



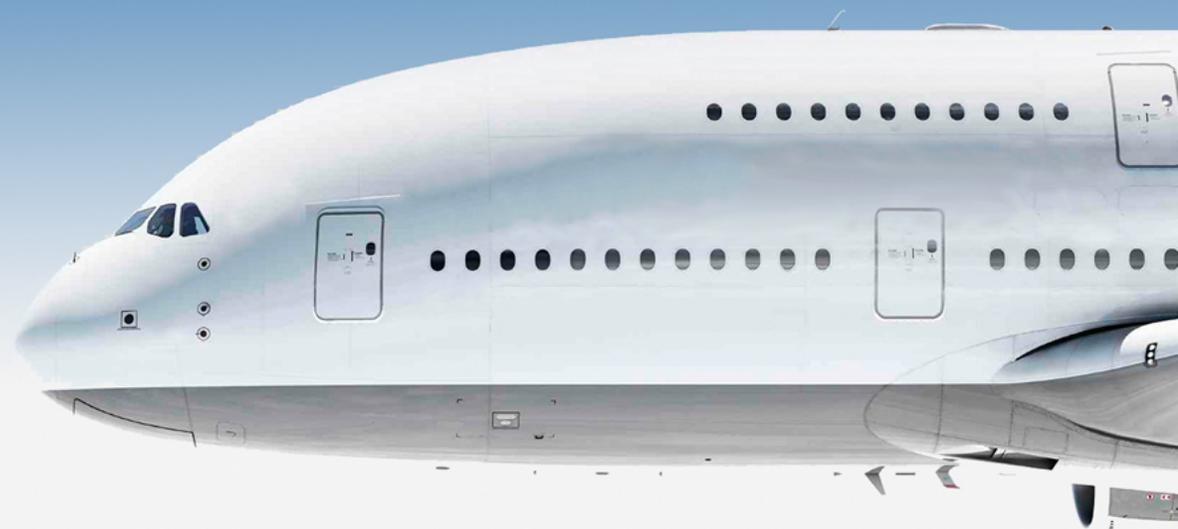
ICAO

RECONNECTING THE WORLD



VDS – Application for Testing and Vaccination Certificates

Janet Chemeli
Facilitation Officer





Aviation Restart & Recovery

- ❑ ICAO has been actively providing aviation-related information on COVID-19 and serving as the key facilitator for States, regional organizations and industry partners.
- ❑ ICAO has been coordinating with WHO and other relevant UN organizations, regional organizations, industry partners and freight forward representatives, sharing information to design together a path for the restart and recovery of aviation.

CART Phase III : Health proofs Recommendations

Recommendation 13 – Testing

*States should apply the COVID-19 risk management strategy approach outlined in the **ICAO Testing and Cross-Border Risk Management Measures Manual**.*



Recommendation 17 – Testing certificates

States are encouraged to request evidence of testing that is secure, trustworthy, verifiable, convenient to use, compliant with data protection legislation and internationally/globally interoperable.

This may be applicable to vaccination certificates.

Recommendation 19 – *Vaccination should not be a prerequisite for international travel.*



Doc 10152



Requirements for health proof certificates

Integrity



Could the data have been altered after issuance?

Authenticity



Can issuance by a trusted authority be confirmed?

Trustworthy/Verifiable



Are my systems capable of verifying integrity and authenticity?

Convenient to use



Will the certificate be efficiently read within existing processes and infrastructure?

Data protection



Compliant with legislation in state of use and state of nationality of the traveler

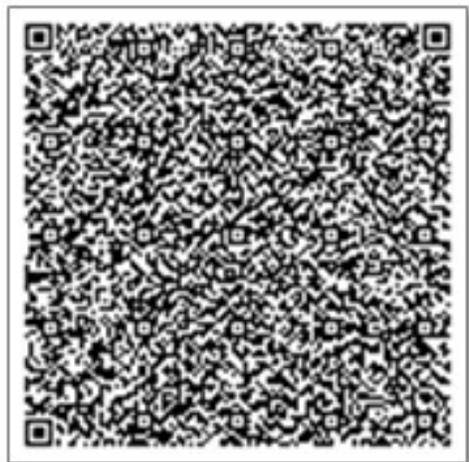
Interoperability



Will cross-border verification be possible?



