CCI Paper-Based VC Summit Summary Report

March 2021

There is a global conversation across many organizations and companies about how to support individuals sharing with legitimate parties information about their COVID-19 health status.

A format to do this that has a lot of interest and potential is **Verifiable Credential (VC)**, standardized at the W3C. VC is a universal data format that can be used for any purpose for one entity to express information about another. There has been a lot of effort and progress made prior to and after the breakout of COVID-19 in using VCs for digital credentials. However, a digital to digital solution is not enough to provide worldwide usability especially when it comes to combating a public health crisis. There must be solutions to expressing VCs on paper so that those in low resource settings and without phones are not excluded and can have an enhanced experience offered by VC systems too.

This summit, convened by the COVID-19 Credentials Initiative (CCI), is to get all groups working on paper-based VC and COVID-19 credential issuance together to rapidly iterate and come to convergent alignment on how VC can be expressed on paper in a simple standard way globally. The goal is to get the outcomes into the hands of those who are working with WHO and other public health authorities and give them a clear idea on how it all comes together -- a coherent story about paper-based VCs.

Join post-summit discussion (open for all) at LFPH Slack (channel: #cci-paper-based-vc)

Event Designer & Facilitator

Kaliya, also known as the Identity Woman, is the Ecosystems Director of CCI. Kaliya co-founded the Internet Identity Workshop in 2005 and still produces it twice a year. She is a subject matter expert on VCs and a designer and facilitator of interactive events for high performance collaborative technical communities. Kaliya joined CCI since day one and has been leveraging her hyper-connectedness across the identity ecosystem to nurture collaboration for CCI and facilitate interoperability of VCs.

Participants

Companies/Projects that presented: Mattr, DIVOC, iRespond, Consensas, Resolve to Save Lives, IBM Digital Health Pass, PathCheck Foundation MIT, IOTA Foundation/Zebra

Companies/Projects/Individuals that attended**:** MITRE, Evernym, Lumedic, IATA, Proof Market, Thoughtworks, Sovrin Foundation, New Context, Zaka, Blockchain Labs, Yoti, metaMe/The Internet Foundation, Dirk-Willem van Gulik (NL), Human Colossus Foundation, ID2020, Agrin Health

Format

Meeting Pre-Work: Feb 23 - Mar 3, 2021

We have asked all presenting companies/projects to prepare 10 min talks articulating all aspects of their solution, along with pointers to documentation and code if there is any, ahead of time and it happens asynchronously before the event.

Virtual Face-to-Face: Mar 4, 2021

- Part 1: Opening - Understand what is on the table from a solutions perspective.
- Part 2: Problem Understanding - Develop Shared Understanding of the Life Cycle of paper based credential.
- Part 3: Problem Solving - Identify 1) what we have, 2) what the missing pieces are that we need to work on together and how, and 3) what problems are not “ours” but need addressing.
- Part 4: Conclusion - Share learnings and plan for next steps.

Follow up:

- A Summit Summary Report: To summarize sessions, projects and discussion points.
- A Draft Proposal for a CCI Paper-Based VC Focus Group for feedback: To outline the most urgent things that need to get alignment and how we can address all or some of them at LFPH/CCI through a Paper-Based VC Focus Group.
- Follow-up Summit: Evaluate if there is the need to convene another summit.

Common Themes Across Projects

Use of QR Codes

- QR Code but several different varieties
- Size Limit? (Most are between 300 - 500 bytes.)
- Scanner crash - when you go above 500 bytes, lots of QR readers start having problems
- Considerations about the QR code relative to the reader capability of the code.
- From a credential reader perspective - the specification and order of operations for compression is important

Normalization of Attributes and Representation

- Semantic level vs byte level "interoperable".
- W3C compliant VCs (but the type is not usually defined)
- Preference for JSON, (VC) -- rather than the "normal" standards of the identity world (MRZ, TLV(icao), etc).

Compression of the original digital format to QR codes

- This is something that is not standardized yet (not in W3C and others)
- Considerations of credential design - does it make sense to include the entire FHIR record into a credential? Full FHIR Immunization Resource/Record in a VC?

Vectors of Fraud Need to be Considered

- What are the vectors of fraud: physical fraud of the doc and fraud around presenter
- Fraud on the verifier side. Who verifies the verifier? How can we insure the ethics and behavior of the verifiers? (IBM - Key learning) Including verifiers that request showing of credentials in an inappropriate situation/way.

Selective Disclosure for Paper-Based Credentials

- Important for those who use paper to be able to do selective disclosure
- Paper VC should be manually verified against the person ID. How then selective disclosure can be achieved if driver license/passport should be revealed?

Identity Binding

- Providers are reluctant to change their process (and even more so if it takes time/ resources and they don't get reimbursed for it).
- Identity binding is a key area of future of R&D
- If we want to include identity binding within the QR on paper (e.g. passport)
- The best way is to do identity binding at the issuance point? Do solid identity proofing at the point of vaccination, and then bind it later to a digital identity e.g. a digital passport?
- A lot of self-attestation. From a process standpoint the only time identity is being checked is during check-in.
- Over time, the issue of identity not being captured upfront will resolve itself.

Presenting Projects Summary

This section provides an overview of each presenting company/project which includes

- the demo videos and other relevant links to their work on paper-based credentials provided during pre-work;
- a summary of information shared and discussed during the virtual face-to-face meeting;
- a paper credential lifecycle table being worked on during a breakout session of the virtual face-to-face meeting.

