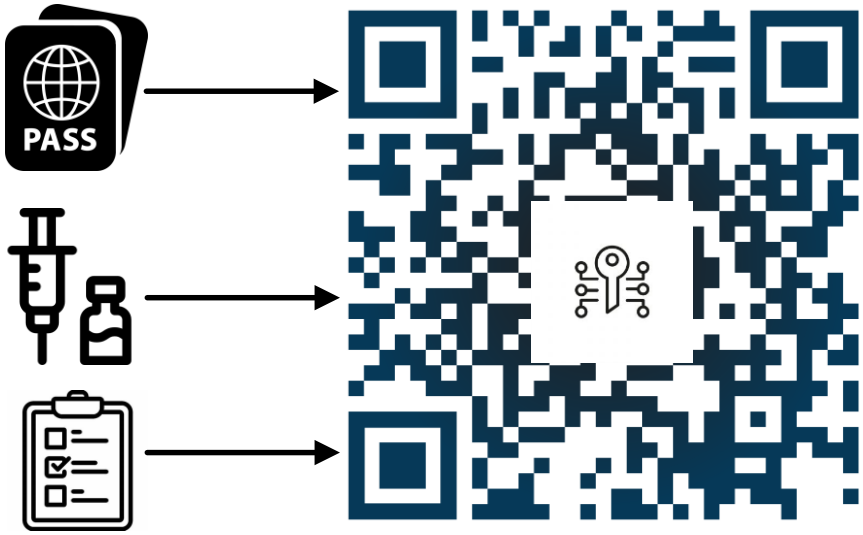
International Civil Aviation Organization

Technical Advisory Group (TAG) on the Traveler Identification Group (TRIP)

GUIDELINES

Visible Digital Seals ("VDS-NC") for Travel-Related Public Health Proofs

***SUMMARY**: A key challenge presented by COVID-19 is the need for global consensus on new approaches for issuance, exchange and verification of various public health status records in some instances required to support cross-border mobility of people in a facilitative way, while still ensuring appropriate risk assessment related to public health. On the basis of the field-proven VDS-technology ICAO presents a solution which combines practicability, security and ease of verification re-using the existing e-passport trust model to address this challenge.*



1.0 BACKGROUND

The COVID-19 global pandemic has resulted in renewed emphasis on assessing an individual's risk to public health as a key component in determining the ability to move freely.

While mobility overall has been affected, perhaps one of the hardest-hit sectors is cross-border air travel. The ability to restart this sector is highly dependent on establishing a baseline of predictability in terms of public health requirements for entry, as well as establishing the means for travelers to provide information relevant to their level of public health risk in order to gain entry. This is a challenge that must be met by both industry and governments, both as it relates to immediate biosecurity measures (ensuring flights are safe, from a public health perspective) and admissibility (limiting public health risks at the point of entry).

ICAO member states fully recognize the immense economic impact of the pandemic on the cross-border aviation sector, and the sector's dire need for immediate solutions to address the specific challenges related to potential future use of public health "proofs" in the cross-border inspection context. Industry and international associations like the International Air Transport Association (IATA) and the World Economic Forum (WEF), as well as other influential industry players, are proposing technical solutions aimed at meeting this challenge. These organizations are also seeking consideration for use of COVID-19 related public health credentials as a use case for the W3C's *verifiable credentials* standard[1], which is not yet used in the global travel document continuum. ICAO has considered these approaches and, along with the CART and its experts, assessed their viability alongside other possible solution frameworks, to arrive at recommendations made later in this document.

As the science around assessing COVID-19 risk levels has become more precise and as more risk mitigation measures become available – including most importantly the roll out of vaccines deemed safe by public health agencies - governments are now collaborating on the challenge of establishing acceptable baselines for assessing public health risks in a variety of situations. Global standards-setting bodies, including the World Health Organization (WHO) and the International Civil Aviation Organization (ICAO) will be key contributors to these efforts, aimed at establishing global baselines for common approaches.

[1] W3C, the "Worldwide Web Consortium", is an international community where Member organizations, a full-time staff, and the public work together to develop web standards. *Verifiable credentials* are tamper-evident credentials which have authorship that can be cryptographically verified – SEE http://www.w3.org, and http://w3.org/vc-data-model/

ICAO's Coordinated Approach

The facilitative efforts of the ICAO, via its *Council on Aviation Recovery Task Force* ("CART"), have been underway since Spring of 2020, with the aim of establishing guidance to restart the cross-border aviation sector. The *CART* has released two rounds of guidance thus far – the first round of guidance reflected the very early days of the pandemic, focusing predominantly on hard public health measures for aviation, like masking and sanitation. The most recent round of guidance, released in November 2020, provided early guidance for states on the implementation of *testing regimes* as part of broader border and health risk mitigation strategies[2].

ICAO – Test Certificates

The ICAO *CART* exercise has now entered its third phase. One of the areas of focus for this phase is developing a global framework for the validation of testing records and or certificates. This involves 1) identifying the standard elements needed on the certificate 2) establishing baseline data components for verification, and 3) the technical means of conveying this data, i.e., the "token", and the system to support its verification. While this work is expected to be completed by the end of February 2021, the working group suggests that the framework specified may be valuable in the future as a possible starting point for elaboration of specifications for health related proofs that might be provided for under the relevant Annexes to the Convention on International Civil Aviation and/or the International Health Regulations.

The WHO Smart Vaccination Certificate Initiative

The WHO is also leading an initiative seeking global consensus on proofs related to *vaccinations*, having struck a team of global experts to advance its *Smart Vaccination Certificate* initiative. The WHO has stated its intention to enhance security of paper-based certificates and develop a digital token, to enable improved safeguards against fraud compared to simple, paper-based health tokens (i.e. yellow book[3]). To advance the *Smart Vaccination* initiative, the WHO, will establish core data requirements based on health care requirements first, and then develop requirements for a secure, trusted, and globally-interoperable token. ICAO travel document specification experts are actively contributing to this exercise, where work is expected to be completed by the end of March 2021.

[2] ICAO Doc 10152 – "*Manual on Testing and Cross-Border Risk Management Measures"*

[3] Officially known as *International Certificate of Vaccination or Prophylaxis (ICVP)*

2.0 A VERIFIABLE PUBLIC HEALTH PROOF - GUIDING PRINCIPLES

Across the various fora of discussions, there are some common guiding principles emerging around a public health-related token intended for globally-interoperable use:

Fraud Resistant	• Impossible to produce without appropriate authority • Non-transferable between bearers • Ability to authenticate proof to establish trust in the document
Convenient	• Easy to issue • Simple to present – paper-based and/or digital • Quick verification for both users and verifiers (i.e., borders and air sector)
Implementable	• Quick to stand-up • Usage of existing infrastructure, verifiable in offline environments • Cost feasibility for all stakeholders
Flexible	• Should be usable in most environments • Options for limited infrastructure (e.g., wifi, kiosks, etc.)
Private	• Should respect privacy of users • Avoid central data repositories (as they will be difficult cross border between countries) • Protect sensitive personal data
Consensus-Based	• Should be internationally-accepted (i.e., examined in detail by experts worldwide) • Interoperable with key stakeholders and their systems
Open Source	• No inappropriate advantage is given to any supplier(s). • Countries can easily build-into the system

3.0 EXISTING GLOBAL TRUST MODEL FOR TRAVEL DOCUMENTS

ICAO, currently composed of representation from 193 states and key stakeholder international organizations (including, for example, the OECD, UNHCR, IOM etc.), facilitates collaborative efforts to establish baseline standards in many areas related to civil aviation. One of those areas is the establishment of *travel document specifications* aimed at enabling both safe and facilitative cross border travel. Here, ICAO, in close cooperation with member states and stakeholder international organizations, has a long and respected history of building member state consensus around interoperable solutions.

