A digital "Yellow Card" for securely recording vaccinations using Community PKI certificates

Stephen Wilson
Lockstep Technologies Pty Ltd
Sydney, Australia
swilson@lockstep. com.au

***Abstract*— The Yellow Card or *carte jaune* is a paper booklet in a standard format set by the World Health Organisation in which a person's vaccinations are recorded by healthcare officials. Numerous initiatives are striving to create both digital vaccination records and new digital identities for people with little or no official documentation; i.e. "low doc" persons. Yet there is no globally agreed model for identity, nor any standardized way to establish identity. Nevertheless, field workers today are able by and large to establish the bona fides of Yellow Card holders with adequate certainty for the paper-based system to function most of the time. This paper contends that vaccinations should be digitized without introducing new identity systems, since a lack of formal identification is obviously not preventing Yellow Cards today.**

This paper describes a new digital Yellow Card, deployable on most regular mobile phones, in which public key certificates represent vaccinations and other credentials, vouched for by officials or field workers. The design has practical benefits for the digital engagement and privacy of low doc persons. It also shows how traditionally hierarchical public key infrastructure can be deployed without dictating identification protocols to communities, thus avoiding some of the controversies that plague this technology. The PKI security function can remain centralized while certificate issuance is decentralized, which leaves community organizations free to carry on their business as usual.

Keywords—PKI, identity, verifiable credentials, public key certificate, mobility, public interest technology, COVID-19.

I. THE NEED FOR DIGITIZED ATTRIBUTES

The drive to digitize credentials typically carried on paper or plastic is well-established [1][2]. Digital credentials are increasingly more relevant in modern economies: they're more convenient to present, more secure against fraud (in principle at least) and safer in the event of loss because they can be backed up and restored relatively easily when needed.

Over the period c. 2000-2010, many traditional credentials were successfully digitized; examples include student cards, health insurance cards and patient IDs. The exemplar is arguably the Chip-and-PIN payment card in which integrated circuits and embedded cryptographic functions supplanted customer account data coded on magnetic stripes. When a Chip-and-PIN payment card transmits cardholder data to a merchant terminal, the merchant is reasonably assured that the data has been presented directly and with consent (thanks to the operation of the PIN), the data originated from the bank which issued the card (because the data is digitally signed by that bank) and the card itself is genuine (because of a unique customer private key held in the integrated circuit). These security properties are collectively often referred to as "cryptographic proofs" in digital identity today.

II. RECENT DEVELOPMENTS

The International Certificate of Vaccination or Prophylaxis (ICVP)—known as the "Yellow Card" or *carte jaune*—is specified by the World Health Organization [3]. Numerous projects are underway to provide digital vaccination and test records, including:

- WHO "Smart Yellow Card" working group https://www.who.int/groups/smart-yellow-card-working-group
- International Air Transport Association (IATA) "Travel Pass" https://www.iata.org/en/programs/passenger/travel-pass/
- CommonPass platform of the World Economic Forum and the Commons Project https://www.weforum.org/projects/commonpass
- COVID-19 Credentials Initiative https://www.covidcreds.com/
- IBM Digital Health Pass https://www.ibm.com/products/digital-health-pass.

These projects all draw on mobile phone technologies for their near universality, but within that mature construct, feature a variety of novel technologies including blockchain and Verifiable Credentials [4].

At the same time, aid programs such as the World Bank's ID4D initiative are seeking to furnish general purpose digital identities for the roughly one billion people worldwide—mostly in the developing world—said to have no official or "legal" identity [5][6]. An important driver of this work is the UN's sustainable development goal SDG 16.9, to "provide legal identity for all, including birth registration" [7].

Some industry consortia, such as ID2020, are joining the issues of digital identity frameworks and vaccination records [8]. One theme of this paper is to argue for digitizing vaccination records and similar personal attributes without the complication of an overarching identity.

III. DIGITAL IDENTITY GETS COMPLICATED

Initiatives to create portable new digital identities for low doc or disadvantaged people can run into difficulties when it comes to codifying what it means to have an official identity. Each sovereign nation has its own way of identifying and, where applicable, registering its people; this is after all largely what *sovereignty* means. For undocumented individuals, the process of bootstrapping a practical identity can be somewhat arbitrary. And by itself a state-issued identity—essentially a name for a natural person registered by government—doesn't necessarily help the person concerned prove what matters about them in practice, such as vaccination status.

