Digital Travel Credentials

R Rajeshkumar

Chair – ISO SC17/WG3/TF5

Editor – Doc 9303-12

Project Editor – DTC-VC specifications

Chief Executive – Auctorizium Pte Ltd, Singapore

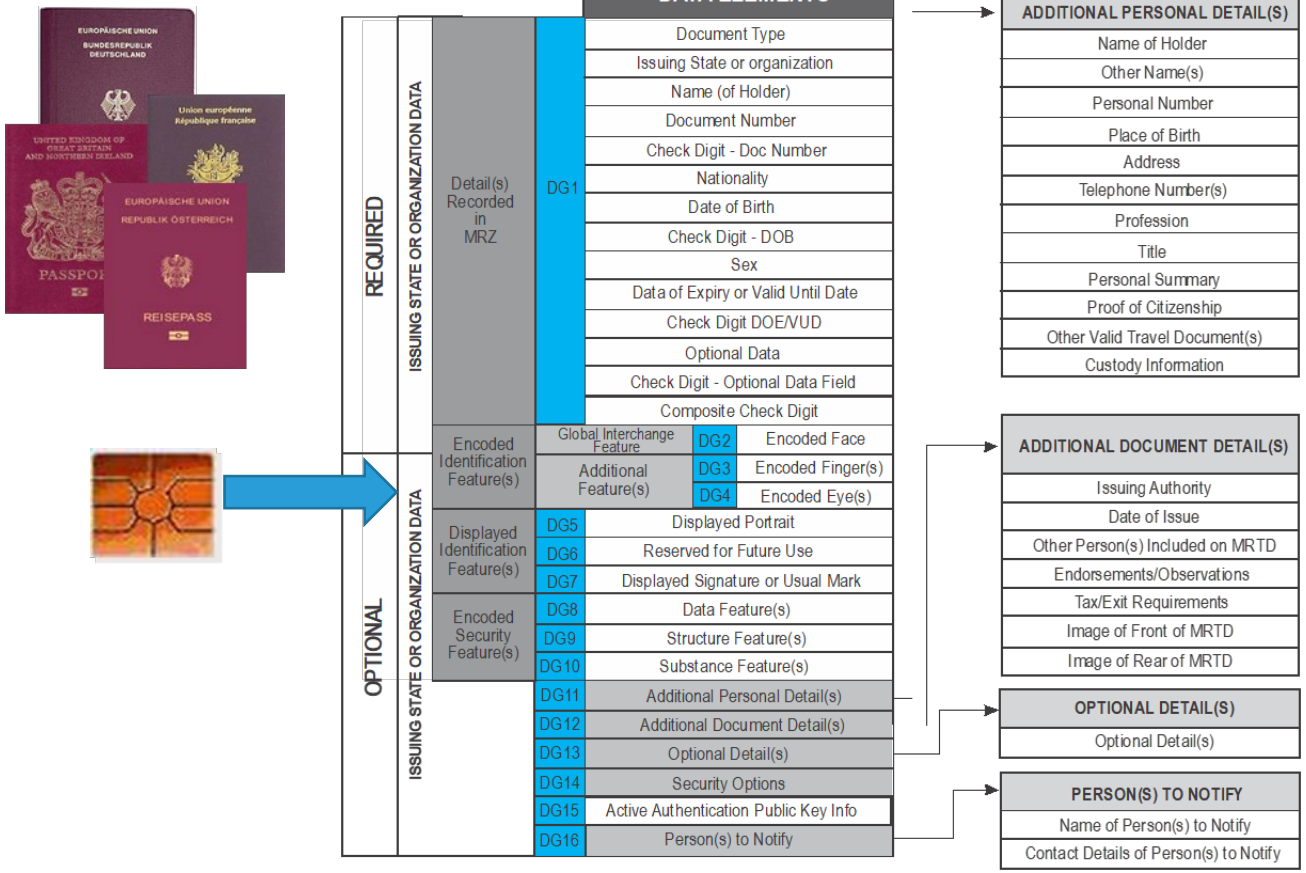
R.Rajeshkumar@auctorizium.com

1. Introducing the DTC concept

Passport Booklet Trends

- Borders increasingly rely on machine authentication to validate the document, trusting the chip and its digital security features
- Entry-Exit stamps now a rarity
- Visa increasingly issued in electronic form:
  - Tied to a record in a database through passport number and verified through iAPI messages
  - Issued as a printable document – maybe protected using Visible Digital Seal
- So … what is the purpose of the booklet?