Aviation Restart with Touchless Solutions





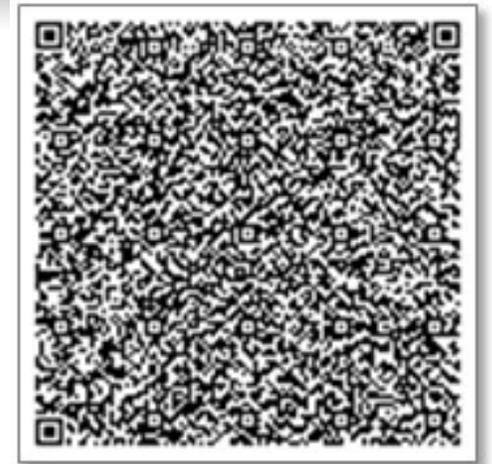
VDS-NC Guidelines and Specifications

- ❑ **ICAO Guidelines VDS for Travel Related Public Health Proofs (vaccinations and test certificates)**
 - Approved by ICAO CART III and the ICAO Council
 - Common approach, based on the existing, globally interoperable trust model for travel documents
- ❑ **ICAO Technical Report for VDS for Non-Constrained Environments**
 - Endorsed by the ICAO Air Transport Committee
 - Specifies data sets and digital signature
 - Mandatory for vaccine certificates
 - Recommended for test certificates



VDS-NC Concept

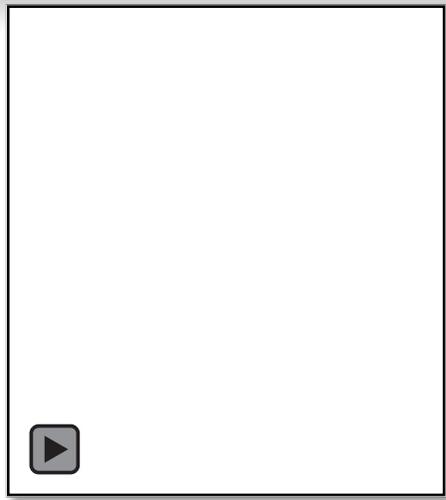
- ❑ Applies the VDS specification to health proofs
- ❑ Extends ICAO PKI infrastructure for digital signatures (security and authenticity) to 2D barcodes
- ❑ Leverages the global trust framework being deployed by 145 States issuing eMRTDs
- ❑ Allows digitally signed medical records to be easily read and validated in a similar way as eMRTDs





VDS-NC Design Principles

- ❑ Globally Interoperable
- ❑ “Human” Readable
→ “Payload” is human readable
- ❑ Offline Verifiable
→ Certificate and Signature contained in the barcode
- ❑ Able to leverage the eMRTD Trust Model
- ❑ Flexible



| Proof of Testing | Issued by UTO | Version 1 | UTCI: 081932 |
|--|------------------------------------|--|-------------------------------|
| 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: nasopharyngeal | |
| OPTIONAL DATA FIELD | | | |
| ID12345 | | | |

```
{ "data": { "hdr": { "t": "icao.test", "v": 1, "is": "UTO", "msg": { "utci": "01932", "pid": { "n": "Cook Gerald", "dob": "1990-01-29", "dt": "P", "dn": "E1234567P", "sp": { "spn": "General Hospital", "ctr": "UTO", "cd": { "p": "+00068765432", "e": "genhosp@mail.com", "a": "12 Utopia Street" }, "dat": { "sc": "2020-12-12T12:00:00+08:00", "ri": "2021-02-11T14:00:00+08:00", "tr": { "tc": "molecular(PCR)", "r": "negative", "m": "nasopharyngeal", "opt": "ID12345" } }, "sig": { "alg": "ES256", "cer": "MIIBeTCCAR2gAwIBAgIBZzAMBggqhkJOPQQDAgUAMB0xCzAJBgNVBAYTA1VUMQ4wDAYDVQQDDAVVVCBDQTAeFw0yMTA0MDcwNDI2MTVaFw0yNjEwMDcwNDI2MTVaMBoxCzAJBgNVBAYTA1VUMQswCQYDVQQDEwIwNTBZMmBMBGByqGSM49AgEGCCqGSM49AwEHA0IABBzop6IWxg_Qo8JV1G-r9EzjoAoXKsSUMkuHCTKZTY-b5atMP8jDtjJaGhaL_2VvrNbz7WDGSwf-7MqqFzxsS6ejTzBNMBIGA1UdJQQLMAkGB2eBCAEBDgIwHwYDVR0jBBGwFoAUymyKsnX8rywn0RH7nDq-Bs2QOqowFgYHZ4EIAQEGAgQLMAkCAQAxBBMCT1QwDAYIKoZIZj0EAwIFAANIADBFAI Ace9uX8UOpdsOtEkAtkDu2GPyzy_S8vQP4qhzGbooa8gIhAO_5ORo2bsTor6CXHngGld4NntUGsXNqXl-9qEfVcsqb", "sigv1": "z_VZDdMyjjRkg06nYLwHt4BP_APEm3MJT8WgOOz_DXTRZA2oxkutZhS0n7yYTHgw-MKZUUmQyhrqZgm7q-267g==" } } }
```



