

For Publication on the ICAO Website



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

DISCLAIMER: All reasonable precautions have been taken by the International Civil Aviation Organization to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall the International Civil Aviation Organization be liable for damages arising from its use. This publication contains the collective views of an international group of experts and does not necessarily represent the decision or the policies of the International Civil Aviation Organization.

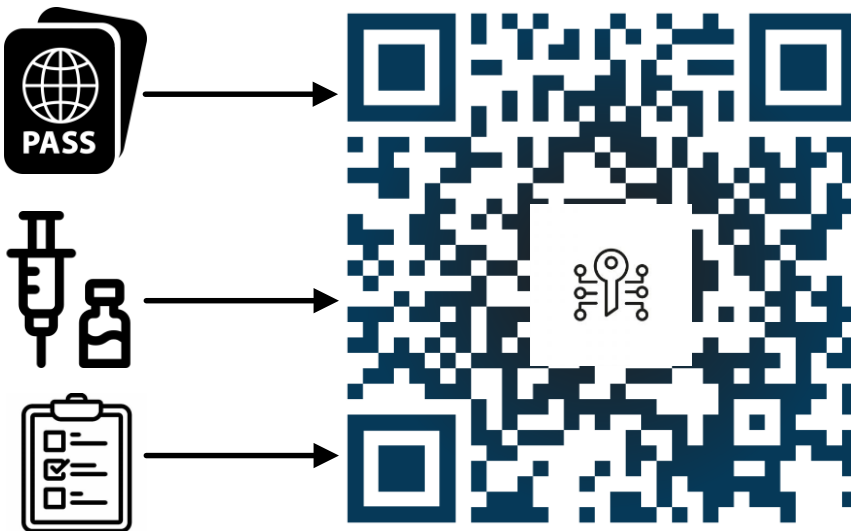
Version: Release 1.0

September 2021

File: Guidance for Visible Digital Seals (VDS-NC) for Travel-Related Public Health Proofs
Author: ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP)

SUMMARY

A key challenge presented by COVID-19 is the need for global interoperability for issuance, exchange and verification of various public health proofs required in some instances for international travel. These travel-related health proofs need to support mobility of people in a facilitative way, while still ensuring appropriate risk assessment related to public health. On the basis of the field-proven visible digital seals (VDS) technology, the International Civil Aviation Organization (ICAO) presents a solution which combines practicability, security and ease of verification re-using the existing ePassport 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 travel.

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 predictability in terms of public health requirements for entry as well as establishing the means for travellers to provide information to States and aircraft operators 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 ensuring flight safety, by reducing the amount of potentially infectious passengers, and border security, by ensuring that public health admissibility requirements are met.

ICAO Member States fully recognize the immense economic impact of the pandemic on international aviation, and the sector's dire need for immediate solutions to support the risk-based application 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 World Wide Web Consortium's (W3C) *verifiable credentials* standard¹, which is not yet used in the global border management and travel document continuum. ICAO has considered these approaches and, along with the ICAO Council Aviation Recovery Taskforce (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 – States 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 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 work of the ICAO CART has been underway since Spring of 2020 and has delivered guidance to restart aviation. To date, the CART has released three rounds of guidance. 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 second 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

ICAO CART Phase III discussed developing a global framework for the validation of testing records and/or certificates. This involved:

- 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, with a view to creating a framework that 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*.

ICAO CART Phase III included a recommendation related to the health proofs potentially used to indicate health risks:

Member States should implement testing certificates based on the protocol, minimum dataset and implementation approaches outlined in the Manual on Testing and Cross-Border Risk Management Measures (Doc 10152) to facilitate air travel. States are encouraged to request evidence of testing that is secure, trustworthy, verifiable, convenient to use, compliant with data protection legislation and internationally/globally interoperable. Existing solutions should be considered and could incorporate a visible digital seal. This may be applicable to vaccination certificates.

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* (SVC) 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 book³). To advance the SVC 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's travel document specification experts are actively contributing to this exercise, where WHO specifications are expected to be completed by the end of June 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. These include:

 Fraud Resistant	<ul style="list-style-type: none"> • Impossible to produce without appropriate authority • Non-transferable between bearers • Ability to authenticate proof to establish trust in the document
 Convenient	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Quick to stand-up • Usage of existing infrastructure, verifiable in offline environments • Cost feasibility for all stakeholders
 Flexible	<ul style="list-style-type: none"> • Should be usable in most environments • Options for limited infrastructure (e.g., wifi, kiosks, etc.)
 Private	<ul style="list-style-type: none"> • Should respect privacy of users • Avoid central data repositories (as they will be difficult cross border between countries) • Protect sensitive personal data
 Consensus-Based	<ul style="list-style-type: none"> • Should be internationally-accepted (i.e., examined in detail by experts worldwide) • Interoperable with key stakeholders and their systems
 Open Source	<ul style="list-style-type: none"> • 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 is currently composed of representation from 193 Member States which facilitates collaborative efforts to establish baseline standards in many areas related to civil aviation. This is complimented by key stakeholder international organizations including, for example, the Organisation for Economic Co-operation and Development (OECD), the United Nations High Commissioner for Refugees (UNHCR), and the International Organization for Migration (IOM), etc. One of the areas where ICAO is active 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 States 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 electronic Machine Readable Travel Documents (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 electronic 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 eMRTDs, in particular the specifications for electronic machine readable 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 were based on what is now known as the Traveller Identification Programme (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

