ICAO SECURITY AND FACILITATION
TRIP-NTWG

VDS – NC: Health-related VDS Specifications

Dr. U. Seidel[1], R. Rajeshkumar[2], T. Kinneging[3]

Chair – ICAO TAG/TRIP New Technologies Working Group
Bundeskriminalamt, Germany[1]

Chair – ISO SC17/WG3/TF5,
Auctorizium, Singapore[2]

Convener – ISO SC17/WG3
Idemia, Netherlands[3]

Agenda

01 **Introduction**
Main drivers

02 **Overview**
What it is - and what it is not.

03 **Infrastructure**
PKI trust model

04 **Data Sets**
Data fields for Testing & Vaccination

05 **Related Initatives**
WHO SVC & EU DGC

06 **Demonstration**
Reading & Validation of the VDS-NC

01

Introduction

Visible Digital Seal – NC

Main Drivers 1: Recovery of air traffic and international travel

ICAO CAPSCA (Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil Aviation) and CART (Council Aviation Recovery Task Force)

- CART Phase III asked for the development of a global framework for the validation of testing and vaccination records and/or certificates.
- Following the approval by the ICAO Council for Guidelines for VDS-NC, the NTWG, PKD and ISO experts developed specifications for special use cases of VDS for “public health proofs” for cross-border travel.

WHO

- Larger scope, defines use cases, e.g. proof of vaccination including “core data set”
- Interim guidance for developing a Smart Vaccination Certificate, Release Candidate 1, 19 March 2021

EU Draft Regulation (Digital Green Certificate)

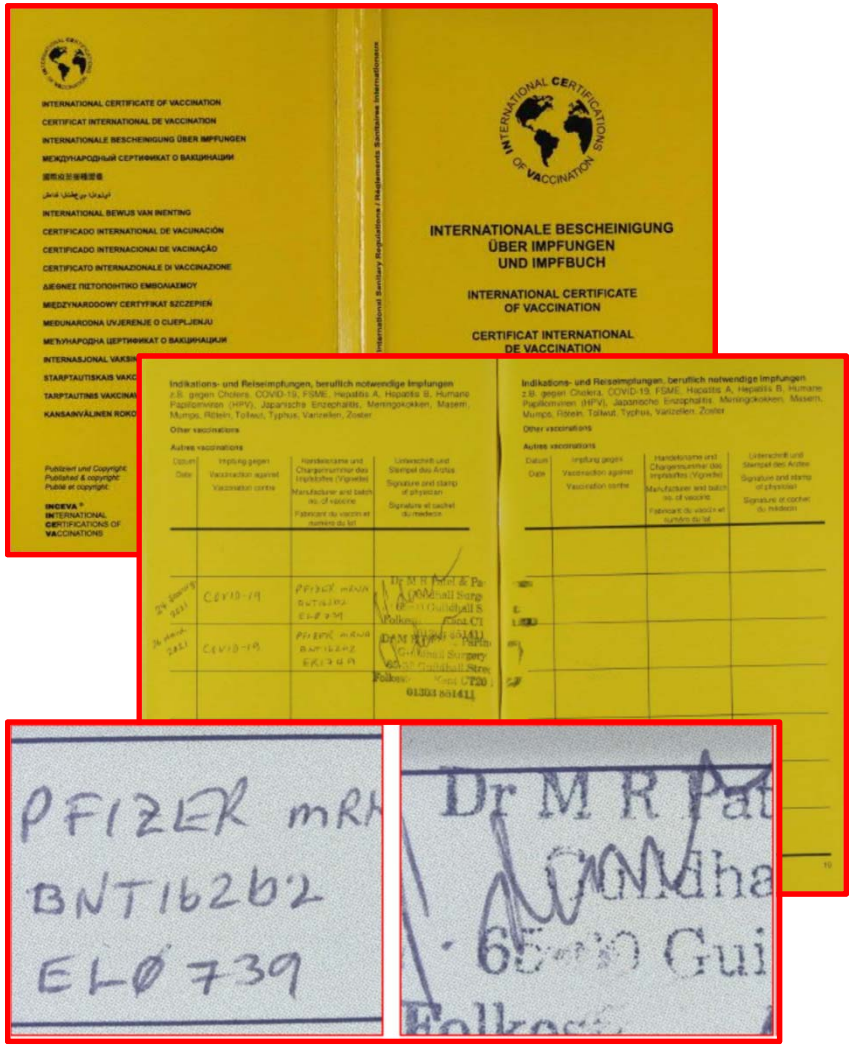
- eHealth-Network (eHN) proposes interoperability requirements and “data fields” for vaccination certificate, test certificate and certificate of recovery, 18 March 2021
- New technical specifications by April 16, 2021

Visible Digital Seal - NC

Main driver 2: Security of health related proofs

Health proofs as target of fraud

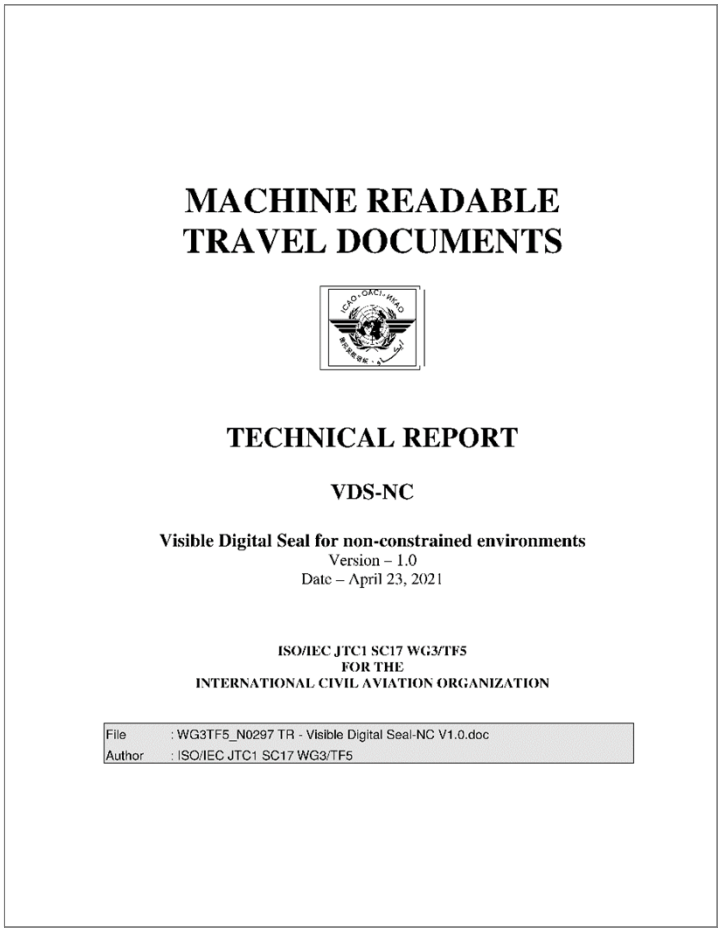
- The counterfeit of vaccination certificates and COVID-test reports have become a mass phenomenon. Blank “yellow books” with complete vaccination entries are sold on Telegram channels for 80 – 150 €.
- The vaccination certification was never intended to be a secure travel document and hence carries no security features.
- The VDS-NC is designed as an accompanying document carrying digitally signed health information – making fraud easily detectable.



