ICAO

TRIP 2022

SEAMLESS AND CONTACTLESS

Sharing data to accelerate the recovery

13 - 15 SEPTEMBER 2022

Visible Digital Seal
(VDS)

R Rajeshkumar

Chair – ISO SC17/WG3/TF5

Editor – Doc 9303-12, DTC, VDS-NC

Chief Executive – Auctorizium Pte Ltd, Singapore

R.Rajeshkumar@auctorizium.com

1. The Rationale

eMRTDs

- Physical Security features protect the datapage
- Substitution attacks can still happen
- Security enhanced through the addition of a RFID chip and Digital Signature

Protecting paper documents

- Paper documents like Visa stickers also need to be protected
- Have physical security features
- Not practical to add a RFID chip to a visa sticker

Hence a Visible Digital Seal (VDS)

2. Visible Digital Seal

Visible Digital Seal (VDS)

- Digitally signed 2D barcode
- Provide security improvement for (usually paper based) documents having no microchip
- Storage capacity of digital seals is usually limited to a few kByte at most and neither the data nor the cryptographic keys or schemes for the digital seal can be updated on existing documents – no cryptographic agility
- does not provide any protection against cloning
- does not implement privacy protection functionality

Visible Digital Seal (VDS)

- The Technical Report defines a message structure and encoding requirements along with Digital Signature specifications
- Defines profiles for two usage scenarios
  - Visa stickers
  - Emergency Travel Documents
- Due to size limitation, only textual data is encoded – no biometric data. In both use cases, only the MRZ is part of the VDS
- Unlike SOD, the VDS does not contain the Signer Certificate. Hence, verification requires the exchange of Signer Certificates

VDS - characteristics

- Primarily designed for Visa sticker. Hence highly space optimized
- Encoding is binary – requires specialist software to decode the contents.
- Might not be readable by normal barcode scanners that do not support UTF8
- Requires mechanism for barcode signer certificate exchange

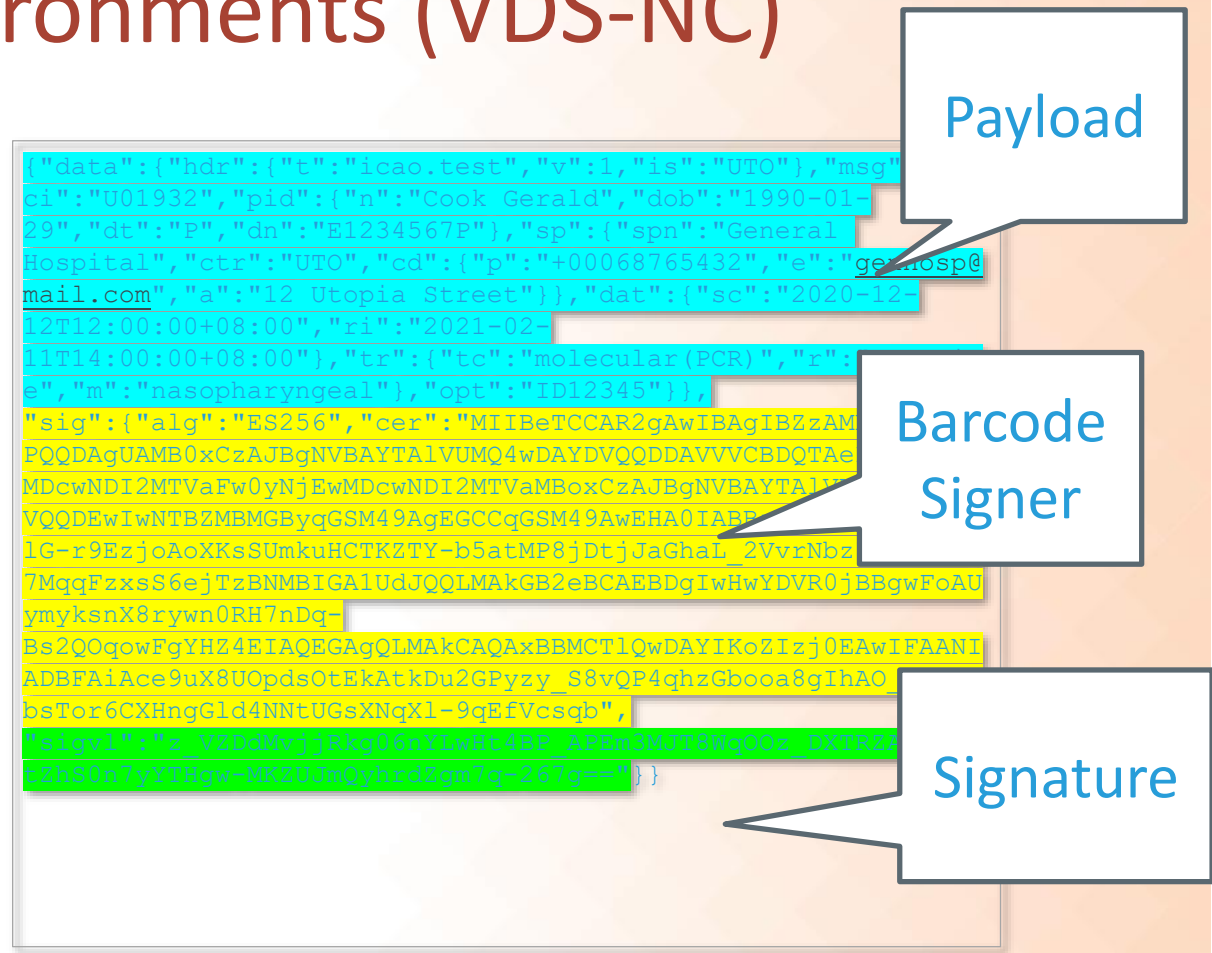
3. Visible Digital Seal for Non-Constrained environments (VDS-NC)

