eHealth Network

OUTLINE

Interoperability of health certificates
Trust framework

V.1.0

2021-03-12

The eHealth Network is a voluntary network, set up under article 14 of Directive 2011/24/EU. It provides a platform of Member States' competent authorities dealing with eHealth.

Table of Contents

1 Introduction

The European Council has repeatedly called for a coordinated approach[1] on interoperable vaccination certificates and the mutual recognition of test results.

[1] https://www.consilium.europa.eu/media/47296/1011-12-20-euco-conclusions-en.pdf

The Guidelines[2] adopted by the eHealth Network[3] rest on three pillars: a minimum data set, a standard unique identifier for such proofs, and a trust framework, which provides the basis for establishing the certificates' authenticity, integrity and validity.

This document outlines the trust framework and provides the basis for discussion with Member States on the implementation of interoperable certificates in EU Member States. Further elaboration on the specifications of the technical implementation will follow. The document may be subject to future modification as the COVID-19 situation evolves.

Figure 1: Mock-ups of a paper and digital vaccination certificate, as an example.

The trust framework defines the rules, policies, protocols, formats and standards needed to ensure that Covid-19 health certificates are issued in such a way that their authenticity and integrity can be verified and trusted.

The trust framework shall be flexible enough to encompass different use cases. It defines provisions that allow both digital and analogue, off-line and on-line versions of the COVID-19 health certificates, as well as the associated verification.

[2] *eHealth Network guidelines on proof of vaccination for medical purposes - basic interoperability elements,* adopted and published on 27 January 2021. Published here.

[3] The eHealth Network is a voluntary network created under article 14 of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare. It provides a platform for Member States' competent authorities responsible for eHealth.

2 Business needs and requirements

The journey of the Covid-19 health certificate is completed in 3 distinct steps:

1. the collection and registration of data about the medical events for competent authorised entities in a health information system,
2. the issuance of the Covid-19 health certificate, and
3. the presentation of the Covid-19 health certificate to a verifier (e.g. a border guard or a healthcare professional) for its verification.

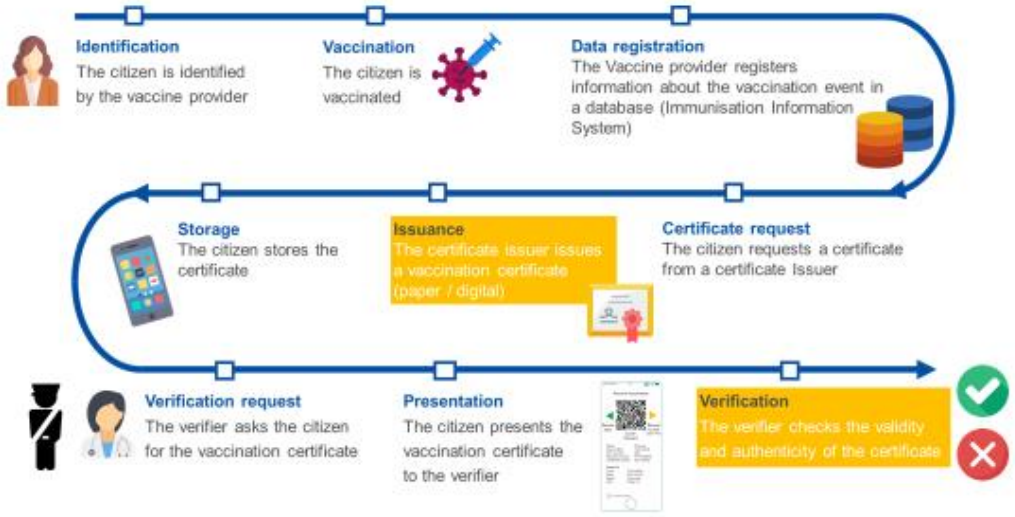

Figure 2: Main steps of the vaccination journey, as an example of the generation and use of a health certificate

A certificate relies on a minimum dataset. Included in the minimum dataset is a Unique Vaccination Certificate/assertion identifier (UVCI), which could be used as a link to the underlying data registry. The use of UVCI or other methods for online verification will be defined in more detail in the next versions of the Trust Framework.

