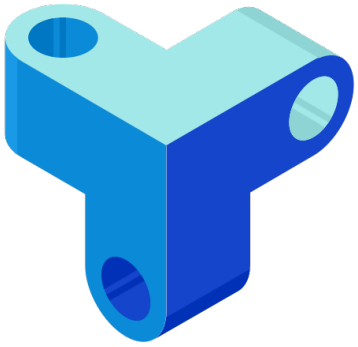


TRUST Over IP FOUNDATION

GHP Holder Wallet Requirements and User Experience Considerations

Version 1.0
11 November 2021

This publicly available requirement and considerations document was approved by the ToIP Foundation Steering Committee November 17, 2021.

The mission of the Trust over IP (ToIP) Foundation is to define a complete architecture for Internet-scale digital trust that combines cryptographic assurance at the machine layer with human accountability at the business, legal, and social layers. Founded in May 2020 as a non-profit hosted by the Linux Foundation, the ToIP Foundation has over 300 organizational and 100 individual members from around the world.

Please see the end page for licensing information and how to get involved with the Trust Over IP Foundation.

Table of Contents

Document Information

Author

Kaliya Young
Gordon Jones

Contributors

Daniel Bachenheimer
Darrell O'Donnell
Jacques Bikoundou
Jo Spencer
John Phillips
Lal Chandran
Lotta Lundin

Revision History

Version	Date Approved	Revisions
1.0	17 November 2021	Initial Publication

Terms of Use

RFC 2119

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and to ensure maximal efficiency in operation. IETF has been operating since the advent of the Internet using a Request for Comments (RFC) to convey "current best practice" to those organizations seeking its guidance for conformance purposes.

The IETF uses RFC 2119 to define keywords for use in RFC documents; these keywords are used to signify applicability requirements. ToIP has adapted the IETF RFC 2119 for use in the <name of this document>, and therefore its applicable use in ToIP-compliant governance frameworks.

The RFC 2119[1] keyword definitions and interpretation have been adopted. Those users who follow these guidelines SHOULD incorporate the following phrase near the beginning of their document:

> **The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.**

RFC 2119 defines these keywords as follows:

- **MUST**: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **MUST NOT**: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
- **SHOULD**: This word, or the adjective "RECOMMENDED", means that there MAY exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood and carefully weighed before choosing a different course.
- **SHOULD NOT**: This phrase, or the phrase "NOT RECOMMENDED" means that there MAY exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications SHOULD be understood, and the case carefully weighed before implementing any behavior described with this label.
- **MAY**: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor MAY choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor MAY omit the same item.

Requirements include any combination of Machine-Testable Requirements and Human-Auditable Requirements. Unless otherwise stated, all Requirements MUST be expressed as defined in RFC 2119.

- **Mandates** are Requirements that use a MUST, MUST NOT, SHALL, SHALL NOT or REQUIRED keyword**.**
- **Recommendations** are Requirements that use a SHOULD, SHOULD NOT, or RECOMMENDED keyword.
- **Options** are Requirements that use a MAY or OPTIONAL keyword.

[1] https://datatracker.ietf.org/doc/html/rfc2119. Accessed June, 2021.

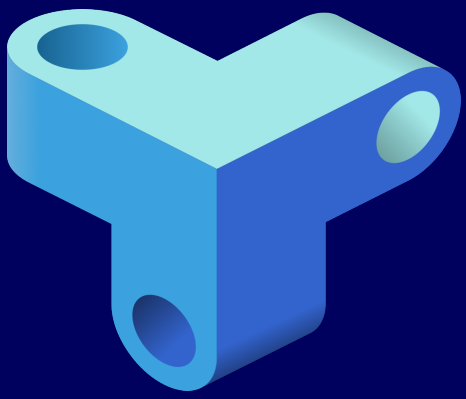
An implementation which does not include a particular option MUST be prepared to interoperate with other implementations which include the option, recognizing the potential for reduced functionality. As well, implementations which include a particular option MUST be prepared to interoperate with implementations which do not include the option and the subsequent lack of function the feature provides.

GHP Holder Wallet Requirements and User Experience Considerations

The need to create a consistent user experience – based on a model of universal acceptance – is the most fundamental interoperability challenge we must meet. In short, a Good Health Pass (GHP) MUST be easy to obtain, use, and update, without any special user knowledge.

Thus, it becomes the responsibility of the digital wallet developers to consider these requirements and considerations critical. Wallet developers and implementers that support the GHP Interoperability Blueprint:

1. SHOULD be user-centric in design by working in the user's interests, support users in the event of malfunctioning, and support the trusted relationship between a user and a third party.
2. SHOULD support guardianship, delegation and segregate users (e.g., parent and child) so that digital certificates and passes cannot be intermingled.
3. MUST be long-lived and reflect users' natural, intuitive processes for using digital credentials.
4. MUST secure all Verifiable Credentials to include Good Health Pass Credentials and Good Health Passes, provide privacy warnings, consent and user rights management, portability, and backup plus recovery to users.
5. SHOULD take advantage of secure enclaves when available on the device to store cryptographic key material, other critical data, and the wallet application itself.
6. MUST provide a means for user authentication in use cases where relying parties expect authentication at the holder wallet to a specified level of authenticator assurance (AAL).
7. MUST be able to interact both in online mode and offline mode.
8. MUST provide a mechanism for the user to audit what data they have shared with whom.
9. MUST enable Holders to remove any personal data directly from debugging logs.
10. MUST display an explicit warning to the holder about the privacy implications if a verifier requests a presentation of an entire credential.
11. SHOULD publicly disclose how the system works, including governance, adaptability, information security policies, and perform internal and external security audits of their information infrastructure.
12. SHOULD use W3C Verifiable Credentials as follows:
    - Formats and Signatures: JSON-LD, with BBS+
    - Issuance Protocol: WACI Pe-X for issuance
    - Presentation Protocol: WACI Pe-X for presentation



TRUST Over IP FOUNDATION

The Trust Over IP Foundation (ToIP) is hosted by the Linux Foundation under its Joint Development Foundation legal structure. We produce a wide range of tools and deliverables organized into five categories:

- Specifications to be implemented in code
- Recommendations to be followed in practice
- Guides to be executed in operation
- White Papers to assist in decision making
- Glossaries to be incorporated in other documents

ToIP is a membership organization with three classes—Contributor, General, and Steering.

The work of the Foundation all takes place in Working Groups, within which there are Task Forces self-organized around specific interests. All ToIP members regardless of membership class may participate in all ToIP Working Groups and Task Forces.

When you join ToIP, you are joining a community of individuals and organizations committed to solving the toughest technical and human centric problems of digital trust. Your involvement will shape the future of how trust is managed across the Internet, in commerce, and throughout our digital lives. The benefits of joining our collaborative community are that together we can tackle issues that no single organization, governmental jurisdiction, or project ecosystem can solve by themselves. The results are lower costs for security, privacy, and compliance; dramatically improved customer experience, accelerated digital transformation, and simplified cross-system integration.

To learn more about the Trust Over IP Foundation please visit our website, https://trustoverip.org.

Licensing Information:
All Trust Over IP Foundation deliverables are published under the following licenses:

Copyright mode: Creative Commons Attribution 4.0 International licenses
http://creativecommons.org/licenses/by/4.0/legalcode

Patent mode: W3C Mode (based on the W3C Patent Policy)
http://www.w3.org/Consortium/Patent-Policy-20040205

Source code: Apache 2.0.
http://www.apache.org/licenses/LICENSE-2.0.htm