Health Proofs

- ICAO Council's Aviation Recovery Task Force (CART) asked for the development of a global framework for the validation of testing and vaccination records and/or certificates
- Was intended to be based on VDS
  - Issue of Size constraint
  - Issue of barcode signer distribution

VDS for Non-Constrained environments (VDS-NC)

- Uses an I-JSON structure – makes it readable using any scanner
- Payload is human readable
- Barcode Signer is included in the barcode – so distribution of barcode signer is not a problem
- Barcode Signer and Signature contained in barcode – so offline verifiable
- Re-uses the eMRTD PKI model
  - CSCA => Barcode Signer => Signature

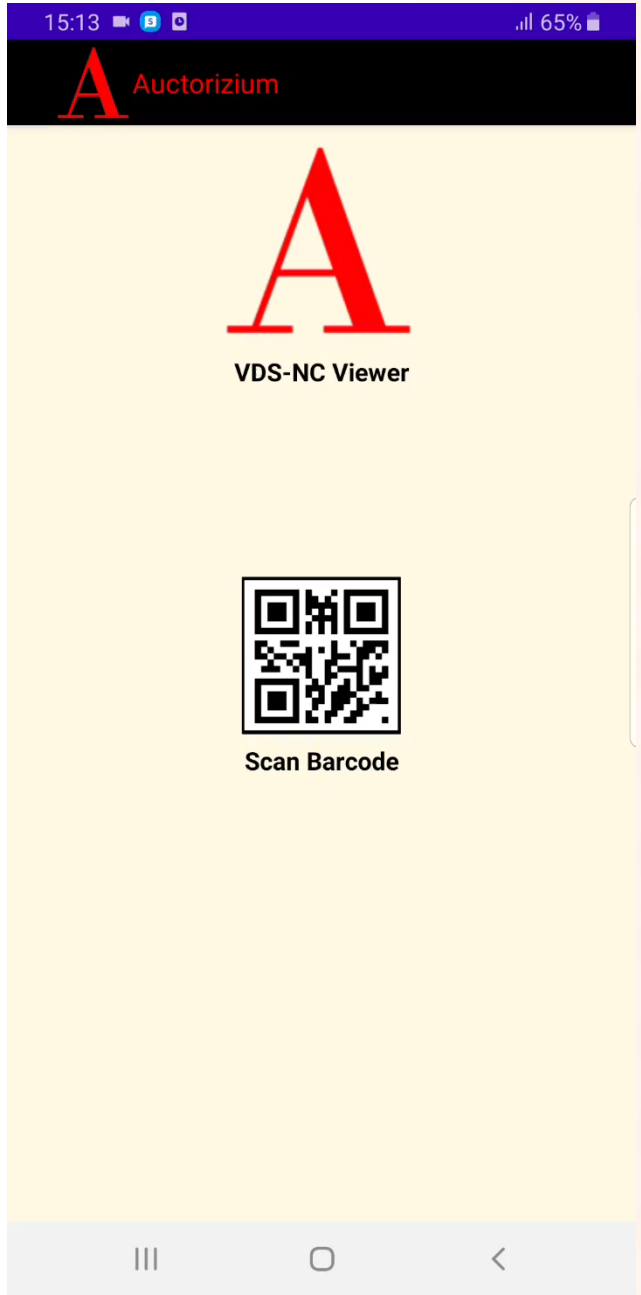


Use cases

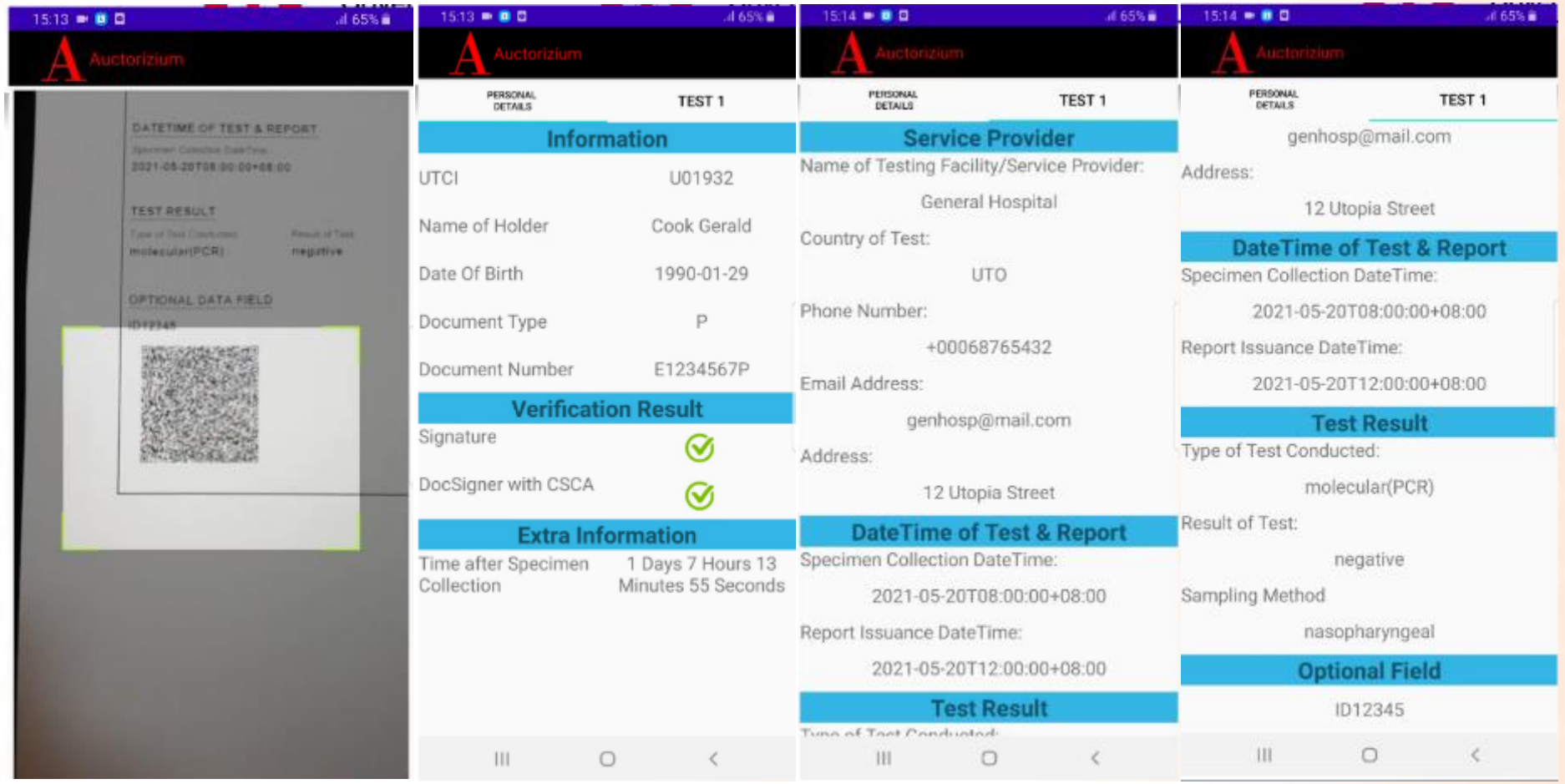
- Four use cases defined
  - Proof of Testing
  - Proof of Vaccination
  - Proof of Recovery
  - Digital Travel Authorization