The verifier of a certificate should be able to establish that:

- *The certificate has been issued by an authorised entity*;
- *The information presented on the certificate is authentic, valid, and has not been altered*;
- *The certificate can be linked to the holder of the certificate;*

2.1 Main design principles and business requirements

The design of the **trust framework for EU-interoperable issuing of COVID-19 health certificates and verification of their integrity and authenticity** relies on key design principles listed below. The list is *not prioritised*. Instead, the trust framework that is specified later in the document attempts to optimise as many of the key design principles as possible.

- **Cross-border interoperability.** National implementations of certificates that comply with the specifications of the trust framework should be interoperable. This means that if Countries A and B implement the specifications, it should be possible for a verifier in Country B to verify a digital vaccination certificate that has been issued in Country A.

Cross-border interoperability should be ensured across EU and EEA countries. The Trust Framework should not prevent interoperability with the solutions designed on a global level, such as the one being developed by the WHO or ICAO. This is one of the primary design principles and it has implications in all components of the proposed trust framework.

- **Data protection (including data minimisation, purpose limitation, etc.).** The trust framework should protect the data of the involved individual stakeholders (most importantly, certificate holders). This covers several data protection dimensions catered by the General Data Protection Regulation, including purpose limitation and data minimisation. In practice, only the bare minimum set of data that is required for the supported use cases should be *processed* (data minimisation) and the purpose of data collection should be checked against the use cases (purpose limitation). Similarly, only the bare minimum set of data that is required for the supported use cases should be *presented* to a specific verifier (data minimisation) and the purpose of data presentation should be checked against the use cases (purpose limitation). In order to achieve the latter, the trust framework may support different presentation datasets for different verifier scenarios. The data protection principle has a strong impact on the specification of the Minimum Dataset and the design of the use cases of the trust framework.
- **Data security and privacy by design and by default**. Abuse of data by actors (especially, the certificate verifiers and holders) and forgery should be prevented by any reasonable means. The trust framework should by design and default ensure the security and the privacy of data in the compliant implementations of digital vaccination certificate systems, ensuring both security and privacy. Available tools should be used for restricting access to data and preventing malicious use of data, while the establishing of the authenticity of data and its link to the certificate holder should be ensured. The design should prevent the collection of identifiers or other similar data which might be cross-referenced with other data and re-used for tracking ('Unlinkability'). Further discussions are needed as to the technological aspects and timeline for the incorporation of these features in the trust framework.
- **Inclusiveness (especially medium-neutrality).** The trust framework should be inclusive both towards Member States' approaches and the individual citizen (*'no citizen left behind'*). The design of the trust framework should attempt to maximize its support for diverse contexts (e.g., high resource vs low resource contexts). To enable this, the trust framework should support a spectrum of certificate presentation media from plain paper certificate to augmented paper certificates (e.g., paper certificate with printed machine-readable parts such as barcodes, QR codes, Machine Readable Zones) and to purely digital certificates (e.g., in-app certificates).
- **Simplicity and user-friendliness**. It is very important that the trust framework is designed with simplicity and user-friendliness of the possible implementation of digital certificate systems in mind. More formally, the trust framework should not have features or functionalities that would unnecessarily complicate the resulting implementation of a digital vaccination certificate system or make them unnecessarily difficult to use. Lack of simplicity could increase the time it takes to implement the compliant digital vaccination certificate systems, while lack of user friendliness could hinder the uptake of the resulting implementations. User-friendliness is relevant for quick and easy processing, specifically to certificate holders and to verifiers.

- **Implementation flexibility**. The trust framework specifications should provide implementers with a variety of options when developing digital vaccination certificate systems according to the trust framework specifications. This key design principle aims at reducing the implementation time and leveraging/reusing existing infrastructures in Member States. To satisfy this principle, the trust framework specifies, whenever possible, a list of alternative methods, flows, architectures and implementation options, for example alternative presentation media, verification options, implementation technologies, etc. whilst still guaranteeing the same level of trustworthiness
- **Modularity and scalability**. This is strongly linked with the previous key design principle. The trust framework architecture should be modular and easily scalable, for instance, to additional usage scenarios, use cases and types of certificates. The trust framework already supports different usage scenarios (e.g. alternative settings in which certificates may be requested or verification may take place). Examples of other types of certificates that could be supported by potential extensions of the trust framework include certificate of negative COVID-19 tests and certificates of recovery from COVID-19, while examples of other use cases that could be supported are travel or (participation in) leisure activities (i.e. proof of vaccination for non-health-related purposes in domestic or international settings). Decisions related to ethical, societal or political questions pertaining to the use cases should be tackled separately. To satisfy this key design principle, special attention has been paid in the design of the trust framework architecture with clear separation of the steps of the user story detailed below.
- **Open standards**. The trust framework should rely for its implementations on open standards, to the extent that this is possible. This will greatly contribute to the interoperability of the resulting implementations, in addition combined with open governance and open source implementations, it will instil trust in the involved stakeholders.

2.2 User roles

The user roles that are associated with the supported user stored of the trust framework are presented in the table below.

ROLE	DESCRIPTION	EXAMPLES
Certificate Issuer	The trusted entity that issues and signs a statement/credential/certificate.	For paper certificates, a healthcare organisation or healthcare authority. For digital certificates, an electronic medical record system, an IIS, a HP portal, a patient portal, a system used by another relevant authority.
Certificate Holder	The person in possession of a certificate.	A person, their guardian, legal representative or another authorized person.
Certificate	The actor (a person or a computer	A healthcare professional or another

ROLE	DESCRIPTION	EXAMPLES
Reader	system) analysing the contents of a certificate presented by a certificate holder.	person or a system entitled to the detailed information on the certificate (e.g., a healthcare appointment system).
Certificate Verifier	The actor (a person or a computer system) checking the validity of a certificate presented by a certificate holder.	An authority, an online system used by the certificate holder (for example, an online check-in).

2.3 ID binding and verification

An important parameter of the trust framework pertains to the identity of the subject of the certificate i.e., the person for whom the certificate is issued. The identity of this subject shall be bound to a certificate when the latter is issued (*ID binding*) and has to be verified when the certificate is being presented and verified (*ID verification*). These two processes (ID binding at the Issuance step and ID verification at the Presentation and Verification step) prevent possible impersonation attempts (i.e., a person fraudulently presenting a certificate that has been issued to someone else as if it were their own), and are in line with the data security and privacy by design and default principles of the trust framework.

The processes of ID binding and/or verification may be optional for some usage scenarios in the scope of the trust framework. For instance, in some settings the simple presentation of the certificate to a healthcare professional for medical purposes might be enough without additional actions for proving the ownership of the certificate if complemented by good clinical practices. However, in those usage scenarios where the aforementioned process cannot be omitted, the trust framework, adhering to the simplicity and user-friendliness principle, shall rely on (nationally and/or internationally) established methods for ID binding and verification. In other words, the trust framework does not specify in its architecture dedicated components or modalities for undertaking the ID binding and verification process.

The recommended methods for performing ID binding and verification employ *nationally issued identity proof documents*, such as national IDs and passports. Such identity proof documents should be presented at the time of issuance (ID binding) and verification (ID verification) of the certificate and therein personally identifying information should be compared against the information in the certificate.

3 Trust architecture

This chapter provides an overview of the trust architecture and describes its main components. The chapter contains requirements directed at the Member States acting in the roles of issuers and verifiers.

The WHO is developing a global trust framework based on a similar approach. The framework is centred around the Global Health Trust Anchor operated and governed by the WHO and based on the technical specifications derived from ICAO’s Public Key Directory (PKD) model.

3.1 Overall description

The EU trust framework is designed to be largely decentralised.

As per the digital contact tracing apps and the European Federation Gateway Service, this reflects the divergent structures and approaches within the EU Member States. That is to say, it aims to avoid centralisation where possible in line with the principle of flexibility.

However, there are some centralised elements:

1. Roots of trust stored in a common directory/gateway (EU Public Key Directory/Gateway), similar to the public key certificate provision process established in the EFGS.
2. Governance model.

