Network Working Group P. Hallam-Baker
Internet-Draft April 4, 2019
Intended status: Informational
Expires: October 6, 2019

# Mathematical Mesh Part VII: Security Considerations
## draft-hallambaker-mesh-security-00

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.

This document is also available online at http://mathmesh.com/Documents/draft-hallambaker-mesh-security.html [1] .

Table of Contents

# 1. Introduction

# 2. 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.

## 2.1. 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 [RFC2119] .

## 2.2. Defined Terms

The terms of art used in this document are described in the Mesh Architecture Guide [draft-hallambaker-mesh-architecture] .

## 2.3. Related Specifications

The architecture of the Mathematical Mesh is described in the Mesh Architecture Guide [draft-hallambaker-mesh-architecture] . The Mesh documentation set and related specifications are described in this document.

## 2.4. Implementation Status

The implementation status of the reference code base is described in the companion document [draft-hallambaker-mesh-developer] .

## 2.5. Shared Classes

The following classes are used as common elements in Mesh profile specifications.a

### 2.5.1. Structure: PublicKey

The PublicKey class is used to describe public key pairs and trust assertions associated with a public key.

UDF: String (Optional) UDF fingerprint of the public key parameters/

X509Certificate: Binary (Optional) List of X.509 Certificates

X509Chain: Binary [0..Many] X.509 Certificate chain.

X509CSR: Binary (Optional) X.509 Certificate Signing Request.

## 2.6. Mesh Profile Objects

Base class for all Mesh Profile objects.

### 2.6.1. Structure: Profile

Parent class from which all profile types are derived

Names: String [0..Many] Fingerprints of index terms for profile retrieval. The use of the fingerprint of the name rather than the name itself is a precaution against enumeration attacks and other forms of abuse.

Updated: DateTime (Optional) The time instant the profile was last modified.

NotaryToken: String (Optional) A Uniform Notary Token providing evidence that a signature was performed after the notary token was created.

### 2.6.2. Keyset Classes

### 2.6.3. Structure: EscrowedKeySet

A set of escrowed keys.

[No fields]

### 2.6.4. Profile Classes

### 2.6.5. Structure: ProfileMaster

Inherits: Profile

Describes the long term parameters associated with a personal profile.

This profile MUST be signed by

MasterSignatureKey: PublicKey (Optional) The root of trust for the Personal PKI, the public key of the PMSK is presented as a self-signed X.509v3 certificate with Certificate Signing use enabled. The PMSK is used to sign certificates for the PMEK, POSK and PKEK keys.

MasterEscrowKeys: PublicKey [0..Many] A Personal Profile MAY contain one or more PMEK keys to enable escrow of private keys used for stored data.

OnlineSignatureKeys: PublicKey [0..Many] A Personal profile contains at least one OSK which is used to sign device administration application profiles.

### 2.6.6. Structure: ProfileDevice

Inherits: Profile

Describes a mesh device.

This profile MUST be signed by the DeviceSignatureKey

Description: String (Optional) Description of the device

DeviceSignatureKey: PublicKey (Optional) Key used to sign certificates for the DAK and DEK. The fingerprint of the DSK is the UniqueID of the Device Profile

DeviceAuthenticationKey: PublicKey (Optional) Key used to authenticate requests made by the device.

DeviceEncryptionKey: PublicKey (Optional) Key used to pass encrypted data to the device such as a DeviceUseEntry

### 2.6.7. Structure: ProfileApplication

Inherits: Profile

Contains the public description of a Mesh application.

[No fields]

### 2.6.8. Structure: ProfileMesh

Inherits: ProfileApplication

Contains the binding of a device to a MasterProfile. Each device has a separate profile which MUST be signed by an OnlineSignatureKey

Account: String (Optional) Account address.

MasterProfile: DareMessage (Optional) Master profile of the account being registered.

AccountEncryptionKey: PublicKey (Optional) Key used to encrypt data under this profile

### 2.6.9. Structure: ProfileMeshDevicePublic

Inherits: ProfileApplication

Inherits: ProfileApplication

DeviceProfile: DareMessage (Optional) Device profile of the device making the request.

Permissions: Permission [0..Many] List of the permissions that the device has been granted.

### 2.6.10. Structure: ProfileMeshDevicePrivate

Inherits: ProfileApplication

Inherits: ProfileApplication

Permissions: Permission [0..Many] List of the permissions that the device has been granted.

ProfileNonce: Binary (Optional) Random nonce used to mask the fingerprint of the profile UDF.