Proof of Testing

- Data set defined by ICAO Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil Aviation (CAPSCA)
- Tied to an Identity document (ID, Passport or Driving License)

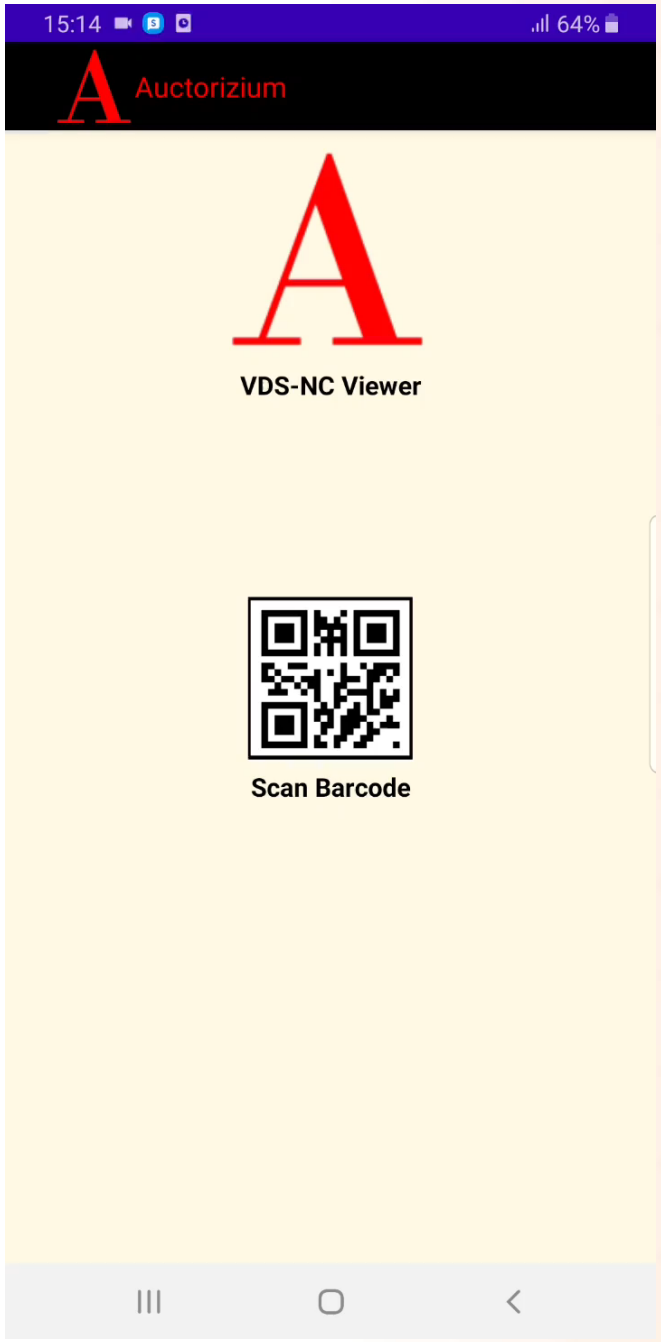


Demo kindly provided by Auctorizium, Singapore

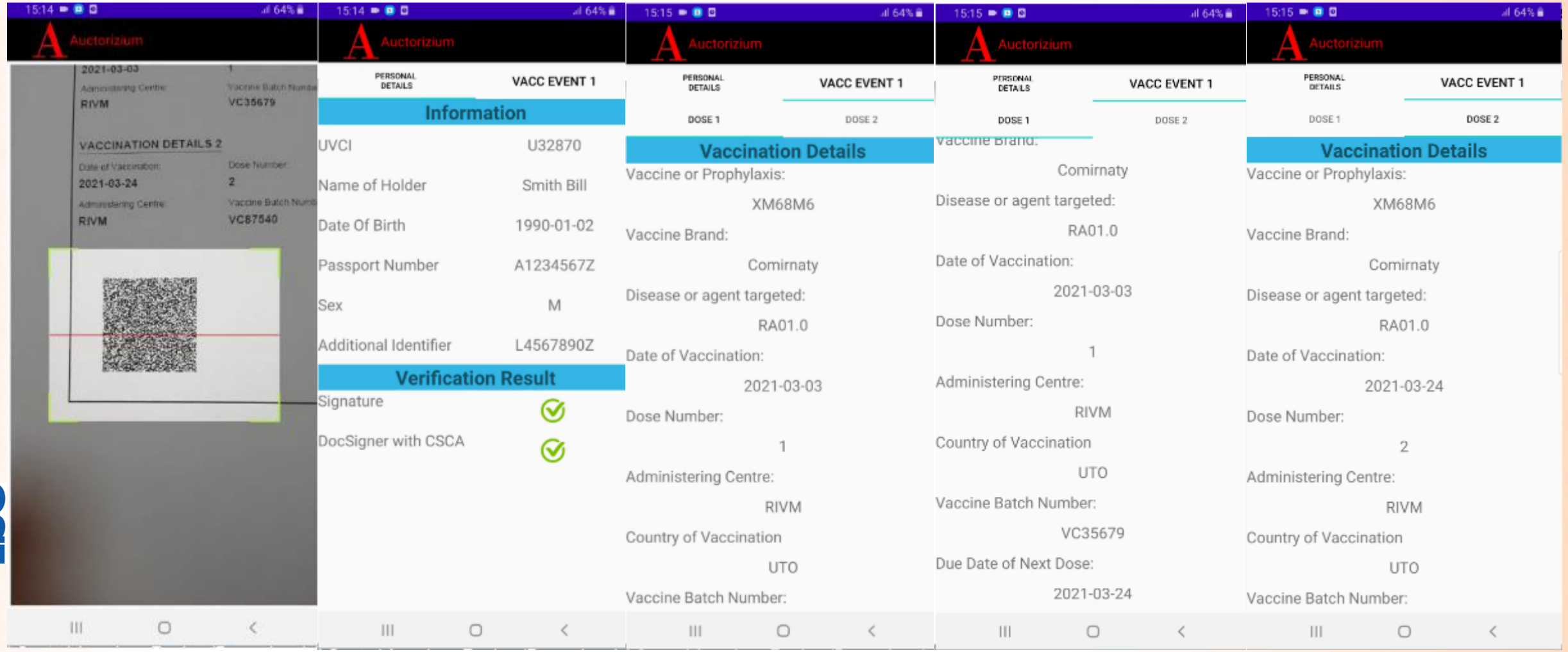

15:13
65%
Auctorizium
DATETIME OF TEST & REPORT
TEST RESULT
molecular(PCR)
negative
OPTIONAL DATA FIELD
PERSONAL DETAILS
TEST 1
Information
UTCI
U01932
Name of Holder
Cook Gerald
Date Of Birth
1990-01-29
Document Type
P
Document Number
E1234567P
Verification Result
Signature
DocSigner with CSCA
Extra Information
Time after Specimen Collection
1 Days 7 Hours 13 Minutes 55 Seconds
15:14
65%
Auctorizium
PERSONAL DETAILS
TEST 1
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:
2021-05-20T08:00:00+08:00
Report Issuance DateTime:
2021-05-20T12:00:00+08:00
