2024-02-20 DMRWG Meeting Notes

Meeting Date

23 Jan 2023 The DMRWG meets bi-weekly on Tuesdays at 12:00-13:00 PT / 16:00-17:00 UTC. Check the ToIP Calendar for meeting dates.

Zoom Recording & supporting material

- Recording

Attendees

- Neil Thomson
- Steven Milstein
- Carly Huitema
- Burak Serdar

Main Goal of this Meeting

Verifiable Data Types - Verifiable Credentials are not the only form of Verifiable Data.

What are the similarities and differences?
What are the steps to establish trust between sender and receiver?
What if the sender did not create/issue the Data/Document?

Verifiable Data Types working document (for paper or blog)

Types to consider

Simple document (including messages)
Self-asserted claims
Complex Financial report (e.g., financial year end)
3rd-party attestation (replacement for "Doctor's Note"
Large Data Set (e.g., entire database or sub-set)
Discrete (events) and continuous (video) streaming data

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes
5 min	- Start recording - Welcome & antitrust notice - Introduction of new members - Agenda review	Chairs	- **Antitrust Policy Notice:** *Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws. Only members of ToIP who have signed the necessary agreements are permitted to participate in this activity beyond an observer role.* - New Members:

55 mins	Discussion	All	**Neil Thomson:** • Discussed verifiable data types and their differences, focusing on the traveler profile projects at Diff. • Highlighted the importance of understanding the packaging and intended purposes of data. • Shared a discussion document about verifiable documents and authentic messages, explaining the process of signing documents using DIDs and ensuring data integrity. • Raised concerns about the effectiveness and verifiability of signatures in PDF documents and the general process of verifying document authenticity. • Explored the concept of a traveler profile, which largely consists of self-attested data but may require third-party attestations for certain claims, like travel restrictions or medical information relevant for activities like scuba diving. • Delved into the complexities of certifying large data sets and the role of hashes in verifying the integrity of these sets. • Suggested developing a document that outlines a deeper understanding of what constitutes verifiable data, beyond the narrow scope of verifiable credentials. **Carly Huitema:** • Asked Neil about the process of signing PDF documents and how one could verify such signatures in the future. • Highlighted the potential use of cryptographic keys in document signing processes like DocuSign and pondered on the security and permanence of these keys. • Discussed the concept of large data sets and how their integrity could be maintained through hashes and attestation, contributing to the idea of complex, verifiable data beyond simple credentials. • Emphasized the importance of considering metasets or composite data, which include various components like cataloging information, interaction scripts, and process notations to ensure reproducibility and integrity. **Steven Milstein:** • Discussed the trust establishment task force at Diff and the concept of a verifiable document, emphasizing the need for author signatures and control over DIDs. • Talked about the financial industry and the importance of multiple signatures on documents like financial reports, highlighting the Glyph project as an example. • Raised concerns about the authenticity of data prior to signatures by CFOs or other officials, noting that there is no way to prove the legitimacy of numbers in financial statements without manual audits. **Burak Serdar:** • Noted that in the US medical data industry, the provenance of data is not a primary concern compared to the plausibility of data. • Explained that large data sets in healthcare often involve plausibility checks rather than in-depth provenance verification, focusing more on whether the data seems reasonable rather than its origin. **Key Points Summary:** • The meeting covered the complexities of verifiable data types, emphasizing the need for a comprehensive understanding beyond verifiable credentials. • Discussions revolved around the authenticity and integrity of data, the process of signing documents and ensuring their verifiability, and the challenges associated with large data sets and metasets. • The conversation highlighted different approaches to data verification in various contexts, such as financial reports and medical data, underlining the varying levels of concern regarding data provenance and plausibility. **Action Items:** • Develop a document or white paper that outlines a richer, deeper understanding of what constitutes verifiable data, including considerations for large data sets, metasets, and the importance of data provenance and integrity across different contexts.

Supporting Material:

- Carly Huitema: https://www.researchgate.net/figure/FMEA-Degree-of-Risk-Severity-Ranking_tbl5_263733916

  information on FEMA (Failure Mode Effects and Analysis)
  https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis

  I'm assuming that the ToIP Risk Assessment approach and worksheet are based on FEMA