Workgroup: Network Working Group
Internet-Draft:
draft-hallambaker-mesh-notarization
Published: 28 June 2023
Intended Status: Informational
Expires: 30 December 2023
Authors: P. M. Hallam-Baker
Venture Cryptography.

Mathematical Mesh 3.0 Part IX: Mesh Notarized Signatures

Abstract

Creation and verification of Mesh Notarized Signatures is described . A notarized signature is a signature whose time of creation is attested by one or more parties in addition to the signer. In the case of Mesh Notarized Signatures, the attesting parties is the set of all parties participating in a Notarization Mesh. This ideally includes the relying parties.

Each participant in a Notarization Mesh maintains their own notary log in the form of a DARE sequence authenticated by a Merkle tree. Participants periodically cross notarize their personal notary log with those maintained by other parties. A Mesh Notarized Signature is bound in time as having being created after time T1 by including one or more sequence apex values as signed attributes. A Mesh Notarized Signature is bound in time as having being created before time T2 by enrolling it in the signer's personal notarization log and engaging in cross-notarization with a sufficient number of Notarization Mesh participants to establish the desired proof.

Defection is controlled through an accountability model. If a trusted notary produces multiple inconsistent signed cross Notarization tokens, this provides non-repudiable evidence of a default.

https://mailarchive.ietf.org/arch/browse/mathmesh/Discussion of this draft should take place on the MathMesh mailing list (mathmesh@ietf.org), which is archived at .

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 30 December 2023.

Copyright Notice

Table of Contents

1. Introduction

This draft specifies the creation and verification of Mesh Notarized Signatures. A notarized signature is a signature whose time of creation is attested by one or more parties in addition to the signer. In the case of Mesh Notarized Signatures, the attesting parties is the set of all parties participating in a Notarization Mesh. This ideally includes the relying parties.

2. Definitions

This section presents the related specifications and standard, the terms that are used as terms of art within the documents and the terms used as requirements language.

2.1. Requirements Language

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 [RFC2119].

2.2. Defined Terms

2.3. Related Specifications

2.4. Implementation Status

The implementation status of the reference code base is described in the companion document [draft-hallambaker-mesh-developer].

3. Architecture

3.1. Sequence Apex Value

3.2. Proof of Inclusion

3.3. Notarized Signature

3.3.1. Before MNT

Proof of inclusion presented in a protected header, i.e. within the signature scope

3.3.2. After MNT

Proof of inclusion presented in the signature header or an external assertion.

3.4. Cross Notarization

A notarized signature over

3.5. Proof of default

4. Notarized Signature Verification

4.1. Proof that a signature was created after a time

4.2. Proof that a signature was created before a time

5. Notarization Architectures

5.1. Bridge Architecture

5.2. Redundant Bridge Architecture

5.3. Full Mesh

6. Notary Default

7. Security Considerations

7.1. Notary Default

7.2. Quantum Cryptanalysis

8. IANA Considerations

This document requires no IANA actions.

9. Acknowledgements

10. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

11. Informative References

[draft-hallambaker-mesh-developer] Hallam-Baker, P., "Mathematical Mesh: Reference Implementation", Work in Progress, Internet-Draft, draft-hallambaker-mesh-developer-10, 27 July 2020, <https://datatracker.ietf.org/doc/html/draft-hallambaker-mesh-developer-10>.