The main elements of the system are outlined in Figure 3 and described further below.

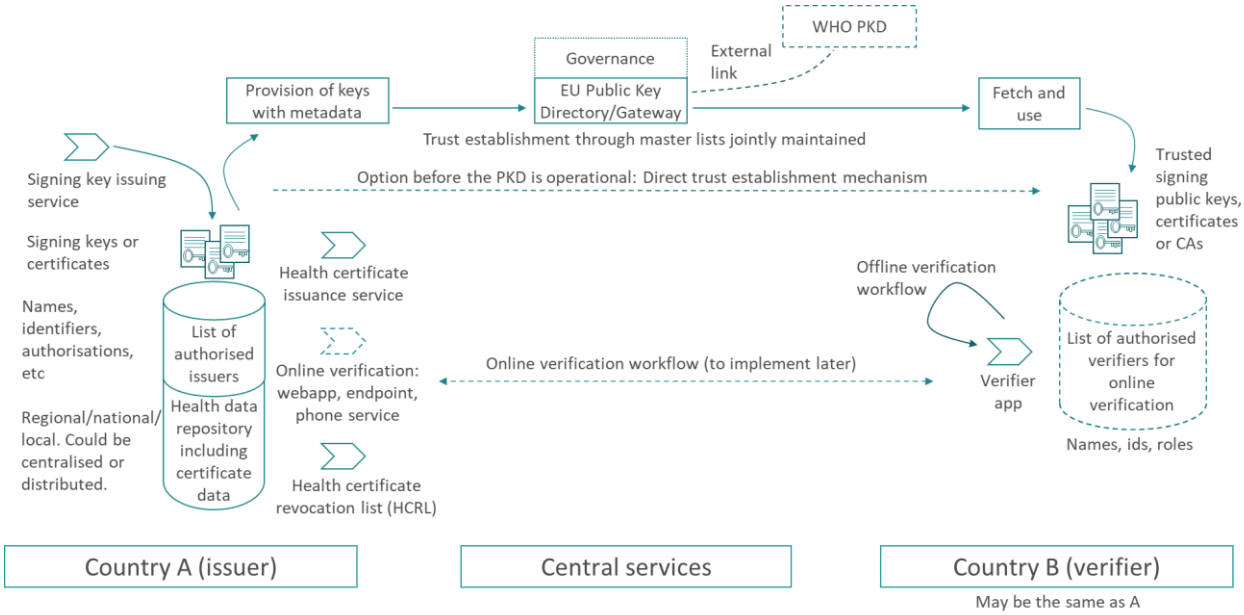

Figure 3: Overall architecture of the system *(solid lines = first version of the trust framework specifications; dashed lines = future versions of the trust framework specifications)*

3.1.1 Country A (country of issuance)

The country of issuance, through its competent health entities, is responsible for the recording of health data and issuing certificates. It is also possible for the issuer to deliver a certificate based on **reliable** information received from other sources.

The Country A that is participating to the interoperability scheme shall issue certificates at least in the form of the augmented paper (paper augmented with digital artefacts such as barcodes or QR codes). In addition, Country A may issue certificates stored as purely digital files in apps or computers.

The Country A shall assign a national Public Health Authority (PHA) responsible for the system. The name of the PHA shall be communicated to other members of the interoperability scheme through the eHealth Network secretariat.

3.1.1.1 List of authorised issuers

A system used by Country A for maintaining details about healthcare organisations authorised to issue health certificates.

The list should be established and maintained by every Country A, and it should be published on its PHA's website (national backend server). In addition, the list may also be published through an open API.

The list should contain the data set following the description given in Table 1.

Table 1: List of certified issuers, data set for each entry

Group and cardinality	Element	Description	Data type and cardinality
Issuer identification **1..1**	Country	Country of the issuer	Coding (ISO 3166-1 alpha-2) 1..1
	Name	Name of the issuer	String 1..1
	Identifier	Identifier of the issuer	Identifier (format to be defined later) 1..1
	Public key or PKI certificate	Public key or PKI certificate assigned to the issuer	Text (format to be defined later) 1..*
	Online verification webapp	Address of the online verification webapp, if offered by the issuer	URI 0..1
	Online verification endpoint	Address of the online verification service, if offered by the issuer	URI 0..1
Issuer authorization **1..***	Health certificate type	The type of health certificates the issuer is capable and authorised to issue	Coding (value set: vaccination certificate) 1..1
	Validity from	Start of the authorisation period	dateTime 1..1
	Validity to	End of the authorisation period	dateTime 1..1
	Status	Status of the authorisation	Coding (active, inactive, entered-in-error, on-hold, unknown) https://www.hl7.org/fhir/valueset-account-status.htmlhttps://www.hl7.org/fhir/valueset-account-status.html 1..1

3.1.1.2 Health data repository

A repository used by Country A for storing health information and information about the issued health certificates.

The system may be part of an Immunization Information System (IIS), a laboratory system or it may be stored by national, regional or local electronic health record systems, or on paper. The system may be centralised on the national level or it may be largely distributed.

Every Country A may use their own arrangements for establishing and maintaining the health data repository. An overall description of the arrangements shall be made publicly available by each Country A.

3.1.1.3 Signing key issuance service

A service such as a Certificate Authority (CA) or another arrangement used by Country A for issuing signing key pairs or certificates, to be used for signing health certificates.

The term “signing key” in this document refers to keys or certificates issued to legal and natural persons and used for creating electronic seals and signatures. No difference is made between electronic signatures and electronic seals in this document, and the terms “signature” and “signing” are used to refer to both of them.

Country A may use any public or private CA (or another option) in order to issue signing keys or certificates used for signing health certificates.

3.1.1.4 Signing keys or certificates

Digital signature keys or certificates used by Country A for signing health certificates.

Signing keys or certificates shall only be provided to entities with active authorisation according to the published List of authorised issuers.

Member States should have a clear policy for revocation of health certificates, including refresh rates for verifiers.

3.1.1.5 Provision of keys with metadata

A process executed by Country A in order to register the signing keys or certificates to the EU Public Key Directory/Gateway (see 3.1.3.1 below).

The process and related procedures for the secure registration of public keys or certificates will be defined by the eHealth Network.

3.1.1.6 Health certificate issuance service

A service used by Country A for issuing health certificates and delivering them to certificate holders.

The service may be implemented as a patient-facing app, as a patient portal, as a healthcare professional portal, or it may be integrated to another national, regional or local system.

Every Country A shall implement at least one health certificate issuance service. Health certificates shall only be issued by entities with active authorisation according to the published List of authorised issuers.

3.1.1.7 Health certificate revocation list (HCRL)

A system used by Country A for publishing information about revoked health certificates.

Each Country A shall publish one and only one aggregate list of all revoked health certificates. Country A is responsible for putting its revoked certificates on the list and signing it using one of its signing keys controlled by the PHA.

3.1.1.8 Online verification (webapp, browser-based) – for future consideration

An online system (website/webapp, to be accessed using a browser) that may be used by verifiers for ascertaining the validity of health certificates presented by their holders.

Country A shall not make the use of the online verification webapp mandatory for the verification of health certificates.

Every Country A may make an online verification webapp available. A Country providing such a webapp should make exactly one online verification webapp available.

More detailed specifications are to be provided in the next revisions of this Trust Framework.

3.1.1.9 Online verification (endpoint, API) – for future consideration

An online system (such as a RESTful API) that may be used by verifiers for ascertaining the validity of health certificates presented by their holders.

Country A shall not make the use of the online verification endpoint mandatory for the verification of health certificates.

Every Country A may make an online verification endpoint available. Countries A providing an endpoint should make exactly one online verification endpoint available.

More detailed specifications are to be provided in the next revisions of this Trust Framework.

3.1.1.10 Online verification (phone service)

A phone service that may be established by Country A for enabling verifiers to check the validity of health certificates presented by their holders.

The service may be implemented through the national contact points for cross-border healthcare. The answer to a verification request should be provided within 2 working days.

3.1.2 Country B (country of verification)

The country of verification is responsible for verifying health certificates presented by their holders. The Country B shall accept valid health certificates that are issued following this Trust Framework.

3.1.2.1 List of certified verifiers

Specifications are to be provided in the next revisions of this Trust Framework.

3.1.2.2 Fetch and use

This is a process executed by Country B in order to retrieve information from the EU Public Key Directory/Gateway.

3.1.2.3 Trusted signing public keys, certificates or CAs

Signing keys are fetched by Country B from the EU Public Key Directory/Gateway and trusted by Country B.

All public keys and certificates marked as valid in the EU Public Key Directory/Gateway by Country A shall be trusted by Country B. If Country A has uploaded a public key certificate of a Certificate Authority (CA), all certificates issued by this CA shall be trusted by Country B.

3.1.2.4 Vaccination certificate verifier app

These are application(s) that are used by verifiers for ascertaining the validity of certificates presented by their holders.

In this version of the Trust Framework, only offline verification is supported. All verifier apps shall support offline verification.

3.1.3 Central services

The central services provide a process and a gateway for sharing trust anchors (public keys or certificates) between Countries A and B.

Before the gateway is implemented, Country B may request trust anchors directly from Country A through a mechanism ensuring the authenticity and integrity of this data, for example through the use of secure email or by downloading the information from the PHA's website of Country A.

After the implementation of the central services, the use of the direct trust establishment mechanism shall be discontinued.

3.1.3.1 EU Public Key Directory/Gateway

A directory that contains information about public keys or certificates published by Country A, as well as their metadata, and acts as a gateway used for providing trust information to national systems.

The directory shall be provided by a public sector body, such as the European Commission.

The directory shall be derived from the Lists of authorised issuers published by all Countries A. The contents shall be made publicly available. The list shall not contain personal information such as names of health professionals.

A flat structure could be foreseen for the PKD; further considerations are ongoing.

Country B shall ensure that the contents downloaded from the EU Public Key Directory (EU PKD) are regularly distributed to the verifier apps.

3.2 Legal basis

The trust framework described in this document is also subject to legal considerations.

As **some of the processing operations described involve personal data** (e.g. issuance and verification of certificates) such processing will fall under the scope of the General Data Protection Regulation (GDPR)[4].

GDPR provides for obligations on controllers (entities determining the purposes and means of processing of personal data, here e.g. organisations issuing and verifying vaccination certificates), such as to have a **legal basis** for their processing operations, **document them**, implement **appropriate security measures**, and to **inform data subjects** (natural persons data relating to whom are processed). It also provides rights for data subjects, such as the right to access the data controllers hold about them and to have it corrected. Additionally, GDPR establishes rules for **transfers** of personal data outside the EU/EEA.

[4] OJ L 119, 4.5.2016, p.1

4 Data formats

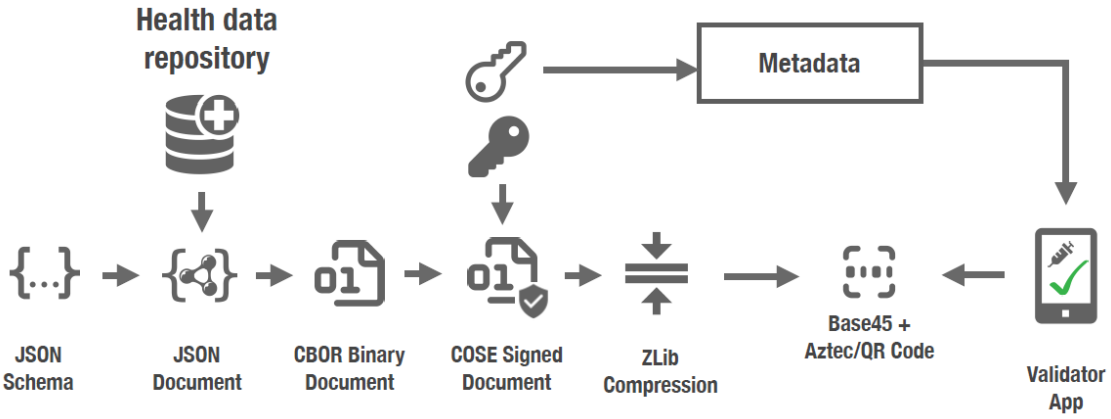

Figure 4: A proposal for data encoding and representation

4.1 UTF-8

UTF-8 will be used for character encoding.