Test Result
15:14
65%
Auctorizium
PERSONAL DETAILS
TEST 1
genhosp@mail.com
Address:
12 Utopia Street
DateTime of Test & Report
Specimen Collection DateTime:
2021-05-20T08:00:00+08:00
Report Issuance DateTime:
2021-05-20T12:00:00+08:00
Test Result
Type of Test Conducted:
molecular(PCR)
Result of Test:
negative
Sampling Method
nasopharyngeal
Optional Field
ID12345

Proof of Vaccination

- Data set defined by WHO
- Some variations – Link to Passport is necessary
- Entire vaccination history recorded in a single barcode



Demo kindly provided by Auctorizium, Singapore


Auctorizium
RIVM
VC35679
VACCINATION DETAILS 2
2021-03-24
2
RIVM
VC87540
PERSONAL DETAILS
VACC EVENT 1
Information
UVCI U32870
Name of Holder Smith Bill
Date Of Birth 1990-01-02
Passport Number A1234567Z
Sex M
Additional Identifier L4567890Z
Verification Result
Signature
DocSigner with CSCA
DOSE 1
DOSE 2
Vaccination Details
Vaccine or Prophylaxis: XM68M6
Vaccine Brand: Comirnaty
Disease or agent targeted: RA01.0
Date of Vaccination: 2021-03-03
Dose Number: 1
Administering Centre: RIVM
Country of Vaccination UTO
Vaccine Batch Number:
Vaccine Brand: Comirnaty
Disease or agent targeted: RA01.0
Date of Vaccination: 2021-03-03
Dose Number: 1
Administering Centre: RIVM
Country of Vaccination UTO
Vaccine Batch Number: VC35679
Due Date of Next Dose: 2021-03-24
Vaccination Details
Vaccine or Prophylaxis: XM68M6
Vaccine Brand: Comirnaty
Disease or agent targeted: RA01.0
Date of Vaccination: 2021-03-24
Dose Number: 2
Administering Centre: RIVM
Country of Vaccination UTO
Vaccine Batch Number:

Proof of Recovery

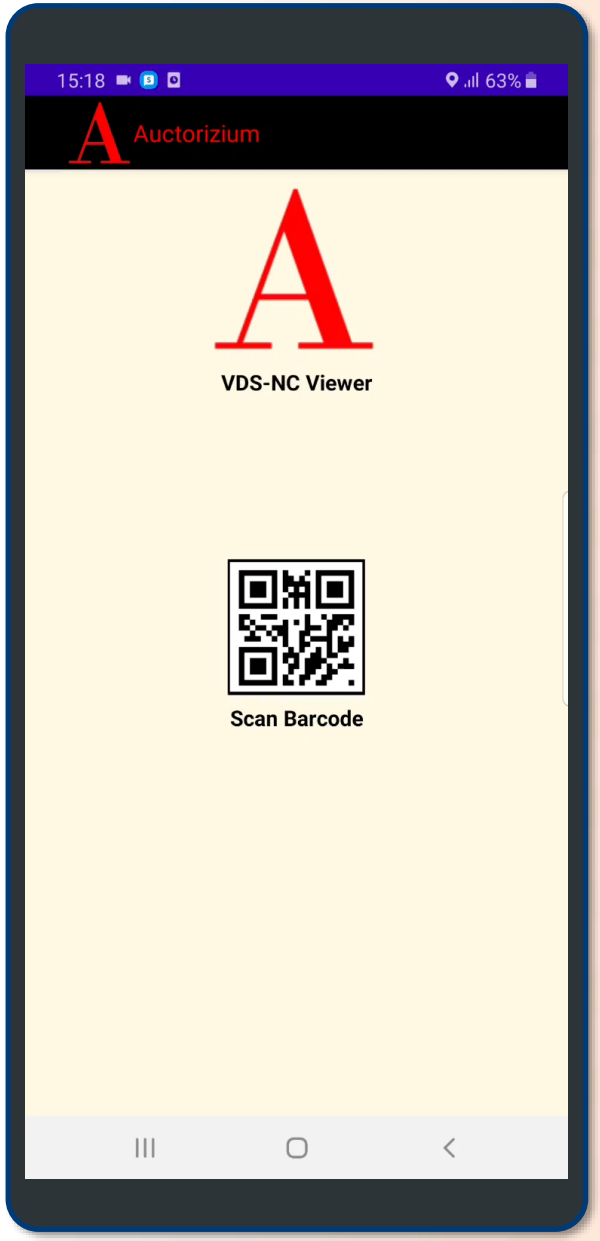
- Data set defined by CAPSCA
- Similar to Proof of Testing
- Approved and included in latest version of the Technical Report

Demonstration Proof of Vaccination

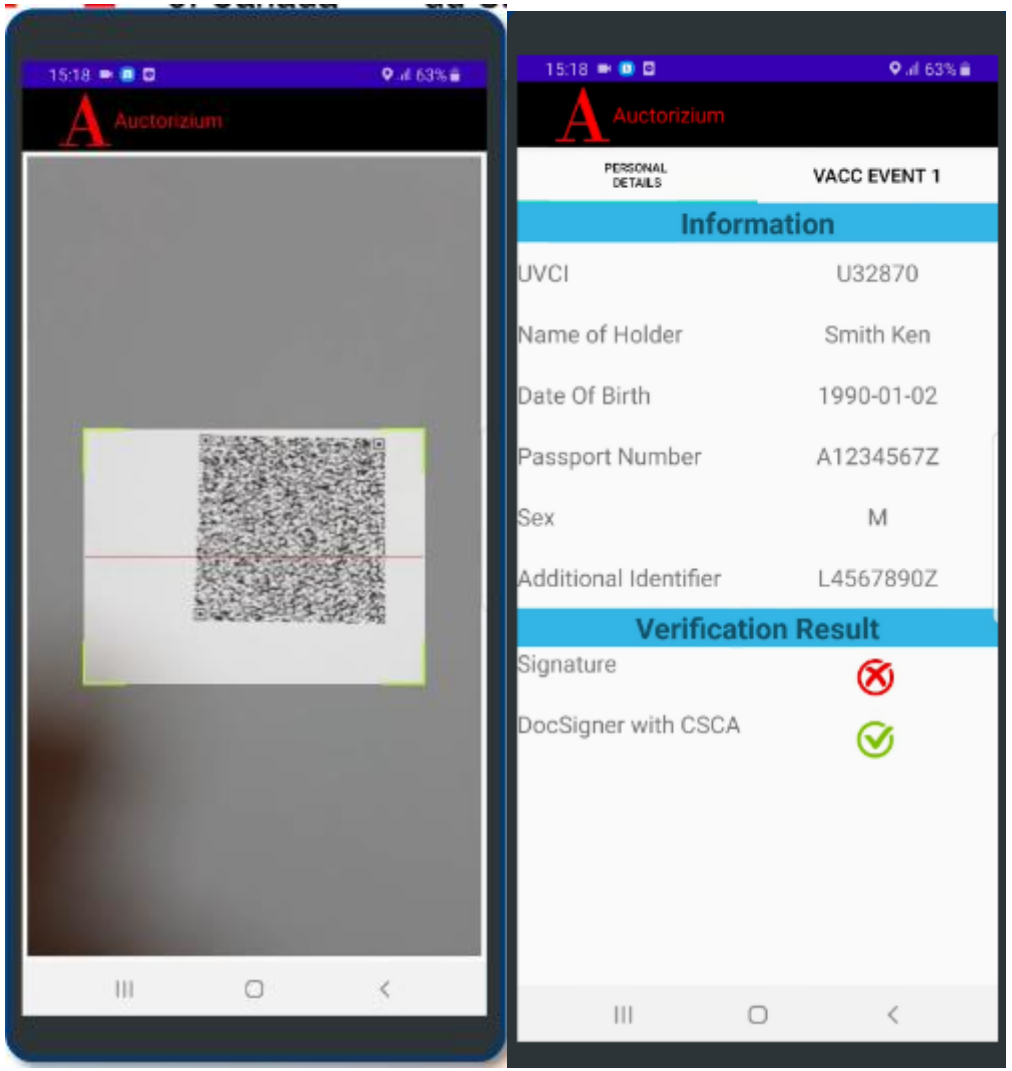
What do you see?

