Certificado Vacunas

Pautas Lectura QR Vacunas formato Unión Europea

Montevideo, Agosto 2021

Ministerio de Salud Pública

Ministerio de Economía y Finanzas

agesic

Uruguay Presidencia

Control de Cambios

Fecha	Versión	Descripción del Cambio
15/07/2021	1.0	Versión inicial.
21/07/2021	2.0	Pautas para la interpretación de los datos contenidos en el QR de las vacunas de las personas.
03/08/2021	3.0	Se modifica JSON, se agregan datos patronímicos y fecha emisión.

Contenido

1. Introducción

El presente documento brinda las pautas para la implementación de una aplicación de lectura de un QR con formato Unión Europea.

Este documento está dirigido a aquellas empresas u organizaciones que requieran implementar una aplicación para el control de acceso a eventos.

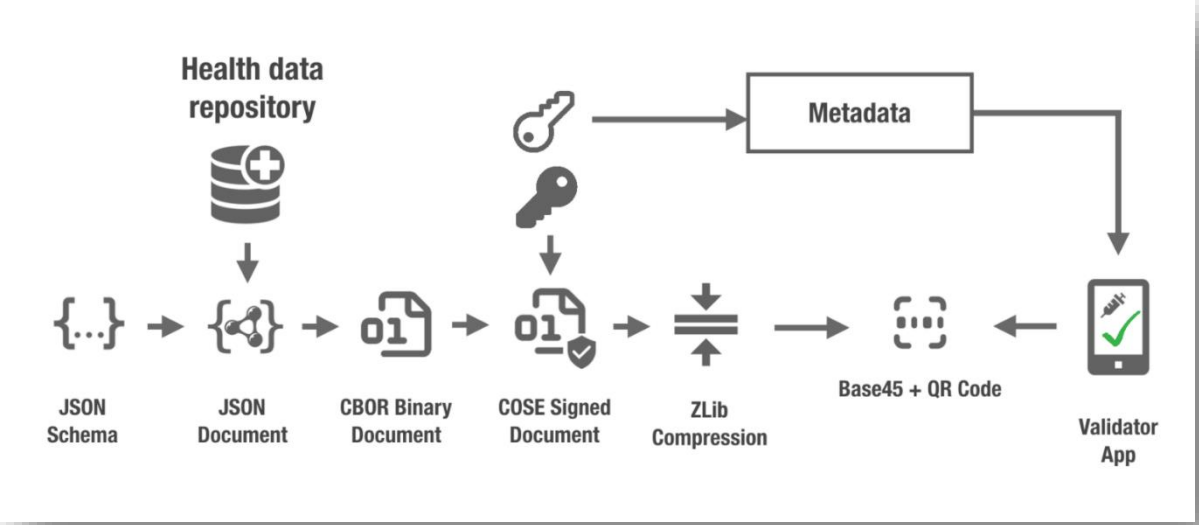
En esta segunda versión del documento se incluye la sección de interpretación de los datos contenidos en el QR de vacunas.

2. Obtener información de QR de Unión Europea (UE)

A continuación, se describen los pasos necesarios para obtener la información del estatus sanitario contenido en el QR con el que van a contar las personas.

QR ejemplo

A continuación se describe el paso a paso y los estándares utilizados para la obtención de la información.



Resultado de lectura de QR

- ✓ Al leer el QR lo que se obtiene es una secuencia de números, caracteres y símbolos que comienzan con “HC1:”. Lo que se obtiene como resultado se encuentra codificado en base45 y se ve de la siguiente manera:

*HC1:NCFOXNYTSFDHJI8Y0PQ8KGXMDVJ S3U 2ZH6.%5I$PSD1K P/X92-LXKC9I951SB2P6+I41A X9SJNQ$AKMG MG1REJED4C9A-KK/FGPLO+IONIHJL+KIM99+V4RIN3:6G6M. K:004EC7EC89C1J5G3B3UJ4HBXLIF%6C-62R6DXGSU10+P:S9ZT56+PTSGMNJ%JCXWDOVDQHJRWDVD1HXSDZ0%00%/TF$2XVG%+TFKB7LJUVI0M6 AKA0$9OYMPK9G*H*XCNMNJDUW5K 0WNBPY-6$FJTV79/RUHPN UR%QXKN:BCA$UY*E4GB/EL4 63EH%X1BE6.3E/ZJBDPXFV-4N-K2PM9+JU9LBMWC /MY/C-T9%MUD:G1D55%1KUSR02XT7S+U4GWZJDC-HDNLM.RHZ5.LNXZ5-UL0NJW:2YDJ:3BNAGG8V2$K+3S9:IMXFP VT/JG98U%O.NM+K7T5QD:EX%N:0VVIA+I135EIHTX9OB5BSLCKXLHV801CCPI13OUSRJHJ11P/T6$1Q684W9 I%+VS2S4-HN%247F5.0$SU O2T5EBT4PFM656KRLAOPAVJ$LH-$11F1D5OTDMDW5MUAJXT84PY3S %P**K0-VAM67DASRA$H8NBOLXT-9142FTJJ8*VMK57 UEWJ3MH5JB%+224NNBU*

- ✓ La cabecera HC1 es parte del estándar de codificación y debe ser removida antes de comenzar el proceso de decodificación. Se obtiene el siguiente contenido:

*NCFOXNYTSFDHJI8Y0PQ8KGXMDVJ S3U 2ZH6.%5I$PSD1K P/X92-LXKC9I951SB2P6+I41A X9SJNQ$AKMG MG1REJED4C9A-KK/FGPLO+IONIHJL+KIM99+V4RIN3:6G6M. K:004EC7EC89C1J5G3B3UJ4HBXLIF%6C-62R6DXGSU10+P:S9ZT56+PTSGMNJ%JCXWDOVDQHJRWDVD1HXSDZ0%00%/TF$2XVG%+TFKB7LJUVI0M6 AKA0$9OYMPK9G*H*XCNMNJDUW5K 0WNBPY-6$FJTV79/RUHPN UR%QXKN:BCA$UY*E4GB/EL4 63EH%X1BE6.3E/ZJBDPXFV-4N-K2PM9+JU9LBMWC /MY/C-T9%MUD:G1D55%1KUSR02XT7S+U4GWZJDC-HDNLM.RHZ5.LNXZ5-UL0NJW:2YDJ:3BNAGG8V2$K+3S9:IMXFP VT/JG98U%O.NM+K7T5QD:EX%N:0VVIA+I135EIHTX9OB5BSLCKXLHV801CCPI13OUSRJHJ11P/T6$1Q684W9 I%+VS2S4-HN%247F5.0$SU O2T5EBT4PFM656KRLAOPAVJ$LH-$11F1D5OTDMDW5MUAJXT84PY3S %P**K0-VAM67DASRA$H8NBOLXT-9142FTJJ8*VMK57 UEWJ3MH5JB%+224NNBU*

- ✓ Luego de decodificar el base45 se obtiene un objeto COSE comprimido con zlib que se ve de la siguiente manera:

<Buffer 78 da bb d4 e2 b7 88 d1 42 85 c5 e3 9f b6 b3 e3 9b cb 1c cb 16 44 32 96 2e 65 cc 54 0a 4e cc 29 4d 29 ad 54 62 91 4a 64 dd ae c6 26 95 70 4f 4b 4d 22 ... 400 more bytes>

✓ Como siguiente paso debemos descomprimir el objeto anterior con zlib y obtenemos el objeto COSE firmado descomprimido:

{
p: <Buffer a2 01 38 24 04 48 fe 2b 43 41 ec d3 08 a6>,
u: {},
cwt: <Buffer a5 01 69 22 53 3a 20 22 38 35 ... 323 more bytes>,
signers: <Buffer 0c d2 8d 5e 3e 14 d4 47 df ... 206 more bytes>
}

