Mesh ceremonies

Onboarding ceremonies

<series>draft-hallambaker-mesh-ceremonies

<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>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

# 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"/>.

# Device Onboarding Ceremonies

## Networked Desktop to Desktop (Fingerprint Verification)

## Networked Mobile to Desktop (Dynamic QR Code)

## Pre-Networked Mobile to Mobile (Dynamic QR Code)

## Pre-Networked Headless Device to Mobile (Static QR Code)

## Mobile proxy to Desktop

# Contact Establishment Ceremonies

## In Person

## Remote

## Registration

## Trusted Third Party Endorsement

# Authentication Ceremonies

## Second Factor Authentication

## Confirmation

# Security Considerations

This section TBS

One concern to be particularly careful of is that when adding two public keys, a rogue key attack is possible. The security of the private keys is the maximum of the two inputs but the trustworthiness of the public keys is the minimum.

# IANA Considerations

This document requires no IANA actions.

# Acknowledgements