Meanwhile, the many Non-Government Organizations (NGOs) on the ground providing vaccinations, permits, health checks and other credentials go about their business, issuing and recording peoples' attributes as best they can, without standing on ceremony, especially when the need is urgent.

Mobile technologies and public key cryptography bring an opportunity to digitize traditional credentials and at the same time clarify and reframe digital identity for low doc persons. There are many ways to digitize paper and plastic credentials, from simple image scanning through to cryptographic tokenization, leveraging the virtual wallet feature now native to many mobile phones. Effective digitization should preserve the integrity and provenance (or origin) of real-world attributes, to make them tamper resistant. We should preserve existing credentialing processes as far as possible, to streamline issuance and lessen unintended consequences for privacy and personal sovereignty.

IV. A DIGITAL YELLOW CARD ARCHITECTURE

The digital Yellow Card of this paper is architected around the recognition that different attributes of people are established through different rules and pathways. Each attribute-issuing authority has its own way of "doing business" and as such is sovereign over respective attributes. The digital Yellow Card is agnostic as to the rules for issuing people with credentials, qualifications or entitlements, and the rules for accepting and relying on them. Further, the design is not dependent on any overarching digital identity. It is deployable on a range of mobile technologies, to securely hold verified records of vaccination and other attributes that a person accumulates as they make their way through the world.

For each personal attribute, the digital Yellow Card records (i) the fact the attribute has been issued to the holder of the Card, (ii) the authority which issued it, (iii) its validity period where applicable, and (iv) a tamper-resistant record pointer (typically a URL) to all pertinent terms & conditions. Each attribute within the digital Yellow Card is separately digitally signed by or on behalf of the issuing authority.

A. Community PKI

Technically, each discrete vaccination record or other event record is represented in the digital Yellow Card as a public key certificate (PKC) where the private key component of the certificate's associated key pair is stored within a secure element of the card holder's mobile device. As with the Chip-and-PIN card mentioned above, vaccination records presented in the form of PKCs carry inherent assurance of provenance, uniqueness, consent and accuracy. They are also highly resistant to copying, tampering or counterfeiting.

The digital Yellow Cards are issued within a Community Public Key Infrastructure in which Certificate Authorities (CAs) and Certificate Management Systems (CMSes) serve respective attribute authorities (issuers) as shown in Figure 1. Certificate subjects (i.e. Yellow Card holders) are registered by local administrators or field workers working for existing authorities.

The Community PKI is hierarchical like typical public key infrastructures—insofar as certificates issued by each CA chain back to a common self-signed Root CA—yet this PKI notably does not dictate Certificate Policies to subordinate issuing CAs. Each CA, working with its respective attribute issuer, sets a local policy that is fit for purpose for the associated Community of Interest.

In particular, each Community CA specifies identification protocols befitting the type of vaccination certificate issued to the digital Yellow Card holder. As discussed, community field workers each have their own local protocols for satisfying themselves that a given individual is a proper candidate for vaccination (or to receive some other service); under this Community PKI, the CAs' rules mirror existing identification protocols.

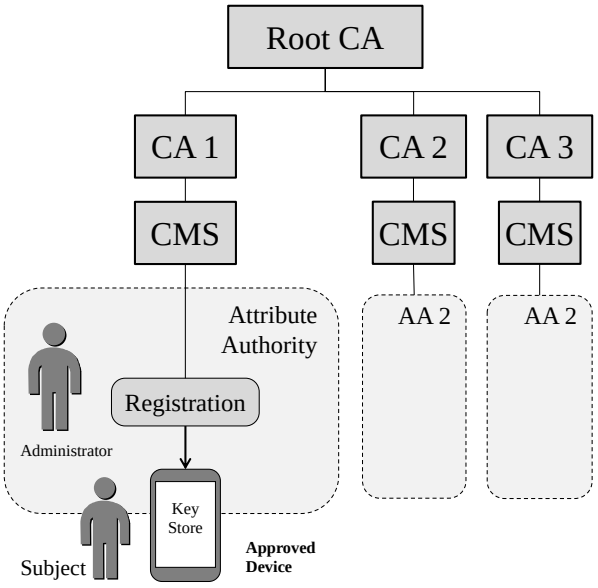

Fig. 1. Community PKI supporting multiple Attribute Issuers

Another policy decision made locally under this PKI concerns the type of mobile device to which vaccination certificates will be issued. In some communities where mobile technology is well established, individuals will bring their own device, and so long as it is cryptographically capable, it can carry the digital Yellow Card. In other cases, NGOs might provide new mobile devices, or they might use other form factors such as smartcards.