Project 1: Mattr

Demo Video: https://www.youtube.com/watch?v=EXvWxFjHvdY
example to the vaccination vocab to show a QR code based example
https://mattrglobal.github.io/vaccination-certificate-vocab/#representation-size

Mattr's paper based verifiable credentials or verifiable credentials on a chip solution delivers a compact QR code representation of JSON-LD Covid vaccination certificate. The size of the resulting vaccination certificate is reduced by applying CBOR-LD compression and Base64 encoding to the certificate yielding an encoded size of < 700 bytes. This is a small enough footprint for the encoded credential to fit on a NFC chip as well read by a low resolution QR code scanner. Mattr's video demonstrates a 'smart' ID card containing both a nfc chip and QR code representation of a vaccine credential.

Focus/Specialty	Focused on Format
Paper-Based QR Code for VC	Yes. Compressed vaccine schema using CBOR-LD. Down to 461 Bytes
Systems Level Infrastructure	- Standard printers - QR code under 500 byte range to support low end infrastructure - Integrates with EHR systems - Government distributes Vaccines to administering centers - No requirements for any specialized systems - Focused on format
Prework / Setup for Holder	- Cards can be preprinted with unique token and handed out to claim a downloadable VC - There are various input states for the holder: Turns up at vaccination clinic with no prior scheduling Has already been vaccinated and needs to claim vaccine record
Pre-Administration Verification	At discretion of health authority
Vaccine Administration	Vaccine record is bound to the token card for claiming vaccine credential later
VC / QR Code Generation	
On Site	QR is a compressed VC how?
Is it a REAL W3C VC?	- Likely issued using token (card) given at vac event if no printing capability - Yes embedded in QR code - Will likely need PII to bind identity - QR paper based does not support selective disclosure

Post Vaccine Administration	Alternatively, if vaccine center has printing capability, VC can be printed on site removing need of token card
Offsite / Follow Up	- Vaccine credential is a Verifiable Credential based on this vocab: https://w3c-ccg.github.io/vaccination-vocab/ - A card or token can be given at event and the VC can be claimed post event - May use knowledge factors such as DOB to validate and claim vaccine credential
QR Code Presentations / Usage	- Verifier is able to scan the QR code (paper, lo-fi digital, mobile wallet) and is able to resolve and verify the Verifiable Credentials - Binding is difficult to maintain
QR Code - Refresh / Revocation	Revocation using 2020 Digital Bazar specification
QR Code EOL	Issuer hosts a list of revoked credentials and verifier performs lookup. This revocation list can be cached as well

Project 2: DIVOC

Demo Video: https://divoc.egov.org.in/demo-videos
Additional resources:

- https://github.com/egovernments/divoc-docs
- https://divoc.egov.org.in/

The DIVOC software is designed to cater to the diversity of use cases in terms of choice of facility (government to private facilities) at various geographies, choice of payment, choice of IDs (digital IDs, mobile numbers, no IDs), etc. It is designed to plug and play with various certificate distribution schemes, e.g. printed with QR code, digital using smartphones, sms/email attachments, digital lockers, blockchain based apps, etc. 15M VCs have been issued and signed by the Indian central government private key so far using DIVOC's system. All issuance sites are assumed to have internet connection, but designed to be verified offline.

DIVOC digital and paper-based credentials are bound to Aadhaar ID as well as 12 other identifiers. To prevent any denial of service, offline authentication using these alternate IDs were also treated as an acceptable provision. Aadhaar is recommended because the program is tying issuance of a new Unique Health ID to the people authenticating themselves using Aadhaar.

Focus/Specialty	Whole system for administering vaccination sites & distribution.
Paper-Based QR Code for VC	Yes
Systems Level Infrastructure	- Module-based, open-API-based interfaces: Registry of facility, vaccinators, etc Registration and appointment Vaccination orchestration Certificate access and integration - DIVOC stack can manage the last-mile administration needs for country vaccination programs - orchestration (registry/entity creation) to DVC generation/access to post-event feedback collection & analytics. - DIVOC in India's case is being used for the VC generation/access. India has a vaccination digital infrastructure - Cowin - which was created to manage the end to end flow for a Govt. run program [spanning across the vaccine supply chain & logistics as well as the last-mile administration functions) - DIVOC is part of a Larger National System in India [Cowin]. DIVOC stack is modular - it can accommodate as it is (all components or specific components like the VC utility for e.g.) for country vaccination programs
Prework / Setup for Holder	- Appointment Registration: pre registered list citizen facing registration system call in to citizen system - assisted registration & walk-ins
Pre-Administration	- Aadhaar Number is requested and verified (demographic + OTP). Other

Verification	identifiers are also supported and can be configured (for offline verification + online authentication where applicable) - request to bring Aadhaar card - Or Any other identity proof like driving license, voter id and other approved ids
Vaccine Administration	Person Received Vaccine - Marked in the records as complete [with details on vaccine product/dose details/batch-lot number, etc...] - The vaccinator name/facility is flagged as attributes to be printed/encoded in the VC - Marking completion of the "vaccination event" in the system - triggers an immutable event record which is an input to generate the VC. The event record records all transactions associated with the event (e.g. demographics related, vaccinator/facility details, certificate metadata, timestamp, etc..). A limited data set is then used for the paper VC [displayed on the paper + encoded on the QR code]
VC / QR Code Generation	
On Site	When the person is ready to leave the facility they can ask for a print out.
Is it a REAL W3C VC?	- DigiLocker account holders can request a VC - beneficiary reference vaccine (from COVIN) - there is also a contact tracing app (Arogya Setu) - Format: JSON-LD verifiable Credentials - Verification Reference implementation on github
Post Vaccine Administration	Once the person leaves the facility (with their VC), they can report side effects on the citizen feedback portal. This can be configured per Govt. protocol (e.g.rules for citizen feedback within 48 hours after vaccination. Confirmation on whether the person has a VC or not, needs to be done before feedback provision is enabled.
Offsite / Follow Up	Plans to link with pharmacovigilance functionality (using a sampled population set - by linking with an anonymized survey & bloodwork results) are planned in DIVOC future releases.
QR Code Presentations / Usage	- Paper based - Digital Wallet (Digilocker) - App (Arogya Setu) - Compression: ZipStream - QR code version 37/38 determined based on size of certificate
QR Code - Refresh / Revocation	- Planned for future roadmap - Individual black listing - Revocation by removing the public key
QR Code EOL	NA

