Kill this – Make part of Cryptography

Mathematical Mesh 3.0 Part XII: Mesh Post Quantum Architecture

Mathematical Mesh Reference

<series>draft-hallambaker-mesh-quantum

<status>informational

<stream>independent

<ipr>trust200902

<author>Phillip Hallam-Baker

<surname>Hallam-Baker

<initials>P. M.

<firstname>Phillip

<email>phill@hallambaker.com

<also>http://mathmesh.com/Documents/draft-hallambaker-mesh-quantum.html

The Mathematical Mesh ‘The Mesh’ is an infrastructure that facilitates the exchange of configuration and credential data between multiple user devices and provides end-to-end security. This document describes.

[Note to Readers]

Discussion of this draft takes place on the MATHMESH mailing list (mathmesh@ietf.org), which is archived at https://mailarchive.ietf.org/arch/search/?email\_list=mathmesh.

# Introduction

## PQC Bootstrap Signatures

## Notarized Signatures

## Interactive Key Exchange

## KEM initialization of Symmetric Key Infrastructure

# 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

The terms of art used in this document are described in the *Mesh Architecture Guide* <info="draft-hallambaker-mesh-architecture"/>.

## Related Specifications

The architecture of the Mathematical Mesh is described in the *Mesh Architecture Guide* <info="draft-hallambaker-mesh-architecture"/>. The Mesh documentation set and related specifications are described in this document.

## Implementation Status

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

# Hybrid Mesh Profile

Specifies two or more signature keys

Fingerprint is calculated over a JOSE sequence of the key fingerprints.

Profile is signed over both algorithms

Authenticate documents under trusted algorithm(s).

# Notarized Signatures

Provide proof that a signature was created in a time interval [T1..T2].

Relying party MAY consider signature to be trustworthy if T2 is believed to be before Quantum cryptanalysis became feasible.

# Interactive Key Exchange

Allows Alice and Bob to jointly establish a shared secret using KEM when they are engaged in interactive exchange.

# Static Data Encryption

# Security Considerations

The security considerations for use and implementation of Mesh services and applications are described in the Mesh Security Considerations guide <norm="draft-hallambaker-mesh-security"/>.

# IANA Considerations

All the IANA considerations for the Mesh documents are specified in this document

# Acknowledgements

A list of people who have contributed to the design of the Mesh is presented in <norm="draft-hallambaker-mesh-architecture"/>.