Interim guidance for developing a Smart Vaccination Certificate

Release Candidate 1

19 March 2021

Interim guidance for developing a Smart Vaccination Certificate

ISBN XXX-XX-X-XXXXXX-X (electronic version) *Will be available for version 1 release*

ISBN XXX-XX-X-XXXXXX-X (print version) *Will be available for version 1 release*

Suggested citation. *Will be available for version 1 release*

Cataloguing-in-Publication (CIP) data. CIP data are available at *http://apps.who.int/iris*.

Sales, rights and licensing. To purchase WHO publications, see http://apps.who.int/bookorders. To submit requests for commercial use and queries on rights and licensing, see *http://www.who.int/about/licensing*.

CONTENTS

ACKNOWLEDGEMENTS

The World Health Organization (WHO) is grateful for the contribution that many individuals and organizations have made to the development of this document.

This document was coordinated by Garrett Mehl, Natschja Ratanaprayul, Derek Ritz, Philippe Veltsos of the WHO Department of Digital Health and Innovations (DHI); in collaboration with individuals in departments across WHO that include Marta Gacic-Dobo and Jan Grevendonk of the WHO Department of Immunization, Vaccines and Biologicals (IVB); Carmen Dolea and Thomas Hofmann of the WHO Department of International Health Regulations and Preparedness; Sara Barragan Montes and Ninglan Wang of the WHO Department of Border Health Risk Dissemination (BRD).

The following WHO staff and consultants contributed to this document at various stages (in alphabetical order): Onyema Ajuebor, Shada Alsalamah, Kevin Crampton, Fernando Gonzalez-Martin, Jennifer Horton, Robert Jakob, Pernille Jorgensen, Mark Katz, Nenad Kostanjsek, Ann Linstrand, Katherine Littler, Bernardo Mariano, Ngum Meh Zang, Derrick Muneene, Craig Nakagawa, Patricia Ndumbi, Andreas Reis, Soumya Swaminathan and Wouter T'Hoen.

The following WHO regional advisors also contributed to this document at various stages (in alphabetical order): Roberta Andraghetti, Housseynou Ba, Andre Arsene Bita Fouda, Vladimir Choi, Marcela Contreas, Marcelo D'Agostino, Jun Gao, Clayton Hamilton, Mark Landry, Ephrem Lemango, Jason Mwenda Mathiu, Mohamed Nour, Roberta Pastore, Alain Poy and Martha Velandia.

WHO extends sincere thanks to (in alphabetical order): Emily Carnahan, Voo Teck Chuan, Konstantin Hyppönen, Carl Leitner, Henry Mwanyika, Alejandro Osornio, Elizabeth Peloso, Maria Soc, Jenny Thompson and all members and observers of the Smart Vaccination Certificate Working Group.

ABBREVIATIONS

AEFI	adverse events following immunization
API	application programming interface
CARE	Continuity of Care scenario of use
COVID-19	Coronavirus disease 2019
CRL	certificate revocation lists
CSCA	country signing certificate authority
DHIS2	District Health Information Software 2
DS	document signer
DSC	document signer certificate
EIR	electronic immunization registry
EMR	electronic medical record
FHIR	Fast Healthcare Interoperability Resources
GHTA	global health trust anchor
HL7	Health Level Seven
HPV	human papillomavirus
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICD	International Classification of Diseases
ID	identifier
IG	implementation guide
IHE	Integrating the Healthcare Enterprise
IHR	International Health Regulations
IIS	immunization information systems
intPHA	international public health authority
ISO	International Organization for Standardization
mRNA	messenger ribonucleic acid
NPKD	national public key directory
OpenHIE	Open Health Information Exchange
PHA	public health authority
PII	personally identifiable information
PKD	public key directory
PKI	public key infrastructure
PROOF	Proof of Vaccination scenario of use
RC	release candidate
SHR	shared health record
SNOMED CT GPS	Systematized Nomenclature of Medicine Clinical Terms Global Patient Set
SVC	smart vaccination certificate
UVCI	unique vaccination certificate identifier
WHO-FIC	WHO Family of International Classifications

EXECUTIVE SUMMARY

The concept of digital vaccination certificates or "smart vaccination certificates" (SVCs) is proposed to provide a mechanism whereby an individual can present documentation that claims they have received a vaccine and this claim can be cryptographically verified by an interested party. This is considered superior to a paper-only vaccination certificate, which can be fraudulently obtained, easily lost and damaged, or simply difficult to read due to illegible handwriting. Although the SVC is initially planned to be used for Coronavirus disease (COVID-19) vaccinations, the intent is to set up a foundational mechanism that will be applicable for use with other vaccinations in the future, such as Yellow Fever, Polio, or vaccinations that have yet to be discovered. Furthermore, the approach is architected to respond to the evolving science and needs of countries. The World Health Organization (WHO) has developed this guidance and technical specifications document, in collaboration with a multi-disciplinary group of partners, in order to support WHO Member States in adopting interoperability standards for SVCs.

What is a Smart Vaccination Certificate?

A vaccination certificate is a medical document that records a vaccination service that an individual has received. Digital vaccination certificates, or cards, refer to digital immunization records that are accessible by the vaccinated person, and serve the same purposes as traditional home-based records: they provide a tool to ensure continuity of care and a proof of vaccination *(1)*.

A smart vaccination certificate (SVC) can be purely digital and stored, for example, on a smartphone application or a cloud-based server. Alternatively, it can be a "digital twin"[1] *(2)* of a traditional paper home-based record. A smartphone is not required to have an SVC. The link between the paper SVC record and the digital record can be established by a barcode[2], for example, that is printed on the paper vaccination card.

The SVC only documents that a vaccination event has occurred. It is not intended to serve as an "immunity passport" *(3)*. As per the "Interim position paper: considerations regarding proof of COVID-19 vaccination for international travellers" *(4)*, "Regardless of any technology implemented in future, the COVID-19 vaccination status of international travellers should be recorded through the International Certificate for Vaccination and Prophylaxis based on the model presented in Annex 6 of the IHR. The same format could be adapted once WHO pre-qualified COVID-19 vaccines become available universally and relevant recommendations are provided under the IHR."

[1] As defined by IBM, a "digital twin" is "the virtual representation of a physical object or system".

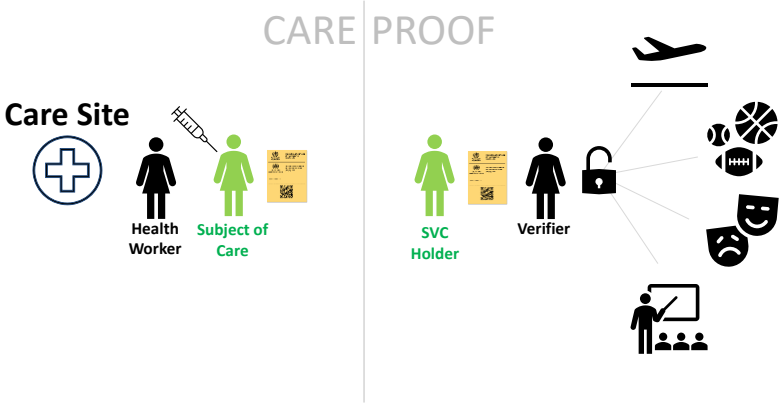
[2] Barcode or 2D data matrix

Figure 1. Smart Vaccination Certificates can take many forms

What are the benefits of a Smart Vaccination Certificate?

SVCs can enhance existing paper home-based records *(5)* and the international certificate of vaccination or prophylaxis *(6)* by combining the functionality of both. Additionally, SVCs can provide a way to mitigate fraud and falsification of "paper only" vaccination certificates by having a "digital twin" that can be verified and validated in a reliable and trusted manner, for health, occupational, educational, and travel purposes (as per national and international policies); without depending on an individual verifier's subjective interpretation. Once an individual's vaccination record is available in a digital format, additional functionality can be built to support things like automated reminders for the next dose or linkages to other immunization information systems (though these are outside the scope of this document). An SVC is intended to allow for multiple types of use without requiring an individual to hold multiple vaccination records per Figure 2.

Figure 2. Multiple use cases for a Smart Vaccination Certificate



Key design principles

In order to guide the creation of a globally interoperable SVC, WHO has adopted the following key design principles.

- Equity: Ensuring that SVCs do not further pre-existing inequities or create new ones
- Accessibility: Ensuring that SVCs are accessible to all, including through the use of open standards
- Privacy protecting: Ensuring that individual privacy rights are respected and protected

- Scalability, flexibility and sustainability: Ensuring that SVCs can reach global scale, are sustainable beyond the COVID-19 pandemic, are adaptable for other contexts and uses, and take into account environmental sustainability of the various solutions implemented.

Scenarios of use and use cases of the SVC

The scope of this document currently covers two scenarios of use of the SVC:

(1) *Continuity of Care:* Vaccination records are an important part of an individual's medical records, starting at birth. The Continuity of Care scenario of use is the primary purpose of a vaccination certificate. It provides individuals with a record of which vaccinations they have received, helping to ensure they are able to make informed decisions on the health services they receive and can provide that information to a health worker as part of their medical history.

(2) *Proof of Vaccination:* Vaccinations are intended to reduce transmission, protect against infection and ensure long-lasting immunity. Vaccination records are an important tool to document and provide proof that an individual has been vaccinated. This allows for public health officials to help manage and minimize the impact of acute public health events that endanger people's health across geographical regions and international boundaries.

There are multiple use cases within the Continuity of Care and Proof of Vaccination scenarios, and it is expected that these use cases will operate within contexts across a broad range of digital health maturity. The recommended core data set for the SVC is intended to reflect the critical data requirements for interoperability, driven by the public health need.

What is the WHO trust framework?

A trust framework consists of technical specifications, interoperability criteria and related governance mechanisms that are agreed upon by multiple entities to establish trust between those entities. The WHO trust framework is intended to be a mechanism by which any Members State can trust that medical documents issued by another Member State are authentic and have not been tampered with. The WHO trust framework will leverage public key infrastructures (PKIs) to establish a cryptographically supported trust framework for SVCs. PKI is widely used to establish global trust frameworks. For example, it is the key mechanism behind online credit card transactions *(7)*. Public health authorities in Member States will need to establish and maintain a domestic PKI system with appropriate authorities, applications, people, and processes in place to support SVC issuance and verification.

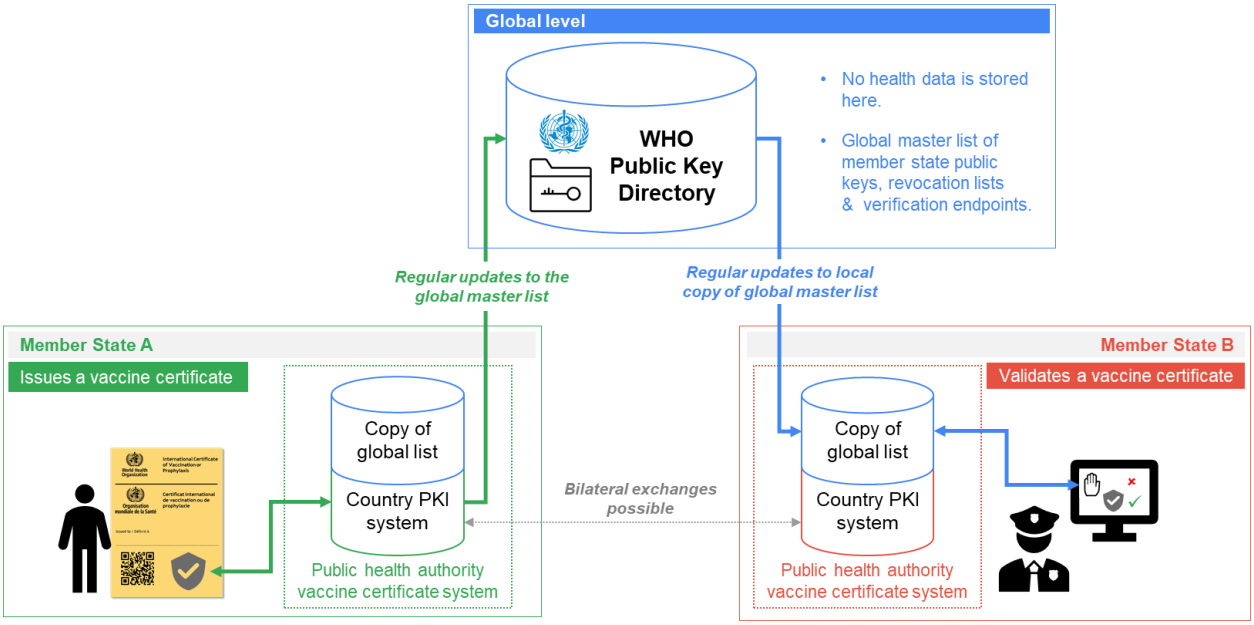
The WHO trust framework relies on a chain of trust between Member States that is operationalized by a public key directory, to be managed by WHO. No personal health data will be stored in the WHO Public Key Directory. The WHO Public Key Directory will be a global registry of public keys linked to Member States' public health authorities. This global directory of public keys will allow cross border verification and validation of SVCs.

By managing a global directory of public keys, WHO can play the role of a trust broker among Member States that meet SVC interoperability requirements. Locally, each Member State would

maintain a copy of the global list of public keys. These locally cached keys could be then leveraged to verify SVCs issued by other Member States.

Member States may also choose to bilaterally exchange public keys, or regional public key directories may also be set up (such as is being contemplated by the European Union). The overall process is illustrated in Figure 3.

Figure 3. WHO Public Key Directory



1 INTRODUCTION

1.1 Background

The Coronavirus disease (COVID-19) caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), first identified in December 2019, has spread to become a global pandemic. The outbreak has forced curtailment of movement, curfews and adoption of preventative measures to try to halt transmission and lower the burden on public health resources and reduce loss of life and severe illnesses. COVID-19 vaccines are being delivered at record speed and countries need a way for individuals to have a record of their vaccination status.

1.2 Assumptions

At the time of writing, four vaccines have been approved by WHO under the emergency use list *(8)* . Given the existing inequities in accessing digital technologies and connectivity, regardless of technologies being implemented in countries, it is currently still recommended that COVID-19 vaccination status be documented on the International Certificate of Vaccination and Prophylaxis (ICVP).

A number of assumptions are being made about the responsibilities of WHO and Member States with regards to the SVC. The following assumptions are being made about WHO's responsibilities with regards to the SVC:

1. WHO will not have access to any identifiable, individual data.
2. WHO will not receive or process personal health data (only public keys).
3. WHO will determine the core data set and the related data standards (data structure and semantics).

The following assumptions are being made about Member States' responsibilities:

1. It will be up to the Member State to determine the format in which to implement the SVC in (such as if it will be augmented paper, smartphone application, or something else).
2. There can be multiple point of service solutions depending on the context of the Member State.
3. Member States will be responsible for implementing the policies necessary to support the SVC workflow.
4. It will be up to the Member State to determine the mechanism for unique identification.

1.3 Purpose of this document

Whereas, the following statement(s) on the sixth meeting of the International Health Regulations (IHR) Emergency Committee regarding the Coronavirus disease (COVID-19) pandemic advised the WHO Secretariat *(9)* to:

- "Rapidly develop and disseminate the WHO policy position on the legal, ethical, scientific, and technological considerations related to requirements for proof of COVID-19 vaccination for international travellers, in accordance with relevant IHR provisions.
- Coordinate with relevant stakeholders the development of standards for digital documentation of COVID-19 travel-related risk reduction measures, that can be implemented on interoperable digital platforms. This should include vaccination status in preparation for widespread vaccine access."

WHO has developed this technical specifications document in order to support WHO Member States as recommended by the IHR Emergency Committee. Furthermore, with the unprecedented scale of vaccination delivery in countries, digital technologies should be leveraged to support capturing of vaccination status for individuals. Digital technologies can provide a way to mitigate fraud and falsification; provide a way to send automated reminders to the vaccinated person of when the next dose is due; and can allow for an individual to more seamlessly have access to their personal record; and more seamlessly provide that information to their health care provider.

As Member States are increasingly looking to adopt digital solutions for a vaccination certificate for COVID-19, this document is intended to provide Member States with a baseline set of requirements and standards specifications that will allow for a compliant SVC solution to be interoperable with other SVC standards-based solutions. With the baseline requirements met, it is anticipated that Member States can adapt these specifications into a local instance and deployment of an SVC with their technology partner of choice. This document is intended to be software-neutral and provide a starting point for Member States to deploy an SVC in whichever mode of distribution (e.g. paper or smart phone application) they would like; regardless of whether it is a paper card with QR code stickers or a fully functioning smartphone application developed internationally or locally.

1.4 Target audience

The primary target audience of this document is national authorities tasked with creating or overseeing the development of a digital vaccination certificate solution for COVID-19. The document may also serve useful to partners, such as local businesses, international organizations, non-governmental organizations, and trade associations, which may be required to support Member States in deploying an SVC solution.

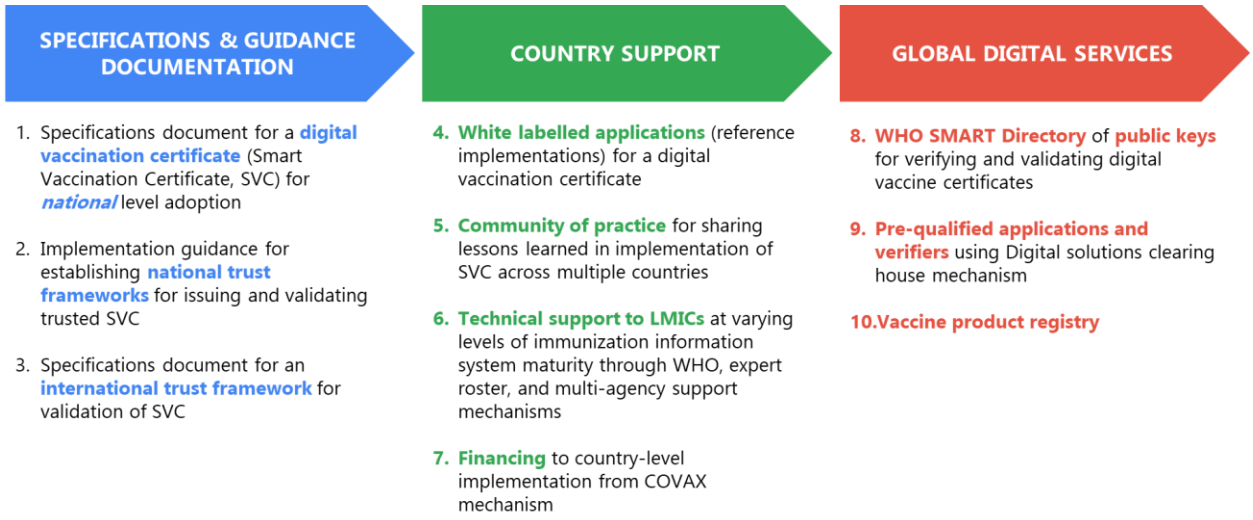
1.5 Scope of this document

This document is part of a larger body of work under the Smart Vaccination Certificate Working Group, which includes key outputs outlined in Figure 4. The scope of this document specifically includes the following three key sections:

1. Business requirements for a digital vaccination certificate (Smart Vaccination Certificate, SVC) for national level adoption.
2. Guidance for establishing national trust frameworks for issuing and validating trusted SVCs.

3. Business requirements for a global trust framework for validation and verification of SVCs.

Figure 4. Anticipated outputs of the Smart Vaccination Certificate Working Group



1.5.1 Planned releases

Due to the rapidly evolving context of the COVID-19 pandemic, this document is intended to have three release candidates prior to a complete Version 1 being released. After release of Version 1, revisions are planned with subsequent versions of the document released every six months for the next three years.

Release Candidate 1 [this document] contains the key business requirements for a digital vaccination certificate (Smart Vaccination Certificate, SVC) for national adoption that includes the prioritized scenarios of use, use cases, key workflows, a core data set mapped to a preferred code set, and a base Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR) Implementation Guide for the SVC Release Candidate 1 scope. The first release candidate also begins to outline a global trust framework and high-level overview of a governance mechanism.

Release Candidate 2, planned for public release at the end of April 2021, is anticipated to build off the business requirements outlined in Release Candidate 1 and to include ethical and privacy considerations of a digital vaccination certificate. Furthermore, Release Candidate 2 will also include greater detail on the technical specifications for a global trust framework for verifying and validating a digital vaccination certificate.

Release Candidate 3, planned for public release at the end of May 2021, will be a further iteration of the technical specifications for a national SVC, including establishing a national trust framework, and a comprehensive specifications document for a global trust framework.

Version 1, planned for public release at the end of June 2021, is intended to be a complete technical specifications document for a nationally deployable digital vaccination certificate that can leverage a global trust framework for verification and validation of a standards-compliant SVC issued anywhere, globally.

1.5.2 Open and closed issues in Release Candidate 1

1.5.2.1 Open Issues

The following are issues for which input is sought from public commenters:

- The best option for formatting 2D barcode (such as a QR code) content is not clear. There is a desire to be able to generate machine-readable, signed artefacts derived from the SVC core data set and leverage these in Proof of Vaccination use cases – but the size limitations of QR codes present challenges for representing a full representation of the FHIR document.
- The present SVC FHIR health data content specification is related to the FHIR International Patient Summary (IPS) specification and the FHIR composition defined there. Other content, such as lab results, is readily persisted in the IPS format. It is not clear whether an IPS-conformant shared health record repository, separate from the SVC Registry, should be identified as a mandatory or optional element of the SVC infrastructure.
- Some Member States have approached WHO for assistance related to the establishment of their PHA's national public key infrastructure. It is not clear what role WHO should or could play. Some options include WHO acting, as the holder of an anchor PKI certificate, could be employed to generate and sign public and private key pairs for Member States' PHAs, and the PHAs can then employ to create Document Signer certificates. Alternatively, WHO may be able to offer a fully hosted and outsourced PKI service bureau for Member States who may need such services. Other options are possible.

1.5.2.2 Closed Issues

The following are closed issues that were decided as part of the expert group interactions that preceded the publishing of Release Candidate 1.

- Many options were considered and evaluated regarding the operational alternatives for a global trust network. Based on WHO's decision criteria, a PKI-based WHO Public Key Directory design, generally based on the Public Key Directory model employed by the International Civil Aviation Organization (ICAO), was decided upon.
- A number of alternatives were evaluated regarding the SVC core data set, its elements, and the cardinality and coding of these elements. The final core data set is described in Section 3.5.
- The normative base code system for the SVC is ICD-11. For COVID-19, a 1-to-1 mapping is included in the specification between ICD-11 and SNOMED GPS.
- HL7 FHIR R4 has been decided upon as the health data standard for expressing the SVC core data set.
- The HL7 FHIR International Patient Summary (IPS) Implementation Guide (IG) has been chosen as the "reference" data model for the SVC IG, with profiling as necessary to support the cardinality and coding decisions related to the SVC core data set.

1.6 How to leverage this document

Release Candidate 1 is intended to be an initial technical specifications document that effectively captures the requirements for a digital vaccination certificate or Smart Vaccination Certificate (SVC) from the immunization programme perspective. The first release candidate can be used to guide initial discussions towards developing a nationally and internationally recognized SVC that is standards-based.

Given the consistently evolving context of COVID-19, this document is intended to be regularly updated with additional details up until the planned release of Version 1. In the interim, this document can provide a baseline set of requirements in which Member States can use as reference for their own planned implementation of a digital vaccination certificate.

1.7 Methods and additional resources

Since the COVID-19 pandemic began and as vaccines were beginning to show signs of successfully preventing deaths and serious illnesses, the number of digital solutions for vaccination certificates has flourished. For WHO to remain software neutral, WHO created the Smart Vaccination Certificate Working Group, with the intention it be a multi-sectoral working group focused on supporting development of key standards for a digital vaccination certificate, sharing joint learnings, and supporting development of a governance model with a trust framework architecture to support roll out of COVID-19 vaccines, globally *(10)*.

The goals of the Smart Vaccination Certificate working group are to:

1. Guide WHO on common standards and governance for security, authentication, privacy, and data exchange;
2. Coordinate and strategically align efforts and collaboration to manage lessons learned and commonalities; and
3. Establish guidance for Member States to facilitate informed adoption.

The objectives of the Smart Vaccination Certificate working group are to:

1. Publish standards for security, authentication, privacy, and data exchange for outlined use cases;
2. Support and learn from successes and challenges via reference implementations and community of practice;
3. Identify and curate multiple tools that conform to security, authentication, privacy, and data exchange standards established by the consortium;
4. Develop appropriate guidance detailing use cases, standards and best practice; and
5. Provide guidance to Member States to ensure they can adopt and support digitized vaccination certificate solutions nationally, and eventually for cross border purposes.

In December of 2020, WHO issued an open call for nomination of experts to contribute to the SVC technical specifications and standards. Through a formal process, experts were selected based on

their expertise (in immunization, standards setting, technology implementation, and/or policy), not their affiliation, with a focus on regional representation and gender balance.

The Smart Vaccination Certificate Working Group was leveraged to inform the contents of this guidance document through a series of consultative meetings divided into the following three workstreams:

- Workstream 1: Vaccination certificate data set standards, workflows, functional requirements
- Workstream 2: Validation and verification of vaccine certificate and enabling technologies
- Workstream 3: Ethics, legislation, privacy, and communications

In addition to the expertise provided by the Smart Vaccination Certificate Working Group, the following existing WHO guidance documents served as a baseline for this work:

- Statement on the sixth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic *(9)*
- Interim position paper: considerations regarding proof of COVID-19 vaccination for international travellers *(4)*
- Monitoring COVID-19 vaccination: Operational guide for the collection and use of vaccination data *(1)*
- Practical guide for the design, use and promotion of home-based records in immunization *(5)*
- Guidance on developing a national deployment and vaccination plan for COVID-19 vaccines *(11)*
- International Health Regulations (2005) Third Edition *(12)*

2 GUIDING PRINCIPLES

As with any digital solution, there are potential impacts on equity and equitable access to such solutions. Thus, there are several guiding principles and frameworks that have informed the formulation of the technical specifications as well as provide guidance on how resulting solutions can be ethically implemented. The guiding principles include the following:

- SVC Design principles
- Ethical considerations for national use
- Ethical considerations for cross border use
- Data privacy principles for a digital vaccination certificate

2.1 SVC Design principles

The following design principles have guided the design of an SVC, the development of this document, and the Smart Vaccination Certificate Working Group:

1. Equity
    - Everyone has the right to obtain and hold an SVC;
    - The SVC should not increase health inequities or increase the digital divide;
2. Accessibility
    - Every SVC should be verifiable;
    - SVCs should work in online and offline environments across multiple platforms, paper and digital;
    - The interoperability specifications will be based on open standards to ensure equitable access to a range of non-proprietary digital tools;
3. Privacy protecting
    - An individual's vaccination record is a medical document, and an individual's privacy needs to be respected accordingly.
    - Individuals are able to have access to their own data and can fully control whether or not they want to disclose their vaccination status;
    - Only data required for the purposes of vaccinations should be captured to minimize data collection and support appropriate usage of those data;
4. Scalability, flexibility, sustainability
    - Given how diverse our world is, the recommendations regarding the technological specification for an SVC solution are intended to be flexible and adaptable for each Member State to meet public health needs, as well as the needs of individuals around the world. There is no "one size fits all".
    - The requirements outlined are intended to allow for SVC solutions to meet the needs of a country's holistic public health preparedness and response plan, while still being usable in others. It is also an overarching expectation that there will be multiple digital health products and solutions that will be implemented to operationalize the requirements described in this document. This allows for support of local and

sustainable development so that Member States have a fair choice of solutions, without excluding products from any institution.

- The most environmentally sustainable options should be pursued to reduce any additional undue harm to the environment.

2.2 Ethical considerations for national use

This section is intentionally left blank and will be included in Release Candidate 2.

2.3 Ethical considerations for cross border use

This section is intentionally left blank and will be included in Release Candidate 2.

2.4 Data privacy principles for a digital vaccination certificate

This section is intentionally left blank and will be included in Release Candidate 2.

3 REQUIREMENTS FOR A SMART VACCINATION CERTIFICATE FOR NATIONAL-LEVEL ADOPTION

This section describes a set of standard functions and capabilities that would be needed in a system to support priority scenarios (Continuity of Care and Proof of Vaccination) and their respective use cases, with descriptions of activity flows, settings and actors, and core data elements. It is anticipated that these use cases will operate within contexts across a broad range of digital health maturity.

3.1 Scope

3.1.1 Priority scenarios of use

The two primary use case scenarios for the SVC are:

Continuity of Care

The vaccination certificate is presented to a medical authority so that the bearer's vaccination status can be considered as part of continuing to provide care to the individual. In this sense, it forms part of the person-centric health record of the individual.

Proof of Vaccination

The vaccination certificate is presented as proof that the bearer has received a vaccination, and this claim can be checked and validated by an interested party.

3.1.2 Out-of-scope

The following uses of a digital solution are out of scope for Release Candidate 1:

- Vaccinations related to diseases other than COVID-19
- Adverse event reporting
- Monitoring and evaluation
- Lab test results
- The format and content of 2D barcodes, other than the barcoded unique vaccination certificate identifiers (UVCI) that is printed on or affixed to the front of an SVC paper card

3.1.3 Dependencies and assumptions

For the purposes of Release Candidate 1, the following dependencies are expected:

- A PHA is able to leverage a national public key infrastructure to:
    - Establish and maintain a country signing certificate authority (CSCA) that anchors the country's public key infrastructure (PKI)
    - Generate and cryptographically sign the Document Signer (DS) PKI certificates
    - Leverage Document Signer private keys to generate and cryptographically sign UVCIs (to be pre-printed on SVC paper cards) and to cryptographically sign the digital SVC documents persisted to the SVC Registry.

    - Broadly disseminate public keys
    - Manage a master list of public keys and other PKI artefacts necessary to support participation in a global trust network
- A health worker is able to ascertain the identity of a subject of care, as per the norms and policies of the PHA. The SVC is not an identity.
- The SVC is not digitally verifiable until the core data set related to a vaccine administration event is captured to a PHA database and a signed SVC document is persisted to the SVC Registry.
- It is assumed that a subject of care's SVC can be searched for and retrieved based on the demographic and vaccine event details (such as to find and reprint a lost or damaged paper card).
- Subsequent vaccine administration events logged to the same SVC paper card will be added as new entries to the signed SVC document on the SVC Registry that is referenced by the SVC paper card's UVCI.

3.1.4 Constraints

For RC1, the following constraints are imposed:

- Where a subject of care receives COVID-19 vaccinations outside of their home country, it is the responsibility of the foreign PHA to issue the subject of care an SVC which faithfully records the vaccine administration details. A PHA-signed SVC document will not contain vaccine administration details from outside the jurisdiction of the issuing PHA.

3.2 Key settings, actors, and their roles

The Continuity of Care and Proof of Vaccination scenarios are expected to involve a few primary, typical settings with a set of human and non-human (such as systems) actors involved at those settings, as described in this section.

For the Continuity of Care scenario, it is expected that there will be two key settings:

1. the **Care Site**, where the vaccination event will take place; and
2. the **Public Health Authority (PHA)**, under whose responsibility the vaccination is performed and the SVC is issued.

At the Care Site setting, there are the following human and non-human actors:

- the **Subject of Care**, who receives the vaccination;
- the **SVC Holder** is the one who has the subject of care's vaccination certificate (it is *usually* the subject of care, but not always – for instance, a caregiver may be the SVC holder for a child);
- the **Health Worker** who administers the vaccine;
- optionally, a **Digital Health Solution** such as an electronic immunization registry (EIR) or an electronic medical record (EMR) solution.

At the PHA setting, there are the following human and non-human (e.g. software systems) actors:

- **Data Entry Personnel**, who enter core data set content (after the fact) that has been manually recorded by Care Sites that do not have a digital health solution in place;
- the **Shared Health Record (SHR)** repository, that is able to persist health data about the subject of care that is, potentially, a superset of the content in the SVC core data set; and
- the **SVC Registry**, where a verifiable, digitally-signed copy of the SVC document is persisted.

For the Proof of Vaccination scenario there are expected to be four key settings:

1. the **Verification Site**, where it is necessary to prove one's COVID-19 vaccination status (such as at a care site, a school, or an airport);
2. the **National PHA**, which has the overall responsibility for vaccinating the country's population and is the maintainer of the SVC Registry.
3. the **WHO Public Key Directory**, which is a quality-controlled, global master list of public keys, revocation lists, and internet endpoints that operationalize the trust network between Member States' PHAs;
4. an **International PHA**, that may have been the issuer of an out-of-country SVC being presented at the verification site.

At the Verification Site setting, there are the following three human and non-human actors:

- the **SVC Holder**, who wishes to assert a claim related to COVID-19 vaccination status;
- the **Verifier**, who wishes to verify the claim;
- optionally, an ICT solution which acts as a **Status Checker** that can inspect and cryptographically verify digital credentials;

At the National PHA setting, the SVC Registry is employed to maintain the documents of record for SVCs it has issued. To support verification of credentials that were issued outside the country, a National PHA may make a status request to another country's PHA's SVC Registry. The mechanics of the trusted transaction (the keys and endpoints) are provided to each PHA by the WHO Public Key Directory. Each PHA is responsible for managing its own national public key directory (NPKD) and other aspects of its public key infrastructure (PKI).

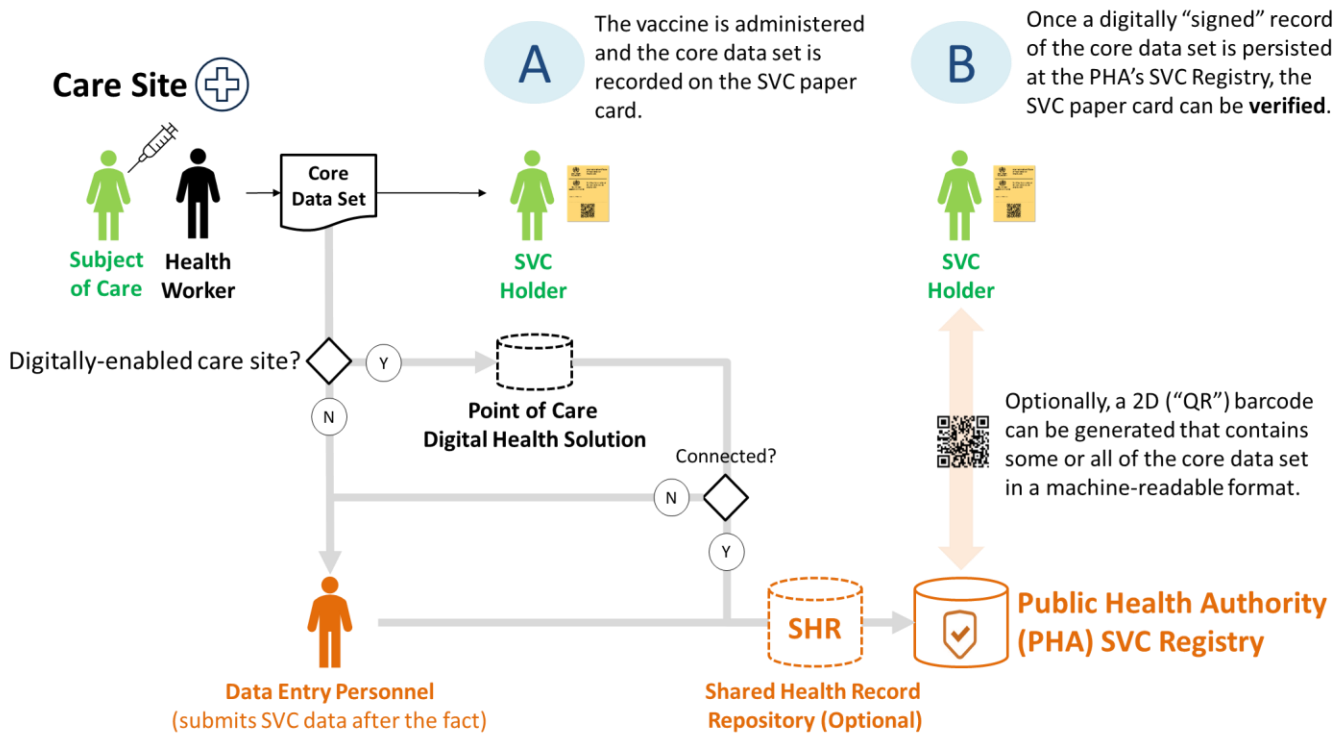
As an important point of clarification – the preceding definitions are expected to be generic workflow actors and workflow settings. Within a specific care delivery network, there may be a hierarchy of occupational groups, such as supervising physicians, nurse practitioners, other nurses, community health workers etc. The Health Worker role, identified above, is intended to generically define an individual that provides the vaccination service. It is intended to describe the role at a generic level to describe the workflow. Likewise, a Care Site may be a temporary vaccination clinic, or it may be a health facility within a larger provider network. These details are not expected to be germane to the workflow descriptions, as they have been framed.

3.3 Continuity of Care

The Continuity of Care scenario is illustrated, at a summary level, in Figure 5. The workflow's actors and settings, and its related high-level requirements, may be described as follows:

- A **Subject of Care** presents at a **Care Site** to receive a **COVID-19 Vaccine** administered by a **Health Worker**.
- The details of the vaccination event SHALL be recorded and persisted according to the Smart Vaccination core data set, or some superset of this specification.
- The care site MAY have a local **Digital Health Solution** (such as an electronic immunization registry or an electronic medical records solution).
- The core data set content SHALL be expressed on the SVC paper card which SHALL have a UVCI. The holder of the SVC paper card is an **SVC Holder** (this is represented at point A).
- The SVC core data set SHALL be electronically captured and shared with the **PHA**, who MAY persist the content to a **SHR** repository. Possibly leveraging the content persisted to the SHR, or leveraging directly uploaded core data set content, the PHA SHALL persist a cryptographically signed SVC document to the **SVC Registry**.
- After the cryptographically signed content is persisted to the SVC Registry, the holder of the SVC paper card and/or a machine-readable version of the SVC, is the holder of a verifiable SVC (this is point B).
- A **PHA** MAY generate one or more 2D ("QR") barcodes representing the SVC core data set, or some subset of it that supports **selective disclosure**. Such QR codes MAY be downloadable by an authenticated subject of care or by a health worker who MAY subsequently print or affix one or more QR codes on a subject of care's SVC paper card or onto a paper insert.

Figure 5. Continuity of Care scenario



SVC: smart vaccination certificate; SHR: Shared Health Record

3.3.1 Continuity of Care use cases

Navigating through the simple workflow diagram shown in Figure 5, there are three possible care pathways. The navigation of the three pathways defines the three use cases related to the Continuity of Care scenario, as listed in Table 1.

Table 1. Continuity of Care use cases

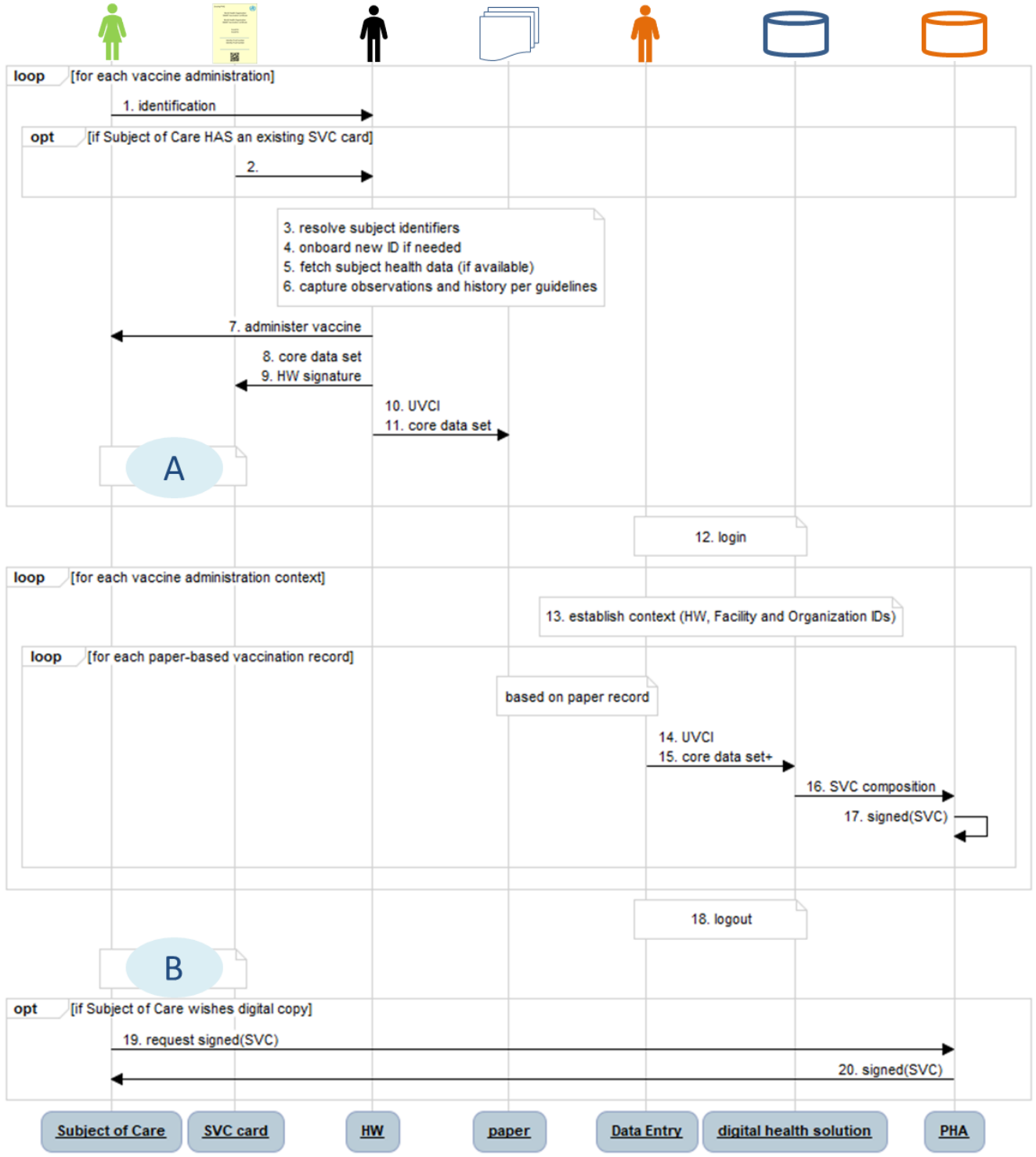
Use case ID	Use case name	Use case description
UC001	"Paper first"	A guideline-based vaccine administration is recorded entirely on paper, with the digital content captured later (as a "back data entry" workflow) and uploaded to the Public Health Authority (PHA).
UC002	Offline digital health	A guideline-based vaccine administration is recorded using an offline digital health solution with the content uploaded, subsequently, to the PHA.
UC003	Online digital health	A guideline-based vaccine administration is recorded using an online digital health solution which updates the content, in real time, to the PHA.

There is significant overlap between these three use cases – and because of its role as the most "basic case", the workflows for UC002 and UC003 may be defined entirely in terms of the steps in UC001. For this reason, only UC001 is explored in detail in this section.

The "paper-first" Continuity of Care workflow is illustrated by Figure 6. The participants in this sequence diagram, listed from left to right, are:

- the Subject of Care;
- the SVC paper card;
- the Health Worker;
- the paper register at the care site;
- the Data Entry Personnel;
- the Digital Health Solution (e.g. the PHA's EIR, or SHR repository); and
- the PHA's SVC Registry.

Figure 6. "Paper-first" Continuity of Care scenario sequence diagram



SVC: smart vaccination certificate; HW: health worker; UVCI: unique vaccination certificate identifier; PHA: public health authority smart vaccination certificate registry.

The sequence diagram steps, and the requirements related to these, are described in Table 2.

501 *Table 2. Paper-first sequence diagram steps and associated requirements*

For each vaccine administration:	
Identification	1. The identity of the subject of care SHALL be established as per Member State processes and norms. 2. The subject of care MAY present an existing SVC card to inform the care delivery process. 3. The health worker MAY resolve the subject of care's identity to one or more unique IDs (such as a passport number, a national ID, etc.).
On the paper register	4. The health worker MAY establish a new ID for the subject of care. Note: Even if no "wallet ID" is created and provided to the subject of care, there SHALL be a system-generated patient ID associated with the subject of care's SVC. 5. The health worker MAY retrieve existing health history data about the subject of care. 6. As per PHA-published guidelines, the health worker SHALL record the subject of care's pertinent health data related to the vaccine administration (e.g. allergies, pregnancy status, etc.).
Care event	7. As per the PHA-published guidelines, the health worker administers the vaccine.
On the SVC card	8. The health worker SHALL record the core data set on the SVC card. 9. The responsible health worker SHALL sign the SVC card as per applicable Member State and IHR regulations.
On the paper register	10. The health worker SHALL record the UVCI of the subject of care's SVC. 11. Associated with the UVCI, the health worker SHALL record the SVC core data set, along with other pertinent health data.
In the digital health solution	12. The data entry personnel SHALL securely login and authenticate to the digital health solution.
For each care delivery session *of the context:*	
	13. The facility, organization, and care-delivery health worker context of the vaccine administration event SHALL be established.
For each vaccine administration event *in the context:*	
Data entry	14. The UVCI SHALL be used to establish a globally unique identifier for the digital SVC Document or to reference the identifier of a previously established digital SVC Document. 15. The health data captured during the vaccine administration event SHALL be recorded as coded content within this FHIR Composition; this content MAY represent a superset of the health data recorded on the paper SVC card. If the data represents a subsequent vaccination event, this content SHALL be added as another event to the same FHIR Composition.

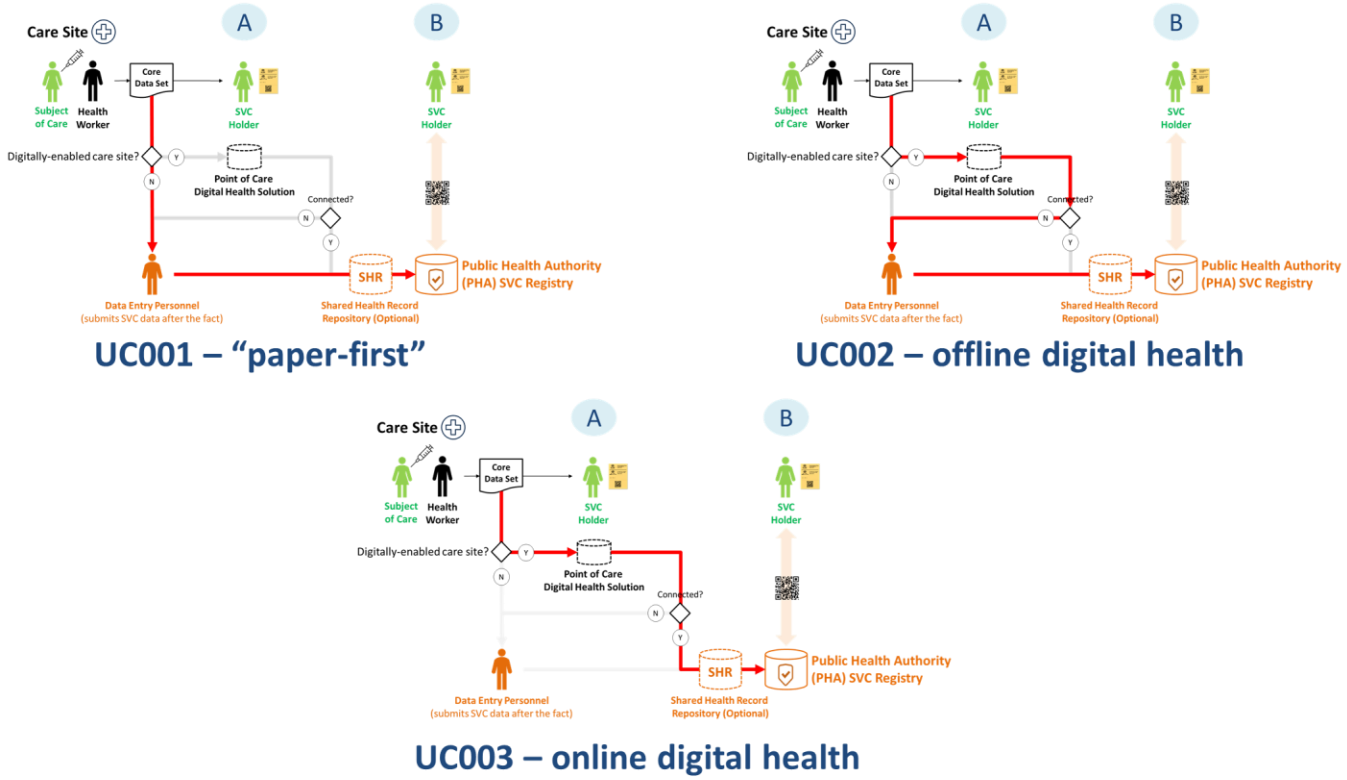
	16. The subset of the FHIR composition that corresponds to the SVC core data set SHALL be generated as a FHIR document and submitted to the PHA SVC-signing webservice. 17. The PHA SVC-signing webservice SHALL digitally sign the SVC FHIR Composition and persist this signed artefact. The webservice MAY generate one or more 2D barcodes representing the SVC. 18. At the conclusion of data entry, the data entry personnel SHALL log out of the secure digital health solution.
***Optional steps (if supported):**	
Digitally signed SVC	19. The subject of care MAY leverage a secure PHA webservice to request a digital copy of a signed SVC. 20. If the subject of care is authenticated by the PHA webservice, and authorized to obtain the requested SVC, the PHA service MAY return a digital copy of a signed SVC.

3.3.2 Discussion of Continuity of Care scenario workflow variations and implications

Figure 7 illustrates, graphically, the three workflow navigation paths. In the diagram, point **A** represents the point in time when the subject of care has completed their vaccination encounter and point **B** represents the point when they will have a *verifiable* SVC card. From this illustration, a number of comparisons and implications may be noted:

- In both UC001 – "paper first" and UC002 – offline digital health, there will be a time delay between point **A** and point **B**.
- For UC002 – offline digital health, and UC003 – online digital health, some steps would be executed in the **Digital Health Solution** rather than in the paper register (workflow steps 4, 5, 6, 10 and 11 in Table 2).
- UC001 – "paper first" relies on the SVC card being pre-printed with a cryptographically signed UVCI barcode. It is expected the content on the SVC card will be handwritten. For UC002 and UC003, it may be possible to print the SVC core data set content on the card at the time of the vaccination event.
- For UC003 – online digital health, it is possible to print the core data set content and the cryptographically signed UVCI barcode on the SVC card at the time of the vaccination event. For this workflow, there is no delay between point **A** and **B**. Release Candidate 2 of this specification will provide more detail about possible options to print barcoded content on the SVC card besides just the UVCI.

Figure 7. Continuity of Care scenario variations



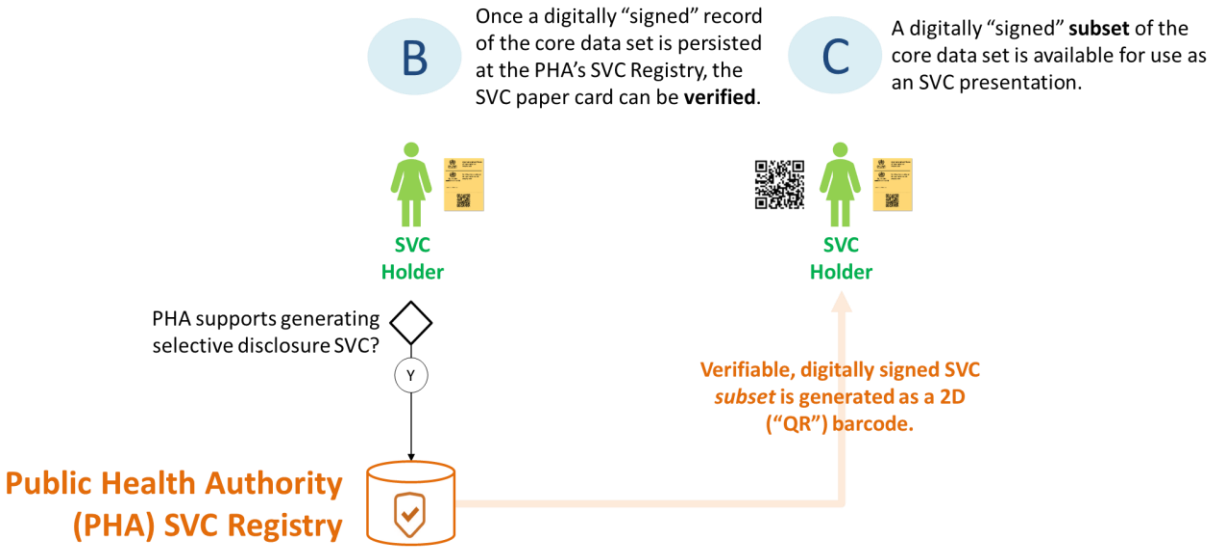
3.4 Proof of vaccination

The Proof of Vaccination scenario relies on the PHA having established and synchronized the national public key directories with the global WHO Public Key Directory. The processes around this are described in Section 5.

3.4.1 Selective Disclosure

The Proof of Vaccination scenario, supports the optional generation of a selective disclosure version of the SVC by the PHA, potentially as a 2D barcode, as described in steps 19 and 20 in Figure 6. This option, UC005, is illustrated by Figure 8. In this option, if a PHA offers the capability to do so, a verifiable SVC Holder (point **B**) MAY request from the issuing PHA a selective disclosure version of their SVC (point **C**); this MAY be a privacy-preserving subset of the SVC core data set.

Figure 8. Optional selective disclosure workflow

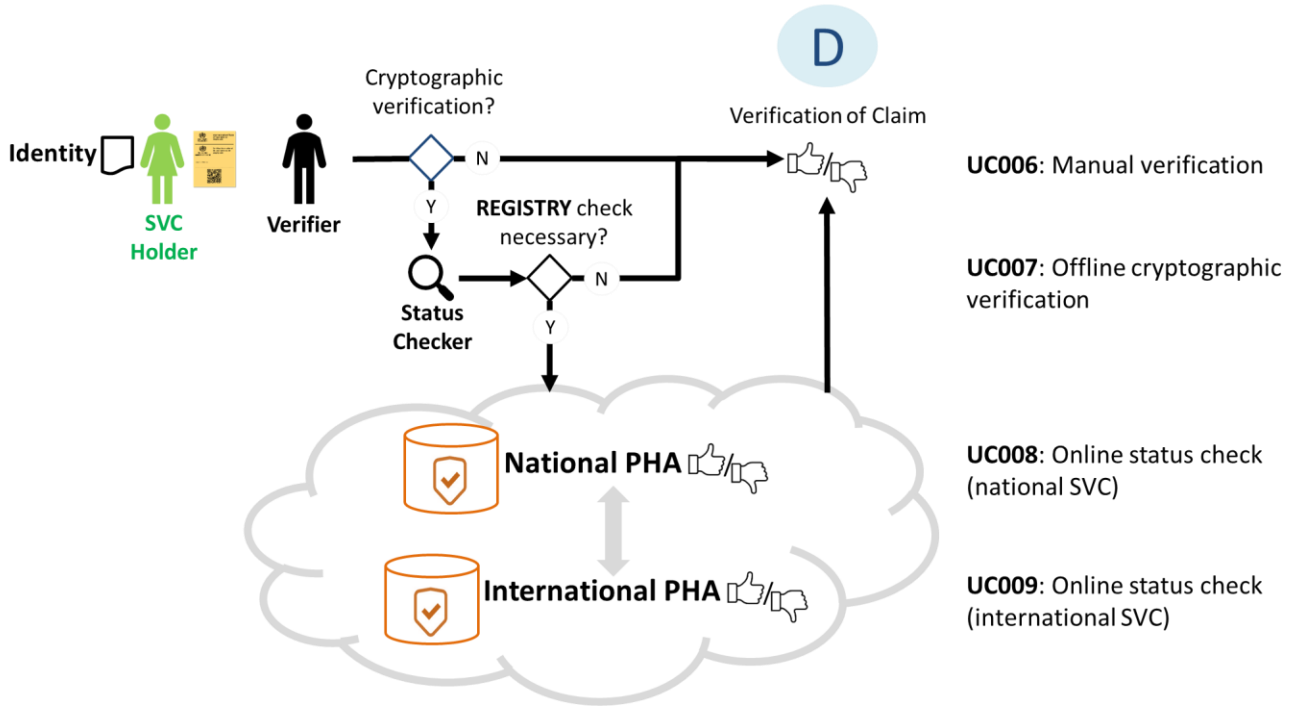


3.4.2 Verification of a Claim

The verification of a claim of vaccination is illustrated in Figure 9. The workflow's actors and settings, and its related high level requirements, may be described as follows:

- An **SVC Holder**, who MAY have a separate identity proofing document, presents to a **Verifier** an SVC in support of a claim of vaccination status.
- To verify the COVID-19 vaccination claim of a *verifiable* SVC Holder (point **D** in Figure 9):
    - a Verifier MAY choose non-cryptographic verification (UC006).
    - a Verifier MAY have a **status checker** application that can cryptographically verify an SVC (UC007) *without* executing an external status check.
    - a Verifier MAY execute a transaction against the **national PHA** to do a status check of a nationally-issued SVC (UC008).
    - a Verifier MAY execute a transaction against the **national PHA** to do a status check that must be communicated to an **international PHA** to check an internationally-issued SVC (UC009).

Figure 9. Verification of a claim of vaccination



3.4.3 Proof of Vaccination use cases

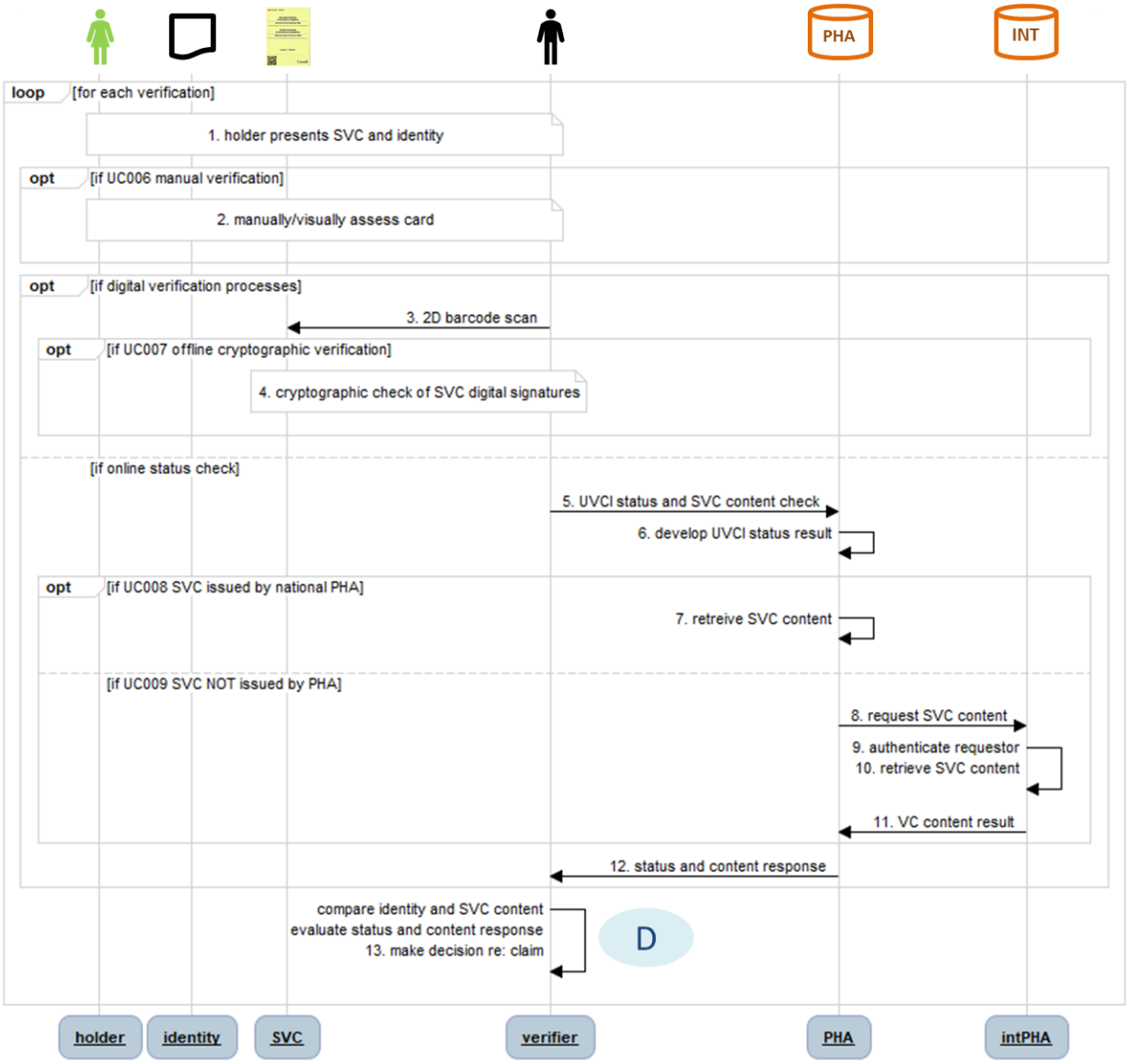
Navigating through the simple workflow diagram shown in Figure 9,, there are four possible verification pathways. The navigation of these pathways defines the four use cases related to the Proof of Vaccination scenario; these are listed in Table 3.

Table 3. Proof of Vaccination use cases

Use case ID	Use case name	Use case description
UC006	Manual verification	A verifier verifies an SVC using purely manual (visual) means.
UC007	Offline cryptographic verification	A verifier verifies an SVC, using digital cryptographic processes, in an offline mode.
UC008	Online status check (national SVC)	A verifier verifies an SVC, using digital cryptographic processes, in an online mode that includes a status check against the public health authority's SVC Registry.
UC009	Online status check (international SVC)	A verifier verifies an internationally issued SVC, using digital cryptographic processes, in an online mode that includes a status check against the national public health authority's SVC Registry, which in turn accesses the international public health authority's SVC Registry.

The Proof of Vaccination sequence diagram that operationalizes the four Proof of Vaccination use cases is illustrated by Figure 10. The participants in this workflow, listed from left to right, are the **SVC holder**, the SVC holder's **identity** document, the **SVC** paper card, the **Verifier**, the **PHA's** SVC Registry, and the international PHA's SVC Registry.

Figure 10. Proof of Vaccination sequence diagram



SVC: smart vaccination certificate; UVCI: unique vaccination certificate identifier; PHA: public health authority smart vaccination certificate registry; INT/intPHA: international public health authority smart vaccination certificate registry.

The workflow steps, and the requirements related to these, may be described as follows:

1. The SVC Holder SHALL present her SVC plus whatever additional proof of identity is appropriate in the context of the claim (it is expected the SVC SHALL NOT be an identity).
2. A Verifier MAY visually verify an SVC. (UC006)
3. A Verifier MAY scan a machine-readable (2D barcode) of the SVC's UCVI or entire core data set.

4. A Verifier MAY verify an SVC based on the scanned 2D barcode, without a network status check. (UC007)
5. A Verifier MAY execute a status check of an SVC by submitting a transaction to the national PHA.
6. For authorized Verifiers, a PHA SHALL develop a cryptographic status result for a submitted UVCI.
7. A PHA SHALL retrieve content for SVCs it has issued, based on its disclosure policies. (UC008)
8. A PHA MAY request SVC content from the international PHA that issued the SVC.
9. An international PHA SHALL authenticate requesting PHAs.
10. An international PHA SHALL retrieve SVC content for SVCs it has issued, based on its disclosure policies.
11. An international PHA SHALL return the SVC content to the authenticated requesting PHA, based on the international PHA's disclosure policies. (UC009)
12. The PHA SHALL return to the requesting Verifier the UVCI status and SVC content response, based on its disclosure policies.
13. The Verifier SHALL decide on the claim (denoted by point **D** on Figure 10)

3.4.4 Discussion of Proof of Vaccination scenario workflow variations and implications

From Figure 10, several comparisons and implications may be noted:

- Although it may seem counterintuitive, the most common verification workflow for SVCs may be a purely manual (visual) check of the card. This workflow matches the workflow used, presently, for existing International Certificate of Vaccination or Prophylaxis (ICVP) cards. Notwithstanding its shortcomings compared to the digitally supported SVC workflows, this simple process is well accepted and is quick and easy to do.
- When doing offline verification of a paper SVC card, the verifier can cryptographically confirm that the UVCI barcode on the card has not been altered and that it was cryptographically signed under the responsibility of the PHA.
- In a selective disclosure situation, or in any case where a machine-readable version of the SVC has been generated and signed and downloaded by the SVC Holder, this downloaded barcode may be verified in an offline mode (as long as the verifier has, locally, a recently synchronized public key database and revocation list).
- Online verification can support content-verification of paper-first SVCs and can also check whether signed barcodes containing SVC content may have become "stale".
- It is expected that a verifier does not ever *directly* access an international PHA. In cases where an international SVC must be verified online, the query is executed, on behalf of the verifier, by the national PHA.
- This release of the specification does not describe normative SMS-based interactions that may be leveraged to verify SVCs. It is anticipated that such a workflow would be valuable in addressing equity challenges and could potentially have implications regarding the format of UVCIs that are SMS "friendly" (for example, purely numeric).

3.5 Core data set

To develop the core data set, the analysis phase mapped data requirements under the International Health Regulations *(12)*, WHO Home-based records guidance *(5)*, WHO AEFI reporting requirements *(13, 14)*, and WHO immunization programme monitoring guidance *(1)*. The core data set has been further informed by analysis of existing digital vaccination certificates currently deployed in a number of countries and pre-existing standards for digital vaccination certificates.

Furthermore, in establishing the core data set, the following key principles were used to specifically guide the formulation of the recommended data elements:

1. Data minimization. Aligned with the principle of privacy protecting, only the bare minimum set of data elements for documenting a vaccination event should be collected. Each data element must have a purpose in accordance to the predefined use cases. This is especially important for personally identifiable information (PII).

2. Open standards. Aligned with the principle of accessibility, proprietary terminology code sets or proprietary standards cannot and will not be recommended to Member States.
3. Balance between digital and paper. Aligned with the principle of equity, data requirements should not increase inequities or put individuals at risk. Additionally, data input requirements should be feasible on paper but take advantage of the benefits of digital technology.
5. Not all data needs to be in the vaccine certificate. Aligned with the principle of capability, flexibility and sustainability, the vaccination certificate is intended to be part of a much larger ecosystem of immunization information systems which include:
    a. EIRs (such as OpenSRP *(15)*)
    b. Reporting systems for vaccine coverage monitoring (such as DHIS2 *(16)*)
    c. AEFI reporting systems (such as Vigiflow *(17)*)

To underscore the importance of the ability to implement, the data content model for the SVC core data set has been developed as a standards-conformant, HL7 FHIR Implementation Guide (IG). This Smart Vaccination Certificate Implementation Guide (SVC IG)[3] *(18)* is, itself, based on the widely adopted IPS health data content model and the HL7 FHIR IPS IG *(19)* that normatively documents it.