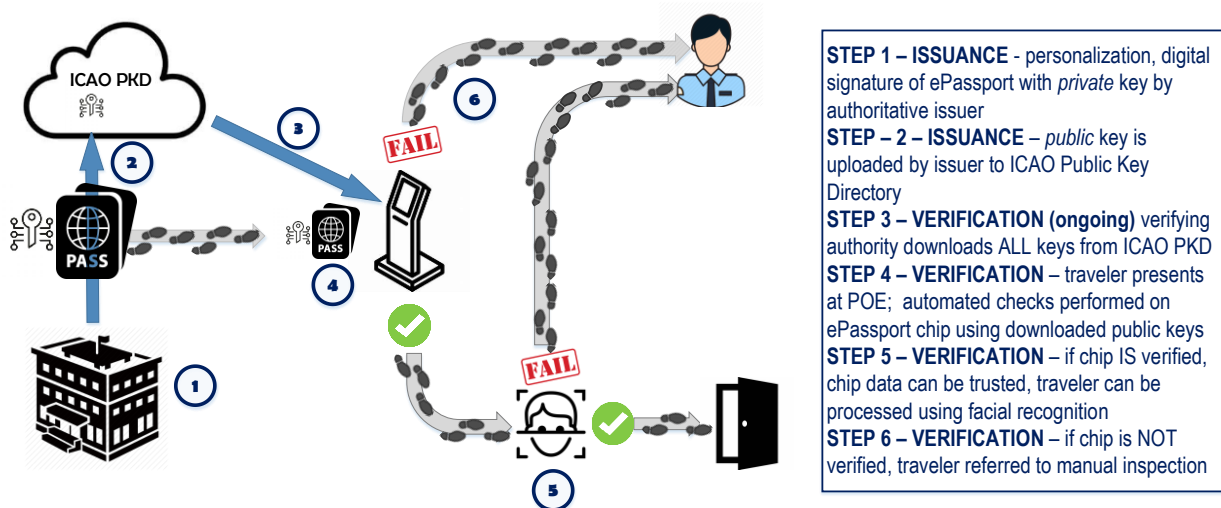
An ePassport's verifiability relies on authoritative issuers (Issuing States) "digitally signing" the data on the ePassport chips at the point of issuance (resulting in an ICAO-compliant ePassport), and, on the verification side, verifiers (receiving State as well as other entities) making use of something 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 Member States 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 ICAO Public Key Directory (PKD). ICAO's PKD is complemented by national master lists and national directories of the public key data necessary for verification of the ePassport, exchanged and shared, meaning that States need only to download one file. 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 terms of issuance, the ePassport has become a global norm. Approximately 145 countries now issue ePassports. In terms of verification, ICAO Members States are leveraging the security benefits of inspecting electronic security 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 travellers.

As borders reopen, States are already requiring proofs of vaccination or test from international passengers. The use of a third health proof, a certificate of recovery from COVID-19 is also being discussed. Such health proofs will often be issued in one State but will need to be verified in another State and/or by the aircraft operator before departure to another State. 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. Accordingly, ICAO would like to exploit the advantage of integrating the check of health proofs into the existing trust framework for eMRTDs. This will enable automating the inspection of health proofs and integrating the inspection into existing procedures.

FIGURE 1 – ePassport Implementation – from Issuance to Verification



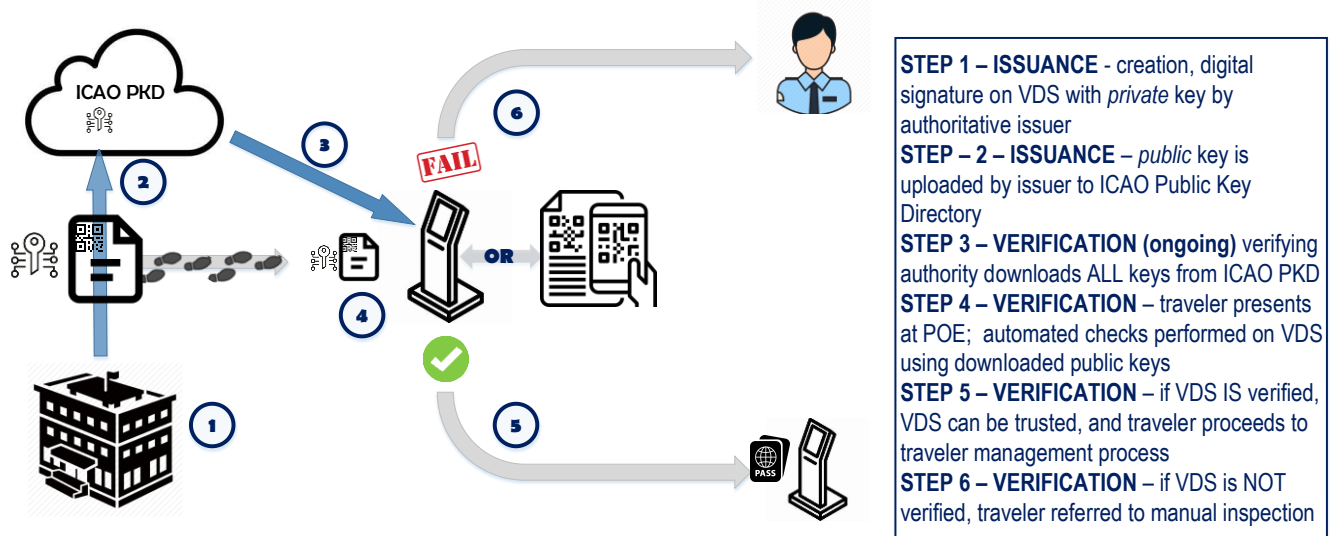
4.0 LEVERAGING THE EXISTING ePASSPORT TRUST MODEL – “VISIBLE DIGITAL SEALS”

In 2018, ICAO Member States endorsed a technology for Visible Digital Seals (VDS) for Non-Electronic Documents (VDS-NED).⁴ The VDS technology allows documents deploying 2D barcodes to be issued and inspected using the same ICAO trust framework and verification model established for ePassports. The envisaged use of the VDS was to add a similar level of digital security to non-electronic documents, i.e. documents issued without a chip, with original use cases developed for a visa counterfoil and emergency travel documents. The technology has already been applied in other real-world scenarios to preserve document security for non-electronic documents, often decentrally-issued (*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 VDS form factor can be anything from paper-based 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’s 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 actual data content, as well as to verify the security features 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 securely issue and verify other documents used in the travel continuum.

FIGURE 2 – Visible Digital Seals – From Issuance to Verification



5.0 VDS FOR PUBLIC HEALTH PROOFS

⁴ <https://www.icao.int/Security/FAL/TRIP/Documents/TR%20-%20Visible%20Digital%20Seals%20for%20Non-Electronic%20Documents%20V1.7.pdf>

In the context of COVID-19, and the resulting pressures on promoting public health while re-opening borders, ICAO's travel document policy and technical specialists recognize that existing VDS technology could be leveraged for another use case, namely the deployment of public health-related proofs to facilitate cross-border travel.

ICAO has published the Technical Report Visible Digital Seals for Non Constrained environments (VDS-NC) and has defined two profiles: one for a Covid Proof of Test (PoT) and another for a Covid Proof of Vaccination (PoV). The VDS-NC is based on *Machine Readable Travel Documents* (Doc 9303) specifications, and reuses the eMRTD trust framework. The VDS-NC contains the barcode signer and requires that only the root certificate of the issuing State be available to verify the integrity of the VDS-NC. ICAO strongly recommends the reuse of the eMRTD root certificate (the CSCA), but also allows for setting up a health root certificate (HSCA), albeit with a specific profile.

The VDS-NC technical specifications describe the data sets and security features of the VDS for the public health proof use case satisfying the guiding principles outlined in section 2.0. The VDS specifications recognize that health proofs allow for more flexibility in deploying a 2D barcode, i.e. there is more space available to place the 2D barcode on the document. Given this additional space (non-constrained environment) the VDS technical specifications for public health proofs defines a data structure for the 2D barcode using JSON (JavaScript Object Notation) a data-interchange format which is easy for humans to read and write. Using JSON enhances interoperability and usability of the VDS. Moreover, the VDS-NC was designed to be read by most barcode scanners. The Signer Certificate is included in the barcode, meaning the certificate can be verified offline.

ICAO's overarching objective in developing the VDS-NC specification was to achieve global interoperability among solutions – thereby assuring common performance and security standards. The VDS-NC specification can be easily deployed by multiple commercial applications (solutions), which would interact directly with the traveller. As an example this would be one of the many travel passes that are being issued by various groups.

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 health proof, thereby assuring that necessary information is consistently provided and facilitating easy and quick reading under transactional circumstance (e.g. at the border, boarding a flight, etc.); 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 for non-constrained environments (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 that 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 States begin to reopen their borders, 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

The ICAO CART Phase III Technical Working Groups has already approved the core data components for a COVID-19 proof of test for international travel. The data sets for both the proofs of test and vaccination, respectively, are contained in the ICAO Technical Report Visible Digital Seal for non-constrained environments (VDS-NC).

Mapping these data elements to the VDS (2D bar code) format and encoding them during issuance would immediately assist verifying entities as they will be receiving the information in a predictable, easily-readable way. With VDS-NC, travellers could also gain the flexibility of many different form factors for presentation of their public health-related data, from simple hard copies to digital representations of the barcode on their smart device.

Implementation of the VDS-NC embedded in a larger proof (e.g. COVID-19 test result), with the VDS barcode designed for efficient and standardized processing of passengers. At the same time, the health proof would also include eye-readable representation of the data, similar to the passport's visual inspection zone, enabling manual review of the data set if inspection systems were to fail as well as to accommodate environments lacking the ability to read a barcode.

Objective #2: Specifications to Enable Verifiability

Digital signing of the VDS-NC increases verifiability in order to guarantee integrity and authenticity of the data.

For vaccine certificates the digital signature is mandatory – this is because the document can be re-used many times for travel over a number of years.

For test certificates the digital signature is recommended and should be considered by an issuer. However, since the proof of test has a very short life span, often expiring 72 or even 48 hours after the test has been taken the security requirements are not as high as for vaccine certificates. However, it is still possible that some States may require a test certificate to be digitally signed to recognize that certificate for entry.

While the WHO does not recommend that States require health-related-proofs for cross-border travel, States, in support of efforts to safely reopen borders, have already included a layer of public health risk assessment into border inspection, by requiring passenger's to present public health-related proofs. As the pandemic progresses, States may also begin to implement higher thresholds for trust placed in public health proofs. This is particularly true for proofs of vaccination, as these will be more enduring in nature than a proof of test, with a traveller potentially using a vaccination proof for years and 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 proof of test 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 to verify the digital signature.

