Covid Pass International QR Technology Summary

Document Control

The controlled copy of this document is maintained by NHSX. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validation.

Document Filename	COVID Pass International QR Technology Summary		
Version	0.1	**Status**	
Programme	Covid19		
Lead	Richard Pugmire	**SRO**	<TBC>
Owner	Michael Measures		
Lead Author(s)	Andrew Kay, Solutions Architect, NHSX, Shepherd Chengeta, Solutions Architect, NHSX		

Revision History

Version	Change notes	Author
0.1		AK

International standards for sharing vaccination certificates (VC) are still evolving and the way in which information is formatted and presented is subject to change. Considering this, the EU's Digital Covid Certificate (DCC, formerly known as Digital Green Certificate or DGC) presents the standard to which the UK will ultimately align.

EU DCC QR Code Specification

Details for the QR Code specification can be found

- Most up to date schema
- Specification overview

The UK implements all EU DCC specification QR code generation steps, which are

1. Obtain personal and vaccination data in JSON format.
2. Map data to full payload (see EU schema), validate health certificate against JSON schema and convert to CBOR document.
3. Convert the CBOR document to a CBOR Web Token (CWT) by signing with ECDsa SHA-256, using the existing private key(s) of the Covid status platform. Along with the payload, the CWT contains security metadata in a header object and a signature both used to validate that the payload was generated by a trusted source.
4. The CWT is then compressed using Zlib in order to reduce the size of the content.
5. The compressed CWT is encoded as a base45 string and prefixed with the context identifier string "HC1:". A new prefix is defined if any future versions of the DCC spec break backwards compatibility.
6. The base45 payload is then encoded as a QR code with a recommended error correction rate of "Q" (25%).

The steps to verify this generated QR code are followed in reverse order. Several libraries can be found that provide this logic open to implementation

- C#, Java, Kotlin, Swift, Python

The generated QR code is presented to the user as PDF or in the NHS app. As of schema version 1.3.0, ***one QR code is to be generated per vaccine dose***. Future releases will also include the option to save to a digital wallet. Sample UK generated QR codes can be provided on request.

Dataset

The table below identifies all the data fields for vaccination certificates specified by the EU DCC standard.

Data Field	Property Name	Expected Values
Name	"nam"	Surname and forename

date of birth	“dob”	ISO 8601 date format restricted to range 1900-2099"
disease or agent targeted	“tg”	SNOMED CT coded.
vaccine/ prophylaxis	“vp”	SNOMED CT / ATC Classification coded
vaccine medicinal product	“mp”	Union Register of Medicinal Products coded. (see section 2.3. of DCC spec)
vaccine marketing authorization holder or manufacturer	“ma”	SPOR-System for ISO IDMP coded. (see section 2.4. of DCC spec)
number in a series of vaccinations/doses	“dn”	Number of dose administered: positive integer, range: [1,9]
Total series of doses	“sd”	Total doses in Series: positive integer, range: [1,9]
Date of vaccination	“dt”	Date of Vaccination. ISO 8601 date format restricted to range 1900-2099"
Member State of	“co”	Preferred Code System: ISO 3166 Country Codes (2-letter codes)
Certificate issuer	“is”	UTF-8 encoded identifier
Certificate identifier	“ci”	Uniquely structured and formatted identifier
Version	"ver"	Defines schema version. Current implemented schema is version **“1.3.0”**

To facilitate interoperability, the dataset presented above is structured in a common coordinated data structure using a JSON schema that constitutes the framing of the European Digital Covid Certificate (DCC). In turn, DCC is carried in the health certificate container format (HCERT), which is designed to provide a uniform and standardised vehicle for health certificates from different issuers. Essentially, HCERT aims to harmonise how certificates are represented, encoded, and signed. DCC therefore defines the data structure and HCERT is the actual wire format.

The detailed analysis of the JSON schema elements is outside the scope of this specification. However, what is important to note is that the object contains several machine-readable properties that are to be interpreted by a verifying application. A full breakdown of each property contained within the objects can be found here within the DCC Value Sets guidelines.

Signed CWT

Once formatted correctly, the health certificate is encoded into CBOR and signed as a CWT (ref). This is a CBOR representation of a JWT and follows a similar structure of header, payload and signature. Contained within the header and payload are a number of claims that can be extracted and used to verify the authenticity of the presented data. One of these claims also represents the health certificate itself.

CWT Claims

Claim	**Claim Key**	**Location**	**Expected Values**
“Alg”	1	Protected Header	-7: Represents the algorithm ES256
“Kid”	4	Protected Header	Byte array, needs to be base64 encoded for key identifier
“Iss”	1	Payload	“GB”
“Exp”	4	Payload	Expiry date in epoch time
“Nbf”	6	Payload	Not valid before date in epoch time
“HCert”	-260	Payload	Health certificate claim containing single property with key of “1” which then subsequently contains the health data to be shared.

Trust Framework

Public key infrastructure development is currently ongoing. Until a PKI solution is fully developed, an interim solution is in place to use self signed certificates. Corresponding interim public keys available here as JSON objects.

Public Key Format

Data Field	Property Name	Expected Values
Key Identifier	“kid”	Base 64 encoded key identifier. The corresponding value can be extracted from the header of the signed CWT.
Public Key	“publicKey”	Base 64 encoded SPKI (Subject Public Key Info) string. X and Y values to be extracted and used to verify the signature of the signed CWT.

Further details will be distributed publicly once the scanner app has been officially announced. It will be possible for third party developers to integrate the PKI developed for our VC solution and scan the NHS Digital app’s QR code.

Considering this, in the current implementation, prevention of impersonation attempts is ultimately the responsibility of the certificate verifier. At the point of issuance of the certificate, the identity of the citizen is based on demographic data (full name, date of birth). These details form the identity that will be bound to the certificate which is issued. At the point of verification, the verifier will use the demographic information as presented in the certificate and compare it with demographic details in a secondary ID (passport, ID card, driver’s license) to verify the certificate holder.

Unique Vaccination Certificate Identifier (UVCI)

Each vaccination certificate contains an identifier under the “ci” property that uniquely identifies it against all other vaccination certificates. Once a VC is issued, a UVCI will be generated and stored in a database and an online lookup service that is currently under development will allow for verification based on that UVCI. Each UVCI is to be globally unique, but for now this service is expected only to be able to verify certificates issued by NHS Digital.

Details of the UVCI, such as its structure and composition can be found within annex 2 of this document.

Further details of the online verification service will be provided once the service is production ready.

It has been decided that individual QR codes for each dose, created for the same person, will be treated as one certificate and therefore will share the same UVCI.

Example Data

Please note that for security reasons, the data provided here has been generated for testing purposes in a non-production environment and cannot be verified via the interim public keys provided. Instead, a separate public key is attached which can be used.


```
JSON: {
"nam": {
 "fn":"GANTES",
 "fnt":"GANTES",
 "gn":"Evan",
 "gnt":"EVAN"
},
"dob":"1918-06-28",
"v": [{
 "ci":"URN:UVCI:01:GB:16251382570319MLZ78XK#P",
 "co":"GB",
 "dn":1,
 "dt":"2020-12-05",
 "is":"NHS Digital",
 "lot":"OBQUJKGQDBCLVDEFWUUQ",
 "ma":"ORG-100030215",
 "mp":"EU/1/20/1528",
 "sd":2,
 "tg":"840539006",
 "vp":"1119349007"
}],
"ver":"1.3.0"}
```

CBOR:
“a401624742041a6105312c061a60dd0580390103a101a4617681ab626369782655524e3a555643493a30313a47423a31363235313338323537303331394d4c5a3738584b235062636f62474262646e016264746a323032302d31322d30356269736b4e4853204469676974616c626d616d4f52472d3130303033303233135626d706c45552f312f32302f313532386273640262746769383430353339303036627670 6a3131313933343930303736c6f74744f4251554a4b47514442434c5644454657555551636 46f626a313931382d30362d3238636e616da462666e664741 4e54455362676e644576616e63666e746647414e54455363676e74644556414e6376657265312e3e”

CWT:
“d2844ea2012604494b6579312d73697431a059010aa401624742041a6105312c061a60dd0580390103a101a4617681ab626369782655524e3a555643493a30313a47423a31363235313338323537303331394d4c5a3738584b235062636f62474262646e016264746a323032302d31322d30356269736b4e4853204469676974616c626d616d4f52472d3130303033303233135626d706c45552f312f32302f313532386273640262746769383430353339303036627670 6a3131313933343930303736c6f74744f4251554a4b47514442434c5644454657555551636 46f626a313931382d30362d3238636e616da462666e6647414e54455362676e644576616e63666e746647414e54455363676e74644556414e6376657265312e332e305840052228a6c42b75cd1076fd9f4553851469dab998139e99a36b78334cae83d849da6dcc3d6f7154adc97fa67bde5a9228ebbad9309a0e34cf56ca6123b39a45a1“