ProfileWitness: Binary (Optional) Witness value calculated over the ProfileNonce and profile UDF

### 2.6.11. Structure: DeviceRecryptionKey

UDF: String (Optional) The fingerprint of the encryption key

RecryptionKey: PublicKey (Optional) The recryption key

DeviceRecryptionKeyEncrypted: DareMessage (Optional) The decryption key encrypted under the user's device key.

## 2.7. Common Structures

### 2.7.1. Structure: Permission

Name: String (Optional)

Name: String (Optional)

Role: String (Optional)

Role: String (Optional)

Capabilities: DareMessage (Optional) Keys or key contributions enabling the operation to be performed

### 2.7.2. Structure: Contact

Identifier: String (Optional)

Identifier: String (Optional)

Account: String (Optional)

Account: String (Optional)

FullName: String (Optional)

FullName: String (Optional)

Title: String (Optional)

Title: String (Optional)

First: String (Optional)

First: String (Optional)

Middle: String (Optional)

Middle: String (Optional)

Last: String (Optional)

Last: String (Optional)

Suffix: String (Optional)

Suffix: String (Optional)

Labels: String [0..Many]

Labels: String [0..Many]

Addresses: Address [0..Many]

Addresses: Address [0..Many]

Locations: Location [0..Many]

Locations: Location [0..Many]

Roles: Role [0..Many]

### 2.7.3. Structure: Role

CompanyName: String (Optional)

CompanyName: String (Optional)

Addresses: Address [0..Many]

Addresses: Address [0..Many]

Locations: Location [0..Many]

### 2.7.4. Structure: Address

URI: String (Optional)

URI: String (Optional)

Labels: String [0..Many]

### 2.7.5. Structure: Location

Appartment: String (Optional)

Appartment: String (Optional)

Street: String (Optional)

Street: String (Optional)

District: String (Optional)

District: String (Optional)

Locality: String (Optional)

Locality: String (Optional)

County: String (Optional)

County: String (Optional)

Postcode: String (Optional)

Postcode: String (Optional)

Country: String (Optional)

### 2.7.6. Structure: Reference

MessageID: String (Optional) The received message to which this is a response

ResponseID: String (Optional) Message that was generated in response to the original (optional).

Relationship: String (Optional) The relationship type. This can be Read, Unread, Accept, Reject.

## 2.8. Catalog Entries

### 2.8.1. Structure: CatalogEntry

[No fields]

### 2.8.2. Structure: CatalogEntryDevice

Inherits: CatalogEntry

Public device entry, indexed under the device ID

Account: String (Optional) The Account to which this entry binds this device.

UDF: String (Optional) UDF of the signature key

AuthUDF: String (Optional) UDF of the authentication ID

ProfileMeshDevicePublicSigned: DareMessage (Optional) The device profile

ProfileMeshDevicePrivateEncrypted: DareMessage (Optional) The device profile

DeviceRecryptionKeys: DeviceRecryptionKey [0..Many] Decryption key entries.

### 2.8.3. Structure: CatalogEntryCredential

Inherits: CatalogEntry

Inherits: CatalogEntry

Protocol: String (Optional)

Protocol: String (Optional)

Service: String (Optional)

Service: String (Optional)

Username: String (Optional)

Username: String (Optional)

Password: String (Optional)

### 2.8.4. Structure: CatalogEntryNetwork

Inherits: CatalogEntry

Inherits: CatalogEntry

Protocol: String (Optional)

Protocol: String (Optional)

Service: String (Optional)

Service: String (Optional)

Username: String (Optional)

Username: String (Optional)

Password: String (Optional)

### 2.8.5. Structure: CatalogEntryContact

Inherits: CatalogEntry

Inherits: CatalogEntry

Key: String (Optional) Unique key.

Permissions: Permission [0..Many] List of the permissions that the contact has been granted.

Contact: DareMessage (Optional) The (signed) contact data.

### 2.8.6. Structure: CatalogEntryContactRecryption

Inherits: CatalogEntryContact

[No fields]

### 2.8.7. Structure: CatalogEntryBookmark

Inherits: CatalogEntry

Inherits: CatalogEntry

Uri: String (Optional)

Uri: String (Optional)

Title: String (Optional)

Title: String (Optional)

Path: String (Optional)

### 2.8.8. Structure: CatalogEntryTask

Inherits: CatalogEntry

Inherits: CatalogEntry

Task: DareMessage (Optional)

Task: DareMessage (Optional)

Key: String (Optional) Unique key.

### 2.8.9. Structure: Task

Key: String (Optional) Unique key.

