ICAO UNITING AVIATION

ICAO Visible Digital Seals (VDS):

For Travel Related Health Proofs

Executive Briefing

Christopher Hornek
Annex 9 Expert
chornek@icao.int

Guiding Principle

ICAO Doc 9303 defines global interoperability as:

> *The capability of inspection systems (either manual or automated) in different States throughout the world to obtain and exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States…*

Objective

ICAO seeks to provide specifications to achieve global interoperability among solutions – thereby assuring common performance and security standards.

ICAO is **not** proposing a solution to replace existing tools.

Technical specifications should enhance the tools, just as eMRTD specifications enhance the travel document landscape globally.

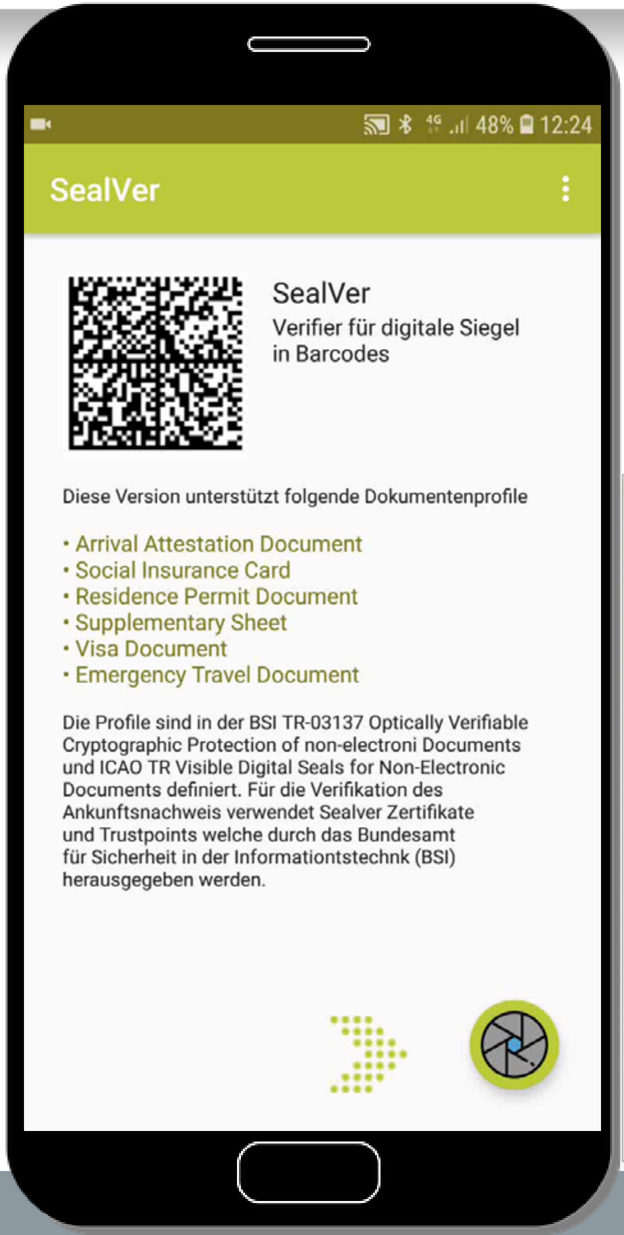
What problem are we addressing?

- As aviation restarts, States will require health proofs (vaccination and test certificates) from international passengers.
- These health proofs will often be issued in one State but will need to be verified
  - in another State on arrival;
  - and/or by the aircraft operator before departure.

What problem are we addressing?

- This additional burden creates a huge Facilitation challenge because no one (*States, airlines, airports*) can afford an additional layer of inspection.
  - It would be too costly and time consuming.
- At the same time, immigration officers and airline staff have no expertise in assessing health proofs.
  - But in the future everything needs to be automated.

VDS Example



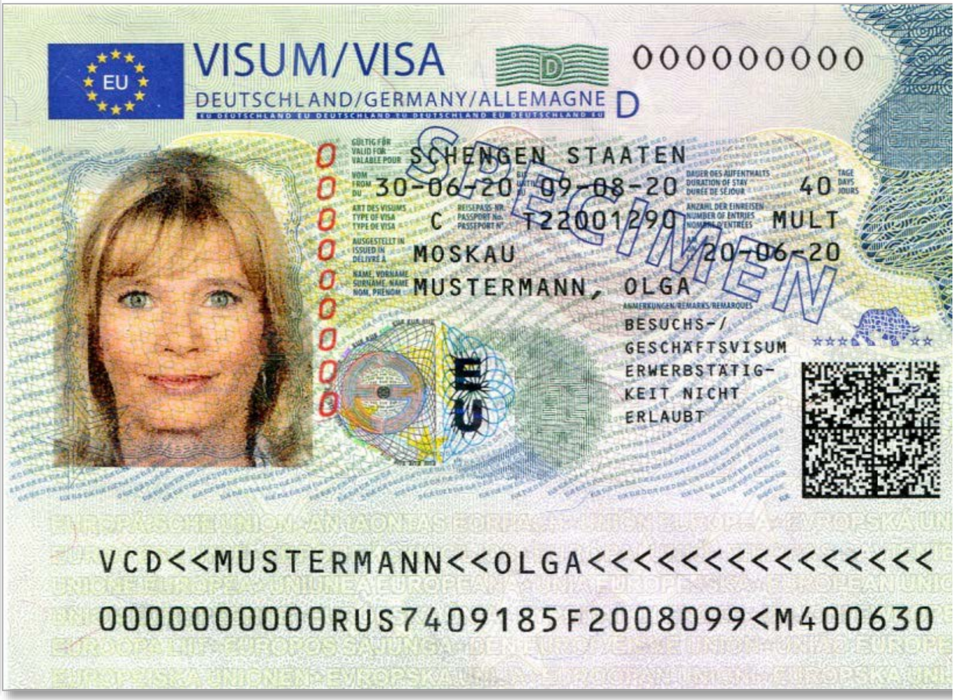
SealVer

SealVer
Verifier für digitale Siegel in Barcodes

Diese Version unterstützt folgende Dokumentenprofile

- Arrival Attestation Document
- Social Insurance Card
- Residence Permit Document
- Supplementary Sheet
- Visa Document
- Emergency Travel Document