Case example: Blank fraudulent yellow book sent from London to Frankfurt carrying vaccination entries, May 2021 (Source: BPOL FRA)

02

Overview



MACHINE READABLE
TRAVEL DOCUMENTS

TECHNICAL REPORT

VDS-NC

Visible Digital Seal for non-constrained environments
Version – 1.0
Date – April 23, 2021

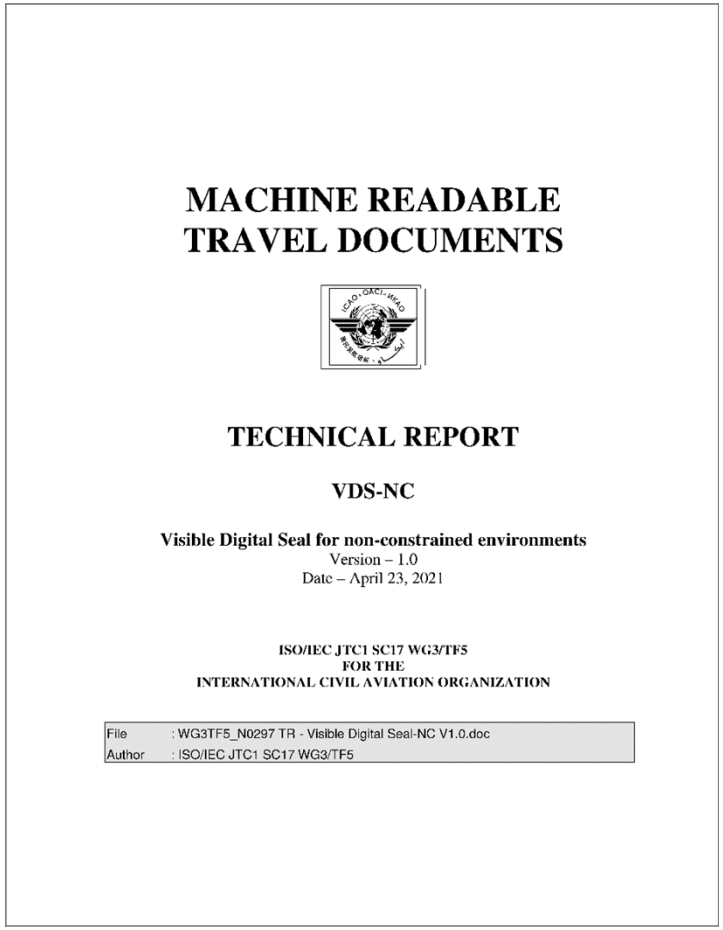
ISO/IEC JTC1 SC17 WG3/TF5
FOR THE
INTERNATIONAL CIVIL AVIATION ORGANIZATION

File	: WG3TF5_N0297 TR - Visible Digital Seal-NC V1.0.doc
Author	: ISO/IEC JTC1 SC17 WG3/TF5

Visible Digital Seal for non-constrained environments

Specifications ready!

- Taking on the challenge, ICAO NTWG and ISO/WG3 experts developed a viable technical solution leveraging existing infrastructure to provide for rapid implementation and global interoperability - Visible Digital Seals for non-constrained environments (VDS-NC).
- The specifications were approved by the Technical Advisory Group on Traveller Identification Programme (TAG/TRIP) on May 6, 2021 and by the Air Transport Committee on May 14, 2021.
- **ICAO is proud to announce this first full set of fully approved specifications for interoperable public health proofs.**
- Based on these specifications, States can begin to develop and implement globally interoperable solutions.
- The specifications can be found at https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx
- https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Visible%20Digital%20Seal%20for%20non-constrained%20environments.pdf



MACHINE READABLE
TRAVEL DOCUMENTS

TECHNICAL REPORT

VDS-NC

Visible Digital Seal for non-constrained environments
Version – 1.0
Date – April 23, 2021

ISO/IEC JTC1 SC17 WG3/TF5
FOR THE
INTERNATIONAL CIVIL AVIATION ORGANIZATION

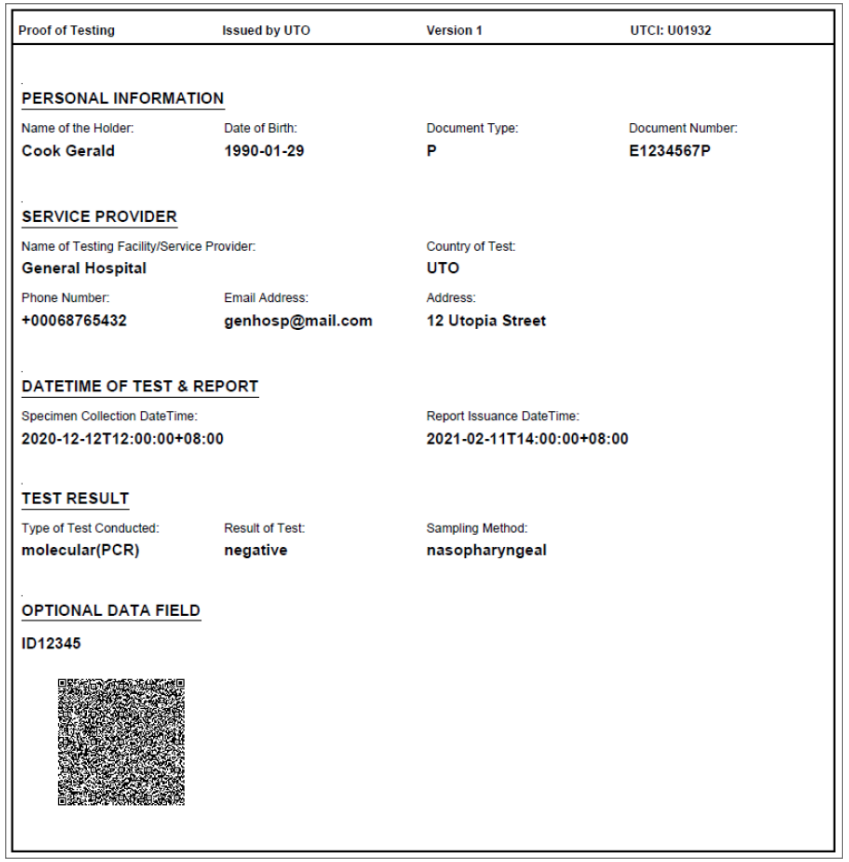
File	: WG3TF5_N0297 TR - Visible Digital Seal-NC V1.0.doc
Author	: ISO/IEC JTC1 SC17 WG3/TF5

Visible Digital Seal - NC

Main Properties

What it is:

1. The VDS-NC is designed as a **specific token for cross-border travel**, as an interoperable proof of health events (test, vaccination).
2. The VDS-NC is a **digitally signed 2D-barcode**, to ensure the data is authentic and not been modified.
3. The VDS-NC **relies on an existing two-level PKI trust model** as it is used for e-passports since 2004. It consists of a root of trust (CSCA), a document (barcode) signer, a Public Key Directory and the document itself.
4. The **CSCA does not have to be the same as for e-passports**, though re-using the same CSCA is recommended. If a different VDS-NC CSCA is set up, then specific profiles to differentiate between the function of the CSCA are defined.
5. The VD-NC shall be **easily readable by most barcode scanners** deployed in the travel/border environment.
6. The VDS-NC is **offline verifiable**, without the need for an online-connection.



Proof of Testing	Issued by UTO	Version 1	UTCI: U01932

PERSONAL INFORMATION

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

SERVICE PROVIDER

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

DATETIME OF TEST & REPORT

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

TEST RESULT

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

OPTIONAL DATA FIELD

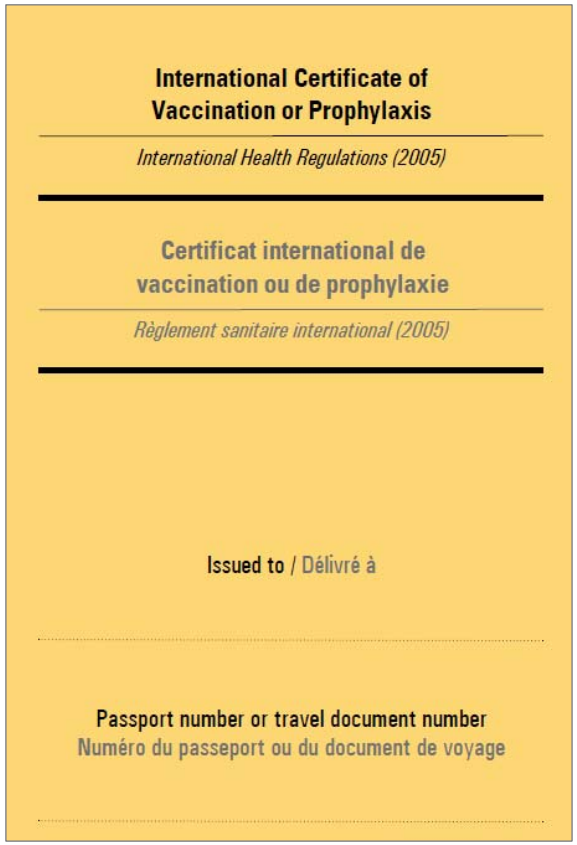
ID12345

Visible Digital Seal - NC

Main Distinctions

What it is NOT:

1. 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.
2. The VDS-NC **is not intended to replace any national/ multilateral vaccination document**.



