Security, Privacy, and Data Protection Drafting Group

Objective

Good Health Pass compliant implementations must meet baseline security and privacy requirements that enable holders to maintain full control of their personal data.

Terms of Reference

All stakeholders in the Good Health Pass Collaborative digital trust ecosystem need to be confident in the security and privacy protections that the ecosystem enforces. In some jurisdictions, these protections are already required by existing data protection regulations; in other cases, governance authorities may seek to pass new legislation to enshrine them in law.

To be consistent with the Good Health Pass principles, it is anticipated that Good Health Pass solutions will need to be built on a decentralized identity architecture that places an emphasis on privacy and personal data control. Such systems seek to put the user in control of their personal identity data – including health attributes – which they can selectively disclose for a specified purpose and duration. Such systems stand in contrast to centralized models, which amass and store large amounts of personal data that is under the primary control of the aggregator.

For Good Health Pass systems, the issuance, holding, presentation, and verification of digital health credentials must – at a minimum – comply with applicable regulations requiring:

- **Privacy by Design and Default**
  - Non-linkable transactions: to prevent unintentional correlation of the holder
  - Data minimization: to enable selective disclosure of only the data strictly required by a verifier
  - Zero-knowledge proofs: privacy-preserving cryptography that supports selective disclosure
  - Privacy-preserving protocols: to help ensure that a user is not tracked when presenting their credentials
  - Transparency: to provide sufficient information to the holder about the processing of their personal data
  - Purpose limitation: to collect personal data for specified, explicit and legitimate purposes and not process it in a manner incompatible with those purposes
  - Auditable and informed consent (or delegation of consent)

- **Security by Design and Default**
  - Secure transmission of verifiable credentials
  - Secure storage of verifiable credentials (e.g, cloud- or edge-based wallet)
  - Secure issuance of verifiable credentials
  - Secure verification of verifiable credentials

Of particular importance with digital health credentials are *privacy-preserving identifiers*. This topic is discussed at length in the W3C Decentralized Identifiers (DIDs) Core 1.0 Specification. Specific DID methods support privacy-preserving identifiers that can provide the benefits of cryptographic verifiability without correlatability.

Responsibilities and Deliverables

Key Interoperability Questions That Must Be Answered

- Which local, regional, national, and international security standards apply?
  - ISO/IEC JTC1/SC 27 Information security, cybersecurity and privacy protection
  - ISO/IEC JTC1/SC 17 Cards and security devices for personal identification
  - ITU-T Study Group 13 - Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructure
  - Others such as SOC 2 Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
- Which privacy laws and regulations apply?
  - GDPR?
  - CCPA?
  - HIPAA?
  - Other?
- Where should Good Health Pass compliant apps and systems mandate the use of privacy-preserving identifiers?
- How do you prove that a specific Good Health Pass solution meets the security & privacy requirements?
  - Testing standards?
  - Self-test/self-attestation?
  - Third-party accreditations or certifications?
  - Open challenges to find vulnerabilities?
  - Data Protection Impact Assessments?
  - Privacy compliance assurance programs?

Chairs/Conveners

- Pagona Tsormpatzoudi (Mastercard)

Members

Only members of the Trust Over IP Foundation who have signed the necessary agreements and charters are permitted to participate in this Drafting Group and contribute to its deliverables.

Please add your name to the list below to indicate you have joined the Drafting Group:

- Ken Adler
- Trev Harmon

Meeting Schedule

The Drafting Group generally meets Tuesdays and Thursdays at 16:00 UTC.

Meeting Page

Please find agendas, presentations, notes and recordings for all Drafting Group meetings **HERE**.

Communications

The Slack channel for this Drafting Group (trustoverip.slack.com) is #ghp-wg-security-privacy