VDS-NC Main distinctions

What it IS:

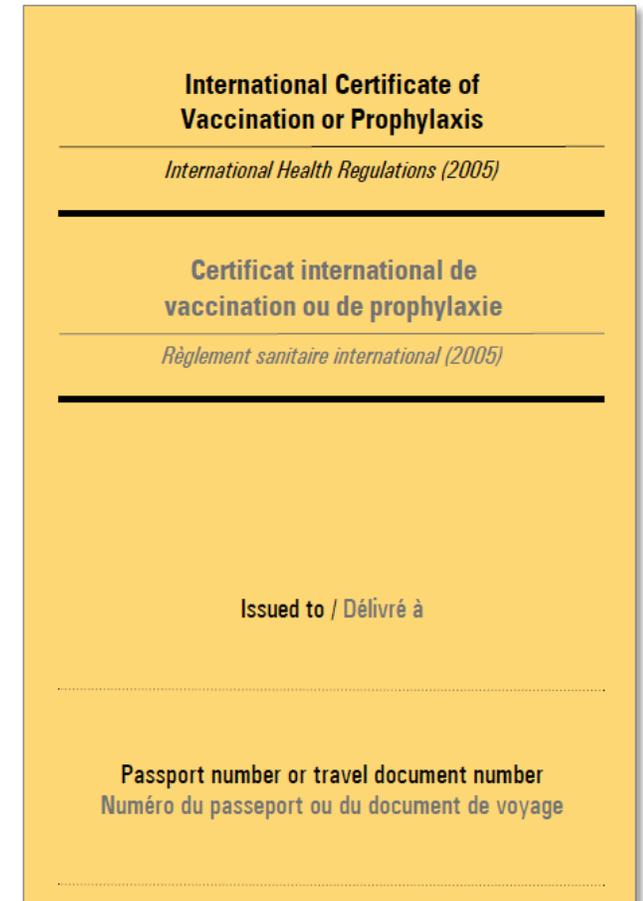
- Specific token for cross-border travel.
- Digitally signed 2D-barcode, to ensure the data is authentic and not been modified.
- Relies on an existing two-level PKI trust model as it is used for e-passports since 2004.
- CSCA does not have to be the same as for e-passports.
- Easily readable by most barcode scanners.
- Offline verifiable, without the need for an online-connection.



VDS-NC Main distinctions

What it is NOT:

- ❑ The VDS-NC is **not the primary medical vaccination document**. This function stays within the health-related environment: vaccination certificates will be treated and governed as health documents.
- ❑ The VDS-NC is **not intended to replace any national/multilateral vaccination document**.



Proof of Vaccination

- ❑ World Health Organization (WHO) is developing Digital Documentation of COVID-19 Certificates (DDCC) specification
- ❑ WHO is focused on ensuring continuity of medical care (dosages)
- ❑ Vaccination certificates can be issued without a VDS-NC
- ❑ ICAO VDS-NC specification to be deployed for an international vaccination certificate, the token used *specifically* for cross-border travel
- ❑ Pax can get an international certificate for travel, well after the vaccination event itself



Proof of Vaccination

- ❑ Digital signature mandatory
- ❑ Data sets for PoV follows WHO recommendations
- ❑ Contains a Unique Identifier (e.g. a document number) and an additional identifier, both optional, but (strongly) recommended
- ❑ Allows for multiple vaccination events, same or different vaccines

| Proof of Vaccination | Issued by UTO | Version 1 | UVCE: 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: | |
|  | | | |