Purpose of the Passport booklet



- Biographic and biometric information contained in chip establish the “claimed identity”
- Binding between the traveler and the “claimed identity” can be established through biometric matching.

The book establishes the “entitlement” of the traveler to the “claimed identity” – A second factor

ePassport

- Logical Data Structure
- Security Object
  - **Digitally signed**

- Crypto chip
- Secure memory
- AA/CA private key
  - **Link to virtual component**

An ePassport can be viewed as a combination of:

- A **Virtual Component (VC)** consisting of the data contained in the chip

- A **Physical Component (PC)** consisting of the booklet and/or cryptographic link between the VC and the PC and acts as an **authenticator** (second factor)

What if ?

- Separate the Data and call it VC – it is a file format
- Use some device as a PC
- As long as we can establish a relationship (cryptographically) between a VC and a PC, the form factor of the PC does not matter
- The PC establishes the entitlement to the claimed identity

DTC – Hybrid Model

DTC Types

Three Types

1. eMRTD bound DTC
   - Chipdata is read from existing travel document creating the VC
   - The eMRTD booklet acts as the authenticator and can be considered a PC
   - Anyone can create this DTC
2. eMRTD-PC bound DTC
   - Chipdata is read from existing travel document creating the VC
   - Option to cryptographically link to a different physical device(PC) with the eMRTD as a fallback
   - Can only be created by the same authority that issued the eMRTD
   - DTC can be issued any time after the issuance of the eMRTD
3. PC Bound DTC
   - No eMRTD is issued, but only a PC with form factor different from an eMRTD
   - Can only be created by an eMRTD issuing authority
   - No eMRTD available as a fallback

DTC Types (2)

	Data Source	eMRTD issued?	Additional Authenticator issued?
eMRTD Bound	eMRTD	YES	NO
eMRTD-PC Bound	eMRTD	YES	YES
PC Bound	Issuer DB	NO	YES

Design Considerations

- Design an envelope for the data
  - The chip is like a hard disk
  - Data groups, SOD etc are individual files in the chip which can be read
  - If extracted, an envelope is required to hold them together
  - For example something like a ZIP file
- The envelope should be common between all three types
  - Common structure for interoperability- States may choose to issue any type
  - Inspection systems should be able to use it regardless of type
  - The envelope should indicate the type of DTC, so that the type of physical component available for second factor authentication is known
- Revocation should be possible
  - Re-use eMRTD revocation mechanism – SLTD
  - For eMRTD-PC bound DTC, the revocation of the DTC MUST NOT

DTC Specifications

The specifications to be published in two parts

- A Technical Report detailing the Virtual Component and the Security Mechanisms – submitted to TAG/TRIP 2020 for approval through the extraordinary procedure and endorsed
- A Technical Report detailing the Physical Component and Security Assurance Levels – In progress

Since the DTC-VC is identical for all the three types

- Implementations using Type 1 can start now
- Will be fully compatible with Type 2 and 3 and hence future proof

DTC VC

- The envelope is a DER encoded ASN.1 structure

```
DTCContentInfo  ::=  SEQUENCE {
  version     Version,
  dtcData     DTCData,
  dtcTBS  [0] EXPLICIT DTCTBSValues OPTIONAL,
              -- MUST be present if DTC is eMRTD-PC Bound or PC
              -- Bound. This field MUST NOT be present if DTC is
              -- eMRTD Bound.
    dtcSignerInfo  [1] EXPLICIT DTCSignerInfo OPTIONAL
                  -- MUST be present if DTC is eMRTD-PC Bound or PC
              -- Bound. This field MUST NOT be present if DTC is
              -- eMRTD Bound.
   }
```

DTC Specifications – Some Key Points

- DTC-VC contains the public keys to establish the Cryptographic link between VC and PC – Will be based on existing mechanisms like Active Authentication and Chip Authentication
- Since the VC does not have space constraint (not stored on a chip), Type 2 and 3 allow for additional information to be added by issuer – could be used for larger photograph for improved FR
- DTC Identifier – unique number different from passport number. Will be used to report loss of DTC-PC to SLTD
- DTC Date of Expiry – ability to issue DTC for validity that is shorter than the eMRTD to allow for obsolescence of the PC
- DTC-PC will have NFC interface, but will allow others e.g BLE…