The ICAO specifications for a digitally-signed VDS-NC for public health proofs define that the Barcode Signer, the equivalent of the Document Signer Certificate (DSC – for ePassport) embedded into the 2D barcode. In turn, the Barcode Signer is linked to the issuer’s root of trust contained either in the Country-Signing Public Key Certificate Authority (CSCA) Certificate⁵ or in a health CSCA. The ICAO trust framework requires only intermittent updating of the CSCA certificate. The CSCA certificate can be obtained from other States bilaterally or via the ICAO Master List or national master lists, publicly available for download from the ICAO PKD. 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).

Core Technical VDS-NC Issuance Requirements

For States to support the issuance of health proofs in an VDS-NC format 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 (DSC) and a PKD. The CSCA does not have to be the same as for ePassports.
2. The **certificate profiles** are defined by ICAO in order to guarantee 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 and to enable offline verification.
4. A standardized **barcode encoding**. This could be finalized at the end of the discussion process. Easy readability is key.

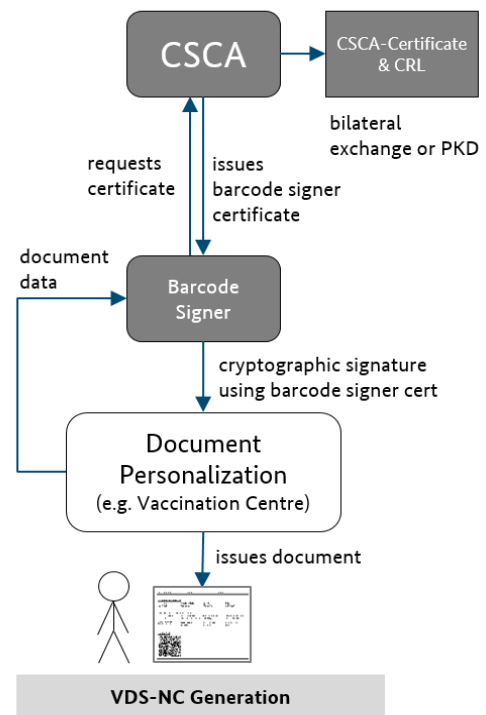


FIGURE 3: High-Level VDS-NC Flow

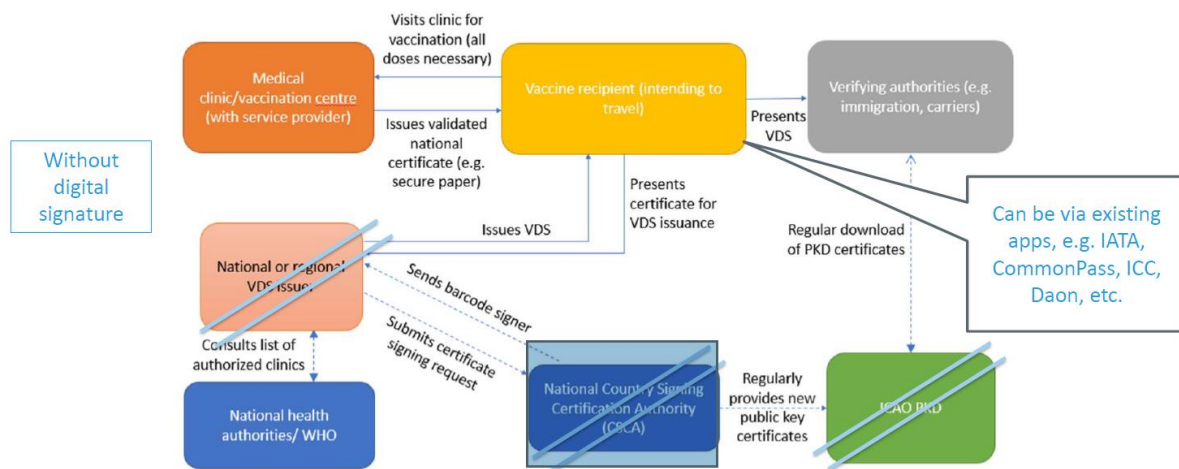
⁵ In the existing global trust/verification model for ePassport, a CSCA is considered the root trust anchor for verifying the data on an ePassport’s chip. This CSCA normally is controlled by a State’s travel document issuing authority (TDIA)

Issuance Models for Digitally-Signing VDS-NC

Building 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 proofs for cross-border travel to the existing CSCA for ePassport, which typically is controlled by a State’s Travel Document Issuing Authority (TDIA). ICAO envisions two different models for issuance of a VDS-NC – centralized and decentralized issuance – both anchored directly by the State trust anchor, either the CSCA or the health CSCA.

FIGURE 4 – Centralized Signature Service (using ePassport CSCA)

****note** this image denotes a central issuance service for a VDS-NC with a digital signature. Essentially a conversion of the health certificate into a secure barcode format that can be used for international travel.



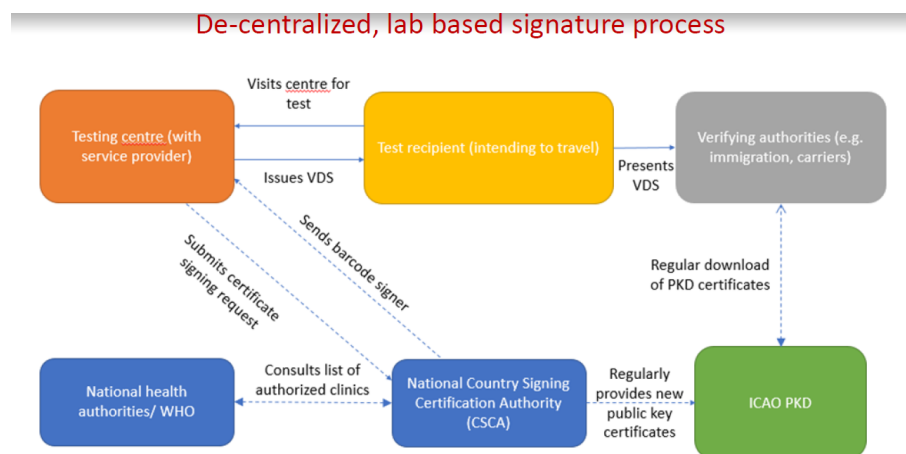
DESCRIPTION – MODEL - Central Signing Service (using ePassport CSCA)

