Biometric Health Card
Adrian Gropper
http://bit.ly/biometricVC -

Background
Converting the COVID CDC Vaccination Card into a standardized digital credential is turning out to be harder than expected. The conversation has become prominent in the news and risks being politicized to the detriment of public health efforts around the world.

The core problem is a combination of privacy and equity. Paper vaccination credentials are only loosely linked to a verified identity like a driver's license. Many vaccination or test sites do not ask for proof of identity and proponents of digital credentials like to talk about how easy it is to buy fake cards.

The privacy and equity problem is aggravated by the range of contexts where the credentials are to be verified. These range from totally voluntary to essential: restaurant > travel > school > employment.

Behind the scenes, there are a handful of groups with different agendas promoting their digital solutions to the privacy and equity problems. Their common denominator is a QR code that can be voluntarily presented on paper, like the current CDC card, or on a smartphone. It's assumed that the presentation will have: name and DOB and some have a photo as well.

Introducing a biometric into the digital credential to prevent fraud is a privacy issue if the biometric is centralized, as in a drivers license authority or Aadhaar in India.

Digital Health Card Concept
The novel concept is to add a quantized face that is still ***human-verifiable*** to the digital credential presentation. The hash of the quantized face, but not the face itself, would be signed and verifiable as part of the digital credential represented by the QR code.

works now - try it - used https://www.online-qrcode-generator.com

Figure 1: A Digital Credential with a Quantized face on paper or screen

To quantize the face, I used GIMP to reduce the resolution to 32 x 32 pixels without interpolation and then indexed to 16 colors. The idea is that any camera that can read a QR code can also reliably recover the 16 colors with zero errors so the hash can be matched with the hash in the QR code credential. The choice of a 512 Byte template is just an example.

The verifier uses a mobile app that combines four functions:

- A typical QR code API returns the digital credential (directly or by reference).
- A typical camera API returns the quantized photo.
- A clustering algorithm, like a trivial JPEG compression algorithm, recovers the 16 indexed colors in the original and calculates the hash of the quantized photo.
- A typical signature verification algorithm compares the locally calculated hash with the one in the signed digital credential and reports Success or Fail.

A smartphone app is obviously needed at the issuer to produce the QR code. That app also needs a face photo, as above, to quantize and hash and add to the credential before signing.

It's important to recognize that, once the digital credential is handed or sent to the patient, the issuer does not need to store either the original or the quantized image.

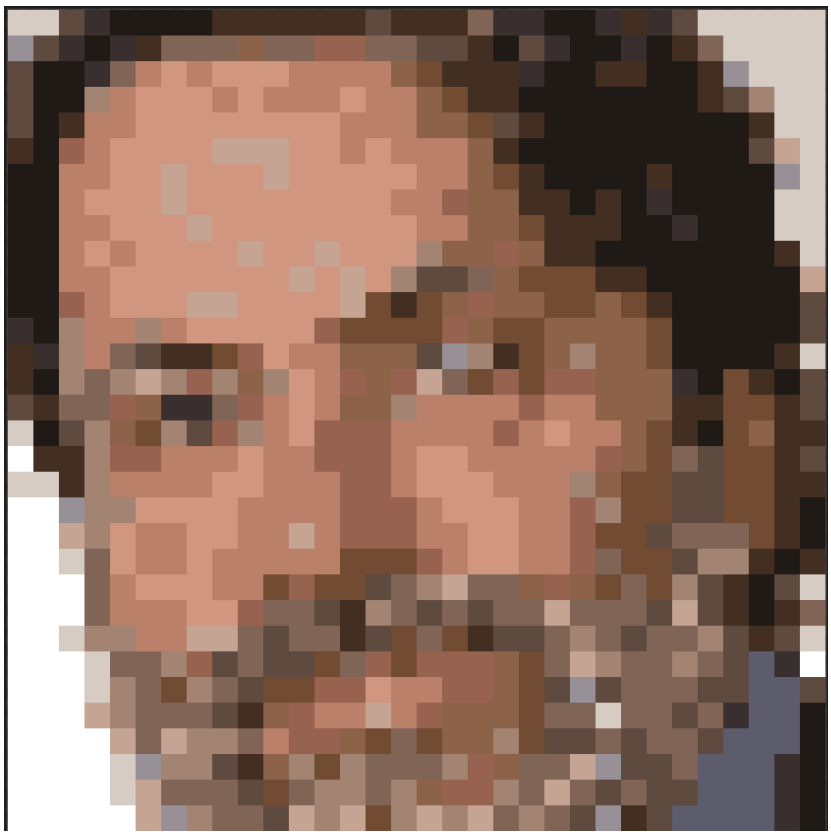
Privacy sensitive patients that don't trust the issuer with any biometric have the option of taking their own selfie and using a quantizer app so they can deliver the hash back to the issuer to sign and then verify. A failed verification results in immediate revocation of the credential. Variations on this semi-self-issue option are possible if revocation is not available.