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

Signature validation fails due to manipulation



Demo kindly provided by Auctorizium, Singapore


15:18
63%
Auctorizium
15:18
63%
Auctorizium
PERSONAL DETAILS
VACC EVENT 1
Information
UVCI
U32870
Name of Holder
Smith Ken
Date Of Birth
1990-01-02
Passport Number
A1234567Z
Sex
M
Additional Identifier
L4567890Z
Verification Result
Signature
DocSigner with CSCA

Digital Travel Authorization

- Intended to be used for eVisa situations
- Normal practice is to send a PDF document with no security features
- VDS-NC for DTA can be used to protect such documents

Digital Travel Authorization | Issued by UTO | Version 1 | DTA Number: N156702B

PERSONAL INFORMATION

Name of the Holder:	Date of Birth:	Nationality:	Sex:
Anna Maria Eriksson	1952-03-11	USA	F

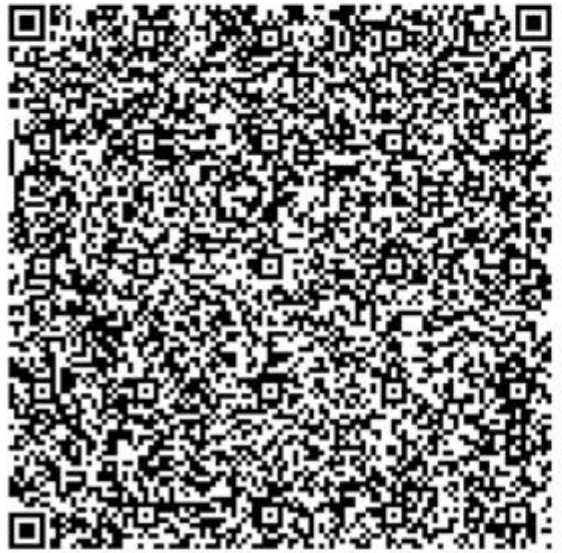
Passport Number:
L8988901C

DIGITAL TRAVEL AUTHORIZATION

Place of Issue:	Valid From:	Valid Until:
Peacetown	2021-06-06	2026-06-06

Duration of Stay:	Number of Entries:	Type/Class/Category:
5 years, 0 months, 0 days	Multiple	Tourist

Additional Information:
Employment Prohibited



VDS-NC extending use cases

- VDS-NC is defined as a generic container
- Can be used for any use case. Could be used for birth certificates, university transcripts etc.
- Each use case requires a profile definition and a namespace – The technical report explains the use of namespaces – used to differentiate the use cases

Newer developments in VDS-NC

- New version allows VDS-NC to be created without including the Barcode Signer is the barcode – size reduction
- Defines a Trust List to publish the barcode signers for distribution

4. Future Developments

New uses cases for Barcodes

- Re-design of TD1 cards is being discussed
  - Currently CAN is printed on front of card and needs to be read using OCR
  - MRZ (3-line) is printed on the reverse
  - Option being discussed
    - CAN encoded in 2D barcode to make it easy for machine reading
    - Add a barcode that encodes the MRZ – possible remove MRZ in the future (space saving)
- DTC-PC requires a means of passing CAN and other parameters to the Inspection System

Secure Messaging Barcode

- Currently under discussion
- Effort is to define a single barcode that can be used to pass Secure messaging parameters – CAN, MRZ, EF.CardAccess (for PACE) etc
- Targeted for approval by end of the year

Thank You

ICAO