2021-04-02 Paper Based Credentials Drafting Group Meeting Notes

Attendees

- Tony Rose
- Rebecca Distler
- Jim Mason
- Marie Wallace
- David Riedel
- David
- David Luchuk
- Jammal Dorsey
- Justin Dossey
- Kaliya Young
- Ramesh Raskar
- Sid Mishra
- Travis James
- Vitor Pamplona

Agenda Items

Time	Item	Who
2 min	Welcome & Antitrust Policy Notice	Chair
5 min	Introductions	All
30 min	JSON Format Discussion (Review of David Janes "Thoughts & Notes" from Slack)	David Janes
20 min	Consensus Points (Review of David Janes "Thoughts & Notes" from Slack)	David Janes
3 min	Wrap Up	Chair

Presentations -

(PDFs posted)

Recording - *Link*

Notes

1. Welcome and Linux Foundation antitrust policy

2. JSON Formats (Based on prompt)

- JSON-LD enables a single representation of a credential that could work as both paper and digital (means trade-off on space, but also meant one single credential). Also enables zero knowledge proofs.
    - You never present VC you present proof of the VC - important in that JSON-LD is common denominator and can help unify this across paper and digital
- There will be multiple flavors in payloads and QR codes no matter what we do.
    - Note that GHPs won’t necessarily have massive data elements (can be constrained if we focus on travel, not full use in epidemiology)
    - QR codes serve two purposes: proof + also something you might use to load credential into wallet (and not every QR code needs to be translated back to digital)

3. Points to gain consensus on (based on prompt)

- There’s never going to be a single set of schemas - we need to design a system that assumes a mess.
    - Group should explore what can we do to address this issue, rather than assuming this needs to be standardized.
    - Group should make a recommendation re: how to distinguish between payloads and codes.
- Need to understand credential vs. pass
    - Pass produced not by the original source of a covid test but by some intermediary - a secondary issuer and a secondary credential that is typically used in a specific context for a specific purpose
    - Terminology can be confusing to customers (e.g., IBM had to walk this language back)
- Pattern of recombining credentials into another credential will come up in a lot of discussion (passes derived from credentials)
    - Need to better help people understand that verifiable credentials don’t go on paper, presentations do (will help better understand credentials vs. proofs)

5. Wrap up

- Next steps

David Janes Thoughts & Notes (Discussion Prompt)

1. Definition of CREDENTIALS and PASSES as per GHPC Interoperability PDF
2. *Consensus Needed*:
    a. **Credentials** transform into Paper and back again **losslessly** - e.g. to the GHPC defined W3C VC
    b. **Passes** transform into Paper as a **one-way operation** (e.g. PathCheck)
3. If we have agreement on (2) and (2a) in particular, what are the ways of encoding the JSON
    a. JSON QR (lol)
    b. JSON CBOR QR
    c. JSON-LD CBOR-LD BASE32? QR (Mattr is here)
    d. JSON CBOR ZLIB QR
    e. JSON CBOR BASE32 QR
    f. JSON CBOR COSE ZLIB BASE32 QR (EU is here)
    g. JSONXT
4. *Consensus Needed*: how should we select from (3)
    a. Ease of Implementation
    b. Readily available and mature libraries in popular languages
    c. Best Size of Compression
    d. Size of Compress “Good Enough” (say, under 500 bytes - cross check with size GHPC is recommending!)
    e. Amount of code required
    f. Works in QR Code - Go/NoGo (cross check with size GHPC is recommending!)
5. *Consensus Needed*: is it OK if there are multiple compression methods - verifiers have a lot of work to do anyway?
6. Note that there are going to be multiple different QR payloads no matter what we do:
    a. GHPC in two flavours
    b. EU defines a JSON-based but non-W3CVC
    c. Multiple other passes now “in the wild”. Variants!
7. *Consensus Needed*: GPHC should make a recommendation how to distinguish between different payload types on QR codes, *even if they are not using GHPC credentials*.
8. PathCheck format:
    a. can GHPC credential be transformed into a PathCheck pass?
    b. how do the digital signatures / trust frameworks line up?
9. *Consensus Needed*: is PathCheck format the recommended format for passes, or is it PathCheck + compressed W3CVC.
10. *Question*: is GHPC defining a pass payload, or just a credential?
11. *Question*: How does DIVOC fit in all this??
12. Future meetings, but not now: identity binding & for (2a) being able to self inspect payload for personal assurance

Action Items

1. Connect with DIVOCC and MagnaCerta on use of JSON-LD