✓ A continuación lo que se debe hacer es validar la firma con la cual está firmado el objeto COSE. Para esto tenemos 2 maneras de implementarlo:

1. Utilizar la implementación del proyecto DIGGSweden.

   - ObjCOSE.verifySignature(PublicKey);
     Donde PublicKey es un objeto PublicKey de Java que tiene la clave pública del certificado utilizado para la firma del COSE. El PublicKey se debe construir utilizando la clave pública del certificado utilizado para la firma.
     (Ver msp-empresa.pub)

2. Validar la firma manualmente como se detalla a continuación:

   Para verificar la firma se usará el dato **signers** obtenido en el paso anterior, para el proceso de firma se usaron los siguientes parámetros a tener en cuenta para la verificación:

   - Algoritmo de encriptación **"SHA256withRSA/PSS"**, más detalladamente sería **PS256(-37, "PS256", "SHA256withRSA/PSS")**, la extensión ***PSS*** se puede definir también como **padding** en caso que no se pueda especificar directamente **"SHA256withRSA/PSS",** estos detalles se conocen por parte del agente que firma los códigos QR.

✓ Luego de verificada la firma del objeto COSE podemos obtener del mismo el objeto cwt que contiene la siguiente estructura, de la cual nos interesa el contenido del claim 99 (objeto CBOR):

```
{
 1 => ISSUER,
 4 => EXPIRATION TIME,
 6 => ISSUED AT,
 99 => 'Objeto CBOR',
 98 => 'Objeto CBOR en array de bytes'
}
```

3. Ejemplo de Referencia

Se adjuntan proyectos de ejemplo:

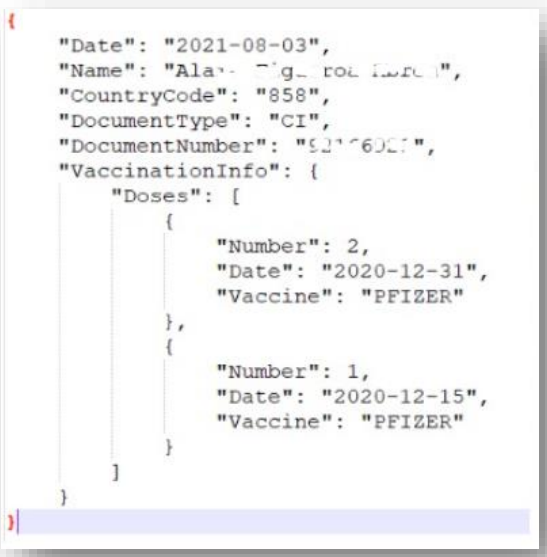
>> *ejemplo-validacion-qrCode-UE.zip* desarrollado en Java.

>> desarrollado en REACT.

4. Contenido e Interpretación de los Datos del QR

4.1. Datos Contenidos en el QR

Los datos contenidos en el JSON del QR de vacunas, son todas las dosis que se le han administrado a la persona ordenadas de forma decreciente (desde la última dosis a la primera).



Ejemplo de JSON 1

Campo	Descripción
Date	Fecha de emisión del certificado.
Name	Nombre de la persona
Country Code	Para los documentos que DocumentTyse =”CI” va a venir cargado el código 858 que es Uruguay.
DocumentType	Posibles valores: “CI”, “PAS”
DocumentNumber	Número de documento
Number	Número de dosis recibidas. Es una secuencia.
Date	Fecha de recibida la dosis. Formato aaaa-mm-dd
Vaccine	Nombre de la vacuna recibida

5. Referencias

https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v1_en.pdf

https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-value-sets_en.pdf

https://github.com/DIGGSweden/dgc-java

https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate_json_specification_en.pdf

https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf