2021-05-05 Credential Formats, Signatures, and Exchange Protocols Drafting Group Meeting Notes

Attendees

- Brent Zundel, Co-chair
- Daniel Bachenheimer, Co-chair
- David Janes
- Drummond Reed
- Kaliya Young, Co-chair & WG Co-chair
- Nuttawut Kongsuwan
- Pam Dingle
- Riley Hughes
- Tony Rose
- Trev Harmon, PM
- Vitor Pamplona
- Wenjing Chu

Agenda Items

Time	Item	Who
2 min	Welcome & Antitrust Policy Notice	Trev
	Review and reconciliation with the work done by Paper Credentials Drafting Group	Everyone
1 min	Wrap up	Brent

Recording - *Link*

Notes

- Did the IP and antitrust announcement.
- David is here today from the Paper Creds drafting groups.
- David said the plan is to take a W3C VC, signed as specified, with payload as specified, and encode it to a QR code.
- They expect that this should work with BBS+.
- Obviously, a picture or biometric would cause issues with the size. They are trying to keep everything under 500 bytes.
- They have a policy that some data may be cached, and with the QR code, you should have everything needed to verify the credential.
- Once a QR code is written, that specific code can't be updated. So, we need to make sure we have all the necessary information.
- They are expecting a signed JSON-LD payload.
- Brent brought up that the signature scheme that is being suggested is a "two-part" signature. We had a discussion regarding how this might be encoded into QR code form.
- Is Paper Creds differentiating between paper-based credentials and paper-based passes? We had a discussion on this subject. Paper Creds is expecting that what is encoded will be in a final, usable form.
- Drummond is planning on updating the credential/pass "swimlane" diagrams. There's another possible path that came from a recent discussion with IATA. We discussed these diagrams.
- David noted that paper is probably going to be the most common use case.
- We had a discussion regarding the corrolatablity of paper credentials. A key point here is that there's a plethora of potential verifiers.
- Even printing out a whole stack of passes, there's still sufficient information to create correlation. Verifiable digital passes also likely have this issue, even with the other anti-correlation techniques available only to digital.
- We had a short discussion on the EU COVID-19 Certificate.
- We had a discussion regarding the verified presentation. This can be simple or a multi-step protocol.
- Raw data should target being no larger than 1500 bytes.
- Brent believes that there's no required verifier binding in the presentation.
- We had a discussion regarding how the signature scheme works with BBS+ with link secrets (ZKP & CL).

Chat Log

```
00:25:20        Trev Harmon:        Link to "review copy" to what Drummond is showing:
https://docs.google.com/presentation/d/1OGWA5bMNFGn3UQlJmb0X0pAxsJc07WyUN4c4HtTHKx0/edit#slide=id.
gd6968dcb86_0_70
00:31:57        Trev Harmon:        As a side note, the newest amendments to what the EU is doing has renamed
the "Digital Green Certificate" to the "EU COVID-19 Certificate".
00:44:14        Drummond Reed:        https://identity.foundation/presentation-exchange/spec/v1.0.0/
00:58:54        Nuttawut Kongsuwan:        https://mattrglobal.github.io/bbs-signatures-spec/
00:59:05        Drummond Reed:        Thanks
00:59:16        Nuttawut Kongsuwan:        ^^^ BBS+ doc by MATTR
01:05:17        Drummond Reed:        I have to run now, but fantastic conversation. It was very badly needed.
I recommend to do another call once both groups have their revised drafts.
```

Action Items

1. Next meeting is Friday (10:00 EDT).