Project 3: iRespond

Demo Video: https://youtu.be/-UTSM7hDm1M

iRespond is primarily a biometric service provider or BSP. Biometric Service Providers are entities that support the enrollment and usage of biometrics for a particular population. The service provider is trusted to maintain biometric templates of enrollees and to perform authentication against those templates. They work in remote areas with refugee populations who do not have government ID. Their system is used to support people enrolling in and accessing health care services - allowing for the persistence and maintenance of healthcare records. They are developing a system to issue an attestation of live births, a record issued by a healthcare worker to the mother shortly after birth. (This should not be confused with a birth certificate issued by a government). This includes printing a record on to secure paper. With COVID they have looked into adapting this system to issue a proof of vaccination in a similar manner.

Focus/Specialty	Has a specialized BSP model linking digital + physical certificates to iris biometrics.
Paper-Based QR Code for VC	Yes
Systems Level Infrastructure	- Most biometric service providers are centralized. A global solution needs to accommodate many BSPs - BSPs would provide their own VC attestation that they plus an individual operator attests to the identity binding / real person's presentation
Prework / Setup for Holder	- Ideally, a holder of a paper credential should require no setup, but have enrolled with a BSP or device - The BSP will have issued an identifier (or a template that ideally conforms to a global standard. Iris templates are not yet standardized.) - iRespond's iris-based solution is IDENTIFICATION based, not verification based (but could also support a true/false verification given an iris scan and an identifier)
Pre-Administration Verification	- Could be the BSP identity presentation.. Assumes online or cached biometric templates - Could be a unique coupon per paper credential... to be claimed later
Vaccine Administration	- A vaccination credential and a person identification verifiable credential need to be cross-linked or one embedded in the other - An iris biometric template (perhaps salted) could be included in a QR code for later offline verification - Offline identity verification could alternately rely on a picture being on the physical credential.
VC / QR Code	

Generation	
On Site	Standardization of biometric templates is desired for cross-vendor (BSP) iris verification
Is it a REAL W3C VC?	Will be
Post Vaccine Administration	Need a path to have the holder load the VC into their own offline wallet or a custodian wallet
Offsite / Follow Up	
QR Code Presentations / Usage	
QR Code - Refresh / Revocation	
QR Code EOL	

Project 4: Consensas

Demo Video: https://www.youtube.com/watch?v=d3oz7kR6ZjU&feature=youtu.be
Demo Video + Explanation of Goals: https://vimeo.com/510703954
Demo Website is here: https://passport.consensas.com/
Detailed presentation / walkthrough here (including how the verification validation process works): https://cccc4.ca/l/ccipaper

Consensas strives to solve the paper problem with existing technology. Their paper and digital solutions have the same processes. They use QR codes resolving to URLs (no DIDs and blockchain involved) and pointing directly to VCs, which make the QR codes relatively lightweight. Holders don't need the internet but verifiers will require internet connection to fetch public keys, access business rules and other things. The solution uses JSON-LD VCs and the payload is encoded as an overlay on schema.org. RSA digital signatures are used.

They have a verification and issuance system and a Raspberry PI system to send QR codes. The proofs are in the QR codes and verification is all done through digital means. If one uses a phone to scan the QR code they will get a HTML document; if one uses the verification system, then they will get a JSON file. The file points to a public key and cert chain which is validated for consistency. No personal identity is revealed in the process. The QR code that exists on paper is a unique persistent identifier but there is a highly random component that can be reassigned.

Focus/Specialty	Fully "walletless", everything works using standard web technologies (e.g. HTTPS, URLs, JSON, JSON-LD). The QR Code encodes a URL, but a future version will encode a signed credential
Paper-Based QR Code for VC	QR Code for URL that points to a VC that can be pulled down by the issuer. The format is C4 Vaccination Credential (https://cccc4.ca/), a JSON-LD based Verifiable Credential, which has wide flexibility for expansion in data captured, FHIR compatibility, and for dealing with different country's medical coding standards.
Systems Level Infrastructure	- Very compact QR code - Expected EHR backend, generating codes directly from data already head - No overhead for doctors or clinicians - QR code can be shared at vaccination delivery, or later via email, SMS, etc. - Standard web stack - Expected highly distributed architecture

Prework / Setup for Holder	- QR code be delivered on-site with no-further followup needed - or post vaccination delivery with SMS, email, vaccinator login (e.g. CVS-account type thing)
Pre-Administration Verification	
Vaccine Administration	
VC / QR Code Generation	
On Site	On site or via email
Is it a REAL W3C VC?	JSON-LD W3C VC (RSA 2018)
Post Vaccine Administration	- none needed
Offsite / Follow Up	
QR Code Presentations / Usage	- Verifier scans QR code, resolves URL - Identity is confirmed with “normal” id - All processes using normal standards (e.g. http) - easy to implement (reference implementation available)
QR Code - Refresh / Revocation	- Normal RSA processes
QR Code EOL	- Normal RSA processes if need be - Business rules for expiration based on vaccination date

Project 5: Resolve to Save Lives

Demo Video: https://www.dropbox.com/s/vslkf6yhkb6e3ow/Screen%20Recording%202021-01-17%20at%2022.43.29.mov
Github: https://github.com/Tribe-On-Purpose
Specifications: https://github.com/Tribe-On-Purpose/specs
White paper: https://docs.google.com/document/d/1IrxIA16qIHhUsuhUbLgRGvS5IMpqy-zUreosbmUHxwQ/edit?usp=sharing

Resolve to Save Lives has a framework that allows a credential to be converted to a QR code that can be printed on paper and using their framework will guarantee readability of QR codes by any system. The framework leverages IOTA database chain. IPFS are used for individuals who have already got vaccinated and received paper cards to upload the pictures of their cards and get verified by the issuers before they are issued a VC. The framework supports encryption based on keys derived from the DID on to IPFS. When the request is made to verify the public key of the user used to decrypt the material, the framework allows the issuer to validate it and issue the credential. Customized business rules distribution is enabled through decentralized nodes. Complex business rules will live on the edge device and can be implemented inside an app that does the verification without internet connectivity.

Focus/Specialty	
Paper-Based QR Code for VC	
Systems Level Infrastructure	
Prework / Setup for Holder	- Person signs up for vaccination via site or appointment with a doctor. - Individual downloads app and creates DID for later association.
Pre-Administration Verification	- Ideal flow: Administrator of vaccine uses an app built with the issuing framework to check a person in - Non-ideal: Person receives vaccine and gets current CDC card.
Vaccine Administration	- Ideal case: someone administering vaccine uses a well-designed app to scan user's QR code at the same time, to save time with registration - But need to support other cases too.Person receives a vaccine and is given a card like the current ones with a unique barcode that is scanned during check-in and associated with the user's current or created DID. - Person can present the paper or scan it to receive their credential and convert to a barcode.
VC / QR Code Generation	- Either on-site or after vaccination - App is used to upload the image of the card for verification by the issuer. - Issuer verifies and creates/signs a credential for the user.

	- User can print QR Code version of credential or present using app,
On Site	Yes, optional
Is it a REAL W3C VC?	JSON-LD BBS+ signatures
Post Vaccine Administration	Supports post-vaccination outreach, based on bulk upload
Offsite / Follow Up	All digital, no paper after-the-fact
QR Code Presentations / Usage	People are encouraged to print QR code to keep for safe keeping. Ability to re-onboard in case you lose your phone, etc.
QR Code - Refresh / Revocation	- VC are kept locally - if you lose them, VC can't be re-issued - Attached to biometrics, not user-local private keys - User needs to take care of backups
QR Code EOL	

Project 6: IBM Digital Health Pass

Demo Video: https://salesforce.vidyard.com/watch/P9ELfjqP7bjppPKzw9YkgC
Tutorial: https://developer.ibm.com/tutorials/getting-started-on-ibm-digital-health-pass/
DID Method Specification (source code coming): https://github.com/IBM/hpass
Personal Blog: https://allthingsanalytics.com/2020/08/27/ibm-digital-health-pass-goes-live/

IBM Digital Health Pass is a SaaS offering that provides micro services for organizations to issue and verify VCs. It follows the standard SSI concept using blockchain underneath which only has public DIDs, schema and revocation registry. It also offers metadata services for business data. The system doesn't store any personal data. There is also an IBM wallet app that individuals can use to load credentials and a verifier app that provides basic verification functionality.

The credential is W3C standard JSON LD document. After credentials are issued, individuals can print out the QR codes on paper and use them for verification. We allow individuals to do selective disclosure on paper through a technique where credentials are issued with field-level obfuscation and individuals can generate a QR Code that selectively "discloses/de-obfuscates" fields on the credential. Individuals can choose to disclose certain fields and generate/print a new QR code that has an additional payload for verification. This technique won't damage the digital signatures so it will still be verifying the same credential issued by the original issuer. Verification happens on the edge device, where the verifier app checks that the credential was issued by a valid Issuer (looking up in the DID in the ledger and retrieving the DID Document), that the signature is valid (using the PK from the DID Document), that the credential has not been revoked (by querying the revocation registry), and that the credential isn't expired. This is the basic verification applied by the free verifier app, however additional rules can be applied on the edge by extending the verifier to call a rules engine. The verifier app does not yet support ZKPs and the DIDcomm method for exchanging credentials, and relies on QR Code scanning at the credential exchange mechanism. This works well for paper-based credentials where it is hard to imagine how ZKPs could be effectively implemented. In order to address the requirement for offline verification, a caching mechanism allows the verifier app to keep a copy of the data retrieved from the ledger for a configurable time-window before re-retrieving from the ledger. This obviously comes with side-effects, as in the data in the app becomes stale if the refresh period is too long, however it does mean that verifications can happen on the edge without Internet access and is a compromise lots of verifiers are happy to accept. We anticipate that there will be an optimal refresh duration that gives the best of both worlds, freshness of ledger data with robustness in unreliable internet situations.

Focus/Specialty	Whole System including Rules Engine
Paper-Based QR Code for VC	Paper based VC Format

Systems Level Infrastructure	
Prework / Setup for Holder	- The vaccination lifecycle is not managed by IBM Digital Heath Pass - We integrate into existing vaccination management systems
Pre-Administration Verification	We rely on the vaccination management system and workflow to be performing identity proofing
Vaccine Administration	- Not an appetite to interfere with existing process - Issuing credential separately after the event - Need to provide a portal for post-vaccination credential request
VC / QR Code Generation	We provide an API allow credentials to be generated on-site or after the event
On Site	After event implies secondary identity authentication (knowledge-based or auth)
Is it a REAL W3C VC?	- JSON-LD w3c VC - Bunde vaccination data into the QR Code so it's peer-to-peer exchange (not URL retrieval)
Post Vaccine Administration	Outside of the IDHP influence, vaccination management systems
Offsite / Follow Up	
QR Code Presentations / Usage	- "QR Code is JSON-LD, requires no Internet (after initial caching of DID Document), free mobile verifier app, generic w3c verification process (check DID, retrieve DID document, ...), if using selective disclosure there is an extra payload that needs to be processed,"
QR Code - Refresh / Revocation	
QR Code EOL	

Project 7: PathCheck Foundation MIT

Demo Video: Introduction, Product Overview (@7:00), Technical Overview(@18.00), Demo (@36:00): https://www.youtube.com/watch?v=9Tx8LH7Mp18&t=0s
Paper Creds GitHub: https://github.com/Path-Check/paper-cred
App, IDEO Design of paper creds and details: https://github.com/Path-Check/vaccine-diary
Our School: https://join.slack.com/t/pathcheck/shared_invite/zt-gs0bf4h0-2I92eiVThkNLojL2e_VQvA
DEMO QR Code generator here: https://vitorpamplona.com/vaccine-certificate-qrcode-generator/index.v5.html

Pathcheck Foundation has built an end-to-end solution, one for vaccinators and one for businesses. The paper card is a part of the end-to-end solution and designed in partnership with IDEO. One can use a standard A4 paper to print out the paper card and fold it up. The foldable paper card allows one to do selective disclosure, The first side has the coupon which allows one to get vaccinated. The second side is a badge which has one's actual vaccination information. If one needs to use the card as a pass, then on the other side, it contains minimal personal information and if one has been vaccinated, which is very little payload. When the card is completely unfolded, it will reveal all information.

They propose "first three bytes" (a URI schema) heuristic/specification to distinguish VCs in QRs vs other local uses. The idea is to standardize the first three bytes so that no matter what technology is used to issue these credentials, those three bytes will help one look into a global directory to figure out what to do with a QR code.

The QR code used, a proprietary format, is alphanumeric (not binary) and has a small payload of ~150 bytes, which allows all readers to be able to read it. The code has the full payload in itself so that the user doesn't need any electronic devices. The verifiers can be offline for a long period of time.

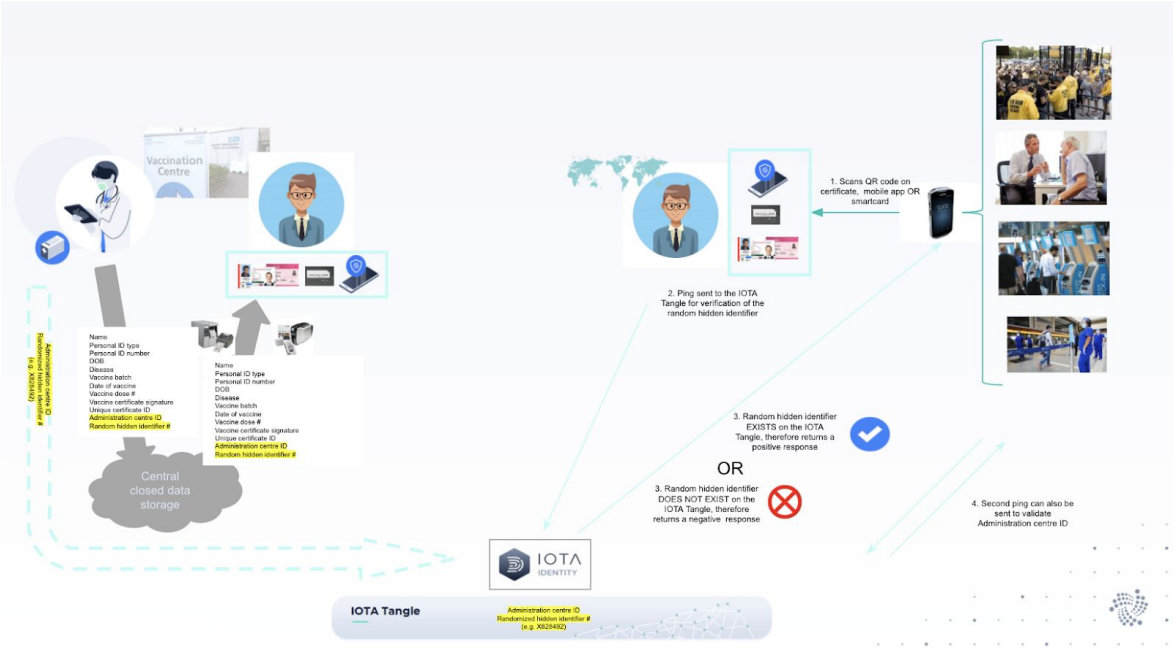
Focus/Specialty	End to end solution with a paper-first approach
Paper-Based QR Code for VC	Yes, there is a redesign of the CDC card to accept VC stickers over time.. There is a bespoke data format and bespoke encoding/signing format. Any VC payload can be compressed into the format using their own specs.
Systems Level Infrastructure	- Issuers add their public keys to DNS TXT Records on their domain name (but can also use standard DIDs) - Issuers can be verified by a trusted source - Gov entity sends Coupon QRs (PHI) and PassKeys (PII) to all citizens (similar idea of the stimulus checks) - via e-mail, sms, app or regular mail
Prework / Setup for Holder	- Person uses the Coupon to book an appointment - Coupon does not have PII, vaccination team does not know who booked
Pre-Administration Verification	- Shows Coupon QR at entrance - Health Worker marks coupon as "Active"
Vaccine Administration	Person receives vaccine
VC / QR Code Generation	Health Worker Scans the Bottle QR Code, which is another VC for the bottle information.
On Site	Health Worker Computer/Smart Phone Uses above Information and Generates several QR Codes
Is it a REAL W3C VC?	- Badge QR Contains Vaccine Event Information - PassKey QR is PII about the person. - Status QR Links the Individual with the Process (via a hash of passkey) - W3C Certificate is converted to the format to fit the QR Standards
Post Vaccine Administration	Coupon ID can be tracked by reporting/dashboard systems at scan
Offsite / Follow Up	Users load the Coupon or Badge into an App to report Symptoms
QR Code Presentations / Usage	Selective disclosure allows users to choose which information set to disclose
QR Code - Refresh / Revocation	- Revocation by removing the public key from the database - Individual cards are not revocable - Issuer keys can be revoked by removing them from distribution
QR Code EOL	

Project 8: IOTA Foundation/Zebra

Demo Video: VC on cards https://www.youtube.com/watch?v=Ivv1JArtHvM&feature=youtu.be
IOTA Selv (mobile app version) demo: https://selv.iota.org/demo/app
GitHub: VC on cards: https://github.com/JamesSwinton/Zebra-IOTA-VerifiableCredentials
IOTA SSI/W3C Identities: https://github.com/iotaledger/identity.rs
Current adoption white paper

IOTA Foundation provides the feeless distributed ledger (not a blockchain) on which IOTA Identities are built. IOTA Identities provides a W3C standard implementation of DID documents and uses VCs data model. Based on the IOTA Identities core tech, an implementation of JSON VCs to provide vaccination tracing is provided. The implementation current focus is on inclusivity and it provides a card and mobile app implementation. Cards are issued to individuals and loaded with VCs stating vaccination proofs. This is achieved thanks to IOTA Foundation collaboration with Zebra, a producer of NFC cards and card printers. Additionally Zebra printers can be used to print watermarked QR codes stickers for any cards. The current solution does not include a paper card based on QR code yet, but can easily expand to it. The NFC cards leverage the IOTA Identities to build a PKI infrastructure - with public keys for entities are stored on the ledger and private keys will always remain private in the card. The cards hold the VCs after an individual is vaccinated and get a VC issued to them. When verification happens, the verifier gets the material needed for verifying the signature from the ledger, meaning the signature and the identity of the issuing organization.

The implemented workflow is presented in the figure below.



IOTA Foundation and Zebra are currently working into moving the VCs representation into QR code to represent the same credential that is stored in the card.The implementation will use QR code stickers that can be verified in two scans, one for the vaccination credential and one for personal identity verification. The VCs implementation already supports selective disclosure. As part of the core identity implementation IOTA Foundation is also looking to integrate disposable identities, creating different identities for each transaction as opposed to bringing all credentials together to the original identity to better protect privacy.

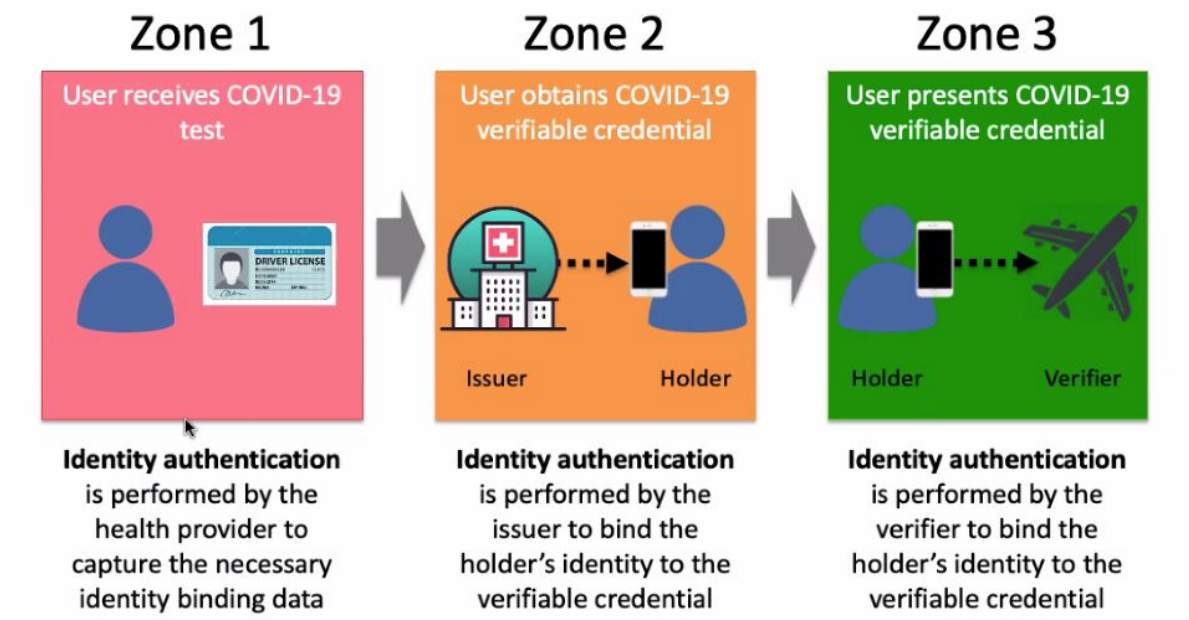
Focus/Specialty	Core/standard decentralized identity core tech and infrastructure for card based credential generation and verification
Paper-Based QR Code for VC	On-going, translate existing VC into QR-code representation
Systems Level Infrastructure	- IOTA node (optional) - Zebra card/QR-codes printers - Register a printer identity using provided APIs
Prework / Setup for Holder	- Receive a card (in case issued at home) - Receive a request to get vaccinated - Goes to designated vaccination center
Pre-Administration Verification	- Ask holder documents - KYC holder Provide a card or take the existing one from the holder Activate the card; request PIN and PUK Card generate Private and Public Key Card is read and public key created in the ledger, DID document
Vaccine Administration	Issuer create credentials in the portal and transfer into the card
VC / QR Code Generation	Card is created by the issuer and transfer into the card (signed)
On Site	A QR code is not printed at the moment but could be in the future and attached to a personal ID
Is it a REAL W3C VC?	Yes, JSON schema
Post Vaccine Administration	Holders makes next appointment, brings the card
Offsite / Follow Up	A new credential is issued (currently stored on the same card and both presented. Final implementation depends on cards and how we decide to manage presentation)