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. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all eMRTDs.***

Over the past two decades, ICAO's travel document specification work has focused on leveraging advances in technology to strengthen a travel document's *verifiability*, through implementation of improved physical and digital security features, while still being backwards-compatible. The outcome of this work is that the cross-border travel continuum already has a trust model established for travel documents, reliable issuance processes, and an established means of document verification.

This trust/verification model has been built around ICAO specifications for *electronic passports* ("ePassports"). In the early 2000s, to combat fraud attacks on traditional paper-based passports like photo substitution and alterations to the data page, ICAO's travel document experts began to discuss ways of leveraging technology to improve the passport's overall verifiability. The outcome of these discussions was based on what is now known as the TRIP strategy specifications for a passport including an integrated-circuit chip which, as well as storing the information on the passport's data page digitally, also has digital security features enabling vastly improved document verifiability. With ePassports, for the first time, verifiers, with the appropriate tools, had the ability to establish trust in a travel document using fully *automated means*, freeing up valuable inspection resources to focus on potentially higher-risk individuals.

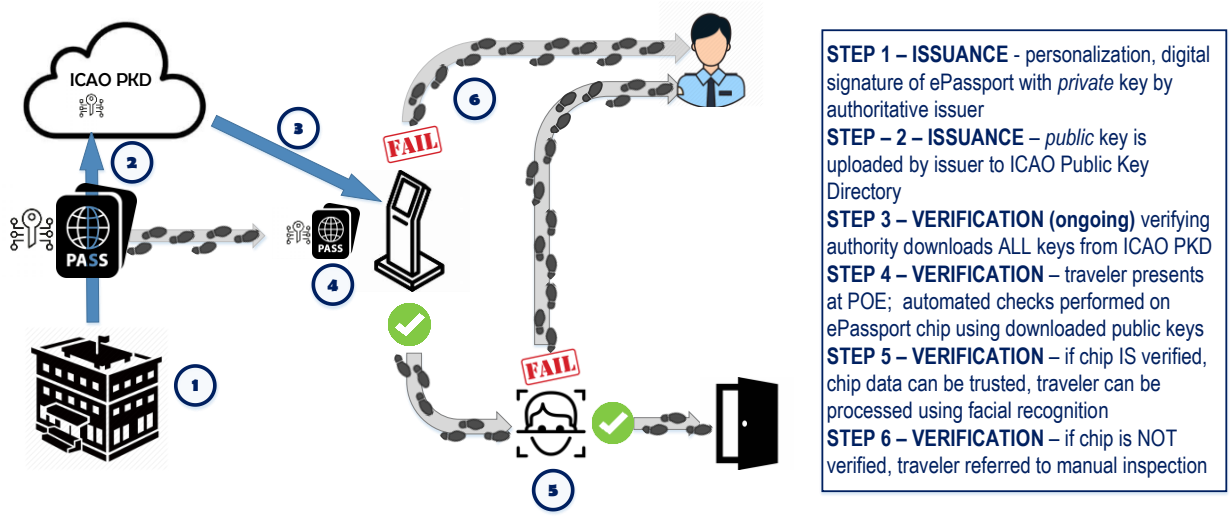
ePassports and Digital Signatures

An ePassport's verifiability relies on authoritative issuers "digitally signing" the data on ePassport chips they issue at point of issuance (resulting in an ICAO-compliant ePassport), and, on the verification side, verifiers making use of something called a public key infrastructure ("PKI") to check that digital signature, thus establishing trust in issuance (authenticity and integrity) of the document. In order to facilitate this verification by verifying entities, ICAO members agreed to establish a central repository of the information required to verify ePassports (NOTE - information in the repository is NOT considered personal information), called the *Public Key Directory* (the "PKD"). ICAO's PKD is complemented by national masterlists and national directories of the public key data necessary for verification of the ePassport, exchanged and shared. Given the proliferation of ePassports globally, the majority

of States have invested in the sharing and acquisition of these certificates in order to verify the documents of those entering their territories. Thus, the infrastructure for ICAO-compliant ePassport verification is highly developed as a result of years of development and refinement in the majority of states. In addition to the ICAO PKD, there also exist other technical possibilities to verify the authenticity and integrity of ePassport information based on the same trust network.

In terms of issuance, the ePassport has become a global norm. Approximately 145 countries now issue ePassports. In terms of verification, ICAO members are beginning to realize the transformative benefits of leveraging the digital security inspection features of ePassports at their borders, through increasing use of automated border control, and of the ICAO PKD. Increased circulation/leveraging of ePassports at borders represents a critical step towards seamless facilitation of low-risk travelers.

FIGURE 1 – ePassport Implementation – from *Issuance* to *Verification*



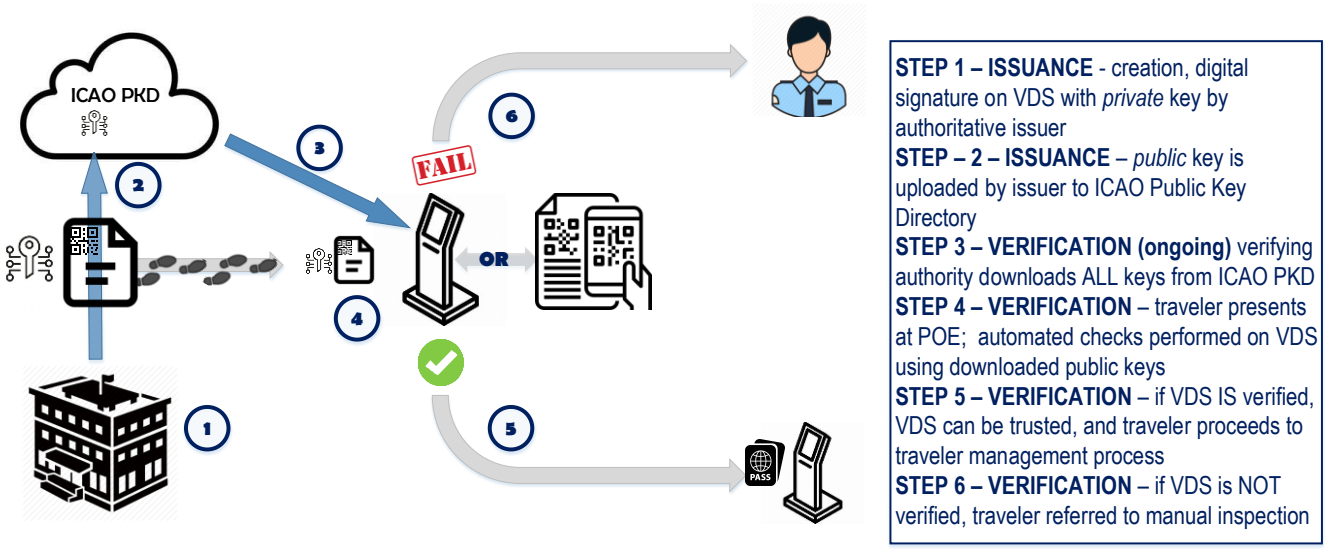
4.0 LEVERAGING THE EXISTING ePASSPORT TRUST MODEL – "VISIBLE DIGITAL SEALS"

In 2018, ICAO member states endorsed a technology involving a simpler implementation of the same trust/verification model established for ePassport, called a *visible digital seal* ("VDS"). The envisaged use of the VDS was to add a similar level of digital security to non-chipped documents, with original use cases developed for a visa counterfoil and emergency travel documents. The technology has, however, been applied in other real-world scenarios to preserve document security for decentrally-issued documents (***See ANNEX 1***).