Start: DateTime (Optional)

Start: DateTime (Optional)

Finish: DateTime (Optional)

Finish: DateTime (Optional)

StartTravel: String (Optional)

StartTravel: String (Optional)

FinishTravel: String (Optional)

FinishTravel: String (Optional)

TimeZone: String (Optional)

TimeZone: String (Optional)

Title: String (Optional)

Title: String (Optional)

Description: String (Optional)

Description: String (Optional)

Location: String (Optional)

Location: String (Optional)

Trigger: String [0..Many]

Trigger: String [0..Many]

Conference: String [0..Many]

Conference: String [0..Many]

Repeat: String (Optional)

Repeat: String (Optional)

Busy: Boolean (Optional)

### 2.8.10. Structure: CatalogEntryApplication

Inherits: CatalogEntry

Inherits: CatalogEntry

Key: String (Optional)

### 2.8.11. Structure: CatalogEntryApplicationEntry

[No fields]

### 2.8.12. Structure: CatalogEntryApplicationRecryption

[No fields]

### 2.8.13. Structure: CatalogEntryApplicationSSH

[No fields]

### 2.8.14. Structure: CatalogEntryApplicationMail

[No fields]

### 2.8.15. Structure: CatalogEntryApplicationNetwork

[No fields]

## 2.9. Messages

### 2.9.1. Structure: MeshMessage

MessageID: String (Optional)

MessageID: String (Optional)

Sender: String (Optional)

Sender: String (Optional)

Recipient: String (Optional)

Recipient: String (Optional)

References: Reference [0..Many]

### 2.9.2. Structure: MeshMessageComplete

Inherits: MeshMessage

[No fields]

### 2.9.3. Structure: MessageConnectionRequest

Inherits: MeshMessage

Inherits: MeshMessage

Account: String (Optional)

Account: String (Optional)

DeviceProfile: DareMessage (Optional) Device profile of the device making the request.

ClientNonce: Binary (Optional)

ClientNonce: Binary (Optional)

ServerNonce: Binary (Optional)

ServerNonce: Binary (Optional)

Witness: String (Optional)

Witness: String (Optional)

PinID: String (Optional) Pin identifier used to identify a PIN authenticated request.

### 2.9.4. Structure: MessageConnectionPIN

Inherits: MeshMessage

Inherits: MeshMessage

Account: String (Optional)

Account: String (Optional)

Expires: DateTime (Optional)

Expires: DateTime (Optional)

PIN: String (Optional)

### 2.9.5. Structure: MessageContactRequest

Inherits: MeshMessage

Inherits: MeshMessage

Contact: DareMessage (Optional) The contact data.

### 2.9.6. Structure: MessageConfirmationRequest

Inherits: MeshMessage

Inherits: MeshMessage

Text: String (Optional)

### 2.9.7. Structure: MessageConfirmationResponse

Inherits: MeshMessage

Inherits: MeshMessage

ResponseID: String (Optional)

ResponseID: String (Optional)

Accept: Boolean (Optional)

### 2.9.8. Structure: MessageTaskRequest

Inherits: MeshMessage

[No fields]

## 3. Mesh Portal Service Reference

HTTP Well Known Service Prefix: /.well-known/mmm

Every Mesh Portal Service transaction consists of exactly one request followed by exactly one response. Mesh Service transactions MAY cause modification of the data stored in the Mesh Portal or the Mesh itself but do not cause changes to the connection state. The protocol itself is thus idempotent. There is no set sequence in which operations are required to be performed. It is not necessary to perform a Hello transaction prior to a ValidateAccount, Publish or any other transaction.

### 3.1. Request Messages

A Mesh Portal Service request consists of a payload object that inherits from the MeshRequest class. When using the HTTP binding, the request MUST specify the portal DNS address in the HTTP Host field.

#### 3.1.1. Message: MeshRequest

Base class for all request messages.

Portal: String (Optional) Name of the Mesh Portal Service to which the request is directed.

### 3.2. Response Messages

A Mesh Portal Service response consists of a payload object that inherits from the MeshResponse class. When using the HTTP binding, the response SHOULD report the Status response code in the HTTP response message. However the response code returned in the payload object MUST always be considered authoritative.

#### 3.2.1. Message: MeshResponse

Base class for all response messages. Contains only the status code and status description fields.

[No fields]

### 3.3. Imported Objects

The Mesh Service protocol makes use of JSON objects defined in the JOSE Signatgure and Encryption specifications.

### 3.4. Common Structures

The following common structures are used in the protocol messages:

#### 3.4.1. Structure: KeyValue

Describes a Key/Value structure used to make queries for records matching one or more selection criteria.

Key: String (Optional) The data retrieval key.

Value: String (Optional) The data value to match.