As a WHO-published specification, the SVC IG references ICD-11 *(20)* as the SVC's normative base code system. Use of ICD-11 addresses important requirements, such as that: the ICD-11 codes satisfy the SVC's primary use scenarios; the ICD-11 code system is multilingual and "digital-ready"; and, as the custodian of the WHO Family of International Codes (WHO-FIC) as a freely-available global public good, WHO is able to ensure all Member States can benefit from the implementable SVC specification. In recognition of its strong uptake by some Member States, the SVC IG also includes a one-to-one map between relevant ICD-11 codes and the functionally equivalent code in the SNOMED Global Patient Set (GPS) *(21)*.

[3] The SVC IG can be found linked here: https://who-int.github.io/svc

3.5.1 Recommended core data set

The recommended core dataset is intended to reflect the critical data requirements for interoperability, driven by the public health need. There are three key sections to the core dataset that include:

1. Header
2. Data elements for each vaccination event
3. Vaccine certificate metadata (to be provided in Release Candidate 2)

The header section data elements reflect the Subject of Care's demographic information (Table 4). The header section is intended to capture information about the vaccinated individual to allow for information on the vaccination event to be linked to a specific person. This data should remain the same regardless of which vaccination a person has received, thus it should only be collected once.

Table 4. Header section of the SVC with preferred code set

Data element	Description	Requirement status	Data type	Preferred code set
Name	The full name of the vaccinated person	Required	String	Not applicable
Date of birth	The individual's date of birth (DOB) if known. If unknown, use given DOB for administrative purposes. The full format of DD MM YYYY is required if known.	Required - If known	Date	Not applicable
Unique identifier	Unique identifier for the vaccinated person, according to the policies applicable to each country. There can be more than one unique identifier used to link records. (e.g. national ID, health ID, immunization information system ID, medical record ID).	Optional - Recommended	ID	Not applicable
Sex	Documentation of a specific instance of sex information for the vaccinated person.	Optional - Recommended	Coding	As defined by Member State

The **data elements for each vaccination event** outlines data that needed to have been collected for each vaccination the vaccinated person received (Table 5). For each dose, all of the data elements in Table 5 would be required to have been recorded. On a paper form, this is equivalent to a separate "row" on a vaccination certificate that is then repeated for each vaccination received.

Table 5. Data required for each vaccination transaction with preferred code set

Data element	Description	Requirement status	Data type	Preferred code set
Vaccine or prophylaxis	Generic description of the vaccine or vaccine sub-type. e.g. Covid-19 mRNA vaccine, HPV vaccine.	Required	Coding	ICD-11

Data element	Description	Requirement status	Data type	Preferred code set
Vaccine brand	The brand or trade name used to refer to the vaccine received.	Required	Coding	As defined by Member State
Vaccine manufacturer	Name of the manufacturer of the vaccine received. e.g. Serum institute of India, AstraZeneca. If the *vaccine manufacturer* is unknown, *vaccine market authorization holder* is REQUIRED.	Required – Conditional	Coding	As defined by Member State
Vaccine market authorization holder	Name of the market authorization holder of the vaccine received. If *vaccine market authorization holder* is unknown, then *vaccine manufacturer* is REQUIRED.	Required – Conditional	Coding	As defined by Member State
Vaccine batch number	Batch number or lot number of the vaccine.	Required	String	Not applicable
Date of vaccination	Date in which the vaccine was provided.	Required	Date	Not applicable
Dose number	Vaccine dose number.	Required	Integer quantity	Not applicable
Country of vaccination	The country in which the individual has been vaccinated.	Required	Coding	ISO 3166
Administering centre	The name or identifier of the vaccination facility responsible for providing the vaccination.	Required	Coding	As defined by Member State
Signature of health worker	REQUIRED for PAPER vaccination certificates. The health worker who provided the vaccination or the supervising clinician's hand-written signature.	Required – Conditional	Signature	Not applicable
Health worker identification	REQUIRED for DIGITAL vaccination certificates. The unique identifier for the health worker as determined by the Member State. There can be more than one unique identifier used. (e.g. system generated ID, health profession number, cryptographic signature, or any other form of health worker unique identifier). This is to be used in lieu of a paper-based signature.	Required - Conditional	ID	Not applicable
Disease or agent targeted	Name of disease vaccinated against (such as COVID-19)	Optional - Recommended	Coding	ICD-11
Due date of next dose	Date on which the next vaccination should be administered	Optional - Recommended	Date	Not applicable

ICD-11: International Classification of Diseases 11th edition; ID: identifier.

The **vaccine certificate metadata** contains data elements that are not visible to the user, but that are required to have linked to the certificate itself (to be provided in release candidate 2)

3.5.2 Preferred code set

The WHO constitution and nomenclature regulations mandate ICD and other WHO standards to be produced by the Organization that serve as a common language in core areas of health information.

Hence, WHO recommends the use of ICD-11 as the health data content standard in the WHO Smart Vaccination Card. ICD-11 is the preferred content standard as ICD-11 is:

- A global public good that is completely free and available for all to use in its entirety. No additional costs will be required to access any additional parts of the code set.
- Kept clinically updated through an open, public and transparent maintenance process.
- Able to provide comprehensive content coverage and granularity required for data fields in individual-level systems, including the SVC.
- Easy to integrate into software systems via a public API for use in all settings, without additional tooling. This is due to ICD-11's digital and multilingual structure.
- Human-readable and machine-readable.

As WHO Member States adopted ICD-11 for morbidity and mortality reporting globally, ICD-11 provides the most suitable and future proof semantic interoperability standard. ICD-11 implementation has already started, and it will become mandatory in January 2022. With this said, however, WHO will provide technical guidance (i.e. identifying crosswalks and mapping principles) for use with legacy systems as part of the ICD-11 implementation support, for ICD-10 or other used freely available classifications and terminologies (such as Anatomical Therapeutic Chemical, ATC, SNOMED CT GPS, etc.).

For guiding principles for WHO Family of International Classifications (WHO-FIC) and other classifications and terminology mapping in the context of the WHO SVC, please refer to Annex 1.

3.6 Requirements

This section provides an overview of the functional and non-functional requirements of an SVC. Functional requirements describe the capabilities the system must have in order to meet the end-users' needs and achieve tasks within the business process *(22)*. Example of a functional requirement is that the SVC must be able to provide the ability for an individual to selectively disclose parts of their SVC. Non-functional requirements provide the general attributes and features of the digital system to ensure usability and overcome technical and physical constraints *(22)*. Examples of non-functional requirements include ability to work offline, multiple language settings and password protection. It is expected that the narrative descriptions provided in the preceding sections may be distilled into a set of normative functional and non-functional requirements.

3.6.1 Functional requirements

This section is intentionally left blank and will be included in Release Candidate 2.

3.6.2 Non-functional requirements

This section is intentionally left blank and will be included in Release Candidate 2.

4 National SVC Architecture

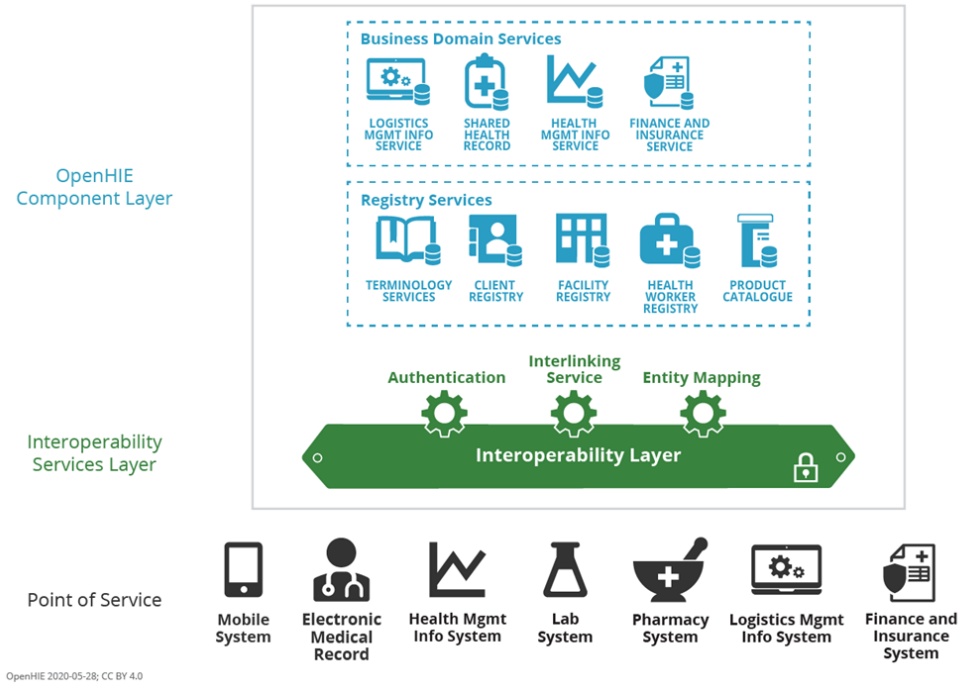
Member States are at different levels of digital health maturity and investment. There is an expectation that, where digital health infrastructure and/or public key infrastructure (PKI) has already been deployed, this infrastructure may be leveraged to support the SVC workflows described in Section 3.

This section describes, in generic terms, a notional health enterprise architecture based on the Open Health Information Exchange (OpenHIE) specification. The registries and repositories, defined in the OpenHIE specification, that are relevant to SVC workflows are identified. A high-level description is given of conformance-testable, standards-based transactions that may be employed to leverage these digital health assets in support of the SVC workflows. Although the transaction processing for populating an SVC Registry is part of the scope of a national SVC architecture, the public key infrastructure that would support this is described as part of the overall global architecture description provided in Section 5.

4.1 Architectural blueprint

If digital health solutions are employed in real time during the vaccine administration event, it is anticipated that complementary digital health infrastructure, such as the architectural elements described by the **OpenHIE** specifications *(23)*, could be leveraged. The OpenHIE high-level architecture is shown in Figure 11.

Figure 11. OpenHIE architecture



Source: OpenHIE.org *(24)*.

This section illustrates how standards-based, health data sharing infrastructure could support point of care digital health solutions. To show this, a set of digital health interactions are described in terms of the conformance-testable IHE specifications *(25)* referenced by the OpenHIE specification.

4.2 Recommended registries

The registries and repositories defined in the OpenHIE architecture (Figure 11) may play a role in providing data that are part of the SVC core data set defined in Section 3.5. These include:

Client registry: A demographic database that contains definitive information about each subject of care. These data can include the subject of care's name, date of birth, sex, address, phone number, as well as other person-specific information such as parent-child or caregiver relationships, family clinician relationships and consent directives. It is also in the client registry that the list of unique identifiers for a particular Subject of Care can be found (e.g. health ID#, driving license number, passport, etc.). The data in the client registry that relates to the SVC core data are:

- Name (required)
- Date of birth (required if known)
- Sex (optional, recommended)
- Unique identifiers (optional, recommended)

Health worker registry: A demographic database of health worker information, including data such the name, sex, address, phone number, date of birth, and qualifications (including cadre, authorizations of practice, etc.). The health worker registry will also reference unique health worker identifiers that may have been issued by a PHA or by care delivery organizations or facilities. The data element in the health worker registry that relates to the SVC core data set is the health worker identifier.

Facility registry: A database of facility information including data such as the facility name, its PHA-issued unique identifier, the organization under whose responsibility it operates, its location (by address and/or GPS coordinates), its type, its hours of operation and the health services it offers. The data in the facility registry that relates to the SVC core data set is the facility name or unique identifier (which is to be represented in the Administering centre data element) and the country.

Shared health record (SHR) repository: Maintains longitudinal health information about each subject of care and is leveraged to support care continuity over time and across different care delivery sites. Health data in the SHR can include content such as the subject of care's: medication list, allergies, current problem list, immunization records, history of procedures, medical devices, diagnostic results, a record of vital sign observations, past history of illness, history of pregnancies and current pregnancy status, social history (e.g., smoking habits and alcohol use, etc.), functional status, current plan of care, and advance directives (19). Such health data may be expressed using

health data content standards such as the IPS specification. Data in the SHR can be important for delivering guideline-based care during vaccine administration.

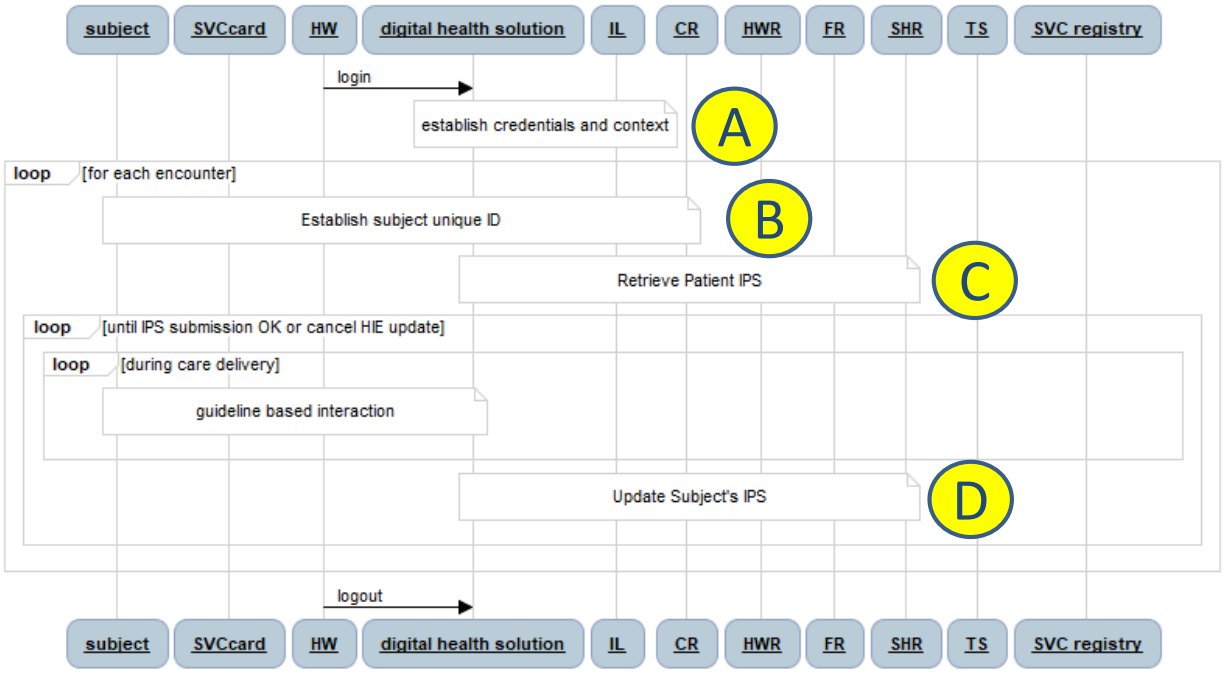
4.3 Standards-based transactions

Where available, existing digital health infrastructure can be employed during the Continuity of Care use cases to facilitate the capturing of SVC core data set content. Specific transaction processing examples include:

A. Establishing the care event context by leveraging the health worker registry and facility registry to identify the health worker and facility identifiers.
B. Retrieving the subject of care's existing demographic record in the client registry, or creating a new record, if needed.
C. Retrieving existing health data about a subject of care from the SHR, if it exists.
D. Updating the SHR with details regarding the vaccine administration event, including the data elements stipulated in the SVC core data set.

As an example, the potential role of these transactions A-D, within the context of the SVC Continuity of Care scenario, is illustrated in Figure 12.

Figure 12. Overview of the role of a national health architecture in supporting the Continuity of Care scenario



SVC: smart vaccination certificate; HW: health worker; IL: interoperability layer; CR: client registry; HWR: health worker registry; FR facility registry; SHR: shared health record repository; TS: terminology service; ID: identifier; IPS: International Patient Summary.