2. Use Cases

Use Cases - 1

- Seamless Travel
  - One to one biometric match is enough for most interaction points in travel continuum
  - DG2 contains anchor image of the traveler
  - For Type 2, the state may choose to add a higher quality image for improved FR match

Use Cases - 2

- Advance Travel Authroization (ETA/DTA/…)
  - Current process is web based enrollment and usually includes a ‘photocopy’ of the data page
  - Submission of DTC data improves the accuracy of the data and is also easily verifiable

Use Cases - 3

- Improving border processing time
  - Secure messaging takes about 2 seconds. Reading an ePassport takes between 3.5 to 7 seconds. Actual validation takes another 200 milliseconds to 2 seconds. AA/CA might add another 1 second. So, a min of 6 seconds to a max of 12 seconds.
  - If DTC is received in advance, Inspection systems will have finished the validation and chip read can be avoided. So, possible processing times of 2-4 seconds.

IC (chip)		*PCD (Inspection system)*
Static key pair (SK_{IC}, PK_{IC}, D_{IC})		
	— PK_{IC}, D_{IC} →	
		Choose random ephemeral key pair ($SK_{DH,PCD}$, $PK_{DH,PCD}$, D_{IC})
	← $PK_{DH,PCD}$ —	
K = **KA**(SK_{IC}, $PK_{DH,PCD}$, D_{IC})		K = **KA**($SK_{DH,PCD}$, PK_{IC}, D_{IC})

Use Cases - 4

- Emergency Travel Document
  - Specify a secure process for remote provisioning of Type 3 DTC.
  - Will allow issuance in locations that may not have a consular presence

Creation and use of DTC

- Type 1 can be created by anybody by reading contents of the ePassport chip
- Type 2 MUST be created by the Issuer of the eMRTD
- Type 3 MUST be created by an Issuer

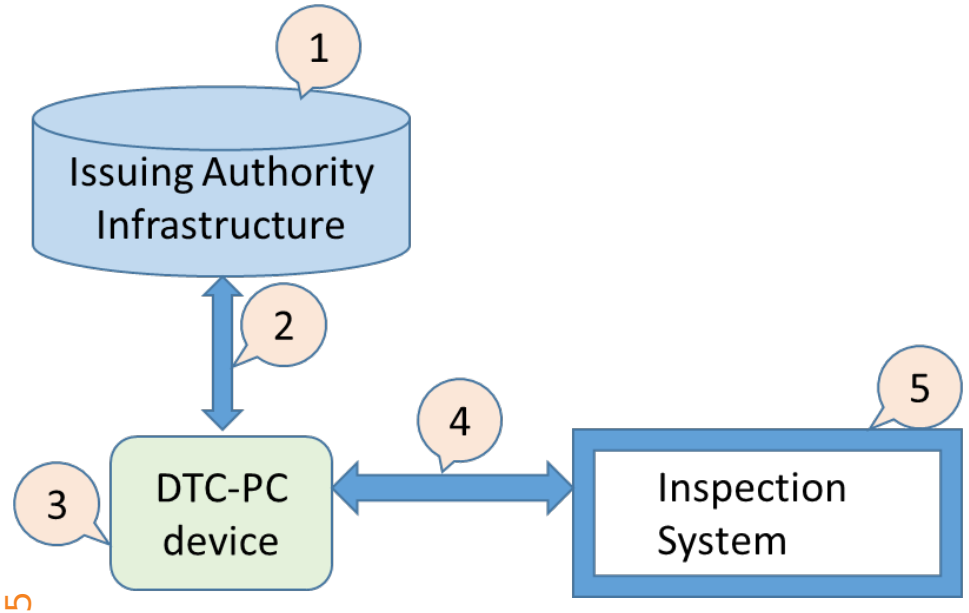
  - ✓ Identity Binding is not required for creation of Type 1
  - ✓ Identity Binding MUST be done when enrolling the DTC within a usage scenario
  - ✓ Binding to PC for higher assurance or in case of ambiguity

Risks Outlined

- Role of the policy paper is focussed on principles required to develop specifications, not outline how to operationalise DTC and mitigate/manage operational risk.
- Some ideas for consideration are included in the Principles and FAQs documents, and will be developed further (by NTWG and ICBWG) as DTC-PC specifications are developed:
  - Relying solely on the DTC-VC (no 2-Factor bind)
  - DTC enrolled to device of an unentitled traveller
  - Collection of DTC-VC Data
  - Provisioned DTC-PC is lost/stolen
  - Non-reporting of lost/stolen DTC-PC
  - DTC-PC keys are extracted – cloned
  - Inspection system outage with no fallback (PC-Bound)
  - False rejection with no fallback (PC-Bound)

3. DTC-PC

DTC PC Specifications - Scope



1. Issuing Infra – outside of scope
2. Interface to provision DTC-PC
   a) ISO/IEC AWI 23220 (identity management on mobile devices)
   b) ISO 18013-5 – mDL
3. DTC-PC device
   a) Key Storage requirements and protection
   b) after the definition of the interface to the inspection system
4. Interface between DTC-PC and Inspection system – Current scope of work
5. Inspection System – Out of scope

DTC PC - Interface Types

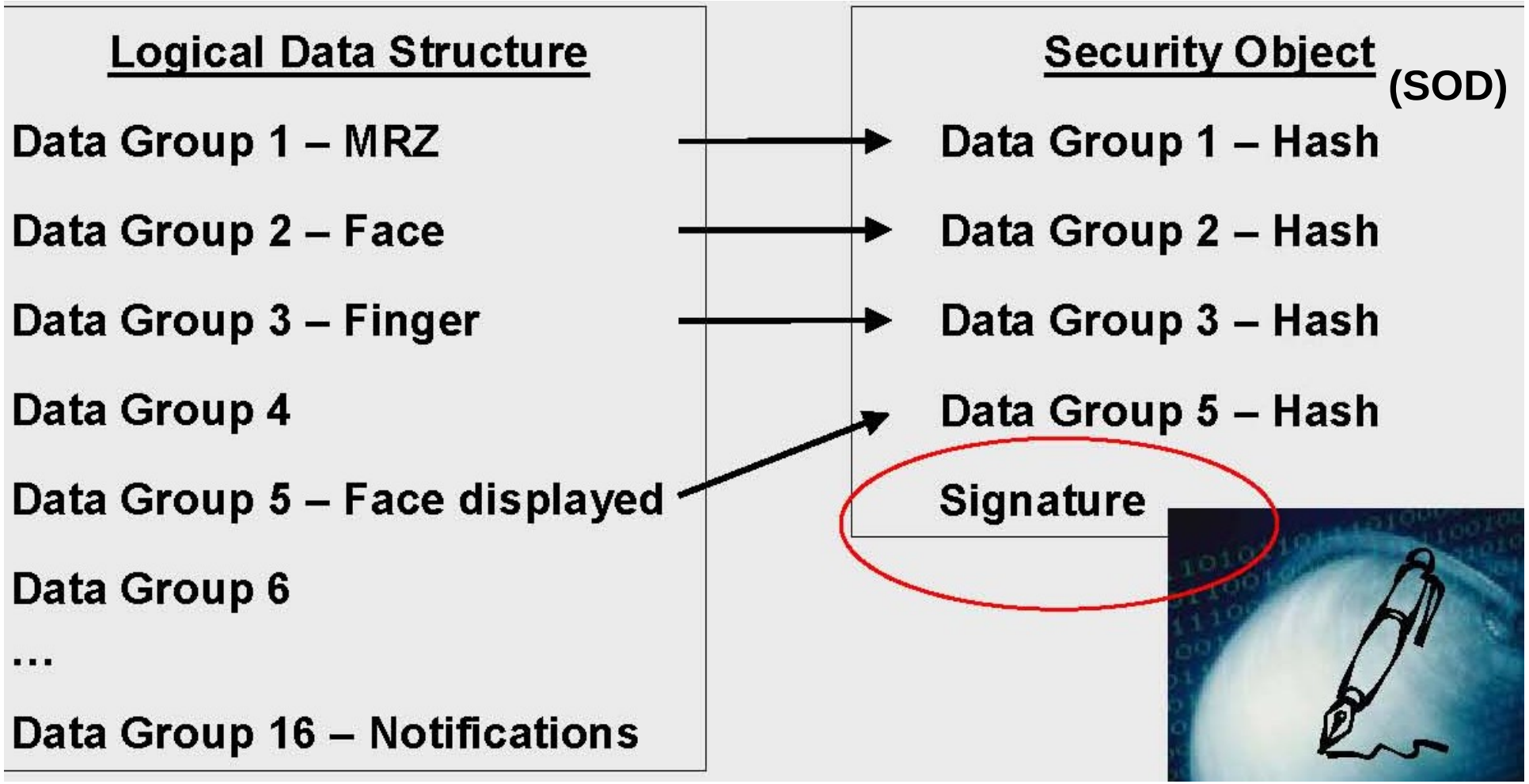
- NFC – Will be ‘almost’ identical to eMRTDs – APDU commands
- Possibly BLE – May be APDU or something more efficient
- Other Interface Types..