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 and issued to the bearer as a medical certificate. This data set can then be sent to a central signing service which:

- recognizes the point of issuance as registered/authorized; and
- 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 traveller as a globally interoperable public health proof. The form factor can be either in paper (printable graphic or .pdf file) or digital, or both if the proof is printed. In either case the public health proof needs to be both human and machine readable.

FIGURE 5 – Decentralized, Lab-Based Solution



DESCRIPTION – MODEL - Decentralized, 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 VDS-NC trust anchor, whether it be the CSCA (trust anchor for ePassport) or the health CSCA. 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 recommends 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.***

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		<ul style="list-style-type: none"> • VDS would be populated with key data points and <i>can</i> be digitally signed • Verification of the digital signature would allow verifier to confirm data is genuine and has not been tampered with
 Convenient		<ul style="list-style-type: none"> • 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		<ul style="list-style-type: none"> • 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		<ul style="list-style-type: none"> • 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		<ul style="list-style-type: none"> • 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		<ul style="list-style-type: none"> • 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		<ul style="list-style-type: none"> • 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

COVID-19 is an unprecedented crisis, especially for aviation, 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's specifications such as the VDS-NC, applied to public health proofs, offers global interoperability and the potential to overcome existing obstacles to cross-border travel by air by meeting the guiding principles identified.

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

Recommendations:

- Now is the time for Member States to consider the appropriate policies and processes for issuance of secure testing and vaccination certificates that will be recognized as widely as possible. To this effect, States should be regularly monitoring guidance from the WHO with regards to proof of COVID-19 vaccination for international travellers⁶ which outlines

⁶ WHO Interim Position Paper - <https://www.who.int/groups/smart-vaccination-certificate-working-group>)

ongoing consideration of COVID-19 vaccinations and applicable existing international law, including the *International Health Regulations*.⁷

- 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 for vaccination health proofs, and to be encoded in a VDS-NC barcode.
- Existing solution providers should work with policymakers and the technology community to align on standards 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.

— — — — —

⁷ WHO *International Health Regulations* (2005) - https://www.who.int/health-topics/international-health-regulations#tab=tab_1

ANNEX 1. Deployed Use Cases for Visible Digital Seals (VDS) in the Travel Continuum

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

In 2015, due to the refugee crisis in Europe, Germany decided to issue a harmonized document as proof of a successful registration to all asylum seekers arriving in Germany. The document includes physical security features, eye-readable data and a VDS containing all the printed personal data, as well as providing a link to a national database containing biometrics. The project involved the rollout of 1,500 decentral mobile enrollment stations for biographic and biometric data collection and issuance. Data was sent to the central signing service, which returned the digitally-signed VDS to the decentralized issuance point for printing on the document. The document can be authenticated by a mobile phone application, as well as by stationary border control equipment.



Use Case 2: EU Schengen Visa (2022)

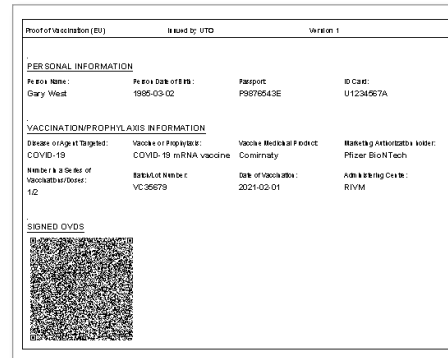
The new Schengen visa counterfoil format was introduced in 2015. In the years thereafter, increasingly good quality counterfeiting of the new format was observed. Accordingly, the EU decided to update the visa sticker with the VDS to protect the issuance of the document, prevent the use of stolen blanks and add a layer of cryptographic security to a non-electronic 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 VDS-NC 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 (test, vaccination).
2. The VDS-NC is a standardized representation of data in a 2D-barcode and, when required, **digitally signed** 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 ePassports since 2004. It consists of a root of trust (CSCA), a document (barcode) signer, a PKD and the document itself.
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:

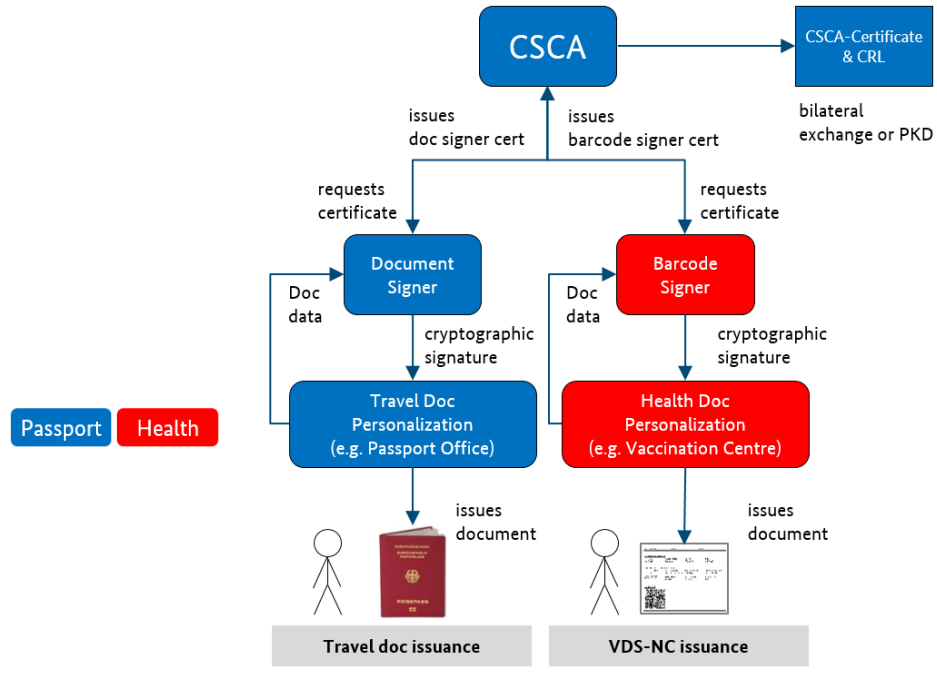
1. The VDS-NC is **not the primary medical vaccination document**. This function stays within the health-related environment: vaccination certificates will be treated and governed as health documents. This is especially important because a vaccination needs to be administered without a requirement to present a travel document.
2. The VDS-NC is **not intended to replace any national/ multilateral vaccination document**.



ANNEX 3. Issuance and PKI Models

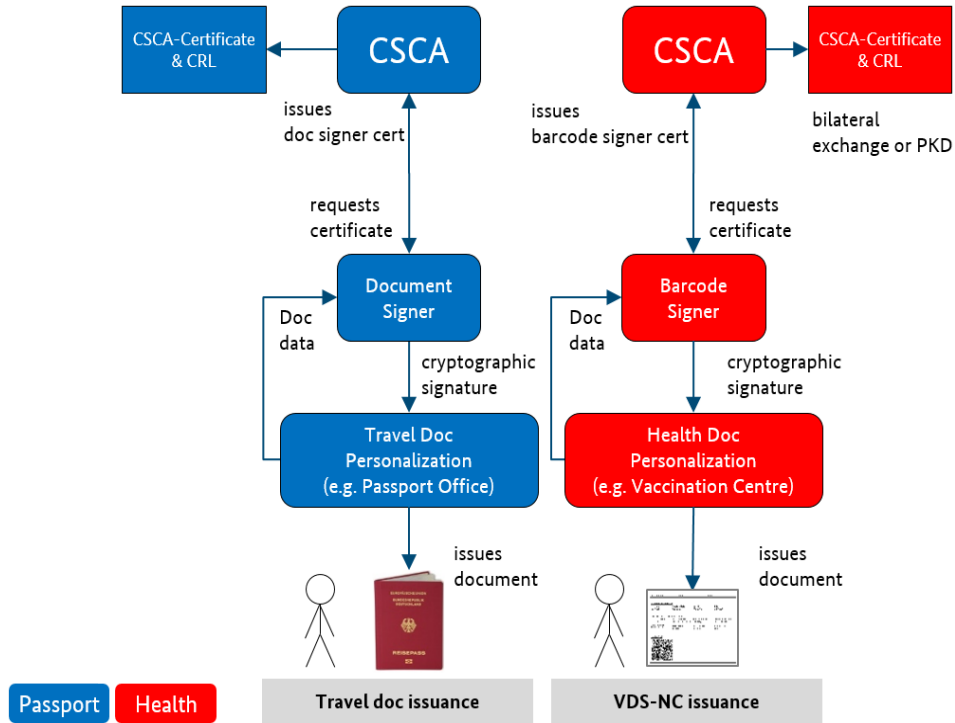
PKI model A: Single CSCA for both travel documents and health proofs

- 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 travel documents and health proofs, respectively.
- The certificate profiles ensure that certificates can be used for the intended purpose only.



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

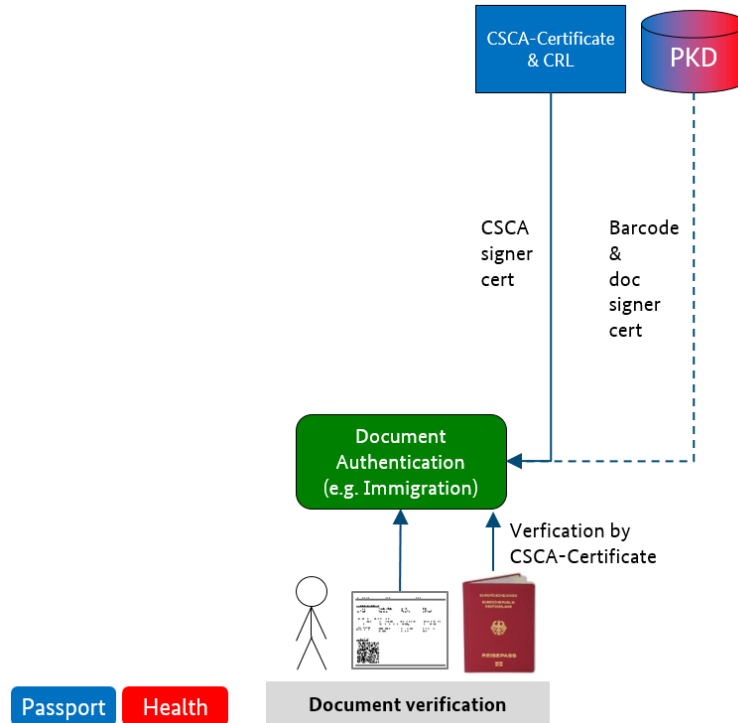
- There are specific CSCA's for issuing travel documents and for issuing health proofs.
- The document signers are specific for each travel documents and health proofs.
- The certificate profiles ensure that certificates can be used for the intended purpose only.