### 3.4.2. Structure: SearchConstraints

Specifies constraints to be applied to a search result. These allow a client to limit the number of records returned, the quantity of data returned, the earliest and latest data returned, etc.

NotBefore: DateTime (Optional) Only data published on or after the specified time instant is requested.

Before: DateTime (Optional) Only data published before the specified time instant is requested. This excludes data published at the specified time instant.

MaxEntries: Integer (Optional) Maximum number of data entries to return.

MaxBytes: Integer (Optional) Maximum number of data bytes to return.

PageKey: String (Optional) Specifies a page key returned in a previous search operation in which the number of responses exceeded the specified bounds.

When a page key is specified, all the other search parameters except for MaxEntries and MaxBytes are ignored and the service returns the next set of data responding to the earlier query.

## 3.5. Transaction: Hello

Request: HelloRequest

Request: HelloRequest

Response: HelloResponse

Report service and version information.

The Hello transaction provides a means of determining which protocol versions, message encodings and transport protocols are supported by the service.

## 3.6. Transaction: ValidateAccount

Request: ValidateRequest

Request: ValidateRequest

Response: ValidateResponse

Request validation of a proposed name for a new account.

For validation of a user's account name during profile creation.

### 3.6.1. Message: ValidateRequest

Inherits: MeshRequest

Describes the proposed account properties. Currently, these are limited to the account name but could be extended in future versions of the protocol.

Account: String (Optional) Account name requested

Reserve: Boolean (Optional) If true, request a reservation for the specified account name. Note that the service is not obliged to honor reservation requests.

Language: String [0..Many] List of ISO language codes in order of preference. For creating explanatory text.

### 3.6.2. Message: ValidateResponse

Inherits: MeshResponse

States whether the proposed account properties are acceptable and (optional) returns an indication of what properties are valid.

Note that receiving a 'Valid' responseto a Validate Request does not guarantee creation of the account. In addition to the possibility that the account namecould be requested by another user between the Validate and Create transactions, a portal service MAY perform more stringent validation criteria when an account is actually being created. For example, checking with the authoritative list of current accounts rather than a cached copy.

Valid: Boolean (Optional) If true, the specified account identifier is acceptable. If false, the account identifier is rejected.

Minimum: Integer (Optional) Specifies the minimum length of an account name.

Maximum: Integer (Optional) Specifies the maximum length of an account name.

InvalidCharacters: String (Optional) A list of characters that the service does not accept in account names. The list of characters

MAY not be exhaustive but SHOULD include any illegal characters in the proposed account name.

Reason: String (Optional) Text explaining the reason an account name was rejected.

## 3.7. Transaction: CreateAccount

Request: CreateRequest

Request: CreateRequest

Response: CreateResponse

Request creation of a new portal account.

Unlike a profile, a mesh account is specific to a particular Mesh portal. A mesh account must be created and accepted before a profile can be published.

### 3.7.1. Message: CreateRequest

Request creation of a new portal account. The request specifies the requested account identifier and the Mesh profile to be associated with the account.

Inherits: MeshRequest

Inherits: MeshRequest

Account: String (Optional) Account identifier requested.

### 3.7.2. Message: CreateResponse

Inherits: MeshResponse

Reports the success or failure of a Create transaction.

[No fields]

## 3.8. Transaction: DeleteAccount

Request: DeleteRequest

Request: DeleteRequest

Response: DeleteResponse

Request deletion of a portal account.

Deletes a portal account but not the underlying profile. Once registered, profiles are permanent.

### 3.8.1. Message: DeleteRequest

Request deletion of a new portal account. The request specifies the requested account identifier.

Inherits: MeshRequest

Inherits: MeshRequest

Account: String (Optional) Account identifier to be deleted.

### 3.8.2. Message: DeleteResponse

Inherits: MeshResponse

Reports the success or failure of a Delete transaction.

[No fields]

## 3.9. Transaction: Get

Request: GetRequest

Request: GetRequest

Response: GetResponse

Search for data in the mesh that matches a set of properties described by a sequence of key/value pairs.

### 3.9.1. Message: GetRequest

Describes the Portal or Mesh data to be retreived.

Inherits: MeshRequest

Inherits: MeshRequest

Identifier: String (Optional) Lookup by profile ID

Account: String (Optional) Lookup by Account ID

KeyValues: KeyValue [0..Many] List of KeyValue pairs specifying the conditions to be met

SearchConstraints: SearchConstraints (Optional) Constrain the search to a specific time interval and/or limit the number and/or total size of data records returned.

Multiple: Boolean (Optional) If true return multiple responses if available

Full: Boolean (Optional) If true, the client requests that the full Mesh data record be returned containing both the Mesh entry itself and the Mesