Mathematical Mesh 3.0 Part XIII: Mesh Carnet

Mesh Carnet

<series>draft-hallambaker-mesh-carnet

<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

The Mesh Callsign Registry

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

# Definitions

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

## Related Specifications

The Mesh Callsign registry 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>

## Reserved Callsigns

# Security Considerations

# IANA Considerations

This document requires no IANA actions.

# Acknowledgements