The workflow participant illustrated in Figure 12 are (from left to right): the subject of care, the subject of care's paper SVC card (if they have one), the health worker, and the point of service digital health solution. Carrying on from left to right are the elements of the OpenHIE health information

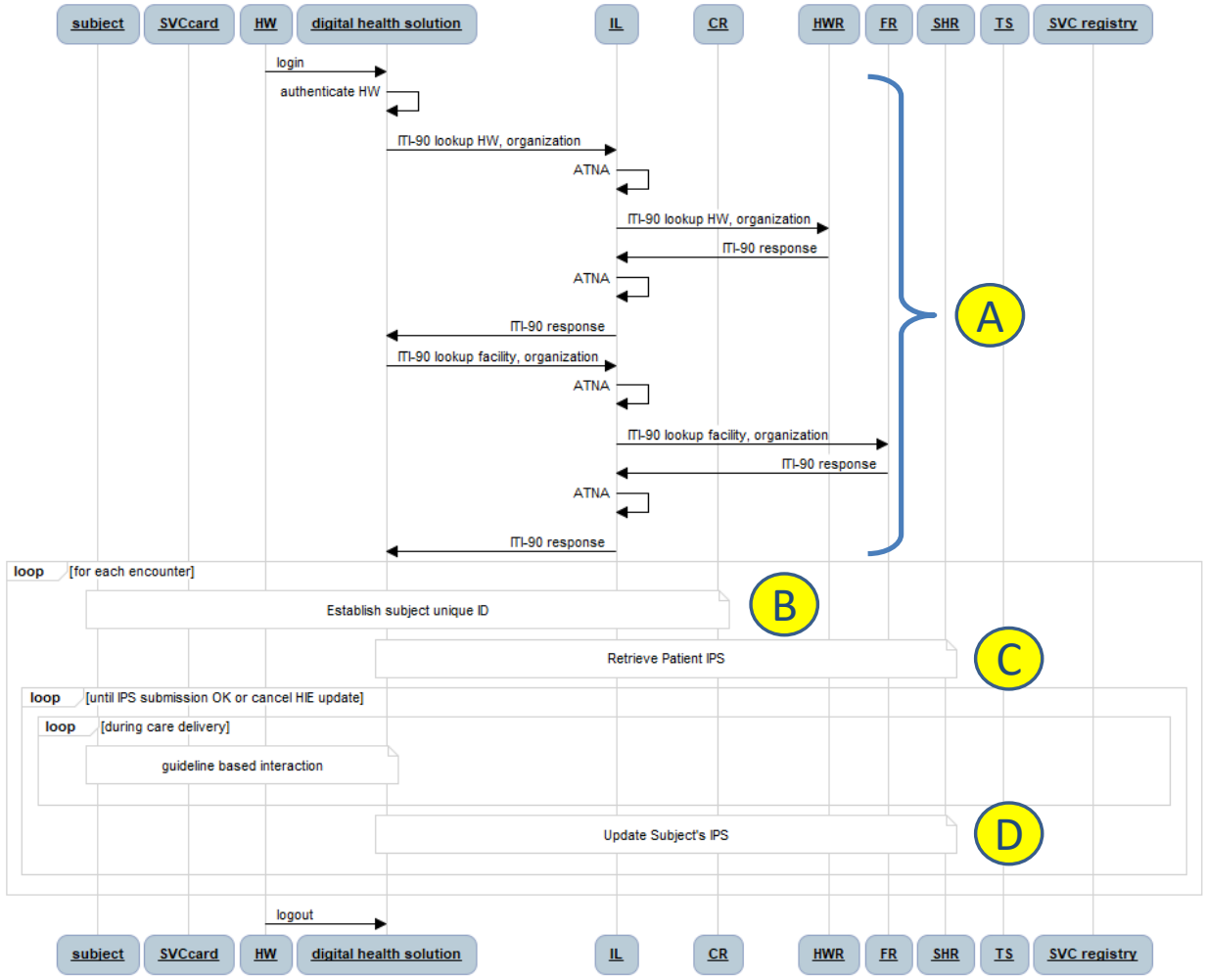
exchange: the interoperability layer, the client registry, the health worker registry, the facility registry, the SHR repository, the terminology service, and the PHA's SVC registry.

At a high level, Figure 12 illustrates:

- A health worker logs into a point of service digital health solution
- The context of the vaccine administration care encounters is established (process **A**)
- For each care encounter:
    - The subject of care's identity is established (process **B**)
    - The subject of care's health history is retrieved from the health information exchange, if applicable (process **C**)
    - The vaccine is administered
    - The subject of care's health history is updated in the health information exchange (process **D**)
- At the end of the care delivery session, the health worker logs out of the digital health solution.

The details related to process A are illustrated in Figure 13.

Figure 13. Process A – establishing the care encounter context



SVC: smart vaccination certificate; HW: health worker; IL: interoperability layer; CR: client registry; HWR: health worker registry; FR facility registry; SHR: shared health record repository; TS: terminology service; ID: identifier; IPS: International Patient Summary.

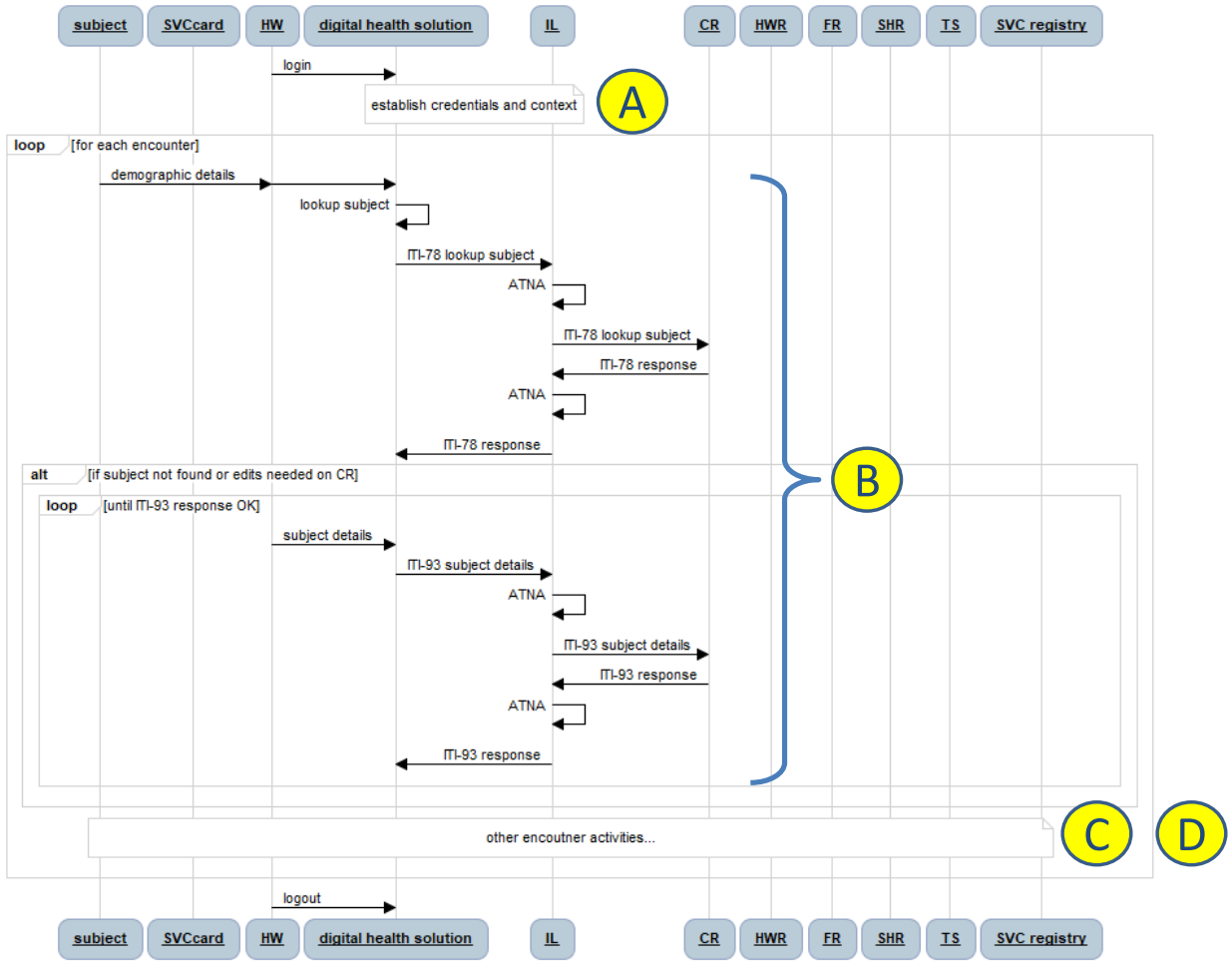
Process A may be described as follows:

- The health worker logs into the digital health solution and is authenticated.
- From the digital health solution, a standards-based transaction is submitted to the interoperability layer to look up the health worker and the organization (IHE transaction ITI-90).
- The interoperability layer creates an audit record (IHE ATNA transaction) and submits the ITI-90 transaction onward to the health worker registry.
- The health worker registry returns an ITI-90 response to the interoperability layer, which the interoperability layer logs in the audit trail (ATNA) and returns onward to the digital health solution.
- This process pattern is *repeated* to retrieve facility and organization data from the facility registry (also using the ITI-90 transaction).

The transactions and their normative patterns are defined in the OpenHIE Architecture Specification *(24)* and in the conformance-testable IHE mobile Care Services Discovery (mCSD) specification *(26)* that OpenHIE references.

The details related to process B are illustrated in Figure 14.

Figure 14. Process B – establishing the subject of care's identity



SVC: smart vaccination certificate; HW: health worker; IL: interoperability layer; CR: client registry; HWR: health worker registry; FR facility registry; SHR: shared health record repository; TS: terminology service; ID: identifier; IPS: International Patient Summary.

Process B may be described as follows:

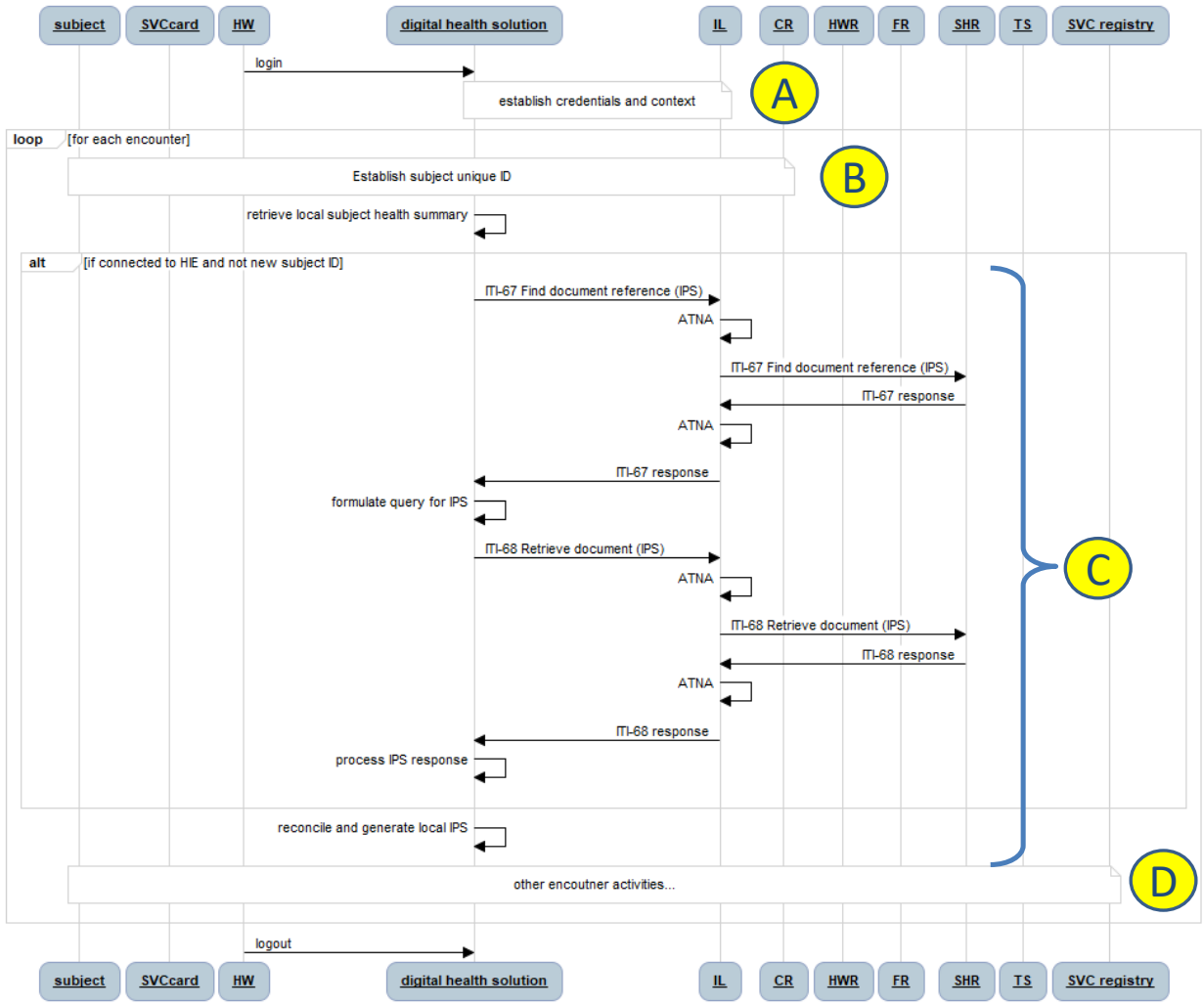
- Process A is executed.
- At the beginning of the care encounter, the subject of care provides demographic information to the health worker who leverages this information to look up the subject of care in the point of service digital health solution. If the subject of care has a unique identifier (such as a health ID#) then this lookup will be "deterministic", and only one record should be matched. If no identifier is available, a "fuzzy search" is made using the demographic details.

- To ensure the most up to date information is leveraged, these details are passed by the digital health solution to the health information exchange's interoperability layer as content in a standards-based IHE ITI-78 query transaction.
- The interoperability layer lays down an audit record (ATNA) and passes the query onward to the client registry. The client registry returns an ITI-78 response which the interoperability layer logs (ATNA) and returns onward to the digital health solution, which ingests the result.
- If the subject of care was not found, or if the details on the client registry need to be updated
    - New or updated demographic details are entered by the health worker into the digital health solution. These details are submitted to the interoperability layer as an IHE ITI-93 transaction.
    - The interoperability layer lays down an audit log (ATNA) and passes the ITI-93 transaction on to the client registry. The client registry is updated with the content and returns an ITI-93 response to the interoperability layer, which lays down an audit log (ATNA) and returns the result to the digital health solution.

These client registry-related transactions and their normative patterns are defined in the OpenHIE Architecture Specification *(24)* and in the conformance-testable IHE Patient Master Identity Registry (PMIR) specification *(27)* that OpenHIE references.

The details related to process C are illustrated in Figure 15

Figure 15. Process C – retrieving the subject of care's health history



SVC: smart vaccination certificate; HW: health worker; IL: interoperability layer; CR: client registry; HWR: health worker registry; FR facility registry; SHR: shared health record repository; TS: terminology service; ID: identifier; IPS: International Patient Summary.

Process C may be described as follows:

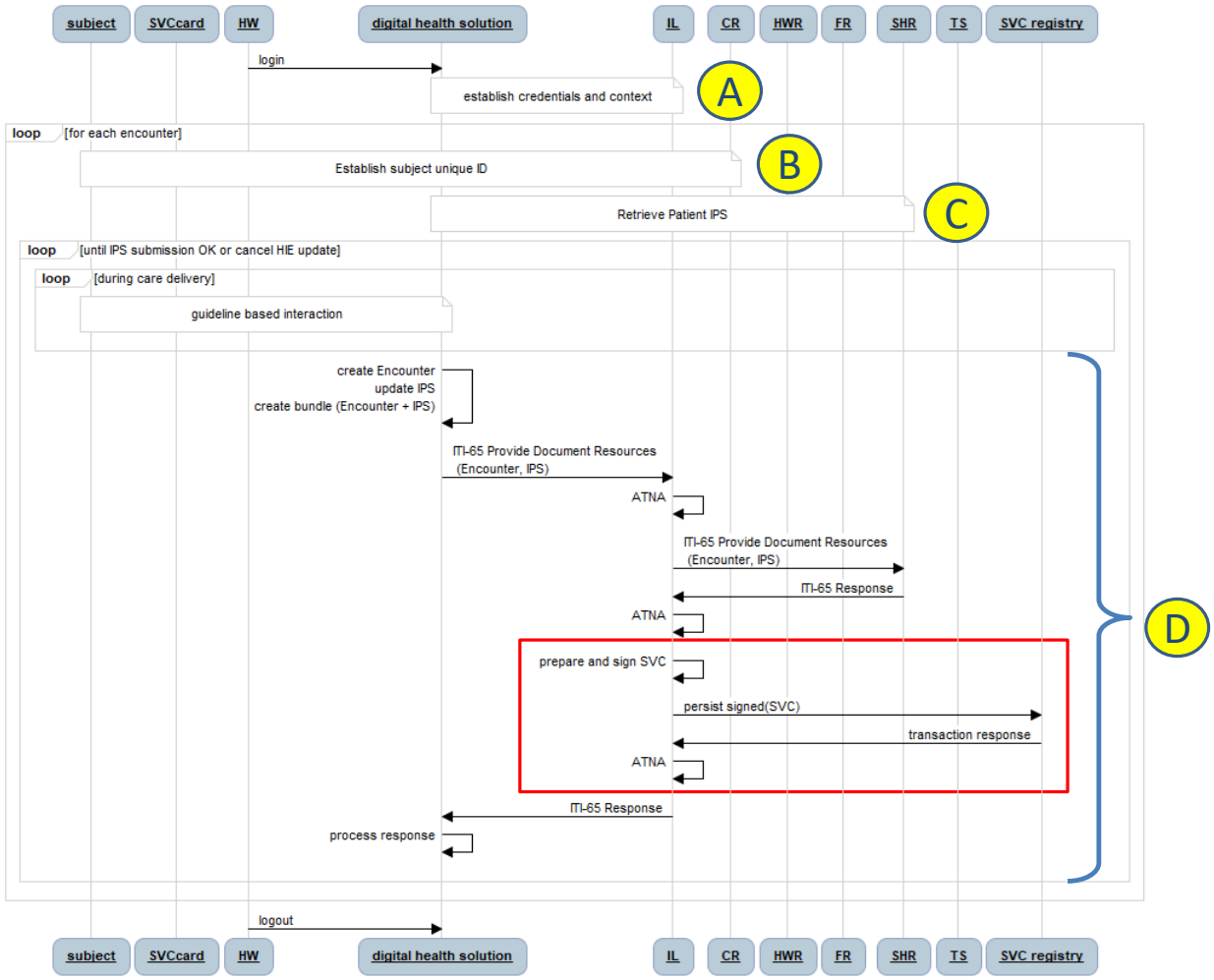
- Process A is executed
- Process B is executed
- If the subject of care had an existing record in the client registry:
    - The client's unique ID is leveraged to look up the reference ID of the subject of care's IPS record. To do this, the digital health solution submits a document ID query IHE ITI-67 transaction to the interoperability layer, which lays down an audit log (ATNA) and passes the query on to the SHR repository.
    - The SHR searches for the subject of care's IPS and returns the document ID in the ITI-67 response to the interoperability layer, which logs the audit record (ATNA) and returns the response to the digital health solution.

- Referencing the document ID, the digital health solution submits a query for the subject of care's IPS to the interoperability layer as an IHE ITI-68 transaction.
- The interoperability layer logs the query (ATNA), passes it to the SHR, which returns the IPS document to the interoperability layer (ATNA) and onward to the digital health solution.
- The digital health solution ingests the subject of care's IPS document.

These SHR-related transactions and their normative patterns are defined in the OpenHIE Architecture Specification *(24)* and in the conformance-testable IHE Mobile Health Document Sharing (MHDS) specification *(28)* that OpenHIE references.

The details related to process D are illustrated in Figure 16.

Figure 16. Process D – updating the subject of care's health history with the SVC core data set



SVC: smart vaccination certificate; HW: health worker; IL: interoperability layer; CR: client registry; HWR: health worker registry; FR facility registry; SHR: shared health record repository; TS: terminology service; ID: identifier; IPS: International Patient Summary.

Process D may be described as follows:

- Process A is executed

- Process B is executed
- Process C is executed
- The vaccine is administered
- The digital health solution creates a data bundle including the details of the care context expressed as a FHIR Encounter resource *(29)* plus the details of the vaccine administration, expressed as an updated version of the subject of care's IPS.
- The digital health solution submits the bundle to the interoperability layer as an IHE ITI-65 transaction.
- The interoperability layer lays down and audit record (ATNA) and submits the bundle to the SHR. The SHR persists the content and returns the ITI-65 response to the interoperability layer, who lays down an audit log (ATNA) record.
- The transactions related to generating and persisting a digitally signed SVC document (described below and boxed in red in Figure 16) rely on a national public key infrastructure that is described in Section 5.
- The interoperability layer leverages the SVC core data set to prepare and digitally sign an SVC FHIR document. This signed SVC document is persisted to the SVC Registry and the transaction response is returned. It is anticipated that, where the SVC Registry operates as a conformant FHIR server, this transaction may *also* employ ITI-65.
- The interoperability layer returns the ITI-85 response to the digital health solution, which processes the response.

These SHR-related transactions and their normative patterns are defined in the OpenHIE Architecture Specification *(24)* and in the conformance-testable IHE Mobile Health Document Sharing (MHDS) specification *(28)* that OpenHIE references.

4.4 Governance considerations

4.4.1 Issuing SVCs

This section is intentionally left blank and will be included in Release Candidate 2.

4.4.2 Revocation of SVCs

This section is intentionally left blank and will be included in Release Candidate 2.

4.4.3 Issues related to verifiers accessing personal health data

This section is intentionally left blank and will be included in Release Candidate 2.

4.4.4 Issues related to verifiers becoming holders of personal health data

This section is intentionally left blank and will be included in Release Candidate 2.

5 GLOBAL SVC ARCHITECTURE

5.1 Guiding design principles for the global architecture

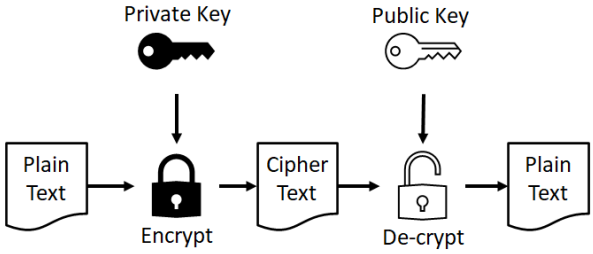
The design of the global trust framework was based on the following principles:

- Given the motivation to rapidly implement SVCs in service of the fight against the COVID-19 pandemic, WHO favoured proven architectural approaches that were demonstrably and reliably implementable at global scale.
- The SVC is a health document. The trust framework design was therefore burdened with the generally applicable constraints related to the management and sharing of protected health data.
- The SVC initiative's overarching imperatives related to equity informed the design's focus on mature architectural approaches for which a range of open source and/or global public goods options would be available to operationalize national solutions.
- Respect for Member State sovereignty. Architectural choices were favoured that would give Member States' broad freedom within the engineering constraints of having to support interoperability across disparate technologies and solutions that are already implemented.
- WHO will not become a holder of personal health data nor a party to transactions that convey personal health data. Architectural approaches must cast WHO as an enabler and facilitator of direct Member State to Member State interactions.
- The design must accommodate federations of regional trust frameworks that can be connected to and interoperate within the overall global framework.
- The design should leverage open standards, software global public goods, OpenHIE architecture, foundational services, and conformance assessment, to facilitate interoperability, usability, reuse, and quality.

5.2 Technical specifications for a global trust framework

The trust framework uses private and public key pairs to operationalize digital signing and cryptographic verification. Content that is encrypted by a private key may be de-crypted by the corresponding public key of the key pair. The process is shown in Figure 17.

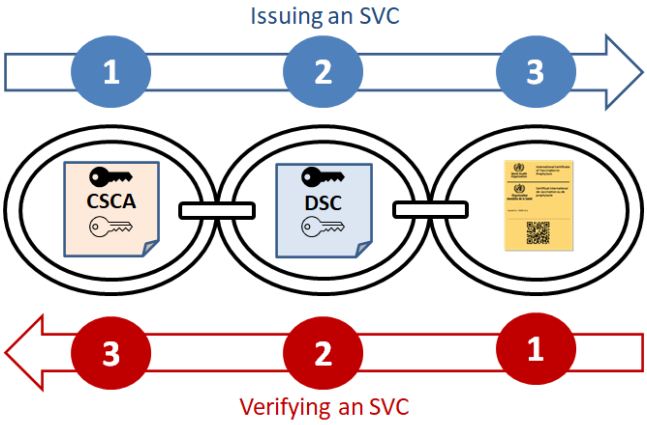
Figure 17. Digital signing using private and public key pairs



Operationally, private keys are kept highly secure and public keys are broadly shared. In this way, content that is "signed" by (encrypted by) a private key may be readily verified by (decrypted by)

anyone who has the corresponding public key. This sign-verify mechanism is leveraged to establish the chain of trust, which is illustrated in Figure 18.

Figure 18. The chain of trust



PHAs in Member States will establish and maintain a domestic public key infrastructure that can be leveraged to issue and to verify SVCs. As shown in Figure 18 the process of issuing an SVC (shown in blue in Figure 18) will involve three steps:

1. The PHA will generate a private and public key pair that will serve as the CSCA. The private key will be kept highly secure; the public key will be widely disseminated.
2. The PHA will generate one or more Document Signer key pairs. Document Signer private keys are kept highly secure; the public keys are widely disseminated. The Document Signer key pair is digitally signed by the CSCA's **private** key.
3. SVC content, such as the UVCI, is digitally signed using the Document Signer's private key. A barcode representation of the signed content is generated. When this signed barcode is printed on or affixed to an SVC card, for example, the paper card becomes cryptographically "linked" (via the UVCI) to its twin: the *digital* SVC.

The verification process (shown in red in Figure 18) reverses this process to verify content on the card:

1. The SVC's cryptographically signed barcode is "read" by a digital solution.
2. The Document Signer's **public** key is leveraged to cryptographically verify that the barcode content has not been tampered with.
3. The PHA's CSCA **public** key is leveraged to cryptographically verify that the Document Signer's signature was issued under the responsibility of the PHA.

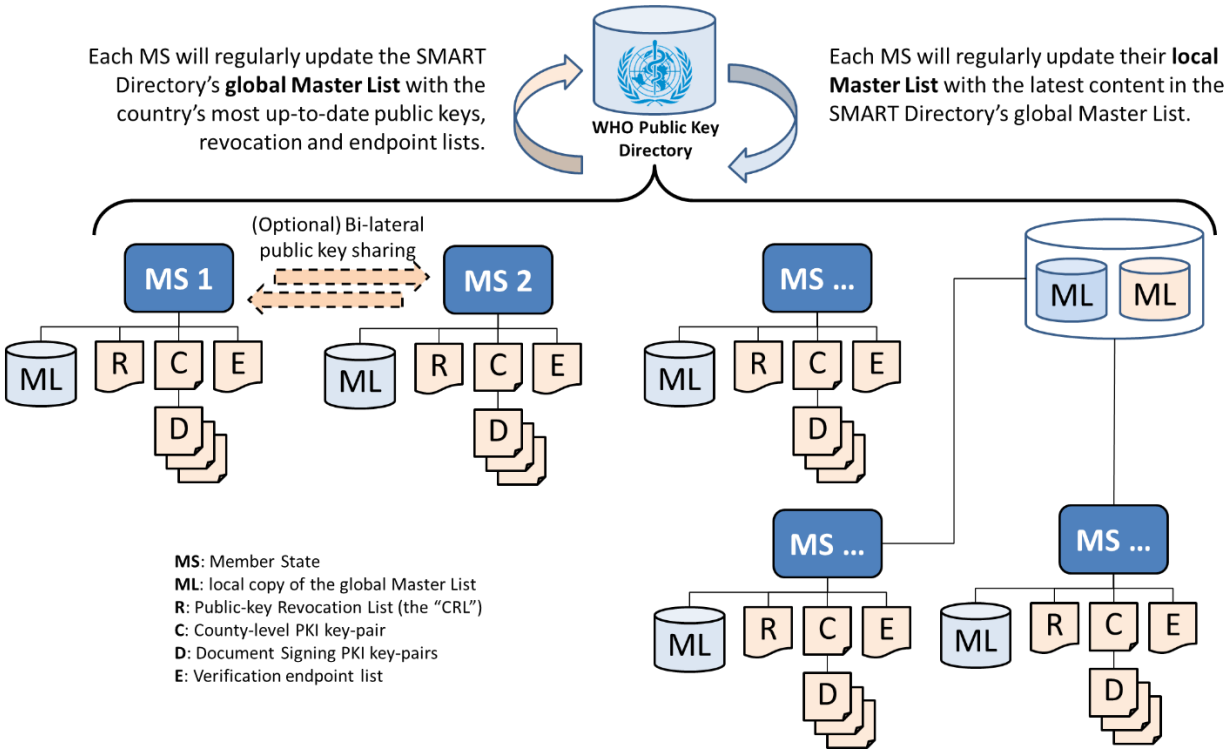
The WHO Public Key Directory provides a mechanism for Member States' PHAs to update their public keys and other supporting artefacts to a central directory (i.e. WHO Public Key Directory). In turn, each Member States' PHA can refresh their local, national public key directory with the global Master List of updated PHA artefacts from all other participating Member States. Each Member State will be responsible for establishing and maintaining its own national public key infrastructure (PKI). This PKI should include the highly secure databases for maintaining their private keys; the directories

needed to store and manage its own public keys; as well as the keys and other artefacts regularly downloaded from the WHO Public Key Directory's global Master List. Member States may choose to bilaterally exchange public keys and regional public key directories may be set up (such as is being contemplated by the EU Member States). All of these scenarios work within the overall global trust framework supported by the WHO Public Key Directory.

Importantly – WHO will never be a custodian of any personal health data. Neither will WHO participate in verification transactions. Rather, the WHO Public Key Directory will play a facilitator and enabler role. The batch uploads and downloads of participating Member States allows them to be part of the global chain of trust related to SVC issuance and verification.

As is illustrated by Figure 19, the technical approach favoured is based on a federated **PKI** supported by a central WHO Public Key Directory. This directory will maintain a regularly refreshed global Master List of Member States' PKI public keys, key revocation lists, and internet endpoints (used for online verification).

Figure 19. The WHO Public Key Directory



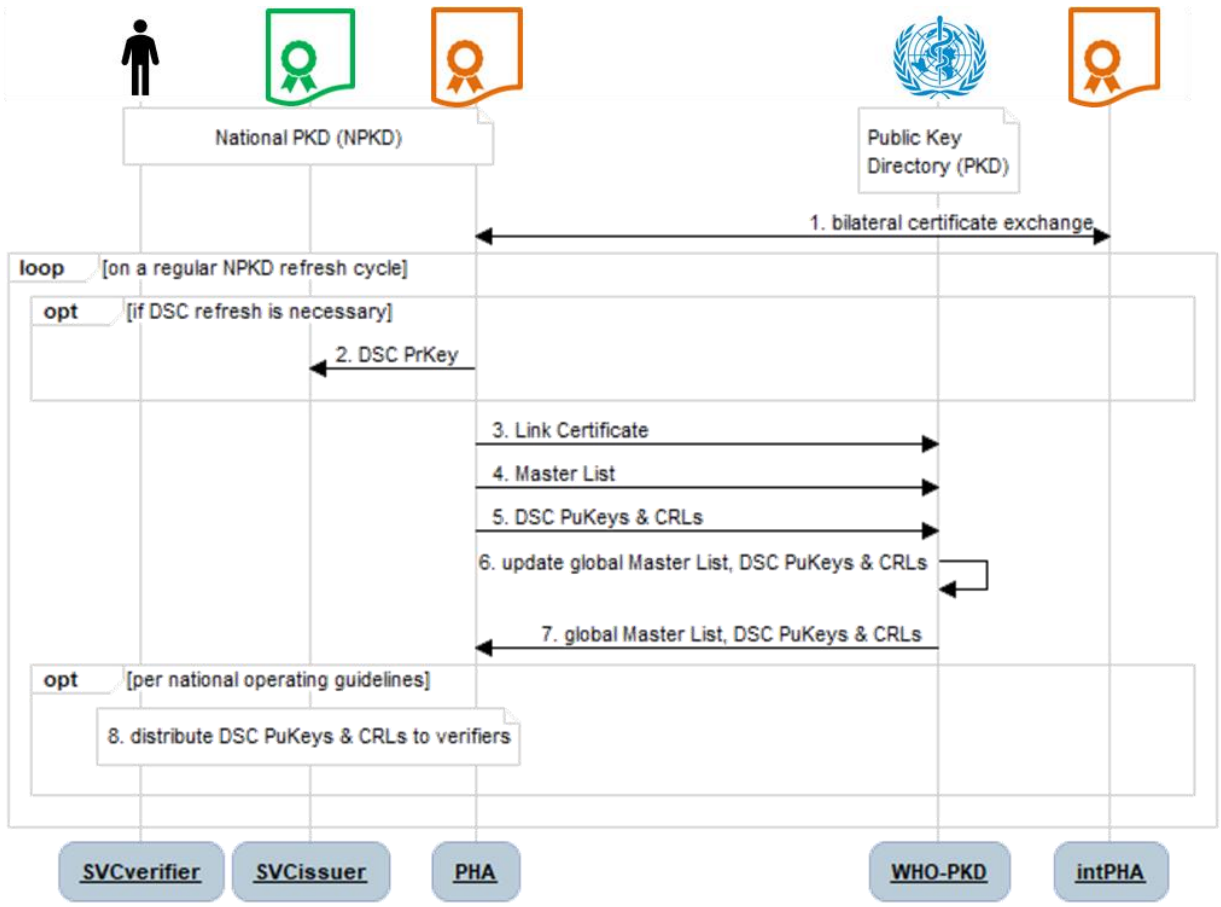
The expected operation of the trust framework will be that:

- Member States will regularly refresh the WHO Public Key Directory with their country's most up-to-date PKI public keys, revocation lists and endpoints.
- Each Member State will be able to download the updated global Master List, which contains the public keys, revocation lists, and endpoints from every other Member State participating in the WHO Public Key Directory.