ANNEX 4. Verification Models

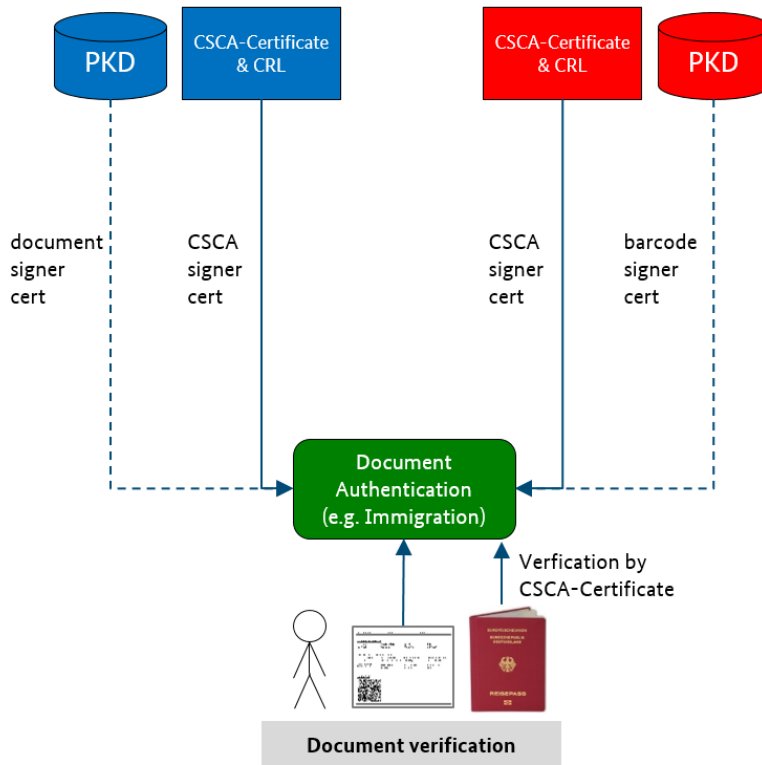
PKI model A: Single CSCA for both travel documents and health proofs

- Inspection systems import the CSCA certificates, as is currently the case for travel documents.
- Inspection systems 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 document signer certificates could be downloaded from the (single) PKD.



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

- Inspection systems import the CSCA certificates for travel documents and for health proofs.
- Inspection systems 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 document signer certificates could be downloaded from the (specific) PKD.



ANNEX 5. Implementation Guidance for States regarding 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, which States, choosing particular implementation models, 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 align 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, 4 and 5 in these Guidelines highlight that different entities may manage the issuance and digital signing 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 then have to define the appropriate trust anchors within the PKI being used. These options are highlighted in Figure A.1 below.

Figure A.1. The main choices that States should make regarding issuance of VDS-NC based travel proofs using proof of test as an example

Choose issuing entity

- Issuance at the testing location (decentralized issuance)
- Issuance by a centralized entity

Choose whether the VDS will be signed

- Digitally sign all issued VDS (recommended)
- Encode data without digital signature

Choose the medium of issuance

- Provide a printed proof
- Provide a digital file (that could be printed or alternatively shown on the screen of a personal device)
- Partner with an external application provider for digital issuance

(If the VDS-NC is to be signed)

Choose the trust anchor

- Use the CSCA defined in ICAO Doc9303 that is associated with travel document issuance
- Put into place (or use an existing) trust anchor in the health domain

The following checklists explain various options and main steps that implementers will have to undertake for issuance according to the model applied. 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.

Implementation checklists with different issuing entities, with and without the application of a digital signature on VDS-NC barcodes

Conversion Model – post facto issuance

The “conversion model” is most applicable to vaccination certificates which have been issued domestically in paper form and which are to be converted into an internationally recognized and globally interoperable vaccination certificate, with digital security features. The digital security features in the VDS-NC barcode are applicable regardless of the form factor (i.e. paper or digital representation of the barcode).

The scenario could apply to both a paper record or a digital credential, either of which could be converted to the internationally recognized certificate supporting international travel after the medical event has taken place and the corresponding certificate has been issued. In some cases this can be supported by a centralized digital registry of health records, managed on a local, regional or even national level.

If, as ICAO recommends, the VDS-NC uses the same root of trust is (e.g. Single CSCA) for both travel documents and certificates/health proofs as described in Annex 3 – Issuance and PKI Models, PKI Model A, then the conversion process could take place at the travel document application centre.

The following guidance should be implemented:

1. The issuer must be familiar with the paper and digital 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 traveller to present the paper or digital certificate to the issuer in person in order to obtain a VDS-NC.
3. Organizational arrangements must be in place so that the 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 traveller).