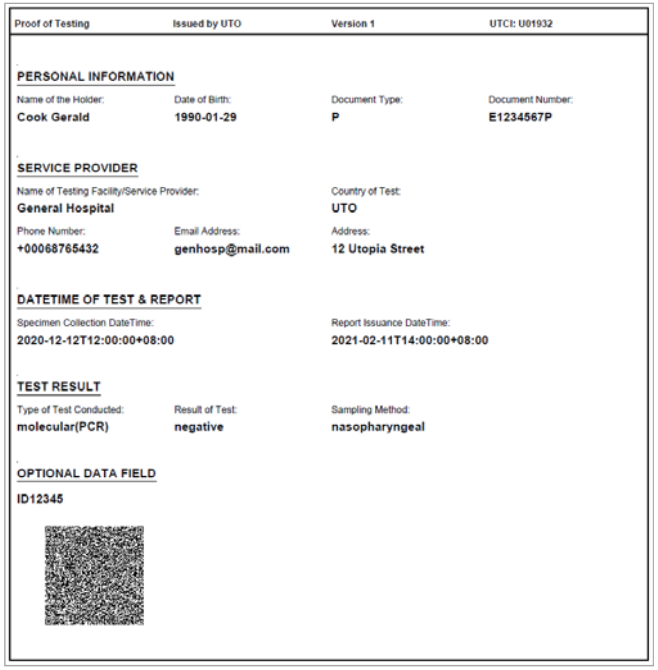
Visible Digital Seal - NC

Why „Non-Constrained“ environment?

- While the VDS’ encoding is highly space optimized and is therefore binary, the VDS-NC encodes the data as a “I-JSON” structure, easily read out by common barcode scanners, e.g. at airports/airlines.
- The VDS is intended to be used on visa labels (EU Schengen visa beginning 05/2022) and similar documents, the VDS-NC is designed to be displayed on standard format paper or smartphone screens carrying no other security features.

VDS

VDS-NC



Proof of Testing	Issued by UTO	Version 1	UTCI: U01932

PERSONAL INFORMATION

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

SERVICE PROVIDER

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

DATETIME OF TEST & REPORT

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

TEST RESULT

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

OPTIONAL DATA FIELD

ID12345

Visible Digital Seal - NC

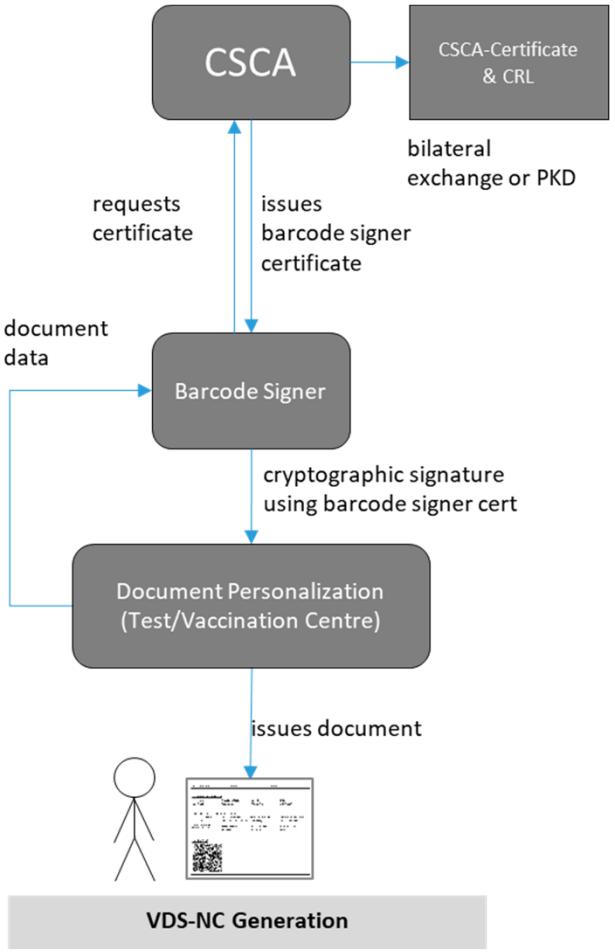
Design Principles

- *Globally Interoperable* – ICAO has followed its global mandate in supporting the development of a globally interoperable specifications.
- *„Human“ Readable* – The VDS-NC is easily readable with barcode scanners deployed in travel/border environment, therefore avoiding reading problems with binary barcodes.
  → “Payload” is human readable
- *Offline Verifiable* – The Barcode Signer Certificate is stored in the barcode itself in order to avoid the complexity of additional certificate exchange;
  → Certificate and Signature contained in the barcode
- *Able to leverage the eMRTD Trust Model* – The VDS-NC is based on the existing 2-level Public Key Infrastructure (PKI) consisting of a national Country Signing Certification Authority (CSCA), a document (barcode) signer and a Public Key Directory.
- *Flexible* – The CSCA does not have to be the same as the one for ePassports, though re-using the same CSCA is recommended. If a different CSCA is setup for VDS-NC, then specifically defined profiles allow differentiation between the function of the CSCAs.


```
{"data":{"hdr":{"t":"icao.test","v":1,"is":"UTO"},"msg":{"utci":"U
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.c
om","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":"MIIBeTCCAR2gAwIBAgIBZzAMBggqhkjOPQQDAg
UAMB0xCzAJBgNVBAYTAlVUMQ4wDAYDVQQDDAVVVCBDQTAeFw0yMTA0MDcwNDI2MTVa
Fw0yNjEwMDcwNDI2MTVaMBoxCzAJBgNVBAYTAlVUMQswCQYDVQQDEwIwNTBZMBMGBy
qGSM49AgEGCCqGSM49AwEHA0IABBzop6IWxg_Qo8JVlG-
r9EzjoAoXKsSUmkuHCTKZTY-b5atMP8jDtjJaGhaL_2VvrNbz7WDGsWf-
7MqqFzxsS6ejTzBNMBIGA1UdJQQLMAkGB2eBCAEBDgIwHwYDVR0jBBgwFoAUymyksn
X8rywn0RH7nDq-
Bs2QOqowFgYHZ4EIAQEGAgQLMAkCAQAxBBMCTlQwDAYIKoZIzj0EAwIFAANIADBFAi
Ace9uX8UOpdsOtEkAtkDu2GPyzy_S8vQP4qhzGbooa8gIhAO_5ORo2bsTor6CXHngG
ld4NNtUGsXNqXl-9qEfVcsqb",
"sigvl":"z_VZDdMvjjRkg06nYLwHt4BP_APEm3MJT8WqOOz_DXTRZA2oxkutZhS0n
7yYTHgw-MKZUJmQyhrdZgm7q-267g=="}}
```

03

Infrastructure

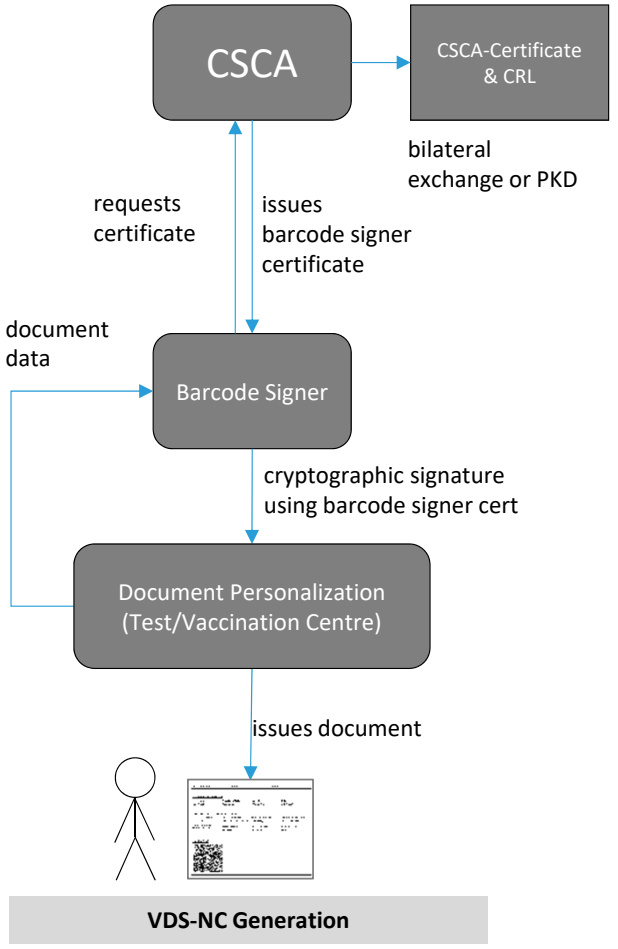


Visible Digital Seal - NC

Trust Framework

It order to function we MUST agree on:

1. The 2-level **PKI model** consisting of a root of trust (CSCA), a document (barcode) signer and a Public Key Directory. The CSCA does not have to be the same as for e-passports.
2. The **certificate profiles** as defined by ICAO. The certificate profile guarantees interoperability and security across the travel document and health proof use case.
3. The **barcode signer certificate is stored in the barcode** itself in order to avoid an additional repository.
4. A standardized **barcode encoding**. Easy readability is key.

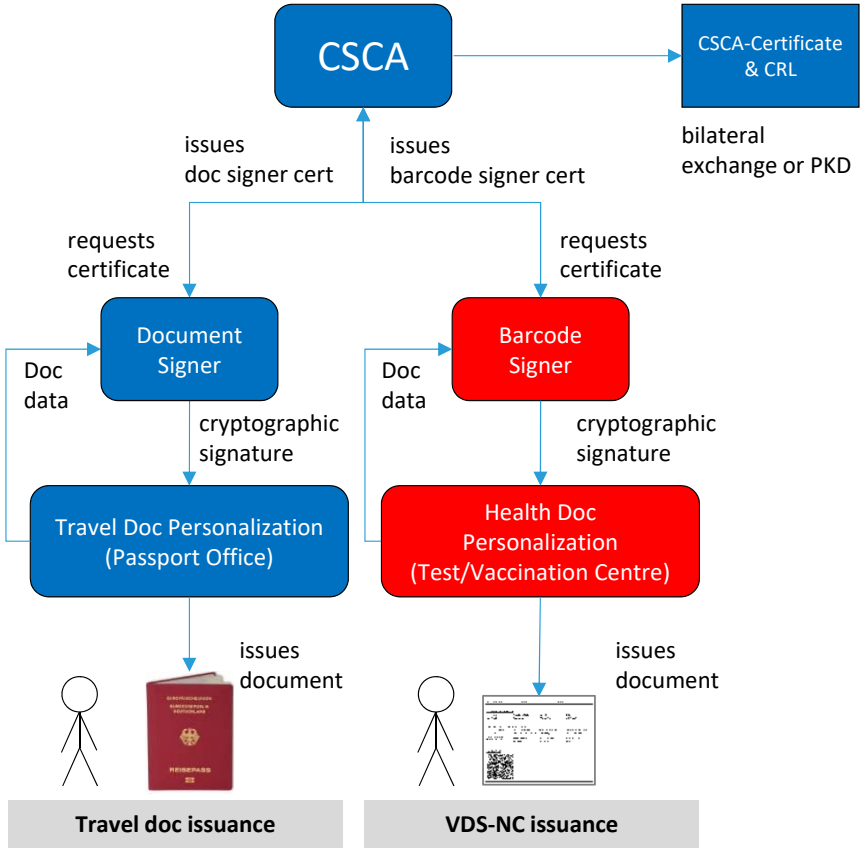


Issuance of VDS – NC

PKI model A: Single CSCA

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

- The **CSCA** for issuing travel documents acts as the **single root of trust** for both travel documents and health proofs.
- The document (barcode) signers are specific for each travel documents and health proofs.
- The certificate profiles ensure that certificates can be used for the intended purpose only.



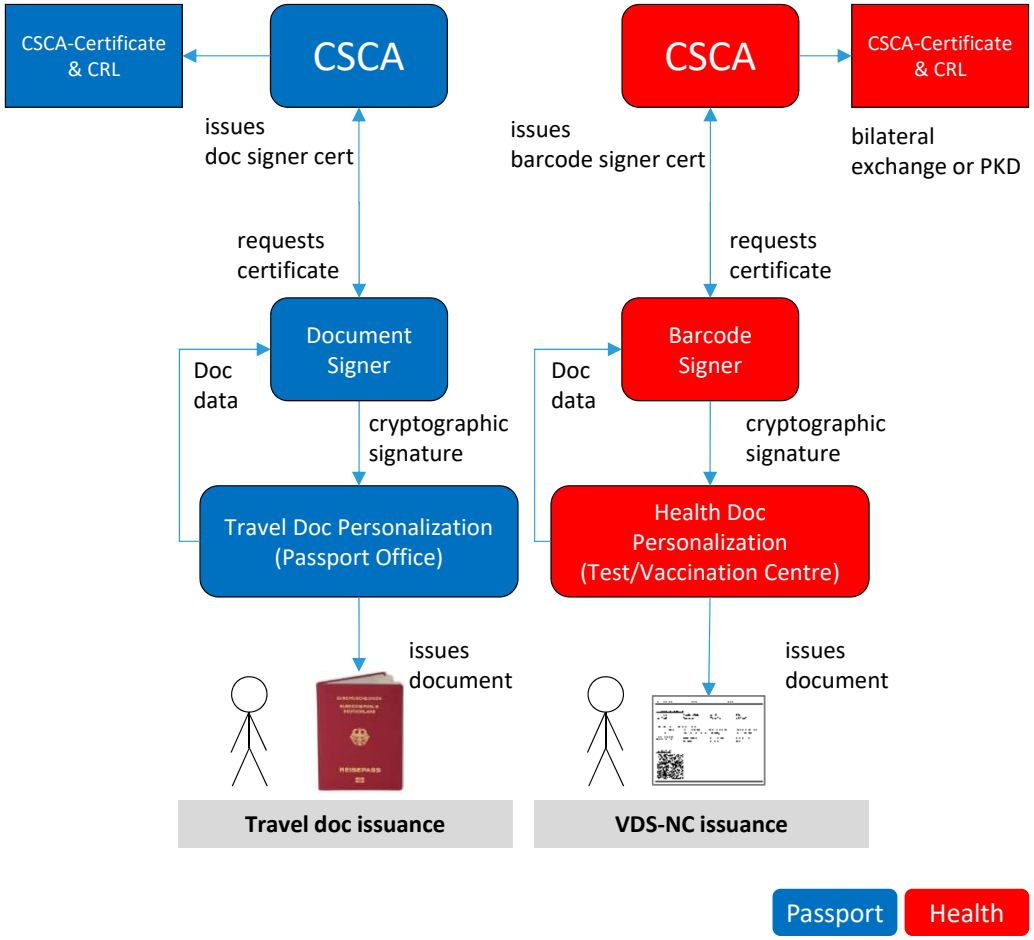
Passport Health

Issuance of VDS – NC

PKI model B: Specific CSCA‘s

PKI model B: Specific CSCA’s for each travel docs and health proofs

- There **are specific CSCA’s** for issuing travel documents and for issuing health proofs.
- The document (barcode) signers are specific for each travel documents and health proofs.
- The certificate profiles ensure that certificates can be used for the intended purpose only.

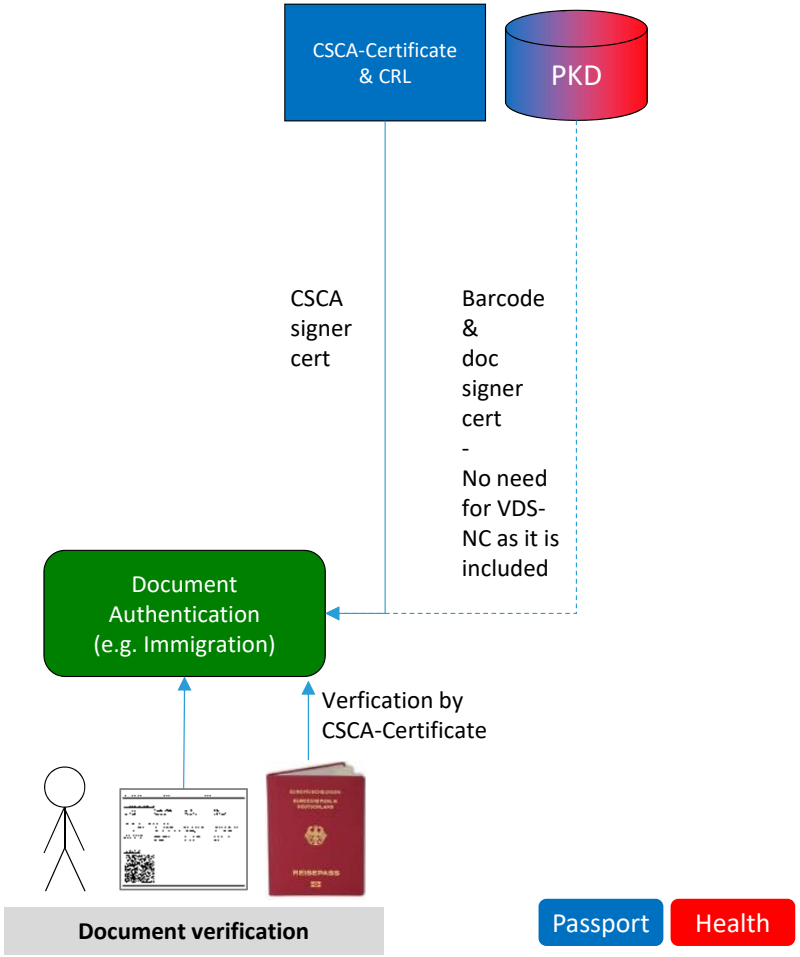


Verification of VDS – NC

PKI model A: Single CSCA

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

- Immigration systems import the CSCA certs as currently for travel documents.
- They are then able to verify both travel documents and health proofs.
- The certificate profiles ensure that certificates can be used for the intended purpose only.
- Barcode and doc signer certificates could be downloaded from the (single) PKD.

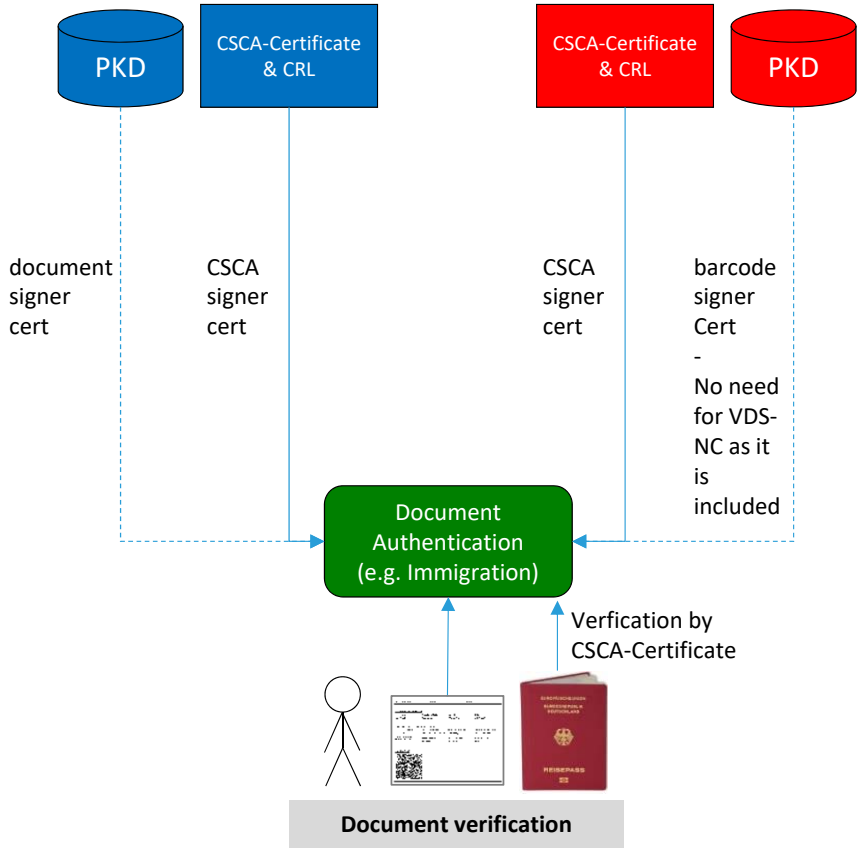


Verification of VDS – NC

PKI model B: Specific CSCA‘s

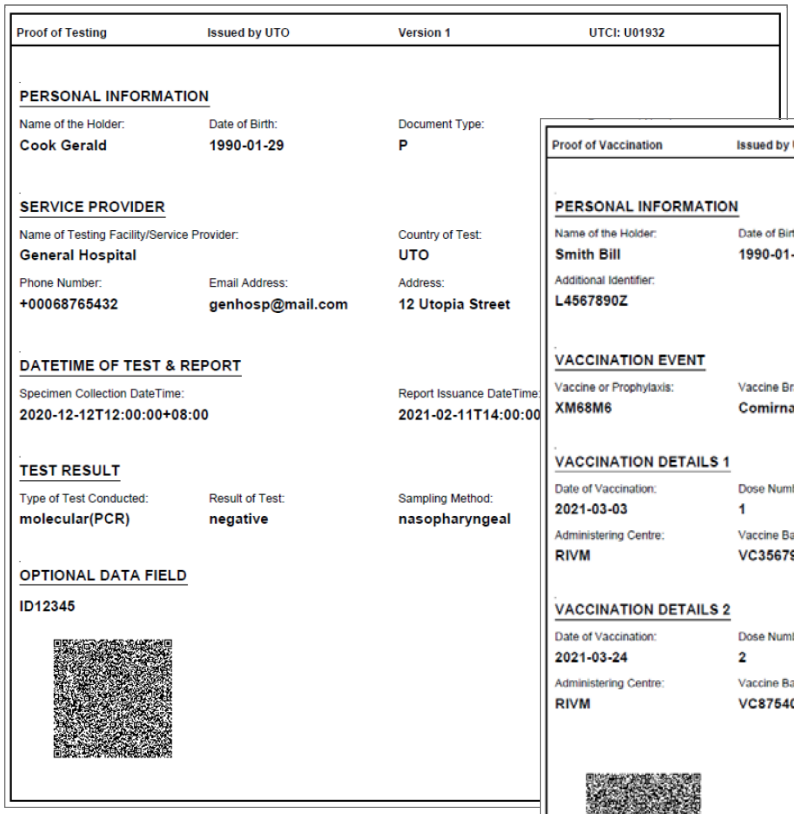
PKI model B: Specific CSCA’s for each travel docs and health proofs

- Immigration systems import the CSCA certs for travel documents and for health proofs.
- They are then able to verify both travel documents and health proofs.
- The 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.



04

Data Sets



Proof of Testing	Issued by UTO	Version 1	UTCI: U01932

PERSONAL INFORMATION

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

SERVICE PROVIDER

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

DATETIME OF TEST & REPORT

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

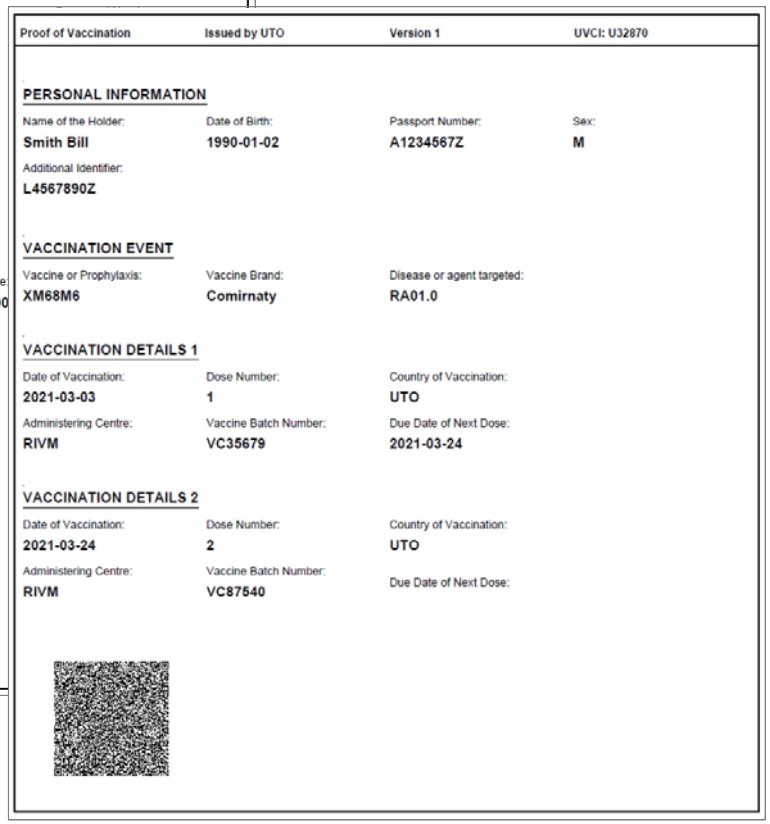
TEST RESULT

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

OPTIONAL DATA FIELD

ID12345

Proof of Test



Proof of Vaccination	Issued by UTO	Version 1	UVCI: U32870

PERSONAL INFORMATION

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

VACCINATION EVENT

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

VACCINATION DETAILS 1

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

VACCINATION DETAILS 2

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

Proof of Vaccination

Visible Digital Seal – NC: Datasets

Proof of Testing and Proof of Vaccination

Proof of Testing:

- The datasets for PoT follows the recommendations of ICAO CART.
- Notably, it contains a mandatory Document Number and a Document Type in order to establish the link between the person and a secure document.