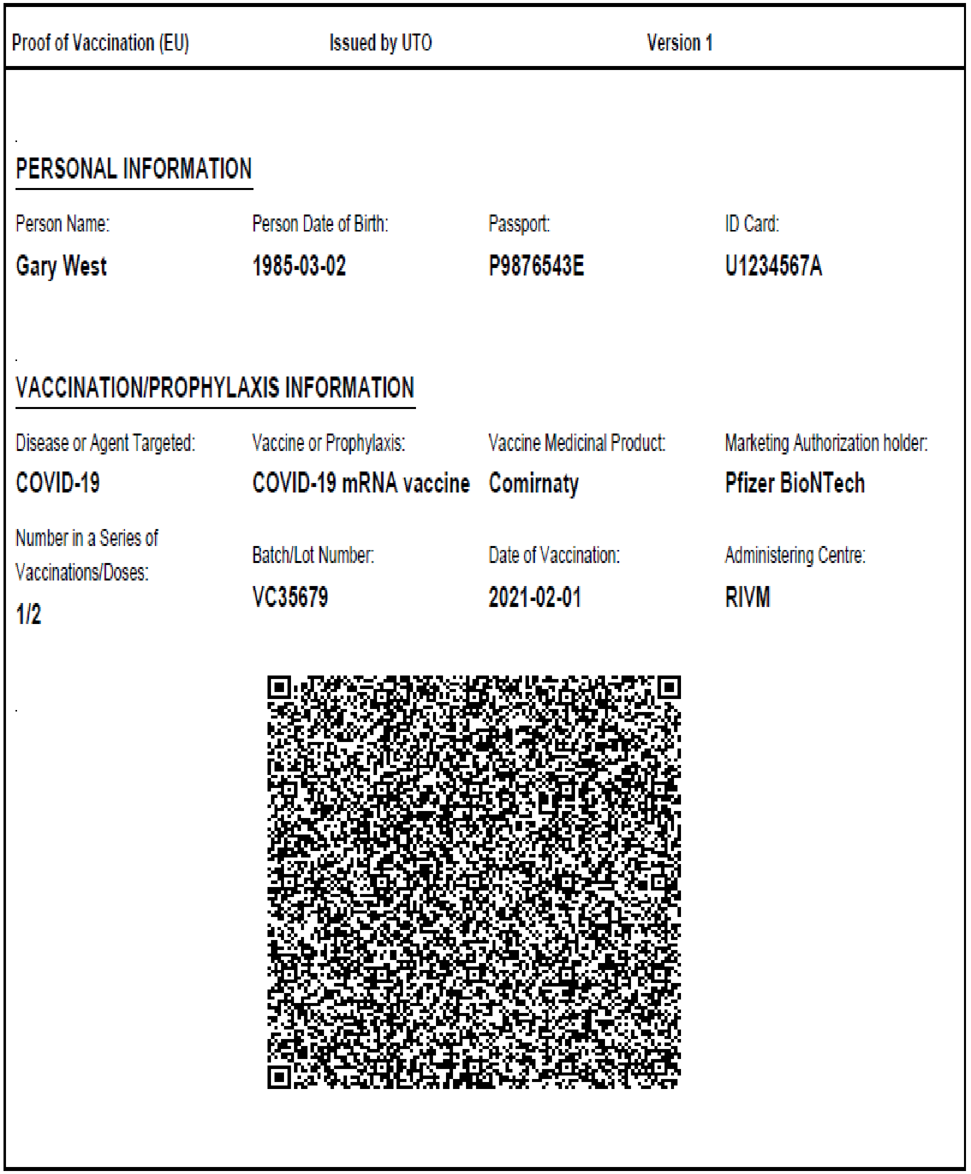
Die Profile sind in der BSI TR-03137 Optically Verifiable Cryptographic Protection of non-electroni Documents und ICAO TR Visible Digital Seals for Non-Electronic Documents definiert. Für die Verifikation des Ankunftsnachweis verwendet Sealver Zertifikate und Trustpoints welche durch das Bundesamt für Sicherheit in der Informationtstechnk (BSI) herausgegeben werden.



VISUM/VISA 000000000
DEUTSCHLAND/GERMANY/ALLEMAGNE D

GÜLTIG FÜR / VALID FOR / VALABLE POUR: SCHENGEN STAATEN
VOM / FROM / DU: 30-06-20 BIS / UNTIL / AU: 09-08-20 DAUER DES AUFENTHALTS / DURATION OF STAY / DURÉE DE SÉJOUR: 40 TAGE / DAYS / JOURS
ART DES VISUMS / TYPE OF VISA / TYPE DE VISA: C REISEPASS-NR. / PASSPORT No. / PASSEPORT N°: T22001290 ANZAHL DER EINREISEN / NUMBER OF ENTRIES / NOMBRE D'ENTRÉES: MULT
AUSGESTELLT IN / ISSUED IN / DELIVRÉ À: MOSKAU 20-06-20
NAME, VORNAME / SURNAME, NAME / NOM, PRENOM: MUSTERMANN, OLGA
ANMERKUNGEN/REMARKS/REMARQUES: BESUCHS-/ GESCHÄFTSVISUM ERWERBSTÄTIGKEIT NICHT ERLAUBT

VCD<<MUSTERMANN<<OLGA<<<<<<<<<<<<<<<<
0000000000RUS7409185F2008099<M400630



Proof of Vaccination (EU)	Issued by UTO	Version 1

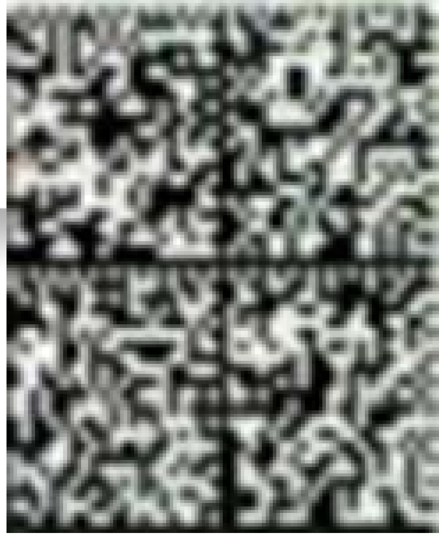
PERSONAL INFORMATION

Person Name:	Person Date of Birth:	Passport:	ID Card:
Gary West	1985-03-02	P9876543E	U1234567A