Another important privacy feature, other credentials issued to the same patient would, of course, use a new face photo each time with different lighting and perspective so the hash of the quantized face would be different (< 512 Bytes of entropy in the example, but still significant). This avoids issuers or verifiers colluding to correlate across credentials on the basis of the hash.

Supporting Materials

	Challenges for VaxCreds	Solutions
Standards	Wait for 'common standard' to emerge for issuance so that verification can become simple	No standards required for QR code in short term. Transfer complexity to free universal scanning apps that can read any QR vaxcred
Ecosystem	Integration complexity with external ecosystem of Blockchain, EHR, identity	Treat vaxcreds as one-way offline output with no linkage back to EHR/Blockchain for verification. With no reverse linkage, no PII audit trail possible. No additional user data collection required.
Biz Model	Companies pushing models with cloud services, pay-per-verification, exploit streaming data	Use offline-offline solution, nearly free to everyone. States can pay for app.
Equity	Govt insist equity, no smartphones, no PII for vulnerable population	Paper-first approach, selective disclosure with initials/year (not full PII),

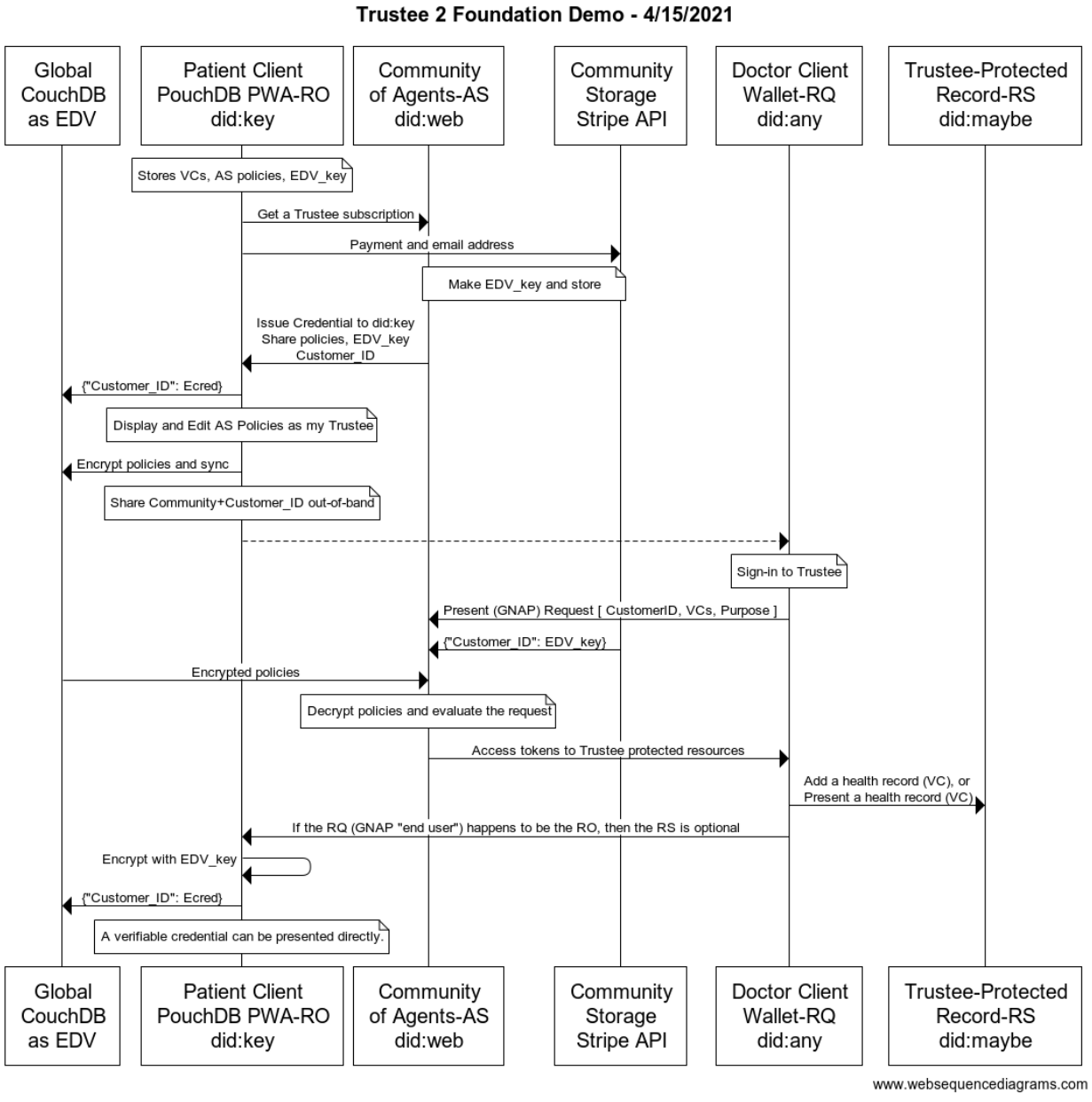
PathCheck.org



32x32x4-3.raw

```
  0   0E 0E 03 01 00 00 00 00|02 02 02 02 02 02 03 02|02 02 07 01 01 00 00 01|02 01 03
 20   0B 03 01 00 01 02 07 07|07 06 07 07 08 08 07 07|03 03 02 00 03 01 00 00|01 00 02
 40   03 00 00 01 07 0A 0C 0A|0C 0C 0C 0A 0A 0A 0A 06|04 02 02 02 01 00 00 02|02 00 00
 60   03 00 00 09 0A 0C 0C 0C|0A 0C 0A 0A 0A 0C 0A 0A|06 04 02 02 00 00 00 00|00 00 00
 80   03 00 02 0A 0A 0C 0C 0C|0C 0C 0C 0C 0C 0A 0A 0A|06 06 04 03 02 00 00 00|00 00 00
 A0   02 00 08 0A 0C 0C 0C 0C|0D 0D 0D 0C 0C 0A 0C 0A|0A 0A 06 02 00 00 00 00|00 00 00
 C0   00 00 0A 0A 0C 0C 0D 0C|0C 0C 0D 0C 0C 0C 0C 0C|0A 0A 06 04 02 00 00 00|00 02 00
 E0   00 00 0A 0C 0C 0C 0D 0C|0C 0C 0C 0C 0C 0C 0C 0A|0A 08 06 06 02 02 00 02|00 01 00