4.2 FHIR

The Fast Healthcare Interoperability Resources (FHIR) standard data format is recommended to be used for expressing relevant health data. The data will be converted though appropriate mapping definitions to form the machine readable part of the certificate dataset using the JavaScript Object Notation (JSON) for data representation.

4.3 CBOR/COSE

The Concise Binary Object Representation (CBOR; RFC 8949) will be used for serializing the JSON data representation as binary data. The CBOR Object Signing and Encryption (COSE; RFC 8152) specification will be then used for digitally signing the machine readable certificate data.

5 Presentation formats

5.1 2D Barcode

Only 2D barcodes whose symbology is specified as an ISO standard SHALL be used. ISO standardized 2D barcodes symbologies include DataMatrix [ISO/IEC 16022], Aztec Codes [ISO/IEC 24778], and QR Codes [ISO/IEC 18004]. However, it is RECOMMENDED that the barcode is encoded as an Aztec code. Verifiers shall support all specified types of 2D barcodes.

5.2 W3C Verifiable Credentials

Decision about W3C Verifiable credentials to be made later.

6 Cryptography

6.1 Data signing

The CBOR Object Signing and Encryption (COSE) specifications will be used for digitally signing the machine readable certificate data.

To meet the timeline of this effort, and to ensure reliable and secure implementations of the technical specifications, the primary signing scheme for digital signatures supported by the trust framework is EC-DSA (Elliptic-Curve Digital Signature Algorithm) for cross-border use where unlinkability does not apply. As a fallback, RSA is also supported[5].

To further address the development of a privacy preserving approach for the anticipated domestic use case, adding further cryptographic schemes such as CL or BBS+ will be supported outside of cross border scenarios.

6.2 Data encryption

Data encryption of the machine readable part of the certificates will not be used. Selected disclosure of information can be implemented using other mechanisms. Adding data encryption of individual fields would increase complexity associated with key management.

7 Verification protocols

7.1 Offline

Offline verification shall be supported. By the term offline we refer to the scenario where the verifier requires at the time of the verification needs no online access to external resources (such as a call centre or a webapp) to perform the verification. Instead, the digital signature included in the 2D barcode will be verified through dedicated verification software. Signature verification will include (1) the verification of its validity against the provided public key and (2) the check that the public key is on the list of trusted keys held by the verifier app. The list will be fetched periodically from the EU PKD, however in the first phases of deployment, direct exchanges of keys may be used, as described in Section 3.1.3. Once this digital signature has been verified, the verification software can decode the information in the 2D barcode and rely on its content.

7.2 Online

Online verification will rely on the UVCI and it will be incorporated in the next version of the specifications (V2).

8 Glossary

Abbreviation	Meaning

[5] The RSA signing scheme should only be used if it is absolutely necessary, as it adds an around 50% size overhead to the resulting health certificate.

Abbreviation	Meaning
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CSCA	Country Signing Certificate Authority
DNS	Domain Name System
EEA	European Economic Area
eHDSI	eHealth Digital Service Infrastructure
EMA	European Medicines Agency
eMRTD	Electronic Machine Readable Travel Document
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation
ISO	International Organization for Standardization
OID	Object Identifier
NITAG	National Immunisation Technical Advisory Groups
PKI	Public Key Infrastructure
QR	Quick Response
RSA	Rivest–Shamir–Adleman
SOG-IS	Senior Officials Group - Information Security
SPOR	Substance Management Services (SMS), Product Management Services (PMS), Organisation Management Services (OMS), Referentials Management Services (RMS)
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
UVCI	Unique Vaccination Certificate/assertion Identifier
VC	Verifiable Credentials
W3C	World Wide Web Consortium
WHO	World Health Organization
ZKP	Zero Knowledge Proof