Electronic Health Certificate Specification

Version 1.0.5, 2021-04-18

1. Introduction

This document specifies a generic data structure and encoding mechanisms for electronic health certificates. It also specifies a transport encoding mechanism in a machine-readable optical format (QR), which can be displayed on the screen of a mobile device or printed on a piece of paper.

Versioning Policy

Versions of this specification follow semantic versioning and consist of three different integers describing the *major*, *minor* and *edition* version. A change in the *major* version is an update that includes material changes affecting the decoding of the HCERT or the validation of it. An update of the *minor* version is a feature or maintenance update that maintains backward compatibility with previous versions.

In addition, there is an *edition* version number used for publishing updates to the document itself which has no effect on the HCERT, such as correcting spelling, providing clarifications or addressing ambiguities, et cetera. Hence, the edition number is not indicated in the HCERT. The version numbers are expressed in the title page of the document using a *major.minor.edition* format, where the three parts are separated by decimal dots.

Version History

version	status	Comments
1.0.0	final	first version
1.0.1	draft	A number of clarifications, remove SSC
1.0.2	draft	Correct CIRCABC spelling
1.0.3	draft	Editorial changes
1.0.4	draft	Optical preamble update, editorial changes
1.0.5	final	As accepted in eHN WC 2021-04-19

2. Terminology

Organisations adopting this specification for issuing health certificates are called Issuers and organisations accepting health certificates as proof of health status are called Verifiers. Together, these are called Participants. Some aspects in this document must be coordinated between the Participants, such as the management of a namespace and the distribution of cryptographic keys. It is assumed that a party, hereafter referred to as the Secretariat, carries out these tasks. The health certificate container format (HCERT) of this specification is generic, but in this context used to carry the European Digital Green Certificate (DGC).

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 (RFC2119, RFC8174) when, and only when, they appear in all capitals, as shown here.

3. Electronic Health Certificate Container Format

The Electronic Health Certificate Container Format (HCERT) is designed to provide a uniform and standardised vehicle for health certificates from different Issuers. The aim is to harmonise how these health certificates are represented, encoded and signed with the goal of facilitating interoperability.

3.1 The European Digital Green Certificate (DGC)

The ability to read and interpret a DGC issued by any Issuer requires a common data structure and agreement on the significance of each data field of the payload. To facilitate such interoperability, a common coordinated data structure is defined through the use of a JSON schema that constitutes the framing of the DGC. The use of these elements is outside the scope of this specification, and is anticipated to be regulated by European Union law.

Note that the DGC defines the data structure, the actual wire format (HCERT) is content neutral.

3.2 Structure of the payload

The payload is structured and encoded as a CBOR with a COSE digital signature. This is commonly known as a "CBOR Web Token" (CWT), and is defined in RFC 8392. The payload, as defined below, is transported in a `hcert` claim.

The integrity and authenticity of origin of payload data MUST be verifiable by the Verifier. To provide this mechanism, the issuer of MUST sign the CWT using an asymmetric electronic signature scheme as defined in the COSE specification (RFC 8152).

3.3 CWT Claims

3.3.1 CWT Structure Overview

- Protected Header
- Signature Algorithm (`alg`, label 1)
- Key Identifier (`kid`, label 4)
- Payload
- Issuer (`iss`, claim key 1, optional, ISO 3166-1 alpha-2 of issuer)
- Issued At (`iat`, claim key 6)
- Expiration Time (`exp`, claim key 4)
- Health Certificate (`hcert`, claim key -260)
  - EU Digital Green Certificate v1 (`eu_dgc_v1`, claim key 1)
- Signature

3.3.2 Signature Algorithm

The Signature Algorithm (`alg`) parameter indicates what algorithm is used for the creating the signature. It must meet or exceed current SOG-IT guidelines.

One primary and one secondary algorithm is defined. The secondary algorithm should only be used if the primary algorithm is not acceptable within the rules and regulations imposed on the implementor.

However, it is essential and of utmost importance for the security of the system that all implementations incorporate the secondary algorithm. For this reason, both the primary and the secondary algorithm MUST be implemented.

For this version of the specification, the SOG-IT set levels for the primary and secondary algorithms are:

- Primary Algorithm: The primary algorithm is Elliptic Curve Digital Signature Algorithm (ECDSA) as defined in (ISO/IEC 14888–3:2006) section 2.3, using the P–256 parameters as defined in appendix D (D.1.2.3) of (FIPS PUB 186–4) in combination the SHA–256 hash algorithm as defined in (ISO/IEC 10118–3:2004) function 4.

This corresponds to the COSE algorithm parameter `ES256`.

- Secondary Algorithm: The secondary algorithm is RSASSA-PSS as defined in (RFC 8230) with a modulus of 2048 bits in combination with the SHA–256 hash algorithm as defined in (ISO/IEC 10118–3:2004) function 4.

This corresponds to the COSE algorithm parameter: `PS256`.

3.3.3 Key Identifier

The Key Identifier (`kid`) claim is used by Verifiers for selecting the correct public key from a list of keys pertaining to the Issuer (`iss`) Claim. Several keys may be used in parallel by an Issuer for administrative reasons and when performing key rollovers. The Key Identifier is not a security-critical field. For this reason, it MAY also be placed in an unprotected header if required. Verifiers MUST accept both options.

Due to the shortening of the identifier (for space-preserving reasons) there is a slim but non-finite chance that the overall list of DSCs accepted by a validator may contain DSCs with duplicate `kid`s. For this reason a verifier MUST check all DSCs with that `kid`.

3.3.4 Issuer

The Issuer (`iss`) claim is a string value that MAY optionally hold the ISO 3166-1 alpha-2 Country Code of the entity issuing the health certificate. This claim can be used by a Verifier to identify which set of DSCs to use for validation. The Claim Key 1 is used to identify this claim.

3.3.5 Expiration Time

The Expiration Time (`exp`) claim SHALL hold a timestamp in the NumericDate format (as specified in RFC 8392 section 2) indicating for how long this particular signature over the Payload SHALL be considered valid, after which a Verifier MUST reject the Payload as expired. The purpose of the expiry parameter is to force a limit of the validity period of the health certificate. The Claim Key 4 is used to identify this claim.

The Expiration Time MUST not exceed the validity period of the DSC.

3.3.6 Issued At

The Issued At (`iat`) claim SHALL hold a timestamp in the NumericDate format (as specified in RFC 8392 section 2) indicating the time when the health certificate was created.

The Issued At field MUST not predate the validity period of the DSC.

Verifiers MAY apply additional policies with the purpose of restricting the validity of the health certificate based on the time of issue. The Claim Key 6 is used to identify this claim.

3.3.7 Health Certificate Claim

The Health Certificate (`hcert`) claim is a JSON (RFC 7159) object containing the health status information, which has been encoded and serialised using CBOR as defined in (RFC 7049). Several different types of health certificate MAY exist under the same claim, of which the European DGC is one.

Note here that the JSON is purely for schema purposes. The wire format is CBOR. Application developers may not actually ever de-, or encode to and from the JSON format, but use the in-memory structure.

The Claim Key to be used to identify this claim is -260.

Strings in the JSON object SHOULD be NFC normalised according to the Unicode standard. Decoding applications SHOULD however be permissive and robust in these aspects, and acceptance of any reasonable type conversion is strongly encouraged. If non-normalised data is found during decoding, or in subsequent comparison functions, implementations SHOULD behave as if the input is normalised to NFC.

4 Transport Encodings

4.1 Raw

For arbitrary data interfaces the HCERT container and its payloads may be transferred as-is, utilising any underlying, 8 bit safe, reliable data transport. These interfaces MAY include NFC, Bluetooth or transfer over an application layer protocol, for example transfer of an HCERT from the Issuer to a holder's mobile device.

If the transfer of the HCERT from the Issuer to the holder is based on a presentation-only interface (e.g., SMS, e-mail), the Raw transport encoding is obviously not applicable.

4.2 Barcode

4.2.1 Payload (CWT) Compression

To lower size and to improve speed and reliability in the reading process of the HCERT, the CWT SHALL be compressed using ZLIB (RFC 1950) and the Deflate compression mechanism in the format defined in (RFC 1951).

4.2.2 QR 2D Barcode

In order to better handle legacy equipment designed to operate on ASCII payloads, the compressed CWT is encoded as ASCII using Base45 before being encoded into a 2D barcode.

The QR format as defined in (ISO/IEC 18004:2015) SHALL be used for 2D barcode generation. An error correction rate of 'Q' (around 25%) is RECOMMENDED. The Alphanumeric (Mode 2/QR Code symbols 0010) MUST be used in conjunction with Base45.

In order for Verifiers to be able to detect the type of data encoded and to select the proper decoding and processing scheme, the base45 encoded data (as per this specification) SHALL be prefixed by the Context Identifier string "HC1:". Future versions of this specification that impact backwards-compatibilty SHALL define a new Context Identifier, whereas the character following "HC" SHALL be taken from the character set [1-9A-Z]. The order of increments is defined to be in that order, i.e., first [1-9] and then [A-Z].

The optical code is RECOMMENDED to be rendered on the presentation media with a diagonal size between 35 mm and 60 mm to accommodate readers with fixed optics where the presentation media is required to be placed on the surface of the reader.

If the optical code is printed on paper using low-resolution (< 300 dpi) printers, care must be taken to represent each symbol (dot) of the QR code exactly square. Non-proportional scaling will result in some rows or columns in the QR having rectangular symbols, which will hamper readbility in many cases.

5 Trusted List Format (DSC list)

Each Participating country is REQUIRED to provide a list of one or more Certificate Signing Certificate Authorities (CSCAs) and a list of all valid Document Signing Certificates (DSCs), and keep these lists current.

For the list of CSCA certificates, each certificate:

- MUST contain a valid Country attribute in the subject DN that matches the country of issuance.
- MUST contain DN that is unique within the specified country.
- MUST contain a unique Subject Key Identifier (SKI) according to (RFC5280)

In addition, for the list of DSC certificates, each certificate:

- MUST be signed with the private key corresponding to a CSCA certificate published on the aforementioned list.
- MUST contain an Authority Key Identifier (AKI) matching the Subject Key Identifier (SKI) of the issuing CSCA certificate.
- MUST have a validity period that is in line with or longer than the validity period of all certificates signed using that key.
- SHOULD contain a unique Subject Key Identifier derived from the subject public key.

5.1 Simplified CSCA/DSC

As of this version of the specifications, countries should NOT assume that any Certificate Revocation List (CRL) information is used; or that the Private Key Usage Period is verified by implementors.

Instead, the primary validity mechanism is the presence of the certificate on the most recent version of that certificate list.

5.2 ICAO eMRTD PKI and Trust Centers

Member States can use a separate CSCA (as per the WHO advice)(#ref) - but may also use submit their existing eMRT CSCA and/or DSC certificates; and may even chose to procure these from (commercial) trustcenters - and submit these. However, any DSC certificate must always be signed by the CSCA submitted by that country.

6. Security Considerations

When designing a scheme using this specification, several important security aspects must be considered. These cannot preemptively be accounted for in this specification but must be identified, analysed and monitored by the Participants.

As input to the continuous analysis and monitoring of risks, the following topics SHOULD be taken into account:

6.1 HCERT signature validity time

It is anticipated that health certificates can not be reliably revoked once issued, especially not if this specification would be used on a global scale. Publishing of recovation information containing identifiers may also create privacy concerns, as this information is per definition Personally Identifiable Information (PII). For these reasons, this specification requires the Issuer of HCERTs to limit the validity period of the signature by specifying a signature expiry time. This requires the holder of a health certificate to renew it at periodic intervals.

The acceptable validity period may be determined by practical constraints. For example, a traveller may not have the possibility to renew the health certificate during a trip overseas. However, it may also be the case that an Issuer is considering the possibility of a security compromise of some sort, which requires the Issuer to withdraw an DSC (invalidating all health certificates issued using that key which is still within their validity period). The consequences of such an event may be limited by regularly rolling Issuer keys and requiring renewal of all health certificates, on some reasonable interval.

6.2 Key Management

This specification relies heavily on strong cryptographic mechanisms to secure data integrity and data origin authentication. Maintaining the confidentiality of the private keys is therefore of utmost importance.

The confidentiality of cryptographic keys can be compromised in a number of different ways, for instance:

- The key generation process may be flawed, resulting in weak keys.
- The keys may be exposed by human error.
- The keys may be stolen by external or internal perpetrators.
- The keys may be calculated using cryptanalysis.

To mitigate against the risks that the signing algorithm is found to be weak, allowing the private keys to be compromised through cryptanalysis, this specification recommends all Participants to implement a secondary fallback signature algorithm based on different parameters or a different mathematical problem than the primary.

The other risks mentioned here are related to the Issuers' operating environments. One effective control to mitigate significant parts of these risks is to generate, store and use the private keys in Hardware Security Modules (HSMs). Use of HSMs for signing health certificates is highly encouraged.

However, regardless of whether an Issuer decides to use HSMs or not, a key roll-over schedule SHOULD be established where the frequency of the key roll-overs is proportionate to the exposure of keys to external networks, other systems and personnel. A well-chosen roll-over schedule also limits the risks associated with erroneously issued health certificates, enabling an Issuer to revoke such health certificates in batches, by withdrawing a key, if required.

6.3 Input Data Validation

This specification may be used in a way that implies receiving data from untrusted sources into systems that may be of mission-critical nature. To minimise the risks associated with this attack vector, all input fields MUST be properly validated by data types, lengths and contents. The Issuer Signature SHALL also be verified before any processing of the contents of the HCERT takes place. However, the validation of the Issuer Signature implies parsing the Protected Issuer Header first, in which a potential attacker may attempt to inject carefully crafted information designed to compromise the security of the system.

Appendix A - Trust management

The signature of the HCERT requires a public key to verify. Countries, or institutions within countries, need to make these public keys available. Ultimately, every Verifier needs to have a list of all public keys it is willing to trust (as the public key is not part of the HCERT).

A simplified variation on the ICAO "*Master list*" will be used, tailored to this health certificate application, whereby each country is ultimately responsible for compiling their own master list and making that available to the other Participants. The aid of a coordinating Secretariat for operational and practical purposes will be available.

The *"Secretariat"* is a functional role; not a person or a piece of software. It is expected that the Digital Green Certificate Gateway (DGCG) will automate most of these tasks.

The system consists of (only) two layers; for each Member State one or more country level certificates that each signs one or more document signing certificates that are used in day to day operations.

The Member State certificates are called Certificate Signer Certificate Authorities (CSCAs) and are (typically) self-signed certificates. Countries may have more than one (e.g., in case of regional devolution). These CSCA certificates regularly sign the Document Signing Certificates (DSCs) used for signing HCERTs. Member States will each maintain a public register of the DSC certificates that is kept current, communicated to the Secretariat and also published at a stable URL for bilateral exchange. Member States MUST remove any revoked or stale certificates from this list.

The Secretariat will regularly aggregate and publish the Member States DSCs, after having verified these agains the list of CSCA certificates (which have been conveyed and verified by other means).

The resulting list of DSC certificates then provides the aggregated set of acceptable public keys (and the corresponding `kids`) that Verifiers can use to validate the signatures over the HCERTs. Verifiers MUST fetch and update this list regularly.

Member States may also bilaterally exchange CSCA certificates with a number of other Member States, verify these bilaterally and thus compile their own lists of CSCA and DSC certificates which is specific to that Member State. Verifiers may choose to rely on such a national list.

Such Member State-specific lists are expected to be adapted in the format for their own national setting. As such, the file format of this trusted list may vary, e.g., it can be a signed JWKS (JWK set format per RFC 7517 section 5) or any other format specific to the technology used in that Member State.

For the sake of simplicity: Member States may both submit their existing CSCA certificates from their ICAO eMRTD systems or, as recommended by the WHO, create one specifically for this health domain.

A.1 The Key Identifier (`kid`s)

The key identifier (`kid`) is calculated when constructing the list of trusted public keys from DSC certificates and consists of a truncated (first 8 bytes) SHA-256 fingerprint of the DSC encoded in DER (raw) format.

Note that Verifiers do not need to calculate the `kid` based on the DSC certificate and can directly match the key identifier in issued health certificate with the `kid` on the trusted list.

A.2 Differences to the ICAO eMRTD PKI trust model

While patterned on best practices of the ICAO eMRTD PKI trust model, there are a number of simplifications made in the interest of speed (and recognising the fact that the EU Regulation for EHN is sharply limited in time and scope):

- A Member State may submit multiple CSCA certificates.
- The DSC (key usage) validity period may be set to any length not exceeding the CSCA *and MAY be absent*.
- The DSC certificate MAY contain policy identifiers (Extended Key Usage) that are EHN specific.
- Member States may choose to never do any verification of published revocations; but instead purely rely on the DSC lists they get daily from the Secretariat or compile themselves.

A.3 Secretariat

In order to alleviate the burden of countries during the initial phase, there shall be a secretarial service which will:

A.3.1 version 1.00 - secretariat tasks

In the first version, the secretariat will:

- Maintain a non-public list of operational and legal contacts for each Member State to further the orderly management of this health specific set of master lists.
- Maintain a public 24x7 incident/security contact point.
- Maintain a public, integrity(secure) protected, single, up to date, aggregated, list of all CSCAs (DGCG).
- Shall validate the DSCs against the CSCA prior to publication (DGCG).
- Maintain a public, integrity(secure) protected, single, up to date, aaggregated, list of all DSAs thus validated (DGCG).
- Provide Member States with a secure (i.e. integrity protected) mechanism by which the Secretariat publishes the Member States aggregated CSCA and DSC lists (CIRCABC, DGCG, t.b.c)

In all cases, the secretariat acts not as content owner, all signatures and certificates must be provided by attendees.

Note 1: The current DGCG design allows for the list to be up to date in real-time (i.e., it is dynamically generated from a database with the most up to date information available at this point in time. So the here aggregated list is the output of a data query to given parameters against the uploaded data by the Member States). The technical requirement is lighter - the lists should be updated within 24 hours of any change submitted by a Member State.

Note 2: While data integrity is important from a security perspective, there are no confidentiality requirements for the lists of CSCAs and DSCs.

A.3.2 future version - secretariat tasks

In a later version - the service may also:

- Maintain a public, integrity (secure) protected, list of URLs with the most up to date CSCA lists for each Member State (DGCG).
- Maintain a public, integrity (secure) protected, list of URLs with the most up to date DSC lists for each Member State (DGCG).

A.3.3 Automation by the DGCG

The tasks that are marked *DGCG* or *CIRCABC are expected to be handled by DGCG automation,* CIRCABC or similar systems under control and responsibility of the Secretariat.

The format for the lists used for the interchange between the Member States and the Secretariat is waiting for the completion of the T-Systems/SAP proposal -- and should be optimised for clarity and interoperability. The ICAO Master List structure as defined in Doc 9303 part 12 may be considered.

This list format for interchange between the Member States is likely to be quite different from the format of the list of DSCs downloaded by the verifiers on a daily basis from the field. The Secretariat should publish the aggregated list of DSCs in an accessible and easy to use format (as seen from a verifier's perspective).

Member States are also expected to publish country-specific lists, in formats adapted to the technological setting at hand in that Member State.

The Secretariat shall also:

- Maintain a similar set of lists with 'test' certificates
- Maintain a set of test certificates - at least one for each country.

A.4 Extended key Usage Identifiers

The document signing certificate MAY contain Extended Key Usage extension fields; these being:

- OID 1.3.6.1.4.1.0.1847.2021.1.1 -- valid for test
- OID 1.3.6.1.4.1.0.1847.2021.1.2 -- valid for vaccinations
- OID 1.3.6.1.4.1.0.1847.2021.1.3 -- valid for recovery

The DSC may contain an extended key usage extension with *zero or more* key usage policy identifiers that constrain the types of HCERTs this certificate is allowed to verify. If present the verifiers SHALL verify the key usage against the stored HCERT.

In absence of any key usage extension, this certificate can be used to validate any type of HCERT. Other documents MAY define relevant additional extended key usage policy identifiers used with validation of HCERTs. _______________

- Fredrik Ljunggren, Kirei AB.
- Jakob Schlyter, Kirei AB
- Dirk-Willem van Gulik - For the Ministry of Public Health of the Netherlands
- Martin Lindström, iDsec Solutions AB