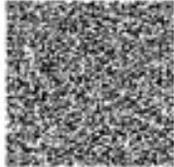
Proof of Tests

- ICAO proposing specifications
- Short validity period of the test result
- Part of a multi-layered risk-based approach
- ICAO is encouraging States requiring a negative test result to consider lifting or limiting quarantine or self-isolation measures



Proof of Tests

- ❑ Digital signature optional, but highly recommended
- ❑ Data set defined by ICAO Manual 10152, follows ICAO CART recommendations
- ❑ Contains a mandatory Document Number/Type to establish link between person and a secure document

| Proof of Testing | Issued by UTO | Version 1 | UTC: 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 | |
| DATE/TIME 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: nasopharyngeal | |
| OPTIONAL DATA FIELD | | | |
| ID12345 | | | |
|  | | | |



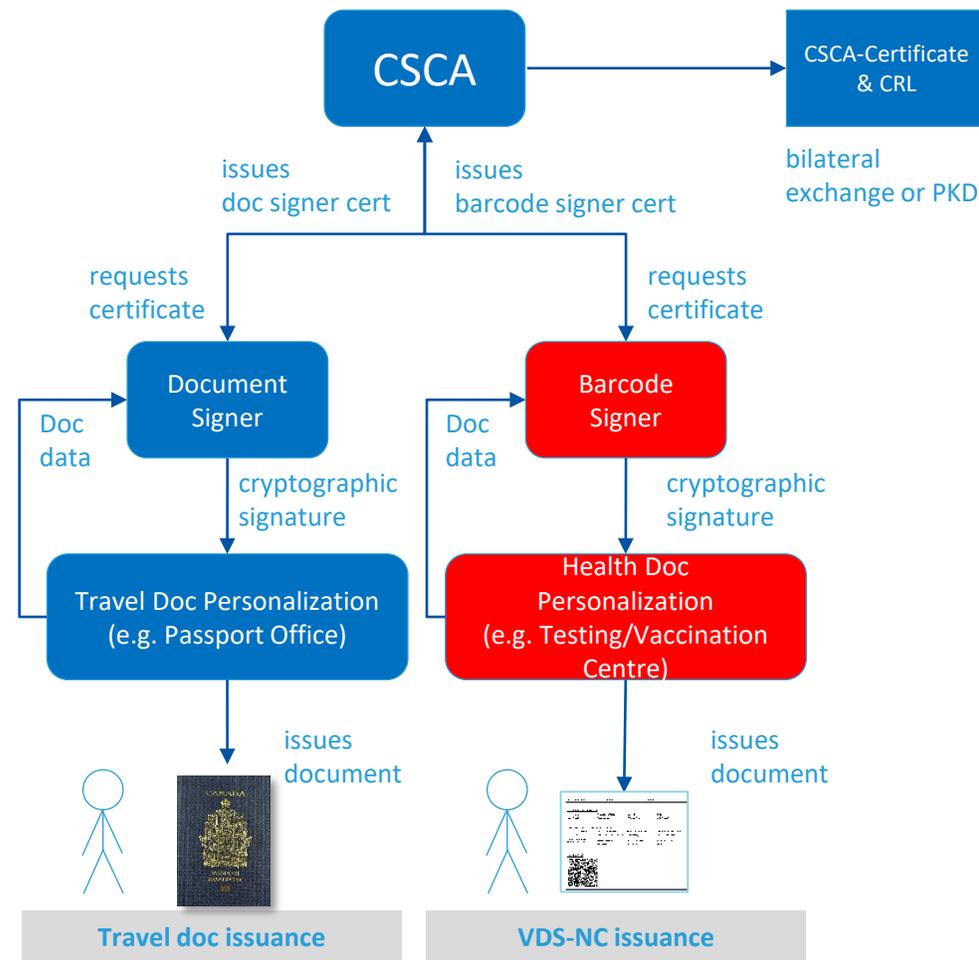
Issuance/digital signing

PKI model A: Single CSCA for both travel docs and health proofs

- ❑ CSCA for issuing travel documents acts as the single root of trust for both TDs and health proofs.
- ❑ Document signers are specific to travel documents and health proofs, respectively.
- ❑ Certificate profiles ensure that specific certificates can be used for the intended purpose only.

Passport

Health



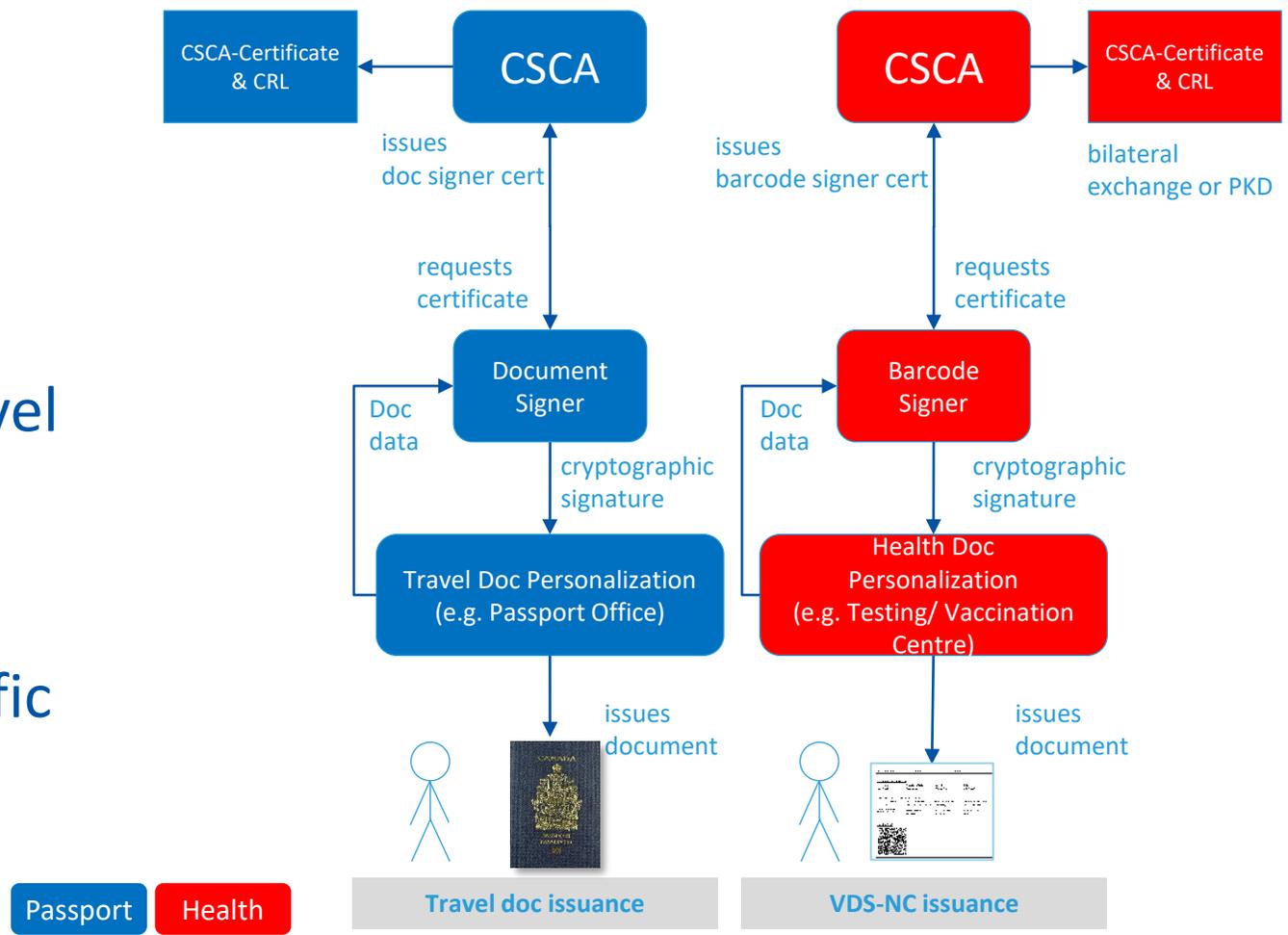


Issuance/digital signing

PKI model B: Specific CSCAs for travel

docs and health proofs

- ❑ Specific CSCAs for issuing TDs and health proofs, respectively.
- ❑ Document signers are specific to travel documents and health proofs, respectively.
- ❑ Certificate profiles ensure that specific certificates can be used for the intended purpose only.

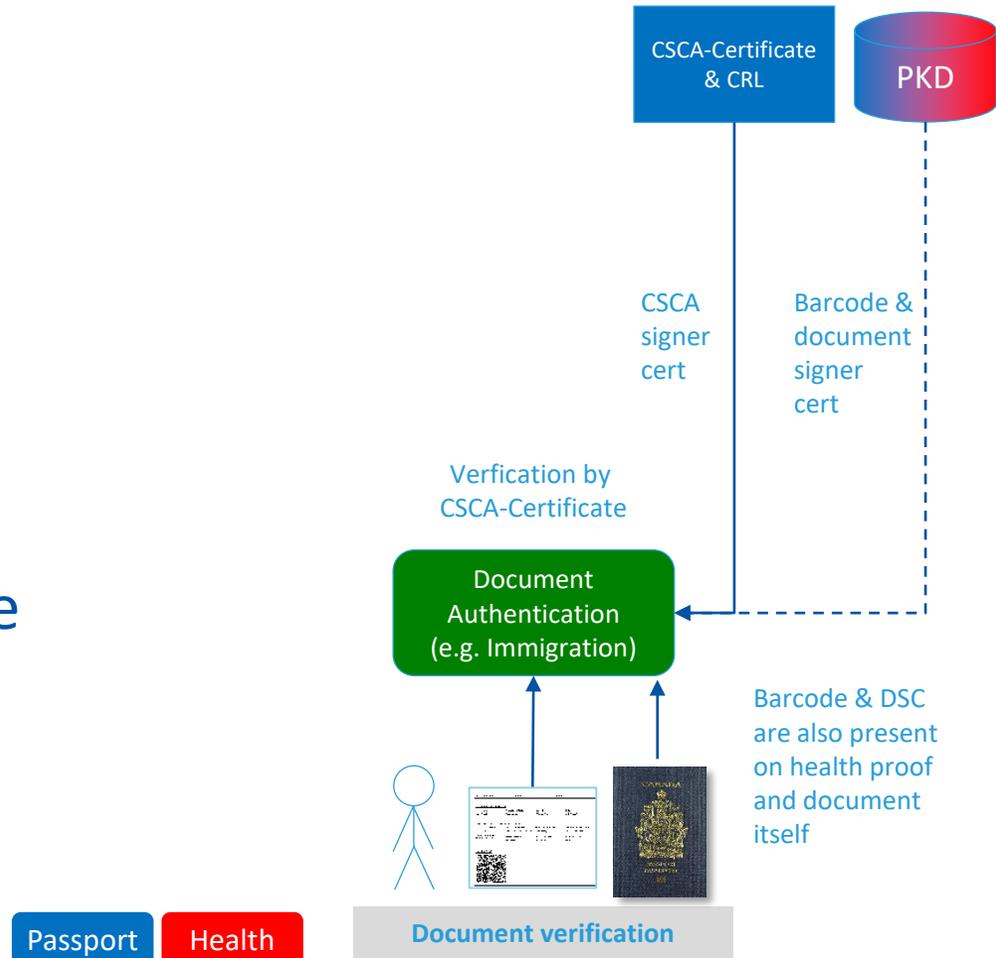




Verification

PKI model A: Single CSCA for both travel docs and health proofs

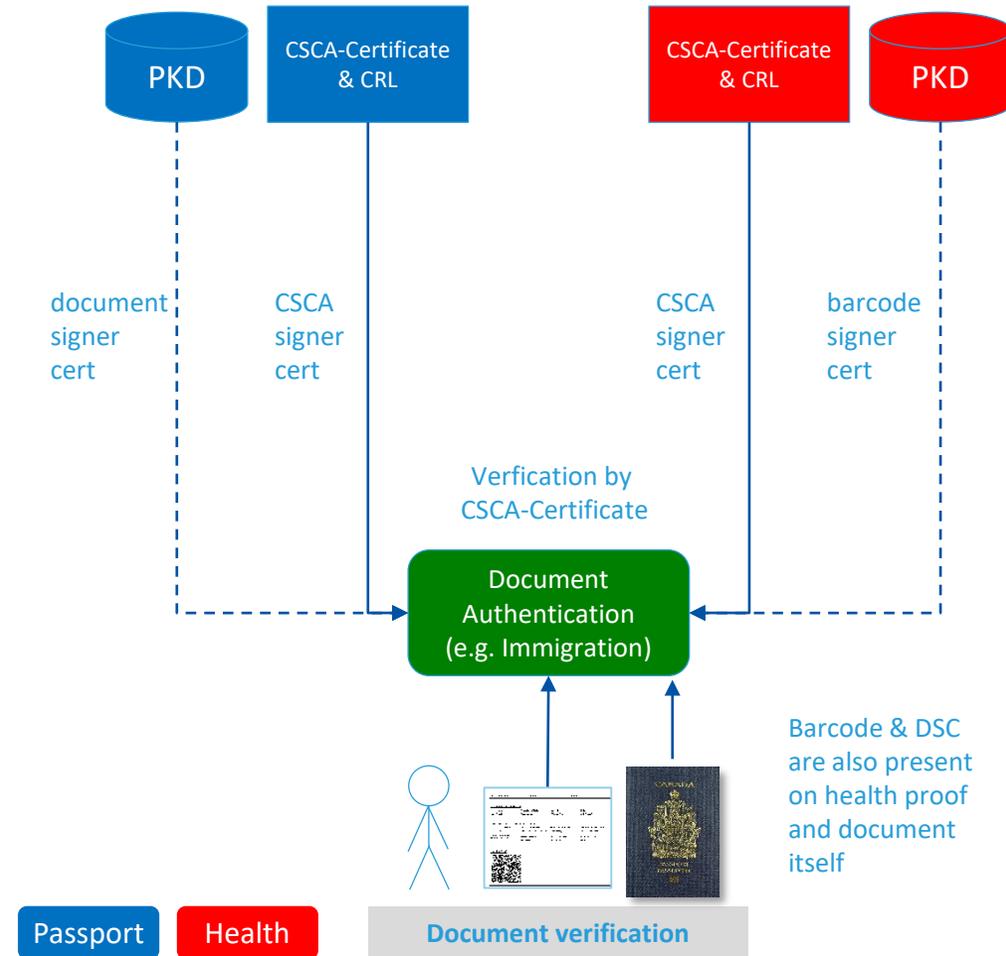
- ❑ Immigration systems import CSCA certs as currently for travel documents.
- ❑ Borders verify both travel documents and health proofs.
- ❑ Certificate profiles ensure that certificates can be used for intended purpose only.
- ❑ Barcode and doc signer certificates could be downloaded from the (single) PKD.



Verification

PKI model B: Specific CSCAs for travel docs and health proofs

- ❑ Immigration systems import the CSCA certs for TDs and health proofs.
- ❑ Borders verify both travel documents and health proofs.
- ❑ Certificate profiles ensure that certificates can be used for the intended purpose only.
- ❑ Barcode and doc signer certificates could be downloaded from the (specific) PKD.

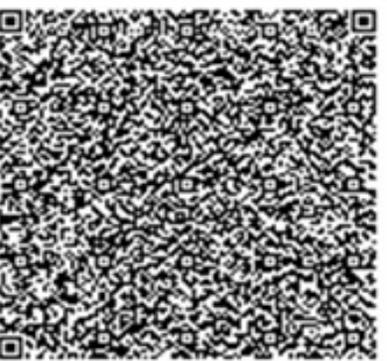




Business processes and needs

- ❑ Globally Interoperable
- ❑ Data stored on VDS only
- ❑ Usable on paper and with digital solutions - similar performance/security in both cases
- ❑ Does not necessitate significant process change
- ❑ ICAO specification – respects state sovereignty in issuance and validation

- Allows unique identification through association with person's ID
- Can be physically printed or shown on a digital screen
- Can be applied to existing paper certificates or digital passes already used
- No storage of data beyond the holder - compliance with data protection

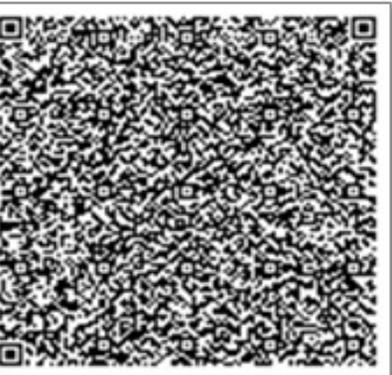




Existing Infrastructure and Systems

- ❑ Cost effective to implement (No Country Left Behind / NCLB)
- ❑ Can be validated offline
- ❑ A low-cost solution – signed barcodes emailed/ uploaded to a central repository and printed at home or stored in digital wallet
- ❑ Border authorities have familiarity and connectivity with existing eMRTD trust model – no need to onboard new verification system.

