Mathematical Mesh: Client-Service Protocol

Mathematical Mesh CSP

<ietf>draft-hallambaker-mathematical-mesh-protocols

<ipr>trust200902

<category>Standards Track

<area>Security

<version>00

<author>Phillip Hallam-Baker

<lastname>Hallam-Baker

<initials>P. M.

<firstname>Phillip

<organization>Comodo Group Inc.

<email>[philliph@comodo.com](mailto:philliph@comodo.com)

# Abstract

The Mathematical Mesh ‘The Mesh’ is an end-to-end secure infrastructure that facilitates the exchange of configuration and credential data between multiple user devices. The core protocols of the Mesh are described with examples of common use cases and reference data.

# Introduction

# Definitions

## 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 [!RFC2119].

# Use Scenarios

## Create Profile

## Connect Device

## Add Application

## Update Application

## Delete Device

## Key Recovery

# Architecture

## Data Model

### First Class Object

### Profile

A profile is a first class object. It has a globally unique identifier that provides an unambiguous reference to the profile in any situation.

### Record

A record describes the state of an object at the completion of a specific Transaction.

### Transaction

A transaction is an event in which the state of an object changes. Every transaction has a globally unique transaction identifier. Transaction identifiers are issued in a monotonic sequence such that a transaction that completes at time t1 will always have a lower transaction identifier than one that begins at time t2 where t2 > t1.

## Profile Types

Master Profile

Personal Profile

Application Profile

Device Profile

Figure : Relationship of Profile Types

Personal

Device 1

Master

Device 2

AppEntryA

AppEntryB

AppEntryC

App A

App B

App C

## Master Profile

The master profile contains the axioms of trust for a Mesh user.

Identifier: “Master” + UDF Fingerprint of the Master Signing Key

Signature: Master Signing Key

The key used to sign the profile MUST be MasterSigningKey

Property: Master Signing Key

The Master Signing key is the ultimate trust axiom for the Master Profile.

Property: Master Escrow Keys

Property: Online Signature Keys

## Personal Profile

Identifier: UDF Fingerprint of the Master Signing Key

Signature: Online Signature Key

The key used to sign the profile MUST be a member of MasterProfile/OnlineSignatureKeys

Property: Master Profile

The Master Profile that this personal profile is an instance of.

Property: Devices

Property: Applications

A list of application profile entries specifying which application profiles are attached to the personal profile

## Device Profile

Identifier: UDF Fingerprint of the Device Signing Key

Signature: Device Signing Key

The key used to sign the profile MUST be MasterSigningKey

Property: Device Signing Key

The Master Signing key is the ultimate trust axiom for the Master Profile.

Property: Device Encryption Key

Property: Device Authentication Key

## Application Profile

Identifier: Randomly chosen

Property: Encrypted Data