The concept of a 2D bar code is already well-known and broadly used within and outside of the travel continuum. The form factor of these codes can be anything from paper hard copy to fully digital (displayed on a mobile device), and they provide a way to convey basic data in a quick, optically-readable way, enabling a basic level of automation. ICAO technical experts sought to advance a 2D bar code that is "verifiable", by applying the trust model/verifiability established for ePassport to enable trust in the data's issuance. So, just as with an ePassport, the VDS would enable a verifying entity to both read the basic data, and verify to establish trust in the authenticity and integrity of the data.

A key benefit of this technology is that it enables ePassport-issuing countries, as well as borders equipped to read ePassports, to potentially re-purpose existing infrastructure and technology to secure/verify other paper/hard copy documents in use in the travel continuum.

FIGURE 2 – Visible Digital Seals – From Issuance to Verification



5.0 VDS FOR PUBLIC HEALTH PROOFS

Now, in the context of COVID-19 and the resulting pressures on safe and healthy cross-border mobility, ICAO's travel document specialists recognize that existing VDS technology could be leveraged for the use case of public health-related proofs, to facilitate cross-border travel. Technical requirements are currently under development for the public health proof use case

for a special VDS-NC[4], which would satisfy most, if not all, of the guiding principles outlined in section 2.0.

ICAO's experts are focused on two related objectives for ALL COVID-19 related public health proofs:

1) Standardizing the information available to the verifying entity when reading a test certificate, thereby assuring that necessary information is consistently provided and facilitating easy and quick reading under transactional circumstance (e.g. boarding a flight), and
2) Building verifiability into the proof, to enable confirmation of trustworthiness and to safeguard against potential fraudulent use (verifiability for authenticity of issuance).

For more on what a VDS-NC in the context of public health proofs "IS" (and "ISN'T"), see *Annex 2*.

There is recognition among the experts that this pandemic has introduced new challenges into the existing cross-border travel system. Therefore, ICAO's aim is to offer a flexible set of guidance which serves not to replace, but to enhance, tools which may already be in use in the global travel document landscape, just as they have aimed to do previously with eMRTD specifications. This guidance may also evolve along with the challenges presented as the pandemic progresses and in particular as border begin to reopen, but will always have the benefit of being anchored in the existing trust/verification model for ePassports widely used by issuers/verifying entities.

Objective #1: Specifications to Assist in Manual (or Machine-Assisted) Inspection

With the ICAO CART Phase III Technical WG having already approved the core data components for a COVID-19 related token for *testing* in the context of cross-border travel, mapping these data elements to the VDS (2D bar code) format and encoding them at the point of issuance would immediately assist verifying entities, as they will be receiving the information in a predictable, easily-readable way, just as with a regular bar code. With VDS-NC, travelers could also gain the flexibility of many different form factors for presentation of their public health-related data - from simple hard copies to digitally, on their smart device.

Early versions of this implementation (for example, for *testing*) would see the VDS-NC embedded in a larger proof, which would also have primary presentations of the data (similar to the passport's visual inspection zone), enabling fully manual inspection if necessary. Digital

[4] "VDS-NC" – a VDS which can be applied in a "non-constrained" environment, ie, where there is control over the amount of space on which to embed the VDS.

signing of the VDS-NC to increase verifiability in order to guarantee integrity and authenticity of the data should be considered by an issuer, but, for this first iteration of the proof and acknowledging time and resource constraints, ICAO will only strongly recommend the digital signature of the data.

Objective #2: Specifications to Enable Verifiability

While the WHO does not recommend that states require health related-proofs for cross-border travel, it can be anticipated that states, in support of efforts to safely reopen borders, will layer some level of public health risk assessment, potentially including presentation public health-related proofs to border inspection. As the pandemic progresses, states may also begin to implement higher thresholds for trust for public health proofs. This is particularly true for vaccination proofs, as these will be more enduring in nature than a testing proof, with a traveller potentially using one proof for multiple journeys. So, while fraud obviously will exist (and already exists) with testing proofs, the risk can be contained to single journeys; whereas a fraudulent vaccination proof, if undetected, could persist in the system across multiple journeys. This consideration may lead to more interest for issuers to ensure verifiability of the token, therefore requiring a mandatory digital signature of the data. As in the case of ePassports, it still remains the responsibility of the receiving entity (State, Airline, etc.) to verify the digital signature.

Specifications for a digitally-signed VDS-NC for the public health would see the equivalent of the Document Signer Certificate (DSC – for ePassport) *embedded* into the 2D barcode. The benefit of this specification is to enable the verifier to conduct offline verification, regardless of the format the VDS-NC is presented in (i.e., paper or digital). In turn, the DSC is linked to the issuer's root of trust contained in the Country-Signing Public Key Certificate Authority (CSCA) Certificate[5]. The ICAO trust framework, however, requires only intermittent updating of the CSCA certificate. The CSCA certificate can be obtained from other States bilaterally or via the ICAO Master List, publicly available for download from the ICAO Public Key Directory (PKD).

[5] In the existing global trust/verification model for ePassport, a CSCA is considered the root trust anchor for verifying the data on an ePassport's chip. This CSCA normally is controlled by a State's travel document issuing authority ("TDIA").

Core Technical VDS-NC Issuance Requirements

For the VDS-NC proposal to proceed, it is critical that stakeholders reach consensus on the following technical points related to VDS-NC implementation:

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**. This could be finalized at the end of the discussion process. Easy readability is key.

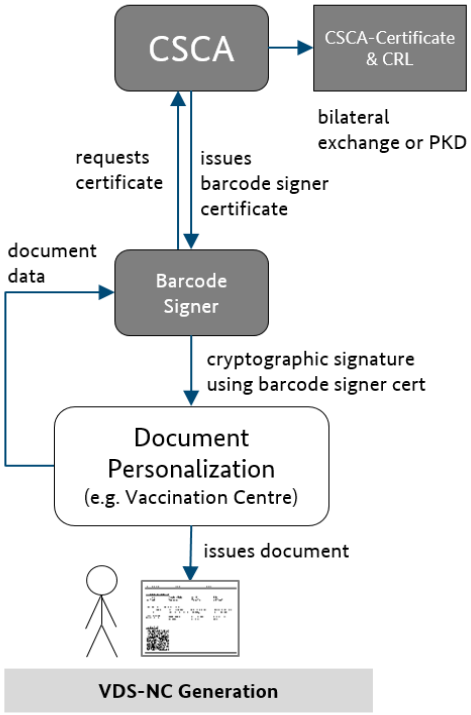
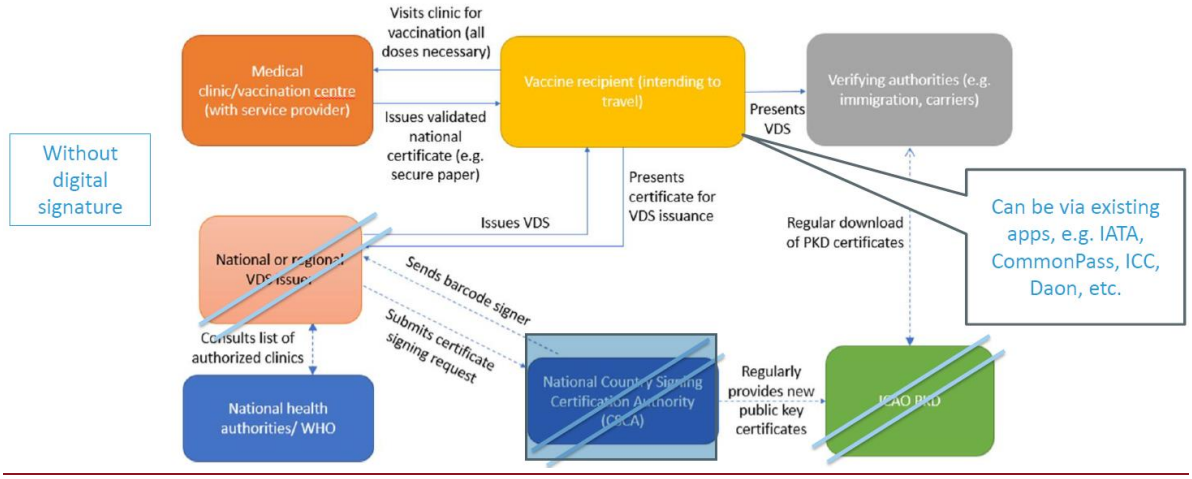


FIGURE 3: High-Level VDS-NC Flow

Issuance Models for Digitally-Signing VDS-NC

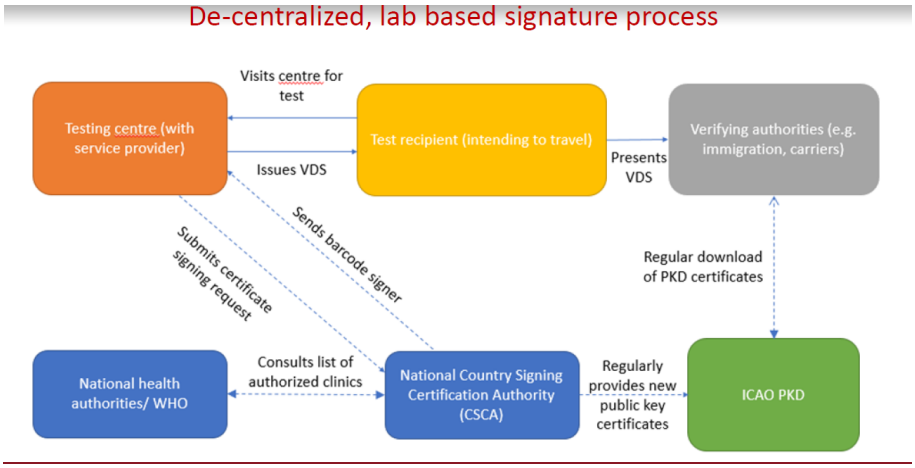
Given the work to build verifiability into a VDS-NC occurs on the issuance side, applying the ePassport issuance model to public health-related proofs could present unique challenges, depending on the State – for example, for proofs related to health, an issuing authority requires connections to health authority systems that may not exist now). Despite this, ICAO will strongly recommend that States anchor issuance of public health related proof for cross-border travel to the existing CSCA for ePassport, which typically is controlled by a State's travel document issuance authority (TDIA). ICAO envisions two different models for issuance of a VDS-NC which is anchored directly by the TDIA's trust anchor (CSCA).

FIGURE 4 – Centralized Signature Service (using ePassport CSCA)
****note** this image denotes a central issuance service WITH or WITHOUT a digital signature



DESCRIPTION – MODEL - Central Signing Service (using ePassport CSCA)
At the point of issuance (vaccination centre or testing facility) the personal data of the traveller are collected and combined with health status-related data elements (e.g. vaccination date and type) into the standardized data set of the public health proof. This data set is then sent to a central signing service which a) recognises the point of issuance as registered/authorized and b) creates the VDS-NC by signing the data using its barcode signing certificate. This could be the same barcode signing certificate for all incoming VDS-NC signing requests or individual barcode signing certificates per lab/institution. The VDS-NC is then returned to the point of issuance (e.g. as printable graphic or .pdf file) and the public health proof is issued to the traveller as a human and machine readable printout of the public health proof and/or by digital means.

FIGURE 5 – Decentralized, Lab-Based Solution



DESCRIPTION – MODEL - De-Centralized, Lab-Based Signature Process
This alternative model, while still anchored by a State's CSCA, would empower labs to directly issue VDS-NC at the time the transaction (for whichever service) is being performed. Therefore, in this model, the State is not involved in real-time generation of the VDS-NC, but establishes regular pushes of the "document signers" to trusted labs, which are anchored in the State's CSCA (trust anchor for ePassport). In using these pushed document signers, the lab is able to establish a verifiable chain of issuance health the State. This model might serve to reduce wait times for return of the VDS-NC to the client/traveller, and does not require a constant on-line connection to a central signing service.

Alternative Issuance Models

ICAO will recommend using the CSCA from the ePassport, given this offers the immediate benefit of making the verification process simpler for border systems globally, many of which already use the CSCA as a trust anchor for ePassport verification. However, it is recognized that some States may find domestic governance with regard to using the TDIA's CSCA to sign a public health-related proof challenging. In these instances, States may need to explore other domestic implementations which still model the issuance of public health proofs for cross-border travel on ePassport, but which potentially use a trust anchor *other* than the CSCA. ***Please refer to Annexes 3 and 4 for suggested Trust Anchor Models – Issuance, Verification.***

Fortunately, a VDS-NC based approach is inherently flexible to implement, offering many different implementation choices for States, depending on their unique domestic circumstances.

For more general guidance for states re Implementation of VDS-NC Based Health Proofs VDS Implementation, see *Annex 5*.

VDS-NC Specifications Check Against "Guiding Principles"

A check of a potential VDS-NC based solution against the guiding principles for a public health proof, outlined in paragraph 2, finds good alignment:

Fraud Resistant	✓	• VDS would be populated with key data points and *can* be digitally signed • Verification of the digital signature would allow verifier to confirm data is genuine and has not been tampered with
Convenient	✓	• VDS could be issued in many form factors, everything from a simple hard-copy print out to a PDF which could be displayed from a mobile device. • All would be read/verified in the same way: read the primary data; and check the signature to establish trust in its issuance.
Implementable	✓	• Issuance/verification infrastructures already exists among ePassport-issuing countries. • Verification of a VDS could be supported by a global public key infrastructure • Building on existing systems would expedite viability of implementation
Flexible	✓	• VDS for public health purposes is being developed to be independently-verifiable, even in offline environments. • Options being developed to eliminate (or minimize) the need for a international distribution mechanism
Private	◐	• Data in the VDS will be streamlined, but will meet the data needs for cross-border travel; selective data disclosure is not an option • Limited personally-identifiable data, most importantly by linking the proof to an existing ID or travel document.
Consensus-Based	✓	• VDS specifications have already been endorsed by ICAO members, and build on the existing trust/verification model established for ePassport • Much work between border and passport issuers to satisfy requirements
Open Source	✓	• Specifications for VDS are publicly-available in ICAO's Doc 9303, and are open for any vendor or State to leverage

6.0 CONCLUSIONS AND RECOMMENDATIONS

The COVID-19 is an unprecedented crisis and innovative solutions are needed to deal with some prominent challenges to facilitate the verification of public health proofs by airlines and border authorities. Ideally, such solutions would also be sustainable going forward.

Technology based on ICAO (globally implemented) specifications such as the VDS-NC, applied to public health proofs, offers the potential to overcome existing obstacles to cross-border travel by air, while meeting most if not all of the guiding principles identified.

Stakeholders from international organizations, as well as the public and private sectors, need to work together to develop the capacities and protections necessary to ensure that the benefits of public health proofs are realized and be part of an integral and reliable immigration process. The ICAO VDS-NC should be an important foundation of success in this work.

Recommendations:

- While early focus will be placed on *testing*, States are already administering *vaccines*, with the expectation that these will soon be more widely available. Now is the time for Member States to consider the appropriate policies and processes for issuance of secure testing *and* vaccination certificates which will be accepted as widely as necessary. In this regard, states should be regularly monitoring guidance from the WHO with regard proof of COVID-19 vaccination for international travelers[6], which outlines ongoing consideration of COVID-19 vaccinations and applicable existing international law, including the *International Health Regulations*[7].

- Proactive adaptation of existing technology developed using open sources and standards – particularly the ICAO VDS-NC – is advised, as this builds on the existing global trust model for travel document verification and offers potential for interoperability and universal access, thereby also making health risk more manageable.

- ICAO, with its partner international organizations and State representatives/experts from all necessary domains, should quickly agree on the key technical and governance considerations necessary for a robust, privacy-protecting credentialing system.

- The WHO should work with ICAO's technical experts and other stakeholders as necessary to agree on the data set to be encoded in a VDS-NC barcode.

- Existing solution providers should work with policymakers and the technology community to align on standards so as to ensure that solutions meet global goals.

- Member States, and their regulatory agencies, should now develop legislation and/or adequate regulation as necessary to ensure proper governance of testing and vaccination certificate systems.

[6] WHO Interim Position Paper - https://www.who.int/groups/smart-vaccination-certificate-working-group)
[7] WHO *International Health Regulations* (2005) - https://www.who.int/health-topics/international-health-regulations#tab=tab_1

ANNEX 1: Real World Use Cases for the Visible Digital Seal (VDS) in Travel Continuum

Use Case 1: **Refugee Registration Document (Germany, 2016)**

In 2015, due to refugee crisis in Europe, Germany decided to issue a harmonized document as proof of a successful registration to all asylum seekers arriving in Germany. It carries classic security features and a VDS containing all the printed personal data as well as a link to a database containing biometrics. The project involved the rollout of 1,500 decentral mobile enrollment stations for alphanumeric and biometric data as well as a central signing service and was accomplished in less than 9 months. Data was sent to the central signing service, which returned the signed VDS to be printed on the document. After enrollment, the document could be authenticated by a mobile phone app, as well as by stationary border control equipment.

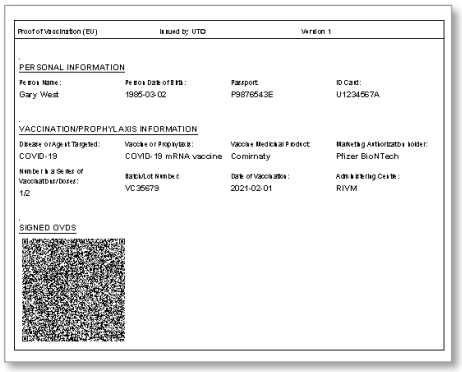
Use Case 2: **EU Schengen Visa (2022)**

In 2015, the new Schengen visa counterfoil format was introduced. In the years following, after observing counterfeiting of the new format which was of increasingly good quality, the EU Commission and the Member States decided to update the sticker with the Visible Digital Seal (VDS) to protect the issuance of the document, prevent the use of stolen blanks and add a layer of cryptographic security to a physical document. The VDS can be authenticated online and offline using the existing ICAO PKI infrastructure in use for ePassports. All EU Member States will issue visas containing the VDS by May 2022.

ANNEX 2: What is a Visible Digital Seal (VDS) in the Public Health Context (and what it is NOT)?

What it IS:

1. The VDS-NC is designed as a **specific token for cross-border travel**, as an interoperable proof of health events (soon test, later 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.


Proof of Vaccination (EU) Issued by: UTO Version: 1

PERSONAL INFORMATION

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

VACCINATION/PROPHYLAXIS INFORMATION

Disease or Agent Targeted: COVID-19 | Vaccine or Prophylaxis: COVID-19 mRNA vaccine | Vaccine Medicinal Product: Comirnaty | Marketing Authorization Holder: Pfizer BioNTech

Number in a Series of Vaccinations/Doses: 1/2 | Batch/Lot Number: VC35679 | Date of Vaccination: 2021-02-01 | Administering Centre: RIVM

SIGNED OVDS

4. The VDS-NC shall be **easily readable by most barcode scanners** deployed in the travel/border environment.
5. The VDS-NC is **offline verifiable**, without the need for an online-connection.

What it is NOT:

1. The VDS-NC is **not the primary medical vaccination document**. This function stays within the health-related environment: vaccination certific ates 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)

