

New Challenge type:  
EMRTD-DATA-01



ACME 125 - Shenzhen

Sebastian Robin Nielsen  
(presented by Mike Ounsworth)

# What is an eMRTD?

## Electronic Machine-Readable Travel Document (ex. “ePassport”)

An eMRTD is a passport or ID card that contains a wireless RFID chip, also so-called “NFC chip”. This chip can be wirelessly read using a USB NFC reader such as ACR122U.

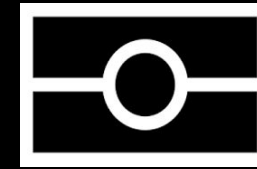
The content on the chip is signed using a x509 infrastructure (PKI), which chains up to a certificate authority owned the country issuing the passport/ID card, and the root list is maintained by ICAO (International Civil Aviation Organization).

The chip is itself password protected using PACE or BAC, requiring either the “CAN” value printed on the passport, or birth date, document number and expiry, so you can’t scan someone’s passport/ID through the pocket.

Passports, ID cards, and driver’s licenses having this technology have the following symbol:



# Why do eMRTD's need ACME?



## Allows automated IV validation

This allows a CA to automate the issuance process even in the cases where IV (“Individual Validation”) is to be carried out, using the ACME protocol.

This is applicable for all certificate types, from Code Signing, TLS, Authentication Certificates, S/MIME, and also organization certificates where an individual needs to be identified in a secure way.

No manual intervention is required by the CA.

## Privacy friendly

Since the eMRTD data is resubmitted for every validation event, the CA does not need to store any PII.

If initial authentication is performed by the CA (for example biometric face scan or known contact details), this initial validation can be tied to ACME account URI, along with a hash of document number, birth date, and first/last name.

Renew can then be done without re-performing initial auth during the validity of the passport (3-10 years).

## Extremely secure and trusted

Since the data, including the face picture, on an eMRTD is signed by a “Country CA”, that is in a trust list maintained by ICAO, which is a highly trusted organization, the process can be trusted even if no human overlooks the process.

This removes the need for the CA to inspect a document for falsification or alteration and removes the need for a human to “approve” the issuance, which lowers the cost of IV issuance.

# Overview of EMRTD-DATA-01

## Offers emrtd-data-01

The ACME server offers emrtd-data-01 to the ACME client

## Signature validation

ACME server validates that all hashes and signatures are correct and chains to a root trusted by ICAO

## Certificate issuance

The CA issues the certificate, which is IV validated with the client's name inside

## NFC submission

ACME client submits SOD and all applicable DG files read by NFC reader to ACME server

## Challenge completion

ACME client gets challenge completion and requests issuance of certificate (after optionally completing more challenges)

```
{  
  "type": "emrtd-data-01",  
  "url":  
    "https://example.com...",  
  "status": "pending"  
}
```

```
{  
  "protected": base64url({  
    "alg": "ES256",  
    "kid": "https://example.com/acme/acct/ExampleAccount",  
    "nonce": "SS2sSI1PtspvFZ08kNtzKd",  
    "url": "https://example.com/acme/chall/Rg5dV14Gh1Q"  
  }},  
  "payload": base64url({"sod": <Security Data Object, b64 encoded>,  
    "dg1": <eMRTD DG1 file, b64 encoded>,  
    "dg2": <eMRTD DG2 file, b64 encoded>,  
    ...  
    "dgx": <eMRTD DGx file, b64 encoded>}},  
  "signature": "Q1bURgJoEslbD1c5...3pYdSMLio57mQNN4"  
}
```

# Key points of EMRTD-DATA-01

- 1** Can be used to issue IV Code signing certs with device-attest-01 & lamps-csr-attestation (IETF drafts)  
This challenge can be combined with device-attest-01 & lamps-csr-attestation ensure private key is in secure storage.
- 2** Can be used to issue S/MIME certificates tied to a identity combined with email-reply-00 (RFC 8823)  
This allows a CA to automatically issue S/MIME certificates with subject's real name in it.
- 3** Highly secure and privacy friendly  
By binding initial authentication to ACME Account URI, it creates a secure long-lived binding, that are valid for the validity of the passport AND are privacy friendly since the CA does not need to store any PII.
- 4** Uses an already established and trusted PKI infrastructure, by creating a bridge between these.  
ICAO is an **EXTREMELY** trusted organization, which is trusted by the whole world, which vouch for safe ID checks.
- 5** Can be tailored by the CA to use different initial authentication, so passport or ID is not stolen.  
Either by using biometric web portal, or by using known contact info from QGIS/QIIS to contact passport/ID owner

# QUESTIONS AND ANSWERS

**What prevents eMRTDs from being stolen?**

The CA does an initial validation, either by a biometric web portal, or contacting eMRTD owner. This validation is tied to ACME Account URI & eMRTD, and survives until eMRTD expires.

**Isn't the initial identity validation a problem for ACME with automation?**

No. Since a eMRTD issuance is a manual process anyways, with travelling to police station or similar to get a eMRTD, kickstarting with a manual validation isn't a problem. Renew goes automatically without having to redo biometric or other validation until eMRTD expires.

**How is this more privacy friendly?**

Since the eMRTD data is resubmitted for every renew or reissuance, the CA does not need to store personal information. They only need to store a hash, to ensure the same eMRTD are submitted, so the eMRTD is not changed to somebody else's eMRTD in-between renews.

**Can this change make IV issuance cheaper?**

Absolutely! The IV issuance can be fully automated, without any human looking at the issuance. This by using biometric algorithms to scan a user's face during initial validation, or contacting eMRTD owner, and then using ACME account private key for subsequent authentications.

# NEXT STEPS

01

Mike Ounsworth will work with Sebastian Robin Nielsen to get the draft published on datatracker.

02

Then we'll start a discussion on the mailing list

03

Looking for an implementer co-author to provide running code -- specifically someone who plays in the ePassport or other eMRTD CA space.