This Community PKI uses conventional X.500 Object Identifier (OID) numbering to uniquely index each CA and the certificates it issues. An example OID schema is depicted in Figure 2.

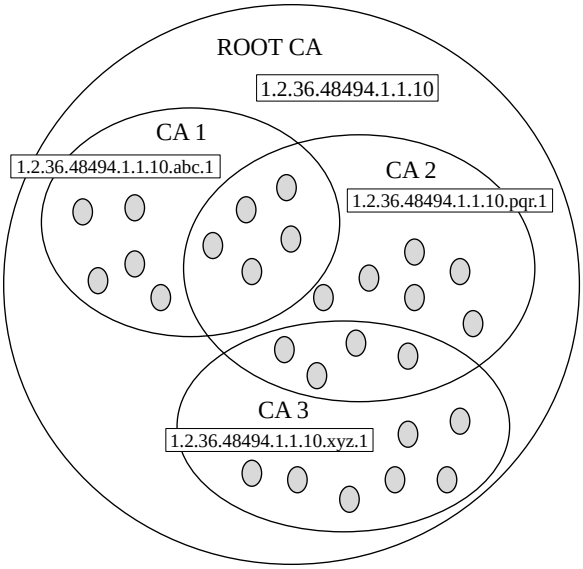

Fig. 2. Policy Object Identifiers for Community PKI (schematic)

The community CAs are assigned a Policy OID of the form *1.2.36.48494.1.1.10.abc.1* where *abc* is an official

business number or other suitable designation of each organisation. Communities may define further OID leaves to codify different attributes and associated terms & conditions of relevance to Relying Parties and particular software applications which consume the certificates. The OID tree allows software applications to distinguish PKCs in this schema from any other PKI certificate, and make fine grained authorization decisions according to the certificate and attribute type.

V. Properties of the Digital Yellow Card

A. Privacy by Design

The design minimizes personal data collection by architecturally separating vaccinations and other personal attributes and allowing each to be presented within the particular context where it applies. There is no extraneous collection of personal data, no arbitrary identity proofing, no new identifiers, and no disclosure of personal data by the digital Yellow Card across domains.

The reliability of separate personal attributes is enhanced by the cryptographic proofs to such an extent that digital verification can occur without needing auxiliary personal data such as shared secrets or Knowledge Based Authentication which bring widely recognised risks to privacy and security. Neither are intermediate identity brokers or "identity providers" necessary, so new honeypots of personal data are avoided. The solution presents the owner's bona fides directly to Relying Parties, peer-to-peer.

If an attribute is not natively identifiable, then the digital Yellow Card enables its owner to transact anonymously.

B. Security

The degree of cryptographic proof inherent in the digital signatures created by device-bound private keys enables Relying Parties to distinguish "original" attributes from stolen or counterfeited data, thus mitigating identity theft.

The design also protects against large scale hacks (as have been experienced by national ID databases in South Korea and Israel among others); such hacks will not invalidate original data safeguarded within digital Yellow Cards and thus business continuity is ensured without needing to re-issue all underlying personal credentials in the worst-case scenarios.

C. Compatibility with Extant Identification

The digital Yellow Card is orthogonal to and works within any existing credentialing or identification system. If a given identification system has issued an individual with an ID and/or attribute, then that ID may feature within the digital Yellow Card's PKCs, together with details of the ID issuer.

Thus the digital Yellow Card provides suitable means for digitizing, storing and presenting regular national IDs. The architecture can form a strategic bridge from extant analog government identifications common in many countries to a digital ID capability, with minimal process change and cost.

D. Interoperability

The digital Yellow Card can store personal attribute values plus details of the issuer and a pointer to terms & conditions, using the open standard X.509 OID syntax. The solution is technologically highly interoperable at the protocol layer. Furthermore, it imposes no business process changes, so the native meaning of stored attribute data is unchanged.

E. Low connectivity operation

Public key certificates are verifiable as being accurate at the time of issue, at any time later, without needing to look up any database, registry or authentication broker. That is, the contents of a digital Yellow Card can be relied upon without "calling home" and therefore little or no network connectivity is required. It should be noted that this technique is best suited to attributes that, while they might expire over a certain period, are not liable to be revoked before expiry. Vaccinations are a good example, as well as kinship, country of birth and certain medical facts such as allergies or blood type.

VI. Proof of Concept

The digital Yellow Card concept has been proven through a minimum viable product called Mobile Device Attributes Validation (MDAV) developed under contract for the U.S. Department of Homeland Security [9]. The MDAV mobile app holds essentially any number of public key certificates issued by CAs in a community PKI under a private Root CA. Each PKC corresponds to a private key held within the mobile phone's secure element. MDAV manages the certified attributes with a graphical user interface with which the user can select a certificate for presentation to a Relying Party. The presentation is made via standard digitally signed QR codes, which are scanned using a reader feature of the app and verified automatically against the scheme Root key. Relying Parties are thus assured that a specific vaccination or other attribute of interest has been issued by a recognised authority, is in the right hands, and has been presented with consent. The MDAV MVP underwent user acceptance testing at the National Urban Security Technology Laboratory in 2018 [10].

VII. Discussion

PKI is perhaps not normally regarded as a Public Interest Technology yet the design presented here shows how hierarchical certificate issuers need not be dictatorial in respect of community rules for dealing individuals. This form of PKI respects established ways of establishing people's bona fides sufficient to correctly render services to them, removing the need for new identity frameworks and streamlining deployment in developing economies. PKI has lower technology risk and lower project risk than many of the novel identity technologies such as blockchain being touted for developing economies [11].

The PKI-based digital Yellow Card provides assurance of the origin and legitimacy of vaccinations and other attributes without needing to connect online to the issuer. Thus the solution is amenable to environments with poor network connectivity, or none at all.

VIII. Conclusions

The digital Yellow Card described here is a new type of application of a mature, low risk cryptographic technology. The solution secretes proof of vaccinations and other personal attributes—issued or vouched for by any authority—within standard public key certificates bound to mobile devices. The provenance of attribute issuers is thus preserved, and the legitimacy of each attribute can be verified on its face, in a decentralised peer-to-peer manner, offline or in poorly networked environments. The digital Yellow Card is able to hold any number of attributes vouched for by community organizations; it can therefore scale to handle many other credentials for low doc and disadvantaged people without depending on new digital identity frameworks.

ACKNOWLEDGMENT

Information in this publication is based on research funded by the U.S. Department of Homeland Security Science & Technology Directorate (DHS S&T). Any opinions contained herein are those of the author and do not necessarily reflect those of DHS S&T. For more information, please contact Anil John, Program Manager Cybersecurity R&D anil.john@hq.dhs.gov.

REFERENCES

[1] Treasury of Australia, "Financial System Inquiry Final Report", 2014 (available at https://treasury.gov.au/publication/c2014-fsi-final-report)

[2] K. Wilson, K. Atkinson, and C. P. Bel "Travel Vaccines Enter the Digital Age: Creating a Virtual Immunization Record." The American journal of tropical medicine and hygiene vol. 94,3, 2016

[3] World Health Organization, "International Health Regulations", 2nd ed., 2006

[4] World Wide Web Consortium, "Verifiable Credentials Data Model" v1.0, 2019 (available at https://www.w3.org/TR/vc-data-model/)

[5] World Bank Group "ID4D Global Dataset", 2018 (available at www.id4d.worldbank.org/dataset)

[6] World Bank Group, "Annual Report, Identification for Development (ID4D) partnership platform", 2019 (available at https://id4d.worldbank.org/)

[7] United Nations General Assembly, "2030 Agenda for Sustainable Development", 2015 (available at https://sdgs.un.org/2030agenda)

[8] D. Gruener, "Immunity Certificates: If We Must Have Them, We Must Do It Right", 2020 (available at https://ethics.harvard.edu/files/center-for-ethics/files/12immunitycertificates.pdf)

[9] Dept of Homeland Security, "Cyber Security Division Technology Guide 2018", 2019 (available at https://www.dhs.gov/sites/default/files/publications/CSD%202018%20Tech_Guide_Web%20Version_508.pdf)

[10] Department of Homeland Security, "Mobile Device Attribute Validation Technology Demonstration Report", 2019 (available at https://www.dhs.gov/sites/default/files/publications/mdav_final_report_190614_approved-508_version.pdf)

[11] E. M. Renieris, S. Bucher, and C. Smith, "The Dangers of Blockchain-Enabled 'Immunity Passports' for COVID-19", 2020 (available at https://medium.com/berkman-klein-center/the-dangers-of-blockchain-enabled-immunity-passports-for-covid-19-5ff84cacb290).