VACCINATION/PROPHYLAXIS INFORMATION

Disease or Agent Targeted:	Vaccine or Prophylaxis:	Vaccine Medicinal Product:	Marketing Authorization holder:
COVID-19	COVID-19 mRNA vaccine	Comirnaty	Pfizer BioNTech
Number in a Series of Vaccinations/Doses:	Batch/Lot Number:	Date of Vaccination:	Administering Centre:
1/2	VC35679	2021-02-01	RIVM

VDS Concept



- VDS cryptographically secures non-electronic documents, often issued decentrally.
- Extend 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 2D barcodes to be easily read and validated in a similar way as eMRTDs.

Electronic MRTD Trust Framework

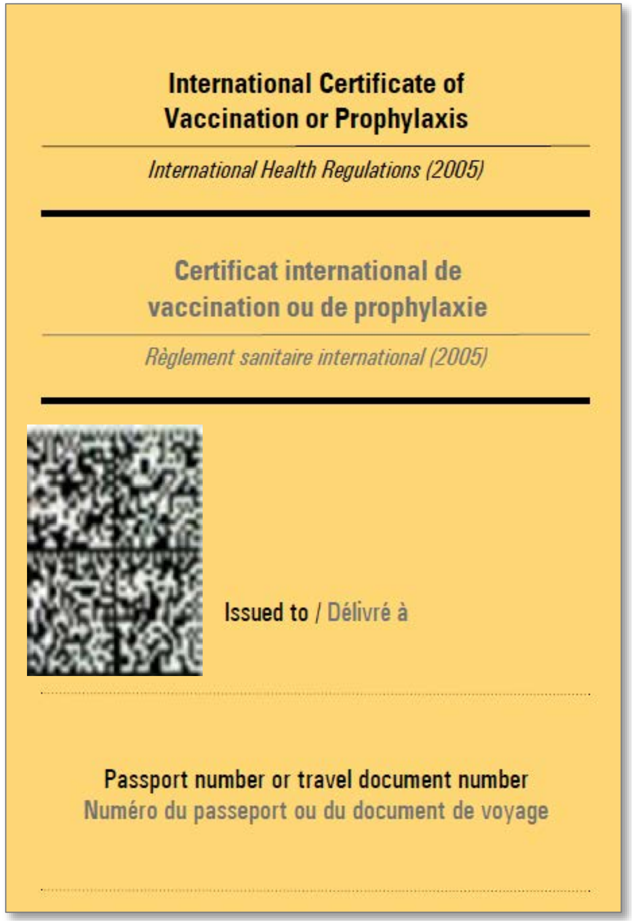
- eMRTD model is a distributed Public Key Infrastructure (PKI).
- Each Issuing Authority is an independent root of trust.
- State managed (Sovereign) trust framework – no single root.
- Because the Document Signer Certificate (DSC) is on the chip, the eMRTD can be validated offline.
- Supported by the exchange of root certificates (country-signing certificates).
- ICAO Public Key Directory (PKD) – multilateral distribution mechanism.

VDS Health Proof Concept

- Apply the VDS for non-constrained environments (VDS-NC) specification to health proofs.
- The VDS-NC contains the data of the document and its digital signature, similar to the eMRTD.
- Authenticity can be cryptographically secured.
- The VDS document can be linked to the MRTD to facilitate and secure international travel.

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**.



International Certificate of Vaccination or Prophylaxis

International Health Regulations (2005)

Certificat international de vaccination ou de prophylaxie

Règlement sanitaire international (2005)

Issued to / Délivré à

Passport number or travel document number
Numéro du passeport ou du document de voyage

Business processes and needs

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

VISIBLE DIGITAL SEAL

- 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

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

VISIBLE DIGITAL SEAL

- 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