8d:56:22:37:
    2b:ac:24:f8:51:1f:36:82:c5:3d:b5:55:53:cd:c1:
    2f:c1:46:0c:ed:f1:a2:fe:1a:7a:85:dd:48:36:da:
    3d:e7:13:bc:f6:f4:7a:71:1b:bb:94:3b:c4:12:06:
    9f:db:e5:90:4c:ab:4a:2f:5b:21:32:49:70:35:25:
    0e:5f:3f:3a:46:18:c3:13:97:0e:52:b6:54:07:47:
    23:d4:7b:d1:11:58:c6
ASN1 OID: secp384r1
NIST CURVE: P-384
```

AMHS Digital Certificate Lifecycle Management

Key Pair Creation and Certificate Signing Request creation

- Example of Certificate Signing Request (CSR) Creation

```
c:\>openssl req -key myMTA.key -addext "subjectAltName=otherName:2.6.5.6.0;UTF8:myMTAName"
 -subj "/CN=example-MTA"  -sha384 -new -out myMTA.csr
```

- Certificate Signing Request format

```
c:\>type myMTA.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIBPzCBxgIBADAWMRQwEgYDVQQDDAtleGFtcGxlLU1UQTB2MBAGByqGSM49AgEG
BSuBBAAiA2IABDLfXK+VnEV3ImGNViI3K6wk+FEfNoLFPbVVU83BL8FGDO3xov4a
eoXdSDbaPecTvPb0enEbu5Q7xBIGn9vlkEyrSi9bITJJcDUlDl8/OkYYwxOXDlK2
VAdHI9R70RFYxqAxMC8GCSqGSIb3DQEJDjEiMCAwHgYDVR0RBBcwFaATBgRWBQYA
oAsMCW15TVRBTmFtZTAKBggqhkjOPQQDAwNoADBlAjEA0PIitHnHEF1iD0YljP1S
uAB320KXE1EVlnYcB92K+FvHQxJqv2KK909hKrBUjfJcAjBs+xCdAZtAwM5/rBqJ
bnh1W/drTTIWpC1kcf7+uBGCqloHyHiOb205PXAVEX18/w8=
-----END CERTIFICATE REQUEST-----
```

AMHS Digital Certificate Lifecycle Management

Key Pair Creation and Certificate Signing Request creation

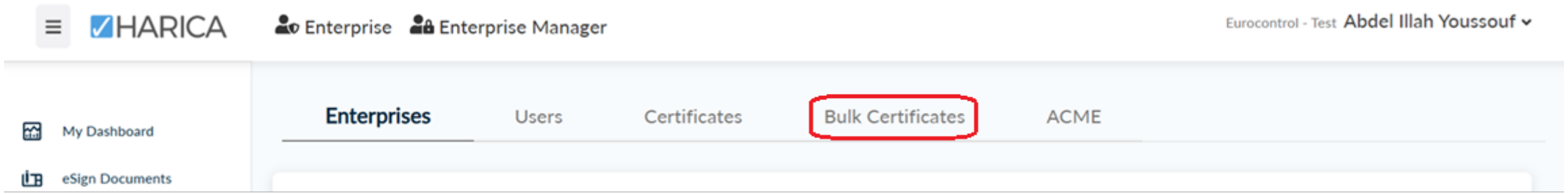
- Parsing the Certificate Signing Request (CSR)

```
c:\>openssl req -text -noout -verify -in myMTA.csr
Certificate request self-signature verify OK
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN=example-MTA
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:32:df:5c:af:95:9c:45:77:22:61:8d:56:22:37:
                    2b:ac:24:f8:51:1f:36:82:c5:3d:b5:55:53:cd:c1:
                    2f:c1:46:0c:ed:f1:a2:fe:1a:7a:85:dd:48:36:da:
                    3d:e7:13:bc:f6:f4:7a:71:1b:bb:94:3b:c4:12:06:
                    9f:db:e5:90:4c:ab:4a:2f:5b:21:32:49:70:35:25:
                    0e:5f:3f:3a:46:18:c3:13:97:0e:52:b6:54:07:47:
                    23:d4:7b:d1:11:58:c6
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        Attributes:
            Requested Extensions:
                X509v3 Subject Alternative Name:
                    othername: 2.6.5.6.0:myMTAName
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:65:02:31:00:d0:f2:22:b4:79:c7:10:5d:62:0f:46:25:8c:
        fd:52:b8:00:77:db:42:97:13:51:15:96:76:1c:07:dd:8a:f8:
        5b:c7:43:12:6a:bf:62:8a:f7:4f:61:2a:b0:54:8d:f2:5c:02:
        30:6c:fb:10:9d:01:9b:40:c0:ce:7f:ac:1a:89:6e:78:75:5b:
        f7:6b:4d:32:16:a4:2d:64:71:fe:fe:b8:11:82:aa:5a:07:c8:
        78:8e:6f:6d:39:3d:70:15:11:7d:7c:ff:0f
```

AMHS Digital Certificate Specifications

AMHS Digital Certificate Provisioning

- Bulk Certificate
- REST API



THANK YOU

eacp@eurocontrol.int

abdel.youssouf@eurocontrol.int

Thank You

ICAO