Proof of Vaccination:

- The datasets for PoV follows the recommendations of WHO.
- Notably, it contains a Unique Identifier (e.g. a document number) and an Additional Identifier, both optional, but (strongly) recommended.
- It also allows for multiple vaccination events, with same or different vaccines.

Proof of Test (PersonalInformation)

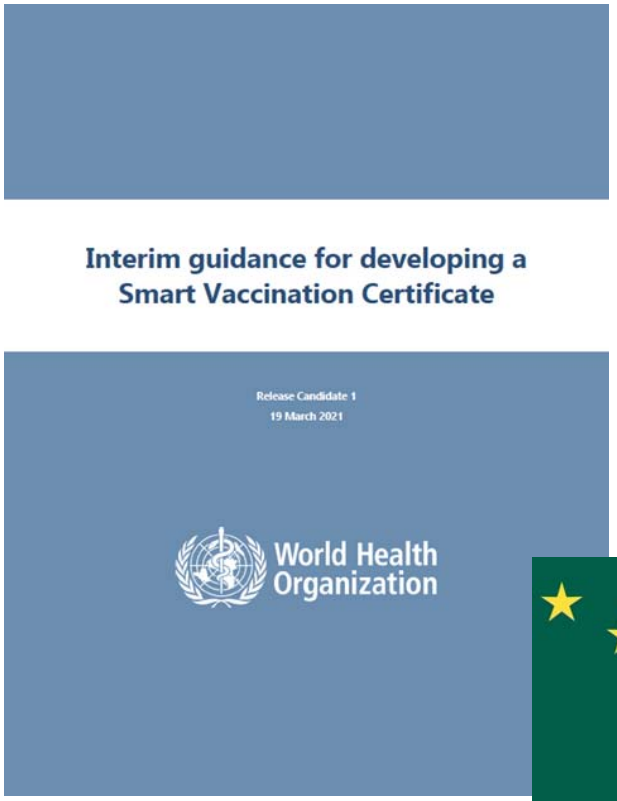
Object: Message				
Data Element (ICAO)	**Short Data Element**	**Content**	**Mandatory/ Optional**	**Max Size**
UTCI	utci	Unique Test Certificate Identifier	M	12
Object: PersonalInformation(pid)				
Name	n	Name of the holder (as specified in Doc 9303-3) MUST be used.	M	39
DOB	dob	The DOB of the test subject. The [RFC 3339] full date format YYYY-MM-DD MUST be used.	M	10
DocType	dt	The ID Document Type of the identity document MUST be used. Only these values MUST be used: P – Passport (any type, Doc 9303-4); A – ID Card (any type, Doc 9303-5); C – ID Card (any type, Doc 9303-5); I – ID Card (any type, Doc 9303-5); AC - Crew Member Certificate (Doc 9303-5); V – Visa (Doc 9303-7); D – Driving License	M	Only values stated can be used
DocNum	dn	The ID Document Number of the identity document MUST be used of the document used in DocType. The ID Document Number is the unique identifier of the test subject.	M	24

Object: Message				
Data Element (ICAO)	**Short Data Element**	**Content**	**Mandatory/ Optional**	**Max Size**
UTCI	utci	Unique Test Certificate Identifier	M	12
Object: PersonIdentification (pid)				
Name	n	Name of the holder (as specified in Doc 9303-3) MUST be used.	M	39
Date of Birth	dob	Date of birth of subject. ISO8601 YYYY-MM-DD	C	10
Unique Identifier	i	Travel Document Number; Single Unique Identifier only. Identifier should be valid Travel Document number	O-R	11
Additional Identifier	ai	Any other document number at discretion of issuer	O	24
Sex	sex	Gender of the subject	O-R	1

Proof of Vaccination (PersonIdentification)

05

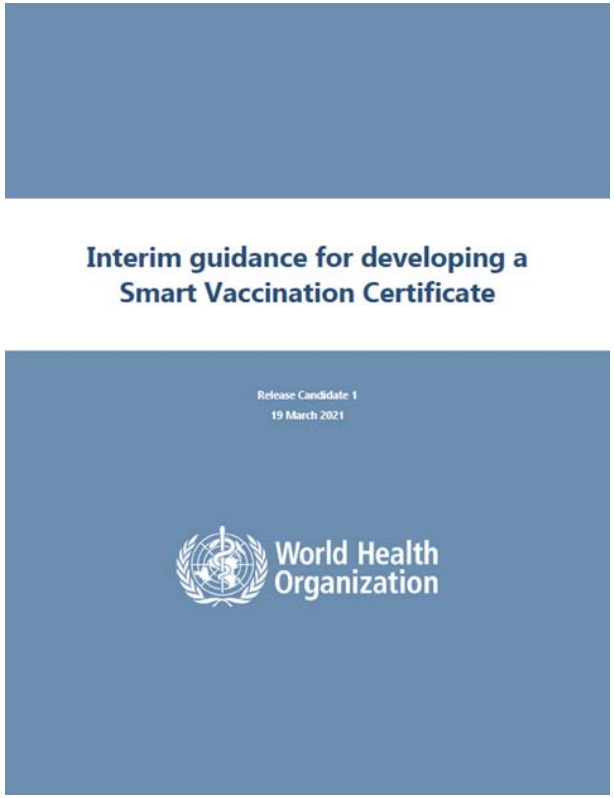
Related Initiatives



Related Initiatives

WHO Smart Vaccination Certificate

- ICAO has been closely working and coordinating with the WHO on the SVC and with the EU with regards to the EU DGC.
- ICAO TAG/TRIP and ISO experts have been actively involved in contributing to both initiatives in order to ensure that any solution to be developed is compatible with the ICAO VDS-NC.
- The first set of specifications for the WHO SVC (Release Candidate 1) were issued on 19 March, 2021. RC2 is going to be published any time soon.
- Based on WHO's decision criteria, the global trust framework outlined is a PKI-based design that follows the ICAO PKI model for ePassports and leverages a Public Key Directory like the one operated by ICAO since now fifteen years.



Related Initiatives

EU Digital Green Certificate

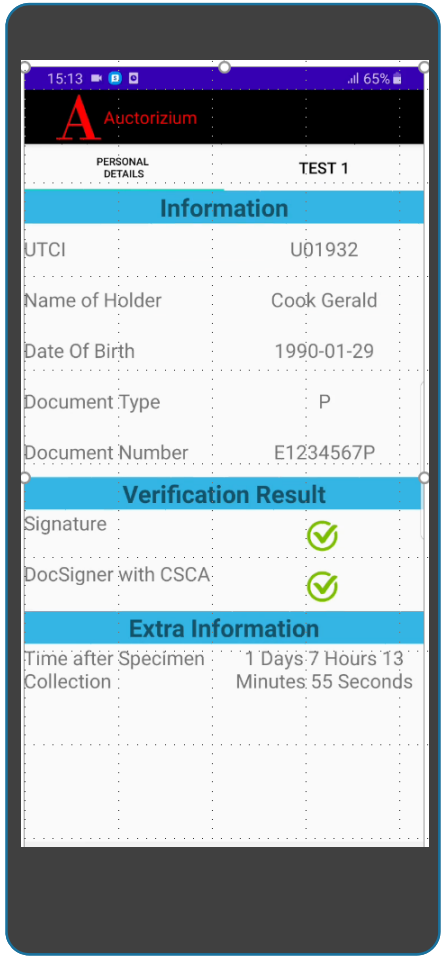
- The EU is working towards deployment of the EU DGC system by June 2021.
- Notwithstanding the good alignment between DGC Guidelines and the ICAO VDS-NC specifications, both parties have initiated technical discussions in order to identify possible compatibility issues between both technologies as well as global interoperability.
- Main differences are:
  - Encoding of the barcode
  - VDS-NC contains signer certificate as well
  - CSCA Masterlist and CRL required for verifying VDS-NC
  - Barcode Signer (as trustlist) and CSCA required for verifying EU-DGC – only available to EU countries