QR Code Presentations / Usage	- Card is presented, mobile reader - Reader get information from the card, public key identity - Reader resolve the identity on the ledger - Reader access credential, reader verify credential and its issuer
QR Code - Refresh / Revocation	- Identity can be disabled in the ledger/card is erased - Medium is reusable - Card is disposed
QR Code EOL	Not applicable at the moment; card can be regenerated

Breakout Sessions on Common Themes [Meeting Notes]

Session 1: Identity Proofing and Binding (Led by Todd Gehre)

- Given the state of the world the credential needs to have PII to bind the holder to the credential.
- VCI is using a FHIR health record that contains enough information to bind the patient to the record.
- Maybe it would be good to understand how to standardize the proofing (identity verification) process.



- When we talk about an identity credential it has to include identity proofing.
- Do we need PII in VC? Can we use DID / wallet proof
  - Yes we have to have a unique identifier
  - A lot of this depends on the verifier requirements
  - Using digital identities and zero knowledge to prove identity
- What can we do now, " to months, " two years.
- Assurance levels are difficult to do if we don't do binding at zone 1
- Given where we are in a world where vaccination has already been administered.
- Machine readability of zone 1 can we read a DL pr passport?
- Binding at zone 2 can be loose and let zone 3 figure it out.
- **It is important to make a declaration as a group that getting identity binding at zone 1 is the only way to avoid fraud.**
- There are millions of dollars on the table for people to solve this problem. There is marginal interest for technical people to solve it.

- At least in the US it's a regulatory issue. Need to get people to understand pair-wise anonymous connections.
- What sources of identity should we be using.
- There should be some recommendation of how to re-identify the individual in the future. How do we support re-identification between zone 2 and 3
- Define a set of protocols that support trust. If we have a protocol for KYC then we can ensure that the protocol was followed.
- There needs to be some protocol for people that don't have identification. If it might be required to access services it is important.
- Possible to add biometrics in QR as proof. It's an issue that it's a lot of data.
- Freestyle and if there is health record and then a health pass - If we can not do binding in zone 1 ath the health record level then the credental created a zone 2 Where does the rules engine go between 1 and 2 or 2 and 3
- The general idea Chris presented is that Zone 1 has to solve the double spend issue, Zone 2 has to handle identity binding. If you place the rules engine between Zone 1 and Zone 2, you have to have identity binding to the holder of Zone 1 credentials in order to allow them to enter them into the rules engine. Then, Zone 2 consists of an identifying URL that allows you to show when rules you comply with. Finally zone 3 just sends acceptable rule identifiers and gets a pass/fail result from Zone 2.
- It would be possible to salt the storage of Zone 2 with a key, pin, metadata or other information that the user controls that would impair unauthorized re-identification. This method does not support offline to offline because the holder is showing a URL for the pass query.

Session 2: Health Pass vs Health Record (Led by Tony Rose)

- Health Pass: Conveys a medical opinion on whether entry should be gained or not.
  Health Record: Conveys health related data
- The reason this is important is if you issue a health pass to a person, the verifier does not need to perform any policy based logic to determine if the person is adherent to the policy.
- A Health Pass may need to be revoked if policies change, which pushes some logic, at minimum, of revocation to the verifier.
- Important question of what is the policy at the point of engagement, or point of making a decision. A health pass pre-compiles that decision for a certain use case.
- Framing of Policy Conveyance vs. Rules Engines. The central user in the design of health policy, is the health department authority. So, the design of the system needs to be around empowering the health authority to convey policy.
- “Rich Code Reader” is a guy working.
- Point of engagement - a decision has to be made
  Precompiled and given to a person.
- How do you provide Health Authorities with a policy conveyancy capability?

Server to inject the policies.
- Verifier - subscribes to local health department rules.
- Good Health Pass definition of a Rules Engine is in a different place than the Common Pass
  Need to empower local health authorities to convey their policies.
- This is the job of governance frameworks.
  Help jurisdictions understand each policy decisions and where they agree
  What data they believe from each other.

Session 3: Compression Definitions - do we need one standard or create a wrapper for V1 and then push to W3C VC as V2 (Led by Vitor Pamplona)

- How many formats do we have?
  How does a QR reader identify each one of them?
  What specific steps the protocol takes from a W3C Credential to the QR?
- URI seems to be better for User-facing apps, Binary for Business cases.
- PathCheck's Format (Alphanumeric QR)
  - Starts with "CRED:" <Payload Type>:<version> Base32URL of the DER Signature : PublicKeyID : payload
  - TODO: turn CRED into byte arra
- Mattr Format (Binary QR)
  - Starts with "d9 05 01" + Base64 encoding of the CBOR-LD binary output
- Divoc Format (Binary QR)
  - Zip String with header "PK" of a Json LD document (UTF-8)
- IBM Digital Health Pass
  - We also use ZIP-style compression in our QR Codes
- Microsoft SmartHealthCards
  - They use "shc:/" prefix on a binary QR with Base10 encoding for the certificate.
- Other Formats?
- Do we want the Linux Foundation to host a directory of these ids? Maybe next steps?

Session 4: Patterns for Selective Disclosure & Data Minimization in Paper Credentials (Led by Marie Wallace)

- Goals of selective disclosure?
  - Equity —your privacy shouldn't depend on your access to technology
  - Currently we do not have anything in the US for selective disclosure—the CDC card discloses PII and PHI to all viewers
  - Paper holders are multiple cohorts, not a single group
  - Hard to address the situations where people can't keep up with a piece of paper
  - Should we treat verifiers differently whether they are a data processor or data controller (where consent, consent revocation, and other processes are required).

    - As a verifier I want to define the minimum set, how could that be handled with paper credentials?
    - Could there be some standardization on pseudo-anonymization of paper credentials that would still link to a physical ID, if required.
    - Don't want doormand to do interpretation… red/green light. There is an opportunity for a middleman to do this for digital. How for paper?
    - Dynamic generation: Not 100% paper based. Need to generate and print
    - What is min disclosure needed in any ecosystem.
    - Verifiers don't want more information than they require, and they don't know which information to require.
    - Governments may set guidelines for entry/access but not necessarily
    - Requiring vaccination for entry has equity implications and potential legal exposure
    - Data processors vs data controllers
        - Verifiers don't want to be in the business of deciding who can and cannot enter based on medical details
        - Good Health Pass puts control with issuers
    - What should be the minimum disclosure?
        - Minimal ID (single digit from date of birth?) + yes/no?
    - We cannot separate the paper from a digital system.
- Some example versions have two options (front/back); one a minimal data set (with just initials, first digit of DoB) and a boolean = true; the other more of a complete record - as one would have to show at the border.
  Both when scanned - are unique and traceable as no ZKP used (as it is on paper, so static - unless you have a big stack of them)
- 3 different things; what is in them; how to verify them; ???
- What do we need for equitable paper-based credentials?
    - To distinguish between Data Processor and Data Controller -- paper is frequently not a controller, so do they have more privacy -- Does Data Processor/Controller need to be visible flagged?
    - Agreement on minimal disclosure; some standards/recommendations on what it is and how it can be achieved, including pseudo-anonymization -- minimum needed to link a person to a credential (via physical ID) and minimize fraud.
    - The verifiers don't want to be responsible for making a business decision around a credential or set of credentials. Could there be a division of responsibilities, so a state or government entity (on citizen request) generates a "health pass" that incorporates the latest and greatest research on deciding whether someone is "green", then all the verifier has to do is just check that it's green and maybe match to ID.
    - Does the type of vaccine need to be included in the minimal viable disclosure?
    - We need some way to address a health status decision which might involve multiple pieces of paper.

- What is the minimum dataset required for a vaccine credential that can be used in a relatively low risk context such as boarding public transportation? We could combine this with the compression definition workstream to develop a minimum credential schema and compression framework that we can drive as a global baseline standard for vaccine and covid status passes.

About the COVID-19 Credentials Initiative

The COVID-19 Credentials Initiative (CCI) is an open global community looking to deploy and/or help deploy privacy-preserving verifiable credential projects in order to mitigate the spread of COVID-19 and strengthen our societies and economies.

The community builds on Verifiable Credentials, an open standard and emerging technology, which could offer additional benefits to paper/physical credentials, the most important being privacy-preserving and tamper-evident.

CCI joined Linux Foundation Public Health (LFPH) in December 2020 to work together on advancing the use of VCs, and data and technical interoperability of VCs in the public health realm, starting with vaccine records for COVID-19. We adopt an open-standard-based open-source development approach to public health, which has been proven very effective and efficient with LFPH's work in exposure notification apps.

Slack (#cci) | Email | Groups.io | Newsletter | Twitter | Linkedin | Medium

About Linux Foundation Public Health

Linux Foundation Public Health (LFPH)'s mission is to use open source software to help public health authorities (PHAs) around the world. Founded in summer of 2020, the initial focus of

LFPH has been helping PHAs deploy an app implementing the Google Apple Exposure Notification (GAEN) system. LFPH just brought in CCI to take lead on creating interoperable standards for sharing pandemic-related health data. As the organization grows, LFPH will be moving into other areas of public health that can take advantage of open source innovation.

Slack | Email | Twitter | Linkedin