2021-04-09 Paper Based Credentials Drafting Group Meeting Notes

Attendees

- Tony Rose
- David Janes
- Rebecca Distler
- Marie Wallace
- Drummond Reed
- Bart Suichies
- Chris Raczkowski
- Dakota Gruener
- Erica Frenkel
- Jammal Dorsey
- Justin Dossey
- Kaliya Young
- Sara Facchinetti
- Sid
- Travis James
- Vitor Pamplona

Agenda Items

Time	Item	Who
2 min	Welcome & Antitrust Policy Notice	Rebecca & Tony
15 min	Overview of Glossary & Assets	Drummond
40 min	Discussion of Key Interoperability Questions	David
3 min	Wrap Up & Next Steps	David & Tony

Presentations

Glossary & Assets (collaborative draft)

Recording

Topic: Good Health Pass - Paper Credentials
Start Time : Apr 9, 2021 11:00 AM

Meeting Recording:
https://zoom.us/rec/share/yC4o2Gz_JkCfZp0VIWyBi9n4z2V50weo1Gpc2aIN7q6v8MFLj2Zs6OmPNpvcf3Ux.zUa4JatPrT2Fx_dj

Notes

1. Welcome and Linux Foundation antitrust policy

2. Overview of Glossary & Assets

- Need to add accompanying diagrams to governance framework / glossary
- Needs to be clear that digital pass could be produced by a digital presentation of a credential
- Two forms of a paper pass (one derived from a digital credential and one paper first)

3. Discussion of Key Interoperability Questions

[KIQ1] Which paper credential format or formats will digital health pass systems support?

DECISIONS

- Encoding / Compress method is undecided, need more information on payload from other TF
- Our recommendation will not be “open ended” and will be likely one strategy for compression of credentials, which must be reversible, and must fit in N bytes (N to be decided)

[KIQ2] Will paper credentials be compliant with the W3C Verifiable Credentials Data Model 1.0 specification?

DECISIONS

- We will recommend two types of encodings
    - one fully compatible

- one non-compatible, for constrained environments

[KIQ3] A. Will paper credentials require a digital signature to be included?

DISCUSSION

- Should be required, but need guidance on how to work with non-signed cards (e.g., CDC)
- Levels of assurance important to consider; if level of assurance is low, can accept non-signed (make attestation as issuer)
- Work in an ecosystem where this is not true, but we specifically recommend it

B. Which signature formats will Good Health Pass systems support?

DISCUSSION

- Signature formats will be specified by other groups and we recommend they give us something small
- Signature system could come with high payload; which encryption do we use? (e.g., list of schemes from paper creds summit?)
- We should define something here because we have unique challenges of what a credential looks like in our work. This paper creds working group should put something very specific out there, as it would really help the ecosystem.
    - Signature - multiple types of signatures methods; the more we allow, the worse for verifiers (have to use multiple cryptographic algorithms)
    - Algorithm - transform JSON into signing for verifying and signing (standardization)
    - Compression - after signing, how do you compress into QR?
    - DID access and schema definition - ideally, if you are on paper (low resource setting) define as best you can. How many characters on field name (push or leave open)?
    - Make a point to get signature group to get something small
    - LD signatures for paper?
    - Does it make sense to support bleeding edge signatures in paper based credentials?
    - Aim to put out set of recommendations to broadly align with WHO and EU so as an implementer, there are best practices out there
    - We can push for the things that are important to make it work on paper
    - We're calling it something different to ensure it could work on paper
    - Play with words/definitions to understand the constraints (e.g., why certain codes won't work with certain scanners)
    - Strong consensus around BBS+ within group

DECISIONS (A + B)

- we will require signatures; working in an ecosystem where it possibly isn't
- we will make a recommendation
- we will ask other groups for small, easy to implement

[KIQ4] Should the same privacy policies be applied to paper credentials, such as data minimization and disclosure limited to what is strictly required?

DISCUSSION

- Streamline definition of pass and what it should look like
    - As a principle (credential in pass), the more the pass itself can already be a form of selective disclosure, the better
        - Note that to meet verifier requirements (e.g., certain governments), you might have to show more data
    - Might introduce encryption needs; main feature of BBS+ (selective disclosure) doesn't make sense in paper bc you always have to show everything
    - Producing a pass from a credential could introduce significant signature size, which doesn't necessarily help interoperability

DECISIONS

- Yes

[KIQ5] How will these digital QR codes relate to the QR codes for paper credentials?

DISCUSSIONS

- Issue with something reduced to credential is that any verifier could go to issuer and rebind credential with full payload (digital online version)
    - Require an identifier to go back online; pass must/should include this field?
    - Opens up other requirements we need to be mindful of
- Also, verifiers talking directly to issuers (vs. talking to a cloud agent for the holder) raises significant privacy issues
    - Interesting idea, but opens up can of worms on identity correlation and privacy
    - Concerns over EU /eHealth Network building in a "phone home"

DECISIONS

- Question is unclear, decision to parking lot items related to it
- We are not solving for account recovery and re-issuance on paper

[KIQ6] Is there a need to turn a paper credential into a digital credential, and vice versa?

DECISIONS

- Our full credential will be transformable back into a digital credential

[KIQ7] What considerations need to be made for smart cards?

DECISIONS

- Smart cards are out of scope for this group
- Send to user experience group for scope (it's a form factor); OR asterisk and form a group later
- Smart cards could be talked about with wearables due to the same protocols potentially being used

[KIQ8] How will interoperability between these choices be tested/verified/certified?

DISCUSSION

- Need to provide basic payloads/JSON to do full test - schema to signature type
    - VCI tested payloads, but it only uses one library to do this
- Issuer job or solution provider-job
    - For some use cases, need to keep it private?
- Need to put in place what it means to be "good health pass compliant"

DECISIONS

- Open source verification
- Issuers issue test suites

4. Wrap Up & Next Steps

- Add QR concerns to next meeting (e.g., color matters, DPI matters, camera of verifier matters, lighting conditions, etc)
    - Will this need to be printed on commodity printers? high security printers (secure documents)?
    - We may want to expand on how these things are created
- Process on issuing and verifying - we may want to talk about quality of readers
    - QR codes, scanner capabilities first thing to discuss next meeting
- Also need to say what is in scope and out of scope for issuing and verifying - do we support really tiny QR codes? What is covered and what is not covered and what does this mean in terms of our recommendation?

Action Items

1. ALL to review assets and glossary (bold terms you need definitions for)
2. Drafting leads to suggest drafters for different sections?
3. Ask Rich (CodeReader) to come give a presentation on QR code reading at scale for real-world