100   00 00 0A 0A 0C 0C 0C 0D|0C 0C 0C 0C 0C 0C 0C 0C|0A 0A 06 06 04 02 02 02|00 00 01
120   00 00 0A 0C 0A 0C 0C 0C|0C 0D 0C 0C 0D 0C 0C 0C|09 06 06 08 06 02 02 00|00 00 00
140   00 00 0A 0A 0C 0C 0C 0C|0C 0C 0C 0D 0C 0D 0C 09|03 03 07 06 04 04 04 02|02 00 00
160   00 00 08 0A 0C 0C 0C 0D|0D 0C 0C 0C 0C 0D 04 02|04 06 08 06 06 04 04 06|04 02 00
180   01 00 09 0A 0A 09 0A 0C|0C 0C 0C 0C 08 04 04 04|04 08 06 04 04 06 06 06|06 04 00
1A0   02 01 09 0A 07 03 02 02|04 08 0C 0A 0A 06 06 06|03 0B 09 02 04 06 09 06|06 04 00
1C0   02 00 09 07 09 0D 09 08|09 06 09 0C 0A 08 06 08|0D 07 04 08 04 08 08 06|06 06 01
1E0   03 02 07 07 08 06 01 01|07 08 0A 0C 0A 06 06 09|0A 0A 0A 0A 08 0A 0A 06|06 06 02
200   0E 00 03 09 06 04 09 03|08 09 0A 0C 08 08 08 0A|0A 0A 0A 08 0A 0C 0A 0A|06 04 02
220   0F 02 02 09 08 08 0A 0A|0A 0C 0A 0A 08 08 08 0A|0C 0C 0A 0A 0A 0A 0A 08|06 04 07
240   0E 0E 02 09 0A 0A 0A 0A|0C 0C 0A 0A 0A 08 08 0A|0C 0C 0C 0A 0A 0A 09 06|04 04 03
260   0F 0F 0B 09 09 0C 0C 0C|0C 0A 0A 0A 0A 08 08 08|0A 0C 0C 0C 0A 0A 08 09|04 04 03
280   0F 0F 0D 09 0C 0A 0A 0C|0C 0A 0A 0D 0A 08 08 08|0A 0A 0C 0C 0A 0A 08 04|04 03 07
2A0   0F 0F 0E 07 0C 0A 0A 0C|0A 0A 0A 0A 0A 04 04 04|08 0A 0C 0C 0A 0A 08 07|04 04 03
2C0   0F 0F 0F 07 0A 0C 0C 0C|0A 0A 04 08 04 04 03 07|09 0D 07 07 06 08 06 04|07 04 09
2E0   0F 0F 0F 07 0A 0A 0A 0C|0C 08 07 07 03 02 09 07|03 07 03 07 07 0D 07 07|07 03 0D
300   0F 0F 0E 09 09 0A 0A 0D|0D 07 03 07 07 02 03 04|07 04 02 03 03 07 09 07|03 07 07
320   0F 0F 0F 0E 07 07 09 08|03 07 03 03 04 07 08 04|08 08 08 06 04 07 0D 09|07 07 09
340   0F 0F 0F 0E 09 07 04 09|07 03 04 04 08 08 0C 0A|0A 08 08 06 04 03 0B 03|07 07 07
360   0F 0F 0F 0D 09 07 07 07|03 02 06 08 0A 0A 0D 0A|08 06 06 06 04 07 07 0E|07 07 03
380   0F 0F 0F 0F 0D 07 0D 09|09 07 0A 08 08 06 04 07|04 06 06 09 04 03 03 07|03 07 07
3A0   0F 0F 0F 0F 0E 0B 09 09|03 02 06 09 04 09 07 07|07 09 08 06 07 07 0D 0B|03 03 07
3C0   0F 0F 0F 0F 0E 0D 07 07|07 03 04 07 09 09 07 09|06 08 08 09 07 0D 07 03|07 03 03
3E0   0F 0F 0F 0F 0F 0D 0B 09|07 07 03 0D 09 0D 04 09|0D 09 0D 07 09 07 03 0B|02 03 05
```