EU-DGC

VDS-NC

06

Demonstration

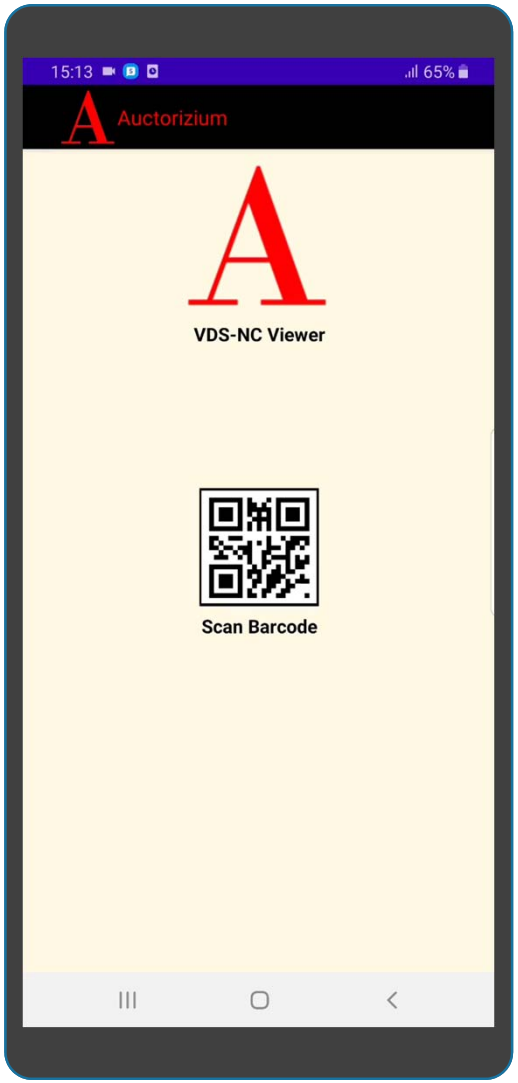


Demonstration Proof of Test

Normal reading and verification

What do you see?

- Personal details with verification of signature and verification of barcode signer against CSCA
- Time since specimen collection (for the 48-72 hour requirement)
- Details of the test facility, specimen and test result date and time
- Type of test and sampling method and the result



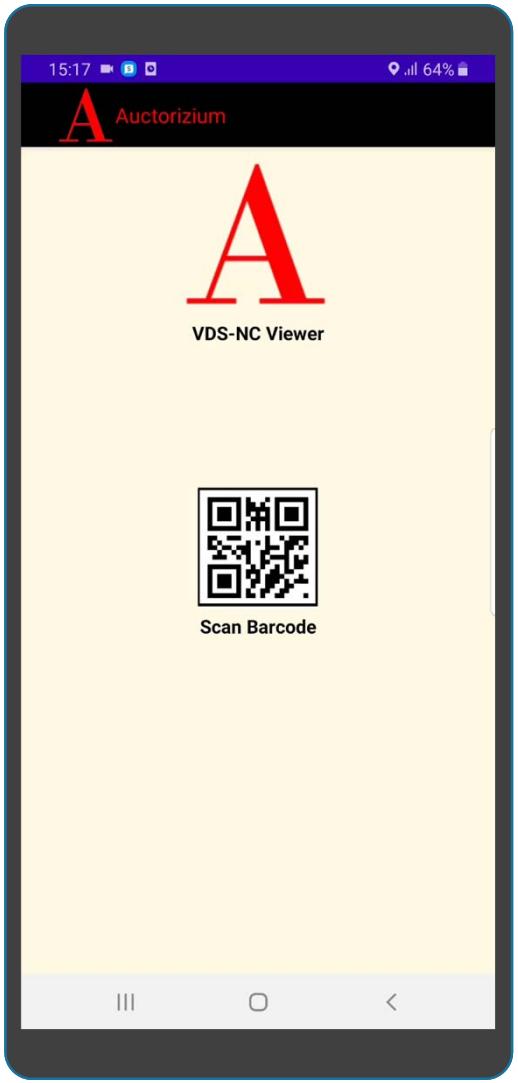
Demo kindly provided by Auctorizium, Singapore

Demonstration Proof of Test

Verification fails due to unknown CSCA

What do you see?

- Proof of testing – unknown CSCA
- Barcode verification successful
- Barcode signer cannot be verified



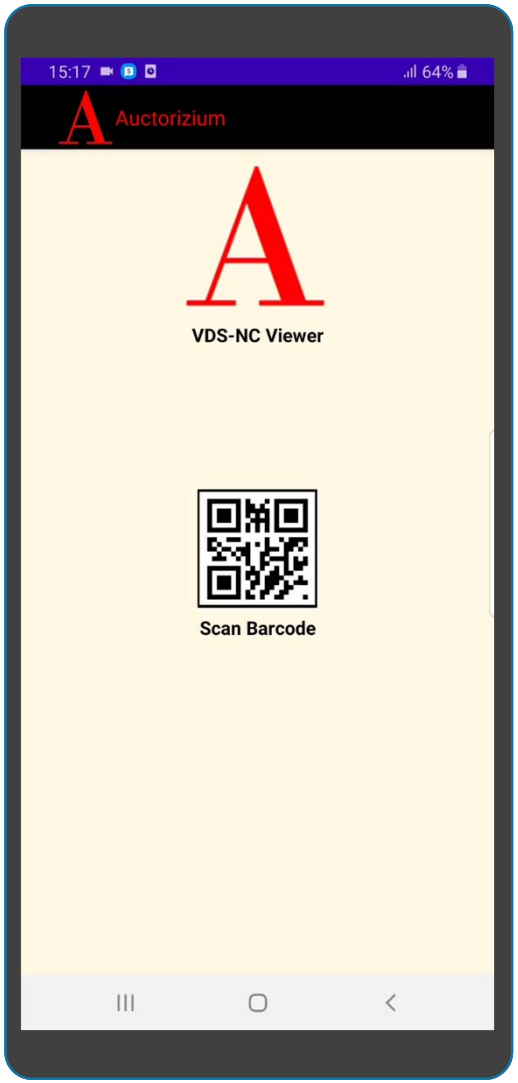
Demo kindly provided by Auctorizium, Singapore

Demonstration Proof of Test

Verification fails due to manipulation

What do you see?

- Proof of Testing – Signature failure due to tampering of data.
- The date of sampling has been modified (2021-05-20 → 2021-05-21).
- The Rest of the data is correct.



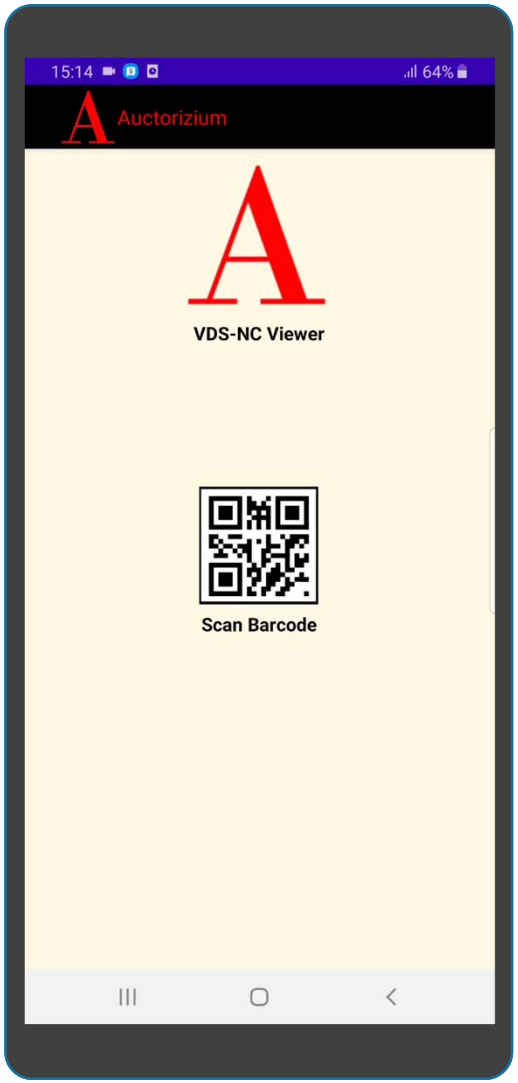
Demo kindly provided by Auctorizium, Singapore

Demonstration Proof of Vaccination

Normal reading and verification

What do you see?