Existing Inspection Systems should be able to use the DTC-PC with no/minimum changes

Upgraded Inspection Systems may be able to use more efficient protocols

4. DTC Validation

ePassport Validation



Understanding E-Passport validation

- Trust is established by proper verification of the e-Passport
  - Verify SOD against DSC
  - Verify DSC against CSCA
  - Verify DSC not in CRL

  - Check that DG hash values
    matches the hash values stored in SOD

  - Compare DG1 with MRZ
  - Compare DG2 with printed photo

  - Compare photo to holder of passport

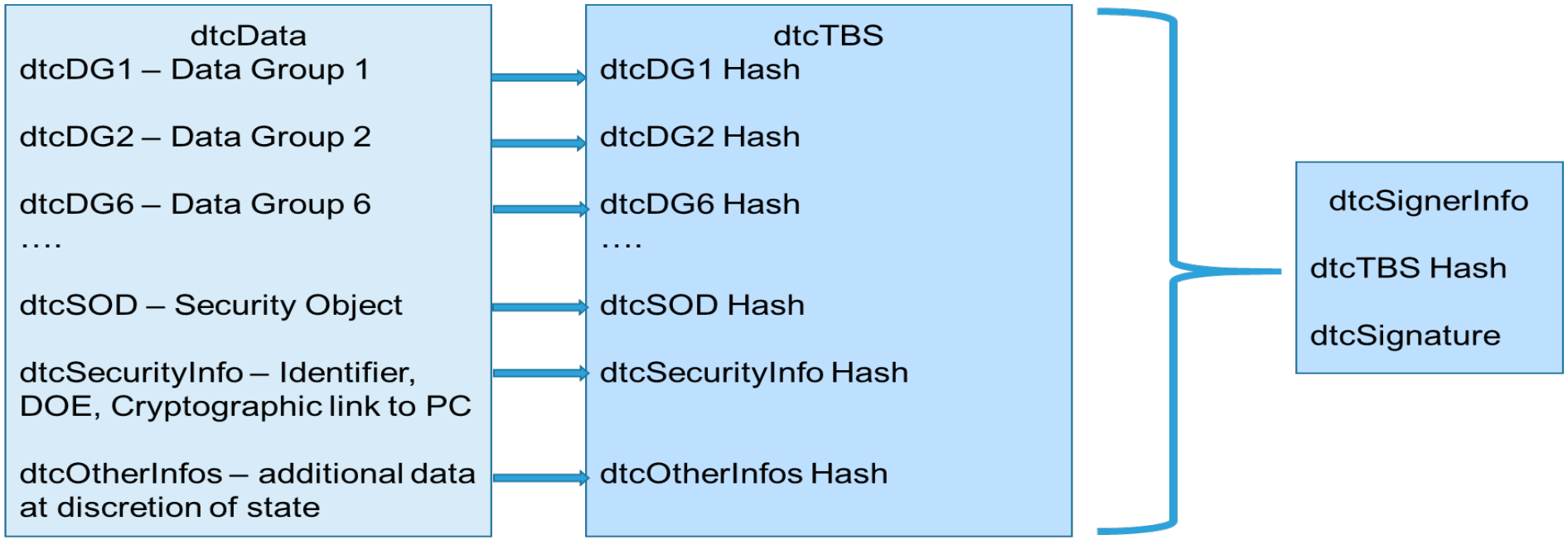
SOD is valid

LDS is valid

eMRTD is valid

Traveller is valid

DTC Validation



dtcData contains the LDS and SOD. The process of verifying this data (Passive Authentication) is identical to eMRTDs

For Type 2 and 3, additional step of comparing the Hash stored in dtcTBS to the hashed values of dtcData

Then validate the Signature on the whole structure

Validation of DTC

Validating DTC contents is the same as validating the eMRTD

For trusting the PC or the additional photo in the DTC, additional validation of the envelope is necessary