For example, here's how the health record credential could be leveraged by the digital identifier (W3C DID), verifiable credentials (W3C VC) and delegated authorization (IETF GNAP) standards.



Comments on this doc are welcome or direct to agropper@patientprivacyrights.org

Health Equity Concerns

With vaccination credentials as an example, it helps to separate the vocabulary credential components from the identity credential components.

The identity aspects relate to equity and involve access to technology such as smartphones, employment discrimination based on the ability to present and inspect credentials at the worksite, and participation by the undocumented who might endanger themselves and the community if they're reluctant to receive vaccines and tests..

There is obviously some relationship between the vocabulary and identity dimensions, if only because the overall size of the credential is limited by printing and technology cost constraints.

One thing that stands out, for example, is the statement that the patient/subject will be identified by Name and DOB. Would we ever identify someone by Name and License Number or would we ever include a code for Level of Assurance of the identity? Do we allow people to self-identify in order to improve access by the undocumented? Are we setting a precedent for documentation of rapid testing, including home self-testing?

Public health is another concern. Every digital credential issued is an opportunity to collect valuable information on prevalence, side-effects, and demographic disparities. Every digital credential could also be associated with voluntary self-reporting. Getting digital privacy right will have more impact on society than anything having to do with the digital vocabulary conversation.

Inspection processing sequence - example

- On a normal ($300 +) smartphone,
- Install an app (a PWA might be even better)
- That uses the available QR code API to return a link to a custodial credential
- That also uses the camera API to capture an image
    - Interactively positioned the way a check deposit image is done
- Digital image is converted to a regular 32x32 grid
    - Represented as 1,000 values in a 1D list
- The list is subject to a clustering algorithm looking for 16 channels
- Replace each value in the list with the most likely 4-bit channel identifier
- Calculate your favorite hash of the 512 Byte list
- Compare the hash with one stored in the digital credential retrieved via QR
- Display a Green Check or Red X

References:

Facial Imaging

This recent paper is a good link to privacy-related modifications to a facial image.
A Study of Face Obfuscation in ImageNet https://arxiv.org/abs/2103.06191

Vaccine Passports

What Are the Roadblocks to a 'Vaccine Passport'?
https://www.nytimes.com/2021/04/14/travel/covid-vaccine-passport-excelsior-pass.html

Governor Cuomo Announces Launch of Excelsior Pass to Help Fast-Track Reopening of Businesses and Entertainment Venues Statewide
https://www.governor.ny.gov/news/governor-cuomo-announces-launch-excelsior-pass-help-fast-track-reopening-businesses-and

https://www.technologyreview.com/2021/04/09/1021934/got-your-covid-shots-you-might-need-vaccine-passport/

https://www.consumerreports.org/personal-information/covid-19-vaccine-data-privacy/

Verifiable Credentials

SMART Health Cards https://github.com/smart-on-fhir/health-cards and
https://github.com/smart-on-fhir/health-cards/discussions/120