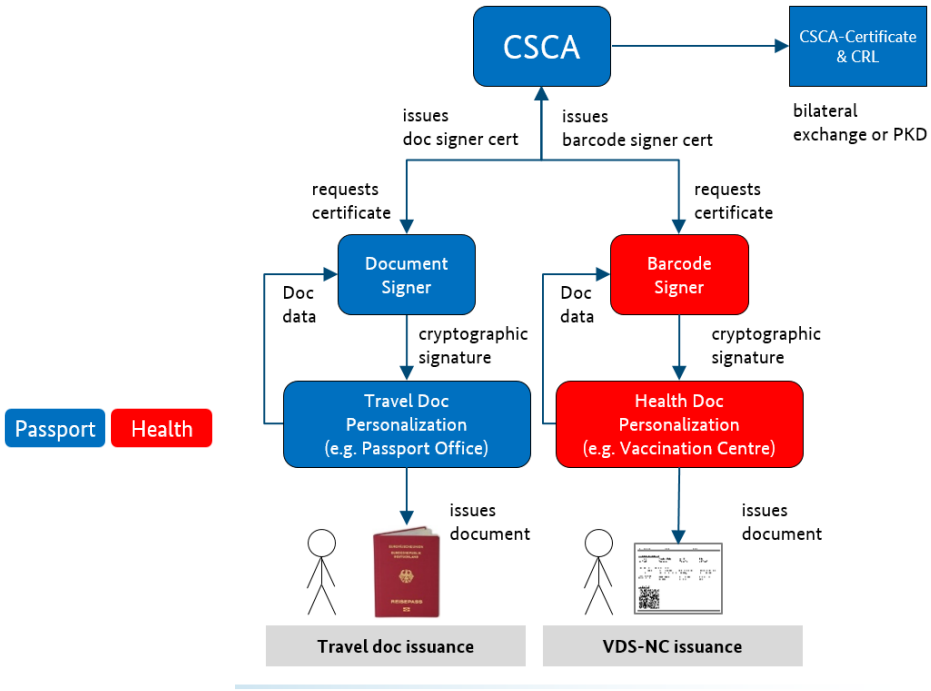
Issued to / Délivré à

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

ANNEX 3 – Issuance and PKI Models

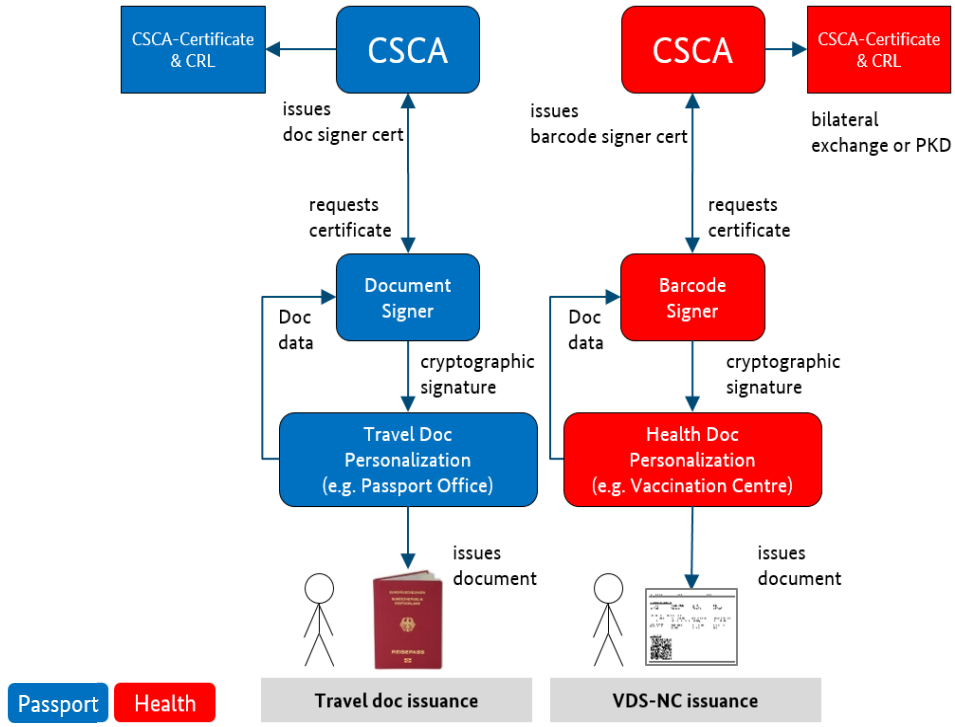
PKI model A: Single CSCA for both travel docs and health proofs

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



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

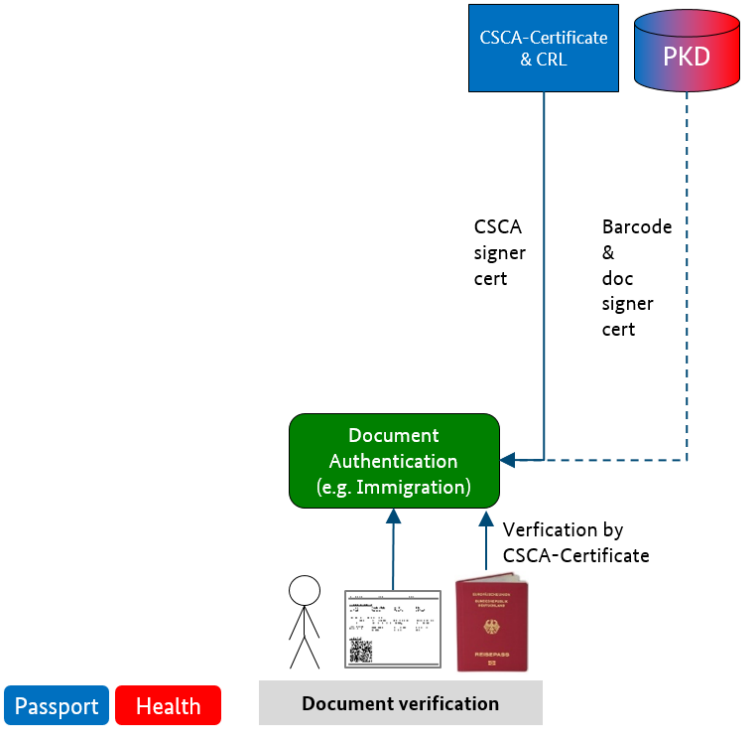
- There are specific CSCA's for issuing travel documents and for issuing health proofs.
- The document signers are specific for each travel documents and health proofs.
- The certificate profiles ensure that certificates can be used for the intended purpose only.



ANNEX 4 – Verification Models

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.



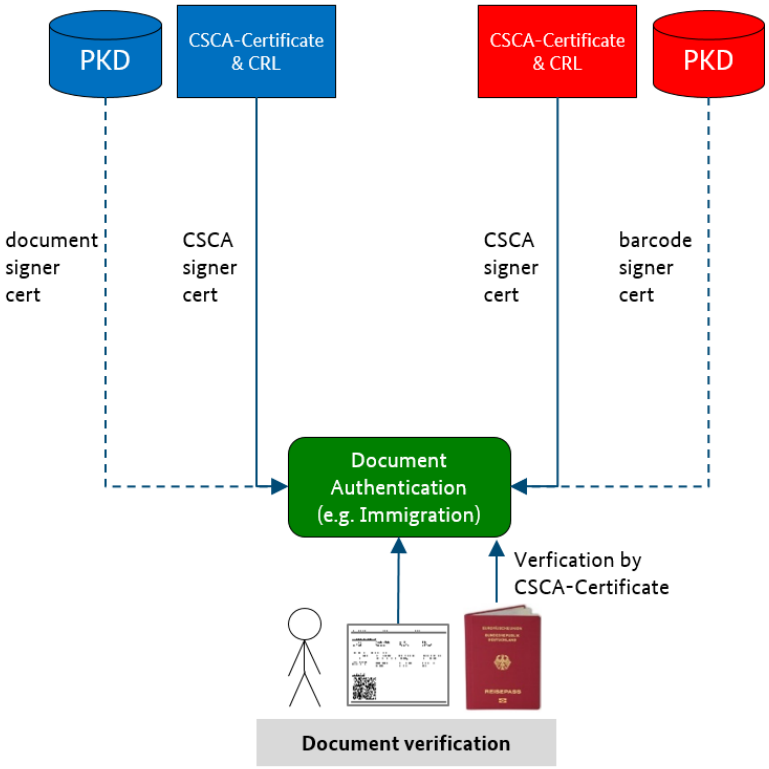
PKI model B: Specific CSCA's for each travel docs and health proofs

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.



ANNEX 5 – Guidance for States re Implementation of VDS-NC Based Health Proofs

A significant benefit of pursuing a VDS-based approach to provision of travel-related health proofs is the inherent flexibility afforded to implementers. Depending on one's existing infrastructure and capabilities, the processes that one has put in place and one's general preferences, different choices can be made that will reduce costs of implementation and operation while maximizing benefits.

This Annex is intended to provide initial guidance to States to support decision-making. Different options for implementation by the various parties involved in an end-to-end process are listed. Additionally, checklists are included that States choosing particular implementations should consider in their rollout efforts. By comparing their existing capabilities and infrastructure against the requirements included in these checklists, States can identify the options that should be easiest and least costly to pursue.

All choices made by stakeholders can be changed over time. Thus, the operational models that States choose might evolve. A State might decide to update its processes in order to issue digitally signed VDS-NC barcodes rather than unsigned barcodes once its capabilities aligned with those listed in the first column of Table A1 below, for example.

It is emphasized that States can implement different processes and make different decisions at different locations within their territory. This could be exemplified with the task of verification of VDS-NC based health proofs, for example, where airports with existing barcode readers integrated into their physical infrastructure might choose to make use of these devices whereas other (typically smaller) locations might simply deploy hand-held devices to appropriate staff for barcode reading and/or verification.