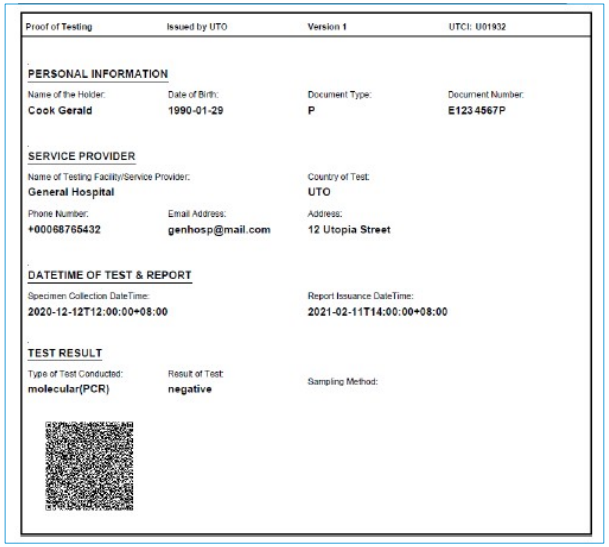
Validation of eMRTDs and DTCs

- **Availability of CSCAs** – Country is still root of trust. But, eMRTD may have been issued by an older CSCA and DTC may have been signed by a newer CSCA
- **Availability of CRLs** – A single CRL will cover all Signers
- **Visualization of Validation Result** – Too much information will confuse the verifier. Becomes even more relevant for DTC compare to eMRTD
- **Handling of defective encodings** – The contents of the eMRTD are copied over, so any encoding defects also get copied over. Defect handling will need to be in place
- **Checking SLTD** – Currently, check is for eMRTD number only. For DTC, an additional check for DTC Identifier. So two step check

5. The Future

Health Proofs – current effort

- Visible Digital Seal for Non Constrained Environments (VDS-NC)
- Paper First approach
- Built on eMRTD trust Framework



Proof of Testing | Issued by UTO | Version 1 | UTCI: U01932

PERSONAL INFORMATION

Name of the Holder: Cook Gerald
Date of Birth: 1990-01-29
Document Type: P
Document Number: E1234567P

SERVICE PROVIDER

Name of Testing Facility/Service Provider: General Hospital
Country of Test: UTO
Phone Number: +00068765432
Email Address: genhosp@mail.com
Address: 12 Utopia Street

DATETIME OF TEST & REPORT

Specimen Collection DateTime: 2020-12-12T12:00:00+08:00
Report Issuance DateTime: 2021-02-11T14:00:00+08:00

TEST RESULT

Type of Test Conducted: molecular(PCR)
Result of Test: negative
Sampling Method:

Proof of Vaccination | Issued by UTO | Version 1 | UVCI: U32870

PERSONAL INFORMATION

Name of the Holder: Smith Bill
Date of Birth: 1990-01-02
Passport Number: A1234567Z
Sex: M
Additional Identifier: L4567890Z

VACCINATION EVENT

Vaccine or Prophylaxis: XM68M6
Vaccine Brand: Comirnaty
Disease or agent targeted: RA01.0

VACCINATION DETAILS 1

Date of Vaccination: 2021-03-03
Dose Number: 1
Country of Vaccination: UTO
Administering Centre: RIVM
Vaccine Batch Number: VC35679
Due Date of Next Dose: 2021-03-24

VACCINATION DETAILS 2

Date of Vaccination: 2021-03-24
Dose Number: 2
Country of Vaccination: UTO
Administering Centre: RIVM
Vaccine Batch Number: VC87540
Due Date of Next Dose:

Health Proofs – Possible future

- DTC Type 2 allows additional information to be added by the Issuer in the otherInfos field
- Potential use case could be Health Proofs
- DTC-VC could contain the Health Proof, which can be sent in advance of travel
- The process of ePassport verification at border could also verify the Health Proofs

Single container for Identity and Health Proofs..

6. Links to download TRs

ICAO Publications

- All ICAO documents can be downloaded from
  https://www.icao.int/security/fal/trip/pages/publications.aspx

- DTC TR: https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Digital%20Travel%20Credential%20%28DTC%29.pdf
- VDS-NC TR: https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Visible%20Digital%20Seal%20for%20non-constrained%20environments.pdf

Thank you!

R.Rajeshkumar@auctorizium.com