Table A1. Checklists for real-time issuance of health proofs

	WITH digitally signature	WITHOUT digital signature
Decentralized Issuance, e.g. at the health facility	<p>In this scenario, the VDS-NC, with a digital signature, is issued immediately after the medical event (test or vaccination) based on electronic data exchanged with a centralized signing authority.</p> <p>Organizational arrangements must be in place so that the health centre (or location where medical event has occurred) can obtain barcode signers from the central trust authority (Figure A.3) for use.</p> <p>If digital signing occurs decentrally, 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 VDS-NC Technical Report (all data required in the dataset).</p> <p>The health centre must have appropriate physical security at the test site to protect this IT infrastructure. This setup requires appropriate security to protect private keys used for signature. It would normally not be a prudent approach unless the site has considerable volume of business.</p>	<p>This scenario would only apply to cases when a Receiving State does not require a proof of test to be digitally signed.</p> <p>The health centre must have access to 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).</p>
Centralized Issuance by a centralized entity	<p>In this scenario the VDS-NC is created centrally based on electronic data exchanged with the health centre and returned to the bearer.</p>	<p>This scenario might be implemented for larger testing labs that have multiple testing locations but a centralized entity for barcode issuance. In this case issuance is done by the centralized entity</p>

	<p>For this to occur the following should be in place:</p> <ol style="list-style-type: none"> 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 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). 	<p>based on electronic data exchanged with the health centre.</p> <p>For this to occur the following should be in place:</p> <ol style="list-style-type: none"> 1. An electronic connection must exist between the health centre and centralized issuing entity (e.g. a dedicated data transfer tool; secure email) that the health centre will use for transfer of the necessary data for VDS-NC issuance. 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).
--	---	--

Table A2. Checklists for implementation with different media for issuance

<p>Provide a printed proof</p>	<ol style="list-style-type: none"> 1. The entity in contact with the intending traveller (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 Doc 9303.
<p>Provide a digital file</p>	<p>Two possibilities are foreseen:</p> <ol style="list-style-type: none"> a. The email address of the intending traveller 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. <p>OR</p> <ol style="list-style-type: none"> b. The centralized entity has an established online portal for receipt of requests for VDS-NC. The intending traveller 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. <p>***ICAO recommends consideration to provide both of the above formats, digital and printout.</p>
<p>Partner with an external application provider</p>	<ol style="list-style-type: none"> 1. A secure electronic connection is in place for the submission of data from the health centre to the application provider. 2. The health centre enrolls all data foreseen in the established dataset and submits it to the application provider. 3. The application has the necessary capabilities to encode the data in a VDS-NC and make the barcode associated with the intending traveller available to him/her within the application. <p>(If the VDS-NC is to be digitally signed)</p> <ol style="list-style-type: none"> 4. The application developer has the appropriate agreements in place with State authorities in order to obtain the necessary barcode signer private key.

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

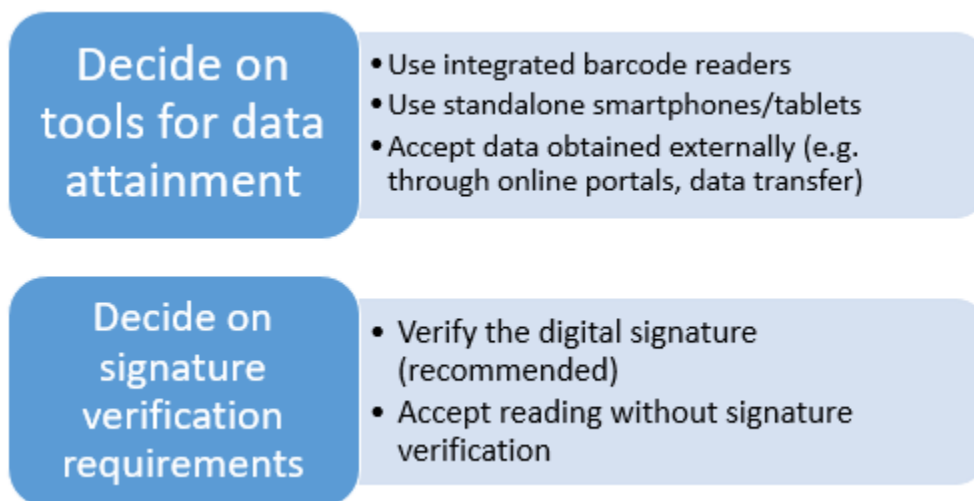
<p>Use the travel document trust anchor, e.g. CSCA</p>	<ol style="list-style-type: none"> 1. Necessary agreements and arrangements are in place between the CSCA associated with the State’s travel documents and the entity (-ies) issuing the VDS-NC barcodes for the signing of Certificate Signing Requests submitted by the issuing entity (-ies) using the CSCA private key. <p><i>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.</i></p>
<p>Use a trust anchor established within the health domain in the State</p>	<ol style="list-style-type: none"> 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. <p><i>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.</i></p> <ol style="list-style-type: none"> 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 PKD.

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.

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

<p>Use integrated barcode readers</p>	<ol style="list-style-type: none"> 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.
<p>Use standalone devices</p>	<ol style="list-style-type: none"> 1. All appropriate parties have easy access to standalone smartphone or tablet devices with an integrated camera and an appropriate reading and barcode decoding application installed. <p><i>Note. Suitable applications are available for public download from application libraries.</i></p>
<p>Accept data obtained externally</p>	<ol style="list-style-type: none"> 1. Secure portals are established for the purpose of enrolling health-related data in the context of travel. <p><i>Note. A typical case might involve a State establishing an online portal for use by those travelling to that State. The traveller will provide all necessary data in advance of their travel. Provision might include the intending traveller scanning the VDS-NC barcode using his/her device in order to provide the necessary data in a secure, efficient and error-reducing manner.</i></p> <ol style="list-style-type: none"> 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 A5. Checklist for digital signature verification of VDS-NC based health proofs

<p>Verify the digital signature</p>	<ol style="list-style-type: none"> 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.
<p>Accept reading without signature verification</p>	<p><i>No additional steps required beyond those in Table A4.</i></p>

— END —