- Same vaccine – two doses
- Shown as single Vaccination Event with two separate doses.
- First dose has date of next dose
- For the second dose, date of the next dose is blank.



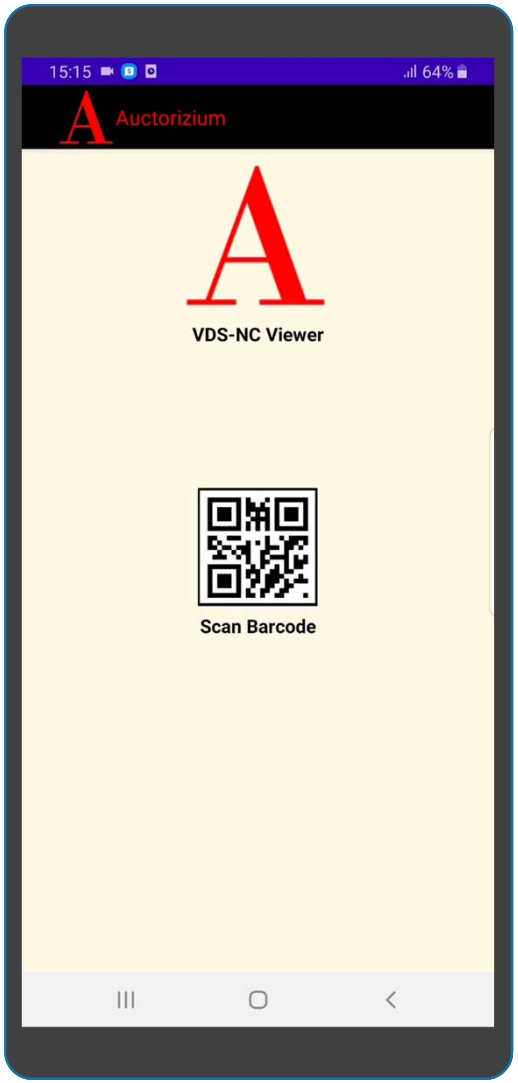
Demo kindly provided by Auctorizium, Singapore

Demonstration Proof of Vaccination

Normal reading and verification

What do you see?

- Two different vaccines for each dose.
- Shows up as two vaccination events
- First is BionTech/Pfizer, next is Moderna.
- First dose in in UTO, second in SGP. Still signed by UTO.



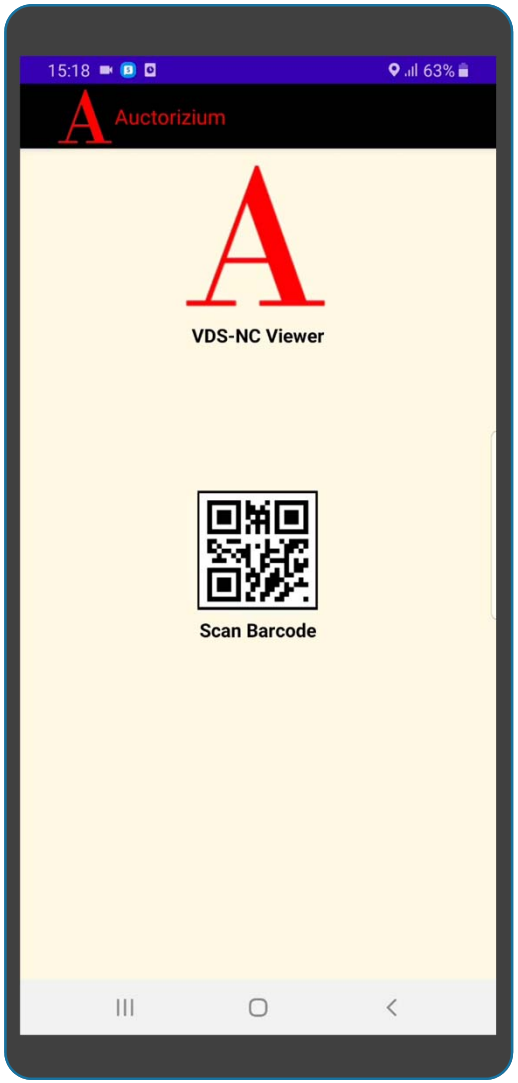
Demo kindly provided by Auctorizium, Singapore

Demonstration Proof of Vaccination

Signature validation fails due to manipulation

What do you see?

- Proof of Vaccination – signature failure due to tampering of data
- Name of the person has been changed (Smith Bill → Smith Ken).
- Anything else is correct.



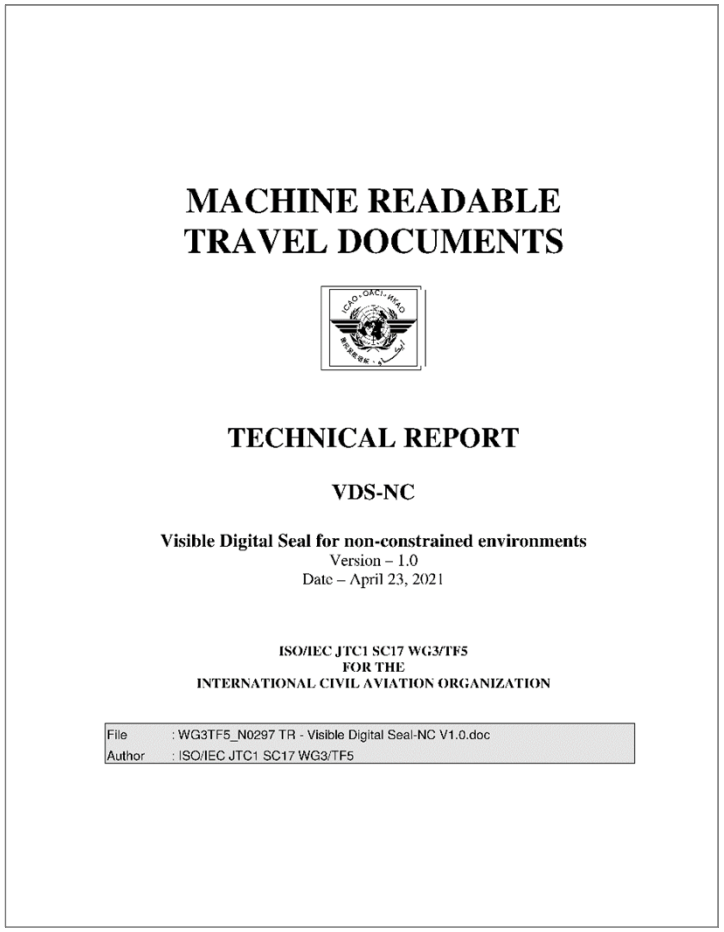
Demo kindly provided by Auctorizium, Singapore

Summary
Next Steps

Visible Digital Seal - NC

Summary & Next Steps

- Accomplishing the task set out by ICAO CART Phase III, a global framework for the validation of testing and vaccination records and/or certificates was developed by ICAO TAG/TRIP and ISO experts.
- Specifications for a viable technical solution leveraging existing infrastructures to provide for rapid implementation and global interoperability were published.
- The specifications can be found at https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx
- ICAO TAG/TRIP and ISO experts will be actively working to ensure interoperability of the VDS-NC with relevant global initiatives such as the WHO SVC and the EU DGC.



MACHINE READABLE
TRAVEL DOCUMENTS

TECHNICAL REPORT

VDS-NC

Visible Digital Seal for non-constrained environments
Version – 1.0
Date – April 23, 2021

ISO/IEC JTC1 SC17 WG3/TF5
FOR THE
INTERNATIONAL CIVIL AVIATION ORGANIZATION

File	: WG3TF5_N0297 TR - Visible Digital Seal-NC V1.0.doc
Author	: ISO/IEC JTC1 SC17 WG3/TF5

Thank You

ICAO