Mathematical Mesh 3.0 Part XI: Mesh Notarized Signatures

Mesh Notarization Token

<series>draft-hallambaker-mesh-notarization

<status>informational

<stream>independent

<ipr>trust200902

<author>Phillip Hallam-Baker

<surname>Hallam-Baker

<initials>P. M.

<firstname>Phillip

<email>phill@hallambaker.com

<organization>Venture Cryptography.

<keyword>Threshold Cryptography

<keyword>Elliptic Curve

<keyword>Threshold Encryption

<keyword>Threshold Key Generation

<keyword>Notary

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.

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

# 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.

# 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.

## 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 <norm="RFC2119"/>.

## Defined Terms

## Related Specifications

## Implementation Status

The implementation status of the reference code base is described in the companion document <info="draft-hallambaker-mesh-developer"/>.

# Architecture

## Sequence Apex Value

## Proof of Inclusion

## Notarized Signature

### Before MNT

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

### After MNT

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

## Cross Notarization

A notarized signature over

## Proof of default

# Notarized Signature Verification

## Proof that a signature was created after a time

## Proof that a signature was created before a time

# Notarization Architectures

## Bridge Architecture

## Redundant Bridge Architecture

## Full Mesh

# Notary Default

# Security Considerations

## Notary Default

## Quantum Cryptanalysis

# IANA Considerations

This document requires no IANA actions.

# Acknowledgements