It is noted that the content presented is not exhaustive. Only the main dimensions of decision-making are presented. Furthermore, while a variety of implementation options are examined, States may identify additional possibilities that they deem more appropriate based on their own circumstances.

A) Guidance for issuance of VDS-NC based health proofs

Figures 3 and 4 in this paper highlight that different entities may manage the issuance of VDS-NC based health proofs in any region or state. Choices can also be made in terms of whether proofs including the VDS-NC barcode are issued on paper or in digital format, and whether the barcode is digitally signed (as strongly recommended above) or not. If the barcode is to be digitally signed, the State will have to define then the appropriate trust anchors within the public key infrastructure being used. These dimensions of optionality are highlighted in Figure A.1.

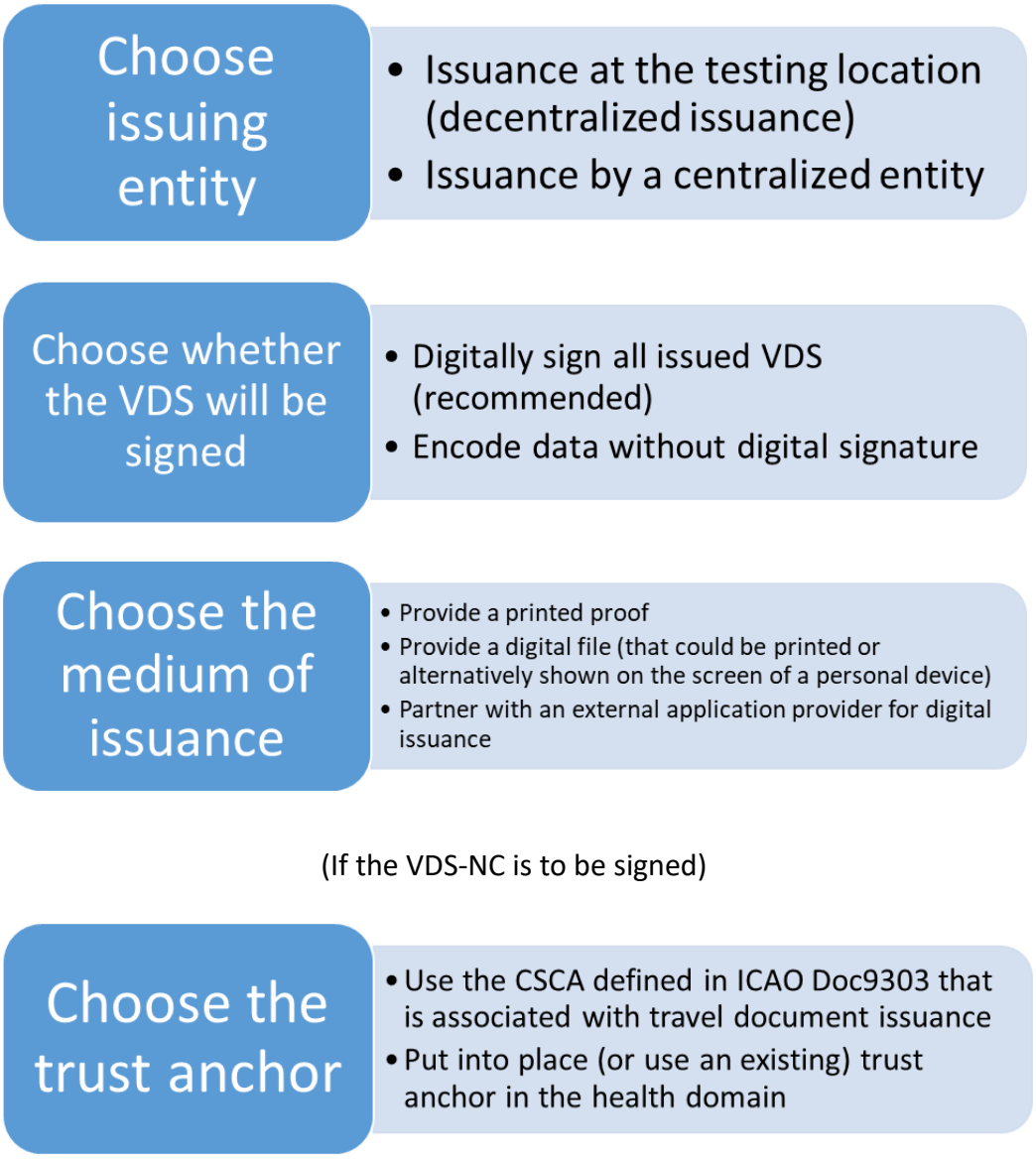


Figure A.1. The main choices that States should make regarding issuance of VDS-NC based travel proofs

The following checklists list the main steps that implementers will have to undertake for issuance according to the choices made. As there is extensive interdependencies between the choice of issuing entity and any decision to digitally sign the VDS-NC, these choices are considered in combination.

	Digitally sign the VDS-NC	Encode data without signature
Issuance at the testing location	*This setup requires appropriate security to protect private keys used for signature. It would normally not be a prudent approach unless testing is undertaken in larger, centralized locations.* 1. The health centre must have access to the necessary IT infrastructure, which will include a Hardware Security Module for secure private key storage and a standard computer terminal with the necessary software for preparing the VDS-NC barcode from data input in accordance with the Technical Report (all data required in the dataset). 2. The health centre must have appropriate physical security at the test site to protect this IT infrastructure. 3. Organizational arrangements must be in place so that the health centre can obtain barcode signers from the central trust authority (Figure A.3) for use.	1. The health centre must have access to the necessary IT infrastructure, which will include a standard computer terminal or other digital device with the necessary software for preparing the VDS-NC barcode from data input in accordance with the Technical Report (all data required in the dataset).
Issuance by a centralized entity	*At least two processes can be envisaged – A) issuance by the centralized entity based on electronic data exchanged with the health centre; or B) issuance based on a paper document provided by the health centre* A) 1. An electronic connection must exist between the health centre and the centralized issuing entity (e.g. a dedicated data transfer tool; secure email) that the health centre will use for trusted transfer of the necessary data for VDS-NC issuance. 2. Organizational arrangements must be in place so that the centralized issuer can obtain barcode signers from the central trust authority. The State must ensure that the issuer has appropriate IT capabilities and security measures in place (it would normally be the case	*At least two processes can be envisaged – A) issuance by the centralized entity based on electronic data exchanged with the health centre; or B) issuance based on a paper document provided by the health centre. It may be noted, nevertheless, that this latter two-step process might be considered excessively laborious for production of a document of limited security.* A) 1. An electronic connection must be in place between the health centre and centralized issuing entity (e.g. a dedicated data transfer tool; email) that the health centre will use for transfer of the necessary data for VDS-NC issuance.

	that an entity that already engages in secure electronic document issuance fulfil this role, implying the existence of necessary IT capabilities and knowledge and implementation of necessary security measures). 3. Processes must be defined for return of the signed barcode to the test subject (e.g. through an email provided by the test centre). B) 1. The centralized issuer must be familiar with the paper certificates issued by the health centres in its region. Ideally, the certificates will incorporate appropriate secure features to assure authenticity and prevent tampering. 2. Procedures must be in place that allow the intending traveler to present the paper certificate to the centralized issuer in person in order to obtain a VDS-NC. 3. Organizational arrangements must be in place so that the centralized issuer can obtain barcode signers from the central trust authority and ensure that the issuer has appropriate IT capabilities and security measures in place (it would normally be the case that an entity that already engages in secure electronic document issuance fulfil this role, implying the existence of necessary IT capabilities and knowledge and implementation of necessary security measures). 4. Processes must be defined for return of the signed barcode to the travelling subject (e.g. through an email provided by the traveler).	2. The process for return of the barcode to the subject will need to be defined (e.g. through an email provided by the test centre). B) 1. The centralized issuer must be familiar with the paper certificates issued by the health centres in its region. 2. Procedures must be in place that allow the intending traveler to present the paper certificate to the centralized issuer in person in order to obtain a VDS-NC (unsigned).

