Mathematical Mesh 3.0 Part XI: Mesh Repository Service

Mesh Discovery Service

<series>draft-hallambaker-mesh-repository

<status>informational

<stream>independent

<ipr>trust200902

<author>Phillip Hallam-Baker

<surname>Hallam-Baker

<initials>P. M.

<firstname>Phillip

<email>phill@hallambaker.com

<organization>ThresholdSecrets.com

<keyword>Threshold Cryptography

<keyword>Elliptic Curve

<keyword>Threshold Encryption

<keyword>Threshold Key Generation

<keyword>Ceremony

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

The Mesh Callsign registry performs X principal functions:

* Provides ground truth for notarized records.

# Definitions

This section presents the related specifications and standards....

## Related Specifications

The Mesh Repository Service is a component part of the Mathematical Mesh <norm="draft-hallambaker-mesh-architecture"/> and makes use of the data formats and service formats described therein. In particular:

Uniform Data Fingerprint <norm="draft-hallambaker-mesh-udf"/>.

Describes the UDF format used to represent cryptographic nonces, keys and content digests in the Mesh and the use of Encrypted Authenticated Resource Locators (EARLs) and Strong Internet Names (SINs) that build on the UDF platform.

Data at Rest Encryption <norm="draft-hallambaker-mesh-dare"/>.

Describes the cryptographic message and append-only sequence formats used in Mesh applications and the Mesh Service protocol.

JSON-BCD Encoding <norm="draft-hallambaker-jsonbcd"/>.

Describes extensions to the JSON serialization format to allow direct encoding of binary data (JSON-B), compressed encoding (JSON-C) and extended binary data encoding (JSON-D). Each of these encodings is a superset of the previous one so that JSON-B is a superset of JSON, JSON-C is a superset of JSON-B and JSON-D is a superset of JSON-C.

## Defined Terms

This document makes use of the terms defined in <norm="draft-hallambaker-mesh-architecture"/>.

## 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 RFC 2119 <norm="RFC2119"/>.

## Implementation Status

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

<include=..\Examples\Colophon.md>

# Repository Operations

## Write

### Create

### Append

### Delete

Depending on the storage type declared when the object is created, a delete operation only causes an object to be removed from the active catalog and added to the deleted catalog. This is to ensure rapid recovery from cases of accidental or malicious erasure.

For files that are generated from a source file, this may be unnecessary. For example, an object file created from a program source which may be easily recreated.

For files that are subject to confidentiality controls, removal of the key is probably more appropriate.

### Index

## Read

### Complete

### Partial

#### By frame

#### By byte

#### Metadata

### Subscribe

# Repository Catalog

Repository catalogs and indexes are read only records that are automatically updated by operations on the registry

## Entry Description

### Path(s)

### Labels

### Deletion policy

Allow delete or erasure.

### Update policy

### Type

Fixed object or sequence?

### Links

Describe the relationship of one object to another.

# Schemas

<include=..\Generated\CallsignLog.md>

<include=..\Generated\CallsignRegistry.md>

<include=..\Generated\CallsignRegistrar.md>

# Security Considerations

## Confidentiality

### Traffic Analysis

## Integrity

### Malicious publication of inappropriate, defamatory or illegal content

## Service

### Data Loss

# IANA Considerations

This document requires no IANA actions.

# Acknowledgements