2021-05-12 Paper Based Credentials Drafting Group Meeting Notes

Attendees

- Vitor Pamplona
- Mustafa Ozcakir
- Lukas Svec
- Kaliya Young
- David Janes
- Rebecca Distler
- Marie Wallace
- Drummond Reed
- Bart Suichies
- Alex Fryer

Agenda Items

Time	Item	Who
2 min	Welcome & Antitrust Policy Notice	Rebecca
15 min	Privacy Concerns	David/Marie
15 min	Verification Process	David/Vitor
15 min	Example Card Presentation	Mustafa
3 min	Wrap up	Chair

Presentations

Topic: Good Health Pass - Paper Credentials
Start Time : May 12, 2021 11:00 AM

Meeting Recording:
https://zoom.us/rec/share/bI52rj7TqB-5My59Tnz2l0FtxwRejyTz1ILMh_pg4H02B_87QnkTbApvFAFcPzbI.T5OUKnGO1oLIH715

Recording - *Link*

Notes

1. Welcome and Linux Foundation antitrust policy

2. Privacy Concerns

- Paper credential legally has to be both machine readable and human readable
  - If it’s not human readable, whole other set of issues
- Signed by trusted authority that anyone can look at - need official secure paper? Does this solve human readable piece?
- What you want to establish with paper-based credentials is answering the question: is the information on the document tampered with (yes/no), is the presenter the subject (yes/no). It's all about how you verify.
- What company/entity would want to take this risk? (certifying verifiers)
- Verifier needs to be legally responsible, governments can enact laws, weak identity binding
  - Paper credential only exposes initials/DOB (or year of birth)
  - Non-techy, simple, and effective
  - Use identifying information vs. identity information
- ZKP for digital credentials; paper-based suboptimal on many levels but it is the world we live in (+ important for inclusion)
- What is the trade-off between perfect and better? For many situations paper is very needed for accessibility even if there are risks.
- Without secure paper, anyone can replicate a QR code
- Paper-based things = mass scraping way harder; remove data from QR (has only a hash)
- Need to do “extreme” data minimization - only works for paper credentials and face to face; just a stamp to say this is smart paper
- Secure paper prevents copy - doesn’t prevent scraping; we need to have weak identity binding and considering that we have it, we need to minimize ability for that to be scraped (not necessarily focused on preventing copy)

3. Verification Process

- Should we make a recommendation about 'how to verify' in general. Could impact if we make the recommendation that we should only ask for minimum amount of info
- Is the information on the document tampered with (yes/no), is the presenter the subject (yes/no)
- The human verification can then be enough, and you have freedom as to what is on the document (stays between verifier and holder)
- Recommend describing this somewhere - verifier will have a significant role of what is a ghp

- Verifiers are big dependencies; if you have someone wanting to board a plane, he'll share whatever needs to be shared - if you don't have this info to begin with, hard to process
- In order to verify QR, need to insert initial into computer (calculating hash / verifying QR); if this step is not needed, could reuse QRs?
- If the human readable information is name/dob/vax status - thats a lot of info to type in; so remove this from QR and require manual insertion?
    - Hard to do anything about bad verifiers that have gone through process
    - If QR leaks, no names on it - can't really use it
    - Verification needs to have a secondary factor - not just about typing in QR code; if verification process is going to ask you to share another piece of information, then it falls into different category
    - Is this an unsolvable problem - need a practical solution, not about technology

4. Example Card Presentation

- Trying to authenticate people with credentials (no internet connection at airports); idea is coming from paper - integrated dynamic QR code in an offline system on the app; very simple system (code can be edited into credit card size); helps to combine two different control mechanisms at once
- Even if you're offline with this, can't copy (changes every 30 seconds)
- Idea that a small card that doesn't display the QR code (e-ink solutions)
- Just show QR and verifier can check if it's valid
- Is there a population that would adopt a new e-ink product but would not adopt an app solution?
- Valid OTP
- Digitally signed so it's valid; rogue verifier will say forget the OTP check

Action Items

1. Section leaders to clear comments from sections:

- Section 1 - @Marie Wallace
- Section 2 - @David Janes
- Section 3 - @David Janes
- Section 4 - @Justin Dossey
- Section 5 - @Bart Suichies
- Section 6 - @Bart Suichies
- Section 7 - @Vitor Pamplona
- Section 8 - @Justin Dossey
- Section 9 - @Tony Rose and @David Janes

2. Vitor to comment on data models draft

3. David and John to connect on JSON-LD