- Optionally, and outside of the WHO Public Key Directory workflows, Member States can bilaterally exchange Master List content with each other. Regional directories could even be established (such as is being contemplated by the EU Member States). In all cases, it is expected that these workflows will be operated in a way that is consistent with the operation of the overall global trust network.

The operation of the global trust network workflow is illustrated by Figure 20. The workflow participants, in order from left to right, are the: **SVC Verifier**, **SVC Issuer**, **national PHA** that will operate the NPKD infrastructure, the **WHO Public Key Directory**, an **international PHA** who will be the operator of their NPKD.

Figure 20. Global trust network operational workflow



PKD: public key directory, DSC: document signer certificate; CRL: certificate revocation lists; SVC: smart vaccination certificate; WHO PKD: World Health Organization Public Key Directory; intPHA: international public health authority SVC directory.

This workflow operationalizes use case UC004 – the establishment and operation of a national public key infrastructure that leverages the WHO Public Key Directory. The workflow participants, their interactions, and the business requirements arising from these interactions, may be described as follows:

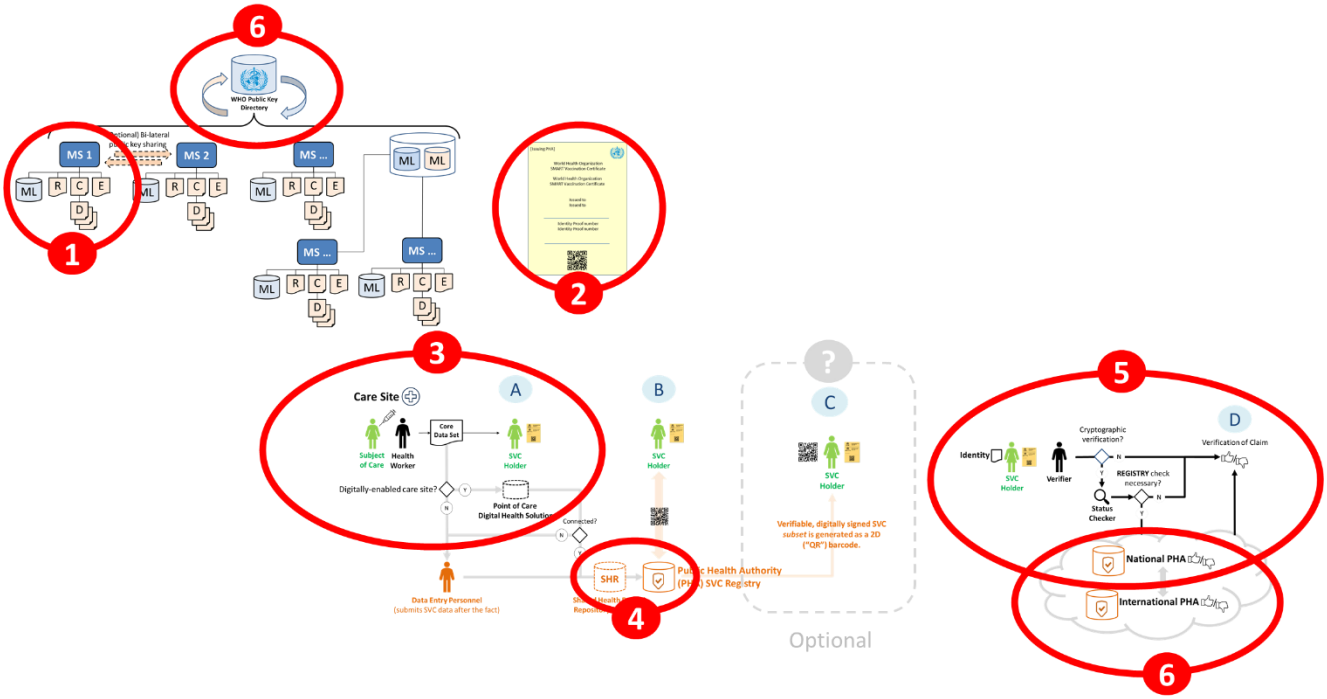
- ❑ WHO SHALL be the operator of a PKD (the **WHO Public Key Directory**).

- ❑ Member States SHALL operate an **NPKD** that SHALL operationalize their domestic **CSCA**. The NPKD SHALL be leveraged to issue, maintain, and manage the sharing of their PKI certificates. The NPKD MAY be operated by the **PHA**.

1. Member States MAY exchange certificates in bilateral relationships outside the purview of the WHO Public Key Directory.
2. The NPKD SHALL leverage the CSCA to issue document signer keys (DSC private key, PrKey) to SVC issuers as per the national norms and standards. Issuers SHALL issue SVCs under the responsibility of the PHA.
3. The NPKD SHALL issue Link Certificates under their CSCA and update the WHO Public Key Directory with these certificates.
4. The NPKD MAY maintain a **Master List** and in this instance, it SHALL update the WHO Public Key Directory with this Master List.
5. The NPKD SHALL update the WHO Public Key Directory with DSC public keys (PuKey) and the updated PKI **certificate revocation list**.
6. The WHO Public Key Directory SHALL maintain the **global Master List** containing countries' CSCA public keys, each country's DSC public keys, their certificate revocation lists, and a directory of SVC verification endpoints.
7. The NPKD SHALL regularly fetch from the WHO Public Key Directory an updated global Master List to refresh its local copy of this list in its NPKD.
8. As per national guidelines, the NPKD MAY distribute the updated global Master List to domestic verifiers.

The overall framework, and how the pieces of it fit together, is illustrated in Figure 21**Error! Not a valid bookmark self-reference.**

Figure 21. Overall implementation pattern for operationalizing SVCs



A notional implementation pattern for realizing this framework may be described as follows:

1. To begin, a national PHA would establish a PKI and operationalize a national public key directory (NPKD).
2. Leveraging its PKI, PHA-signed UVCI barcodes can be added to paper vaccination cards to create SVC cards.
3. SVC cards can be employed to support the Continuity of Care scenario.
4. The SVC core data set, once captured to a digital health solution in a format compatible with the HL7 FHIR International Patient Summary (IPS) standard, may be leveraged by the PHA to generate signed SVC documents and save them to an SVC Registry.
5. Once populated in the PHA's SVC Registry, digital or paper SVCs issued by the PHA can be verified.
6. Participation in the WHO Public Key Directory operationalizes the ability to verify SVCs issued by international PHAs. This may be important to the resumption of travel and tourism.

More detailed technical specifications of the global trust network will be included in Release Candidate 2 of this specification.

5.3 Global governance framework

This section is intentionally left blank and will be included in Release Candidate 2.

ANNEXES

Annex 1: Guiding principles for mapping WHO-FIC and other classifications

Mapping from classification and terminologies used in legacy systems to ICD-11 and other WHO FIC classifications should follow the below listed principles.[4]

1. Establish use case(s) prior to developing the map.
2. Clearly define the purpose, scope, and directionality of the map.
3. Maps should be unidirectional and single purposed. Separate maps should be maintained for bidirectional maps (to support both a forward and a backward map table). Such unidirectional maps can be very useful to support data continuity for epidemiological and longitudinal studies. Maps should not be reversed.
4. Develop clear and transparent documentation that is freely available to all, and that describes the purpose, scope, limitations, and methodology of the map.
5. Ideally the producers of both terminologies in any map participate in the mapping effort to ensure that the result accurately reflects the meaning and usage of their terminologies. At a minimum, both terminology producers should participate in defining the basic purpose and parameters of the mapping task, reviewing and verifying the map, developing the plan for testing and validation, and devising a cost-effective strategy for building, maintaining, and enhancing the map over time.
6. Map developers should agree on the competencies, knowledge, and skills required of team members at the onset of the project. Ideally, target users of the map also participate in its design and testing to ensure that it is fit for its intended purpose.
7. Quality Assurance (QA) and Validation: A key item for QA and validation is ensuring the reproducibility, traceability, and comparability of the maps. Establish the QA and validation protocols at the beginning of the project and apply them throughout the mapping process. Factors that may be involved in quality assurance include quality-assurance rules, testing (test protocols, pilot testing), and quality metrics (such as computational metrics or precisely defined cardinality, equivalence, and conditionality). Clear documentation of the QA process and validation procedures is an important component of this step in the mapping process. If conducting a pilot test is feasible, it will improve the QA/validation process. Mapping is an iterative process that will improve over time as it is used in real settings.
8. Dissemination: Upon publication and release, include information about release mechanisms, release cycle, versioning, source/target information, licence agreement requirements, and a

[4] Further mapping guidance details is provided in the White Paper on WHO-FIC Classifications and Terminology Mapping produced in collaboration with the WHO FIC Network. The document can be download from the following URL www.who.int/classifications

feedback mechanism for users. Dissemination of maps should also include documentation as stated above, describing the purpose, scope, limitations, and methodology used to create the maps.

9. Maintenance: establish an ongoing maintenance mechanism, release cycle, types and drivers of changes, and versioning of maps. The maintenance phase should include an outline of the overall lifecycle plan for the map, continuous improvement process, and decision process around when an update is required. Whenever maps are updated, the cycle of QA and validation must be repeated.

10. When conducting mapping manually, it is recommended to provide map specialists with the necessary tools and documentation to drive consistency when building the map. These include such items as the tooling environment (workflow details and resources related to both source and target schemes); source and target browsers, if available; technical specifications (use case, scope, definitions); editorial mapping principles or rules to ensure consistency of the maps, particularly where human judgement is required; and implementation guidance. Additionally, it is best practice to provide an environment which supports dual independent authoring of maps as this is thought to reduce bias between human map specialists. Development of a consensus management process to aid in the resolution of discrepancies and complex issues is also beneficial.

11. In computational mapping, it is advisable to include resources to ensure consistency when building a map using a computational approach, including a description of the tooling environment, when human intervention would occur, documentation (e.g. the rules used in computerized algorithms), and implementation guidance. It is also advisable to always compute accuracy and error rate of the maps. It is also important to manually verify and validate the computer-generated mapping lists. Such manual checking is necessary in the quality assurance process, as maps that are generated automatically will almost always contain errors. Such manually verified maps can also assist in the training of the machine-learning model when maps for different sections of terminologies are being generated sequentially.

12. Cardinality as a metric in mapping must be clearly defined in terms of what is being linked between source and target and how the cardinalities are counted. For example, SNOMED CT codes for functional impairments are semantically different from ICF codes. A 1-to-1 map between the two does not mean semantic equivalence. In terms of counting, what SNOMED International considers to be a 1:1 map include what others may consider to be a 1-to-many map.

13. Level of equivalence, such as broader, narrower, or overlap, should be specified.

14. Maps must be machine-readable to optimize their utility.

15. ICD-11: When creating maps using ICD-11, consider mapping into the Foundation Component first, then generating maps to Mortality and Morbidity Statistics through linearization aggregation.

REFERENCES

1. Monitoring COVID-19 vaccination: Considerations for the collection and use of vaccination data - Interim Guidance. Geneva: World Health Organization and the United Nations Children's Fund; 2021. (https://www.who.int/publications/i/item/monitoring-covid-19-vaccination-interim-guidance, accessed 18 March 2021). Licence: CC BY-NC-SA 3.0 IGO.
2. Armstrong MM. Cheat sheet: What is Digital Twin? : IBM; 2021. (https://www.ibm.com/blogs/internet-of-things/iot-cheat-sheet-digital-twin/, accessed 18 March 2021).
3. "Immunity passports" in the context of COVID-19: Scientific brief. Geneva: World Health Organization; 2020. (https://www.who.int/publications/i/item/immunity-passports-in-the-context-of-covid-19, accessed 18 March 2021). Licence: CC BY-NC-SA 3.0 IGO.
4. Interim position paper: considerations regarding proof of COVID-19 vaccination for international travellers. Geneva: World Health Organization; 2021. (https://www.who.int/news-room/articles-detail/interim-position-paper-considerations-regarding-proof-of-covid-19-vaccination-for-international-travellers, accessed 18 March 2021).
5. Practical guide for the design, use and promotion of home-based records in immunization programmes. Geneva: World Health Organization; 2015. (https://apps.who.int/iris/bitstream/handle/10665/175905/WHO_IVB_15.05_eng.pdf?sequence=2, accessed 18 March 2021).
6. International Certificate of Vaccination or Prophylaxis. Geneva: World Health Organization; 2005. (https://www.who.int/ihr/IVC200_06_26.pdf, accessed 18 March 2021).
7. Visa Public Key Infrastructure Certificate Policy (CP) v3.8: Effective: August 25, 2020. Visa; 2020. (http://enroll.visaca.com/VisaPublicKeyInfrastructureCertificatePolicy.pdf, accessed 18 March 2021).
8. COVID-19 Vaccine EUL issued Geneva: World Health Organization; 2021 (https://extranet.who.int/pqweb/vaccines/covid-19-vaccines, accessed 18 March 2021).
9. Statement on the sixth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic. Geneva: World Health Organization; 2021. (https://www.who.int/news/item/15-01-2021-statement-on-the-sixth-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic, accessed 18 March 2021).
10. World Health Organization open call for nomination of experts to contribute to the Smart Vaccination Certificate technical specifications and standards. Geneva: World Health Organization; 2020. (https://www.who.int/news-room/articles-detail/world-health-organization-open-call-for-nomination-of-experts-to-contribute-to-the-smart-vaccination-certificate-technical-specifications-and-standards-application-deadline-14-december-2020, accessed 18 March 2021).
11. Guidance on developing a national deployment and vaccination plan for COVID-19 vaccines. Geneva: World Health Organization; 2020. (https://www.who.int/publications/i/item/WHO-2019-nCoV-Vaccine_deployment-2020.1, accessed 18 March 2021).
12. International Health Regulations (2005), third edition. Geneva: World Health Organization; 2016. (http://www.who.int/ihr/publications/97892415804%2096/en/, accessed 18 March 2021).
13. Global manual on surveillance of adverse events following immunization. Geneva: World Health Organization; 2014. (https://www.who.int/vaccine_safety/publications/aefi_surveillance/en/, accessed 18 March 2021).

14. Covid-19 vaccines: safety surveillance manual. Geneva: World Health Organization; 2020. (https://www.who.int/docs/default-source/covid-19-vaccines-safety-surveillance-manual/covid19vaccines_manual_aefi_20210104.pdf, accessed 18 March 2021).
15. About OpenSRP. OpenSRP; 2021. (https://smartregister.org/, accessed 18 March 2021).
16. About District Health Information Software 2 (DHIS2). University of Oslo Health Information Systems Programme; 2021. (https://dhis2.org/, accessed 18 March 2021).
17. VigiFlow: Supporting national and regional pharmacovigilance and vaccine surveillance processes.: Uppsala Monitoring Centre; 2021. (https://www.who-umc.org/global-pharmacovigilance/vigiflow/, accessed 18 March 2021).
18. WHO Smart Vaccination Certificate - RC1: World Health Organization; 2021 (https://who-int.github.io/svc, accessed 18 March 2021).
19. International Patient Summary Implementation Guide: 1.0.0 - CI Build. Health Level 7 International; 2021. (https://build.fhir.org/ig/HL7/fhir-ips/ipsStructure.html, accessed 18 March 2021).
20. International Classification of Diseases 11th Revision World Health Organization (https://icd.who.int/, accessed 18 March 2021).
21. SNOMED Global Patient Set (GPS). SNOMED International; 2021. (https://gps.snomed.org/, accessed 18 March 2021).
22. Digital adaptation kit for antenatal care: operational requirements for implementing WHO recommendations in digital systems. Geneva: World Health Organization; 2021. (https://www.who.int/publications/i/item/9789240020306, accessed 18 March 2021). Licence: CC BY-NC-SA 3.0 IGO.
23. OpenHIE Architecture & Standards. Open Health Information Exchange; 2021. (https://wiki.ohie.org/pages/viewpage.action?pageId=8454157, accessed 18 March 2021).
24. OpenHIE Architecture Specification Version 3.0. Open Health Information Exchange; 2020. (https://ohie.org/architecture-specification/, accessed 18 March 2021).
25. Technical Frameworks. Integrating the Healthcare Enterprise International; 2021. (https://www.ihe.net/resources/technical_frameworks/, accessed 18 March 2021).
26. Mobile Care Services Discovery (mCSD). Integrating the Healthcare Enterprise; 2020. (https://wiki.ihe.net/index.php/Mobile_Care_Services_Discovery_(mCSD), accessed 18 March 2021).
27. Patient Master Identity Registry (PMIR). Integrating the Healthcare Enterprise; 2020.
28. Mobile Health Document Sharing (MHDS). Integrating the Healthcare Enterprise; 2020.
29. HL7 FHIR Resource Encounter - Content. Health Level 7 Fast Healthcare Interoperability Resources; 2019.