Table A1. Checklists for implementation with different issuing entities and with both digitally signed and unsigned VDS-NC barcodes

Provide a printed proof	1. The entity in contact with the intending traveler (this will be the health centre in all cases except that of issuance by a central entity based on a paper document provided by the health centre) must have a locally available printer of sufficient quality. Suggested specifications are provided in section 2.1 of Part 13 of ICAO Doc9303.
Provide a digital file	Two possibilities are foreseen: a. The email address of the intending traveler is included in the dataset provided. The procedures must be defined to ensure sending of the file by either the centralized entity or the health centre. This option is feasible irrespective of the issuer. OR b. The centralized entity has an established online portal for receipt of requests for VDS-NC. The intending traveler receives the digital file through this portal following request submission, based on data shared by the health centre with the centralized entity. This option is only envisaged in the case of centralized issuance. ***ICAO recommends consideration to provide both of the above formats, digital and printout.
Partner with an external app provider	1. A secure electronic connection is in place for the submission of data from the health centre to the app provider. 2. The health centre enrolls all data foreseen in the established dataset and submits it to the app provider. 3. The app has the necessary capabilities to encode the data in a VDS-NC and make the barcode associated with the intending traveler available to him/her within app.

	(If the VDS-NC is to be digitally signed) 4. The app developer has the appropriate agreements in place with State authorities in order to obtain the necessary barcode signer private key.

Table A2. Checklists for implementation with different media for issuance

Use the travel document CSCA	1. Necessary agreements and arrangements are in place between the Central Signing Certificate Authority associated with the State's travel documents and the entity (-ies) issuing the VDS-NC barcodes for the signing of Certificate Signing Requests submitted by the issuing entity (-ies) using the CSCA private key. *Note. These agreements should include, inter alia, detail on the private key usage periods that will define the regularity of new barcode signer certificate issuance and the definition of communication focal points for regular liaison in case of need, e.g. should certificate revocation become necessary.*
Use a trust anchor established within the health domain in the State	1. Necessary agreements and arrangements are in place between the trust anchor authority and the entity (-ies) issuing the VDS-NC barcodes for the signing of Certificate Signing Requests submitted by the issuing entity (-ies) using the CSCA private key. *Note. These agreements should include, inter alia, detail on the private key usage periods that will define the regularity of new barcode signer certificate issuance and the definition of communication focal points for regular liaison in case of need, e.g. should certificate revocation become necessary.* 2. Arrangements are in place for the necessary sharing of the public keys associated with the PKI with all verifying entities. Appropriate distribution mechanisms, as per the Technical Report, include bilateral exchange and sharing through the ICAO Public Key Directory.

Table A3. Checklists for implementation with different trust anchors of the Public Key Infrastructure used

B) Guidance for *reading/verification* of VDS-NC based health proofs

A number of different parties will normally be involved in the reading and/or verification of VDS-NC based health proofs, both around the point of departure and arrival. At departure, carriers are frequently required to ascertain the health status of the intending traveller and his/her compliance with the rules for entry into the State of destination. The authorities of the State of destination, meanwhile, will normally want to confirm such compliance. Authorities might include those involved in immigration, customs and public health monitoring. Reading of the VDS-NC barcode should provide the necessary data in all cases, with verification confirming the veracity and integrity of that data.

These parties will need to make choices as to the equipment that they use for reading. State authorities will normally wish to verify the data to the greatest extent feasible. Private sector entities may choose to do so, particularly if required by the relevant legal or administrative frameworks in place. Figure A2 depicts these two main dimensions of choice on the reading/verification side.

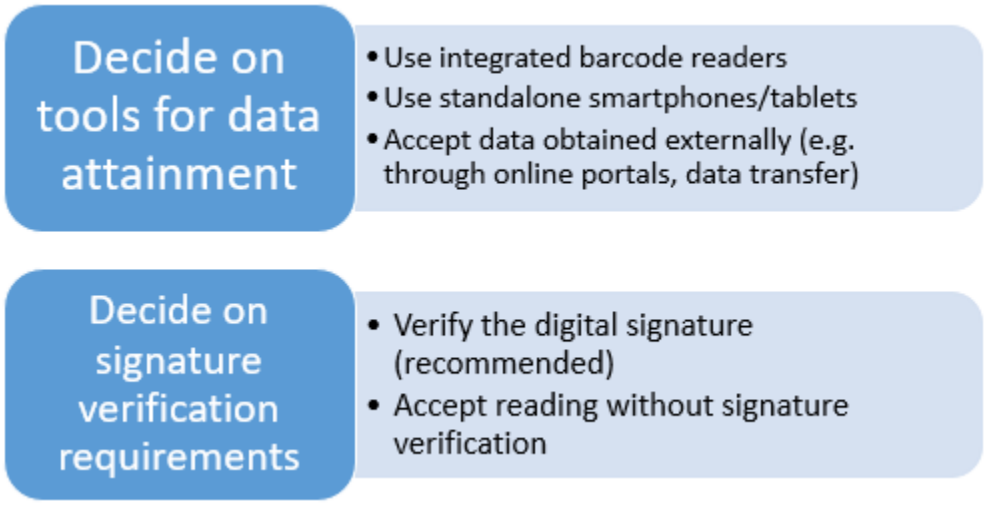


Figure A2. The main choices that verifying entities will have to make

The following checklists list the main steps that implementers will have to undertake for reading and verification according to the choices made.

Use integrated barcode readers	1. Visible light barcode readers are in place at the points of check, e.g. in boarding gates, e-gates, kiosks etc. 2. The barcode readers are connected to IT equipment necessary to decode the data presented in the format defined in the accompanying Technical Reports.
Use standalone devices	1. All appropriate parties have easy access to standalone smartphone or tablet devices with an integrated camera and an appropriate reading and barcode decoding app installed. *Note. Suitable apps are available for public download from app libraries.*
Accept data obtained externally	1. Secure portals are established for the purpose of enrolling health-related data in the context of travel. *Note. A typical case might involve a State establishing an online portal for use by those travelling to that State. The traveler will provide all necessary data in advance of their travel. Provision might include the intending traveler scanning the VDS-NC barcode using his/her device in order to provide the necessary data in a secure, efficient and error-reducing manner.* 2. All parties have access to the relevant data obtained from these portals in order to execute the health-related tasks requested of them.

Table A4. Checklists for different data attainment possibilities based on VDS-NC based health proofs

Verify the digital signature	1. The IT system connected to the data attainment device (Table A4) has access to the appropriate barcode signer public key (obtained from a different source than the key stored in the barcode itself),

	CSCA public key and/or other trust anchor public key. 2. The system can accomplish digital signature verification based on the protocols defined in the accompanying Technical Reports.
Accept reading without signature verification	*No additional steps required beyond those in Table A4.*

Table A5. Checklist for digital signature verification of VDS-NC based health proofs