- Readable using existing scanners in airport, e.g. for boarding passes
- On-paper use allows for cost-effective implementation
- No transactional costs following initial implementation
- Technical specifications are already developed, understood and agreed



The Health Credential Situation

- ❑ Numerous formats - > Work towards Mutual Recognition (i.e. global verifiability)
- ❑ Persistent use in international travel - > Consider the specificities of border management and international travel

Leverage knowledge and capabilities gained from experience to achieve these goals



ICAO

RECONNECTING THE WORLD



DIVOC (India)

No defined trust registry



VDS-NC (ICAO)

ICAO PKD



Common Formats of Health Proofs used in Travel

Smart Health Card (VCI)

The CommonTrust Network



Digital COVID Certificate (EU)

EU Gateway





ICAO

RECONNECTING THE WORLD



Enhancing verifiability of Health Proofs

Collect certificates
needed for
verification of
health proofs

Share the public
certificates in a
trusted manner

Ensure wide
capacities to utilize
the certificates to
verify international
health proofs

The ICAO Health Master List

A Common International Trust Registry

- Health Public Key Cert 1
- Health Public Key Cert 2
- Health Public Key Cert 3
- Health Public Key Cert n.



- Open** - No certificate format requirements
- Accessible** - No dependency on PKD participation status
- Trustworthy** - Validation based on same requirements as for the ICAO PKD



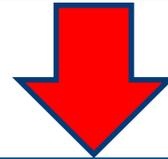
ICAO

RECONNECTING THE WORLD

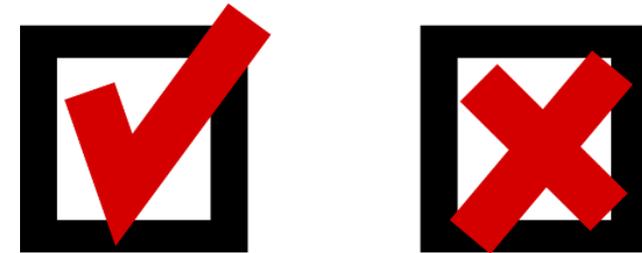


ICAO Health Master List provides trusted information necessary for verification

- Health Public Key Cert 1
- Health Public Key Cert n..



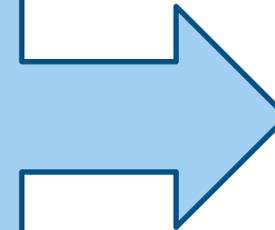
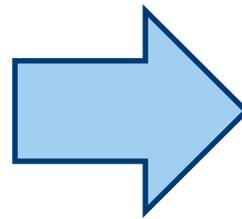
Software with multi-format processing logic



Automatic indication of authenticity, integrity and compliance with rules



Scan a health proof barcode, e.g. a VDS-NC barcode





The ICAO Health Master List

- ❑ Available from the ICAO public webpage, first version 31.01.2022
- ❑ Certificate collection leveraging ICAO's unique network position, list digitally signed by ICAO for trust
- ❑ Published in known, trusted, established format, easing use (especially in restricted border environments)



ICAO

RECONNECTING THE WORLD



Leverage knowledge and capabilities gained from experience to achieve these goals

For ICAO:

- ❑ Knowledge in PKI and certificate sharing underpinning global trust
- ❑ Capabilities in trustworthy certificate collection based on in-house network
- ❑ Experience in delivering public key certificates trusted for international travel

For States:

- ❑ Knowledge in use of public key certificate-based verification
- ❑ Capabilities to use Master List data to verify digitally-signed credentials at borders
- ❑ Experience in incorporating digital credentials into processes to facilitate safe and seamless travel



| ICAO

RECONNECTING THE WORLD



States are encouraged to provide all public key certificates necessary to validate their digital health proofs to ICAO for inclusion in the ICAO Health Master List

icao-pkd@icao.int



Thank you!



ICAO