Covid Pass PKI Specification

Document Control

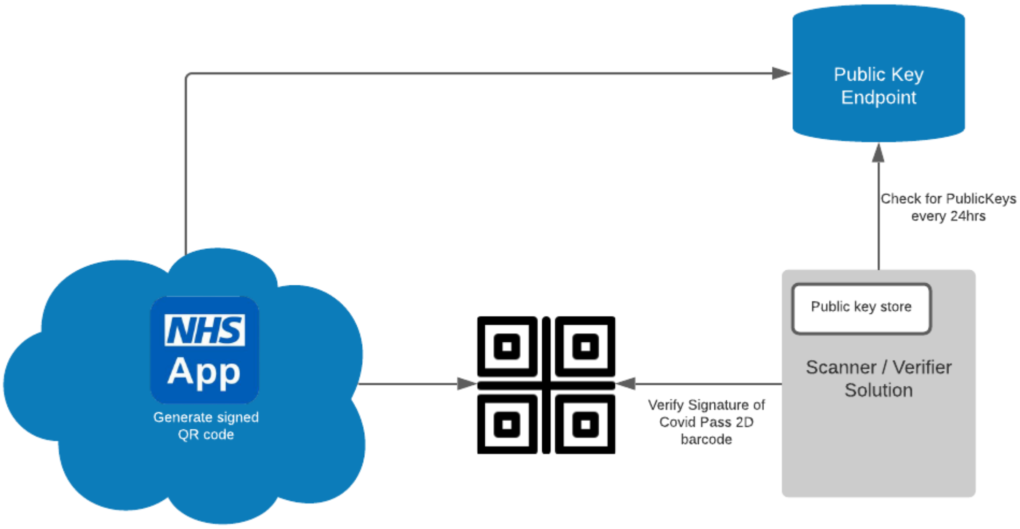
The controlled copy of this document is maintained by NHSX. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validation.

Document Filename	PKI Specification		
Version	0.2	**Status**	
Programme	Covid19		
Lead	Richard Pugmire	**SRO**	<TBC>
Owner	Michael Measures		
Lead Author(s)	Andrew Kay, Solutions Architect, NHSX		

Revision History

Version	Change notes	Author
0.1		AK
0.2	Add staging environment info	AK

The purpose of this document is to detail acceptable usage of the Interim Covid Pass PKI solution and outline the means in which a third party can access public keys to be used for verification.


Public Key Endpoint
Check for PublicKeys every 24hrs
NHS App
Generate signed QR code
Public key store
Scanner / Verifier Solution
Verify Signature of Covid Pass 2D barcode

All public keys are accessible from the Public Key endpoint described in this document. The endpoint is publicly available to anyone and there are no restrictions on who can access it or from where.

It's important to note that each of the keys available have been generated from a number of self-signed certificates and are designed to be a temporary solution while the procurement of a commercial Certification Authority (CA) is underway.

Signing keys are rotated every few weeks and a set of new public keys will be deployed in September 2021 so it is important that you continue to check for new public keys.

Public Key Endpoint - PRODUCTION

Attribute	Value
URL	https://covid-status.service.nhsx.nhs.uk/pubkeys/keys.json
Query parameters	No query parameters required
Authorisation	No authorisation required
HTTP method	GET
Response structure *(EXAMPLE, single key)*	[{ "kid": "S2V5MVJF", "publicKey":"MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEtWokvmqrJOv/0PO9Vy8lpb6SgWw+rao0qIXntO/Bf7ExryL3yyKRI73IqAh38Lk4joqHrZK8XLZV9PMclgmTVg==" }, {*...more keys, repeating field...*}]

Public Key Endpoint - STAGING

Attribute	Value
URL	https://stage.covid-status.service.nhsx.nhs.uk/pubkeys/keys.json
Query parameters	No query parameters required
Authorisation	No authorisation required
HTTP method	GET
Response structure *(EXAMPLE, single key)*	[{ "kid": "S2V5MS1kZXYx", "publicKey":"MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAECBWpEPxHu8occBOj9PbyMHDlQtcjuvh9GSF0tqTLSrEixzMP20NW09tlnox34rwJkcdLA7KEP39nR+7J8lOV4w==" }, {*...more keys, repeating field...*}]

JSON Key Format

Data Field	**Property Name**	**Values**
Key Identifier	“kid”	Base 64 encoded unique key identifier.
Public Key	“publicKey”	Base 64 encoded SPKI (Subject Public Key Info) string. X and Y values to be extracted and used to verify the data signature.

Usage

In the case that one of the keys has been compromised, revocation will be managed manually by removing the compromised key from the response. Post September 2021 a CRL will be issued via a different endpoint, TBD.

Because of this, in order to ensure third parties wishing to verify a Covid Pass have the most up to date version of the keys, it would be advised that the public key endpoint be hit every 24 hours.

Updates

Our github repository will contain the current version of this guidance and it may be updated from time to time. Please subscribe for updates by signing up to the github repo if you implement this service in your application.