COMPRESSED:
“789cbbd4e2b788518dc5d33bb5d250b738b3c470412423d712c624772716a94456431d36a984bbac0d968ccc0b1997249635ae4e4aceac500b0df2b30a0d73f6b43230b47277b2323433323534b6303235373036b4f4f58932b788f0560e484ace071a939492c79894529265646064a06b68a46b609a94599cede711ace092999e59929893949b98eb1fe4ae6b686060606c6064689a945b90e31aaa6fa86f64a06f686a6491549cc29454929e696162606a6c6960609654569065686868696c02e49927e7e49794f83b05867a79bb07ba3839fb84b9b8ba8587860626a7e42765195a1a5ae81a98e91a5924e725e62e494acb4b7377f40b710d4e4acf4b712d4bcc4b4ecb2b810a25a7e795a4b88639fa2597a516a51aea19eb194438b02a692c3ba25d7a56a0ecef7cd7e05691cc5b3b6708cf9bb938bbc2d8675df30dcf5bb9676cf30b43d69eac5f567d2f6a92c6eb5d370d66f1999c0f3b95a8bc7996eb420051c87600“

BASE45:
“6BFOXNYTSMAHN-HUVQG:M89AP77N$OQA8+N4G2KR4G.4.HLX+A8V3GJLTWNDW1:ZH6I1$4JN:IR1MPK9CZL*H1VUU8C1VTE5ZM3768LEXNM/Q6SF6*T6846XW6C46J*M$1VNI61EHP*AB6932Q8G39ZILAPZXI$MI1VCKWC1QDGZKP9C.XIX$JN9TL%L:NI$0K/NIPTI7UJQWT.+S1QDC8CO8CG8C3AD:XIBEIVG395EV3EVCK09D5WCFVA.QO5VA81K0ECM8CXVDC8C90JK.A+
C/8DXEDKG0CGJ9ETE7J7HVJV0XLF:SNHON%E72ZG+FNS*GK.G+4.$S6ZCQHB7MBDG34LT5CB/9TL4T.B9NVP*QEF%U6DEH+9C9Q%DE9Q9IN9UP4EG9Y4KCT3$KQ/G2SVV7J$%25I3KC3X83M77CG5SQ5UNK/KFLFKICU4DRL.AP$P.M7551+UJX77KSO13DVWUS9QXJN
YD3J1.5RRZL1.AX:5:OI/XT8/6S0DIJT-1H-I9$NP3JLF8BFAD-E”

PREFIXED:
“HC1:6BFOXNYTSMAHN-HUVQG:M89AP77N$OQA8+N4G2KR4G.4.HLX+A8V3GJLTWNDW1:ZH6I1$4JN:IR1MPK9CZL*H1VUU8C1VTE5ZM3768LEXNM/Q6SF6*T6846XW6C46J*M$1VNI61EHP*AB6932Q8G39ZILAPZXI$MI1VCKWC1QDGZKP9C.XIX$JN9TL%L:NI$0K/NIPTI7UJQWT.+S1QDC8CO8CG8C3AD:XIBEIVG395EV3EVCK09D5WCFVA.QO5VA81K0ECM8CXVDC8C90JK.A+
C/8DXEDKG0CGJ9ETE7J7HVJV0XLF:SNHON%E72ZG+FNS*GK.G+4.$S6ZCQHB7MBDG34LT5CB/9TL4T.B9NVP*QEF%U6DEH+9C9Q%DE9Q9IN9UP4EG9Y4KCT3$KQ/G2SVV7J$%25I3KC3X83M77CG5SQ5UNK/KFLFKICU4DRL.AP$P.M7551+UJX77KSO13DVWUS9QXJN
YD3J1.5RRZL1.AX:5:OI/XT8/6S0DIJT-1H-I9$NP3JLF8BFAD-E”

Resulting QR:

Public Key:

{

"kid": "S2V5MS1zaXQx",

"publicKey":
"MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAECyzJjCOd6AZI85tOFAtvagr0MUcnM11ces2tHHsjg/TiEUX0M6tfNJloc27xeLbvrphVUDM5RoLtinu5bCQ1ug=="

}

Scanner Specification

The EU DCC standard community provides example implementation data and QR Scanner demo.

- Verifier demo app repository
- Test data for different countries

NHSx is currently developing a “QR Scanner” app solution to be publicly distributed. The goal of this app is to allow a user to verify that a presented VC, in the form of a QR code, is valid and has been issued from a trusted source. This QR code holds a citizen's personal and vaccination details such as: name, date of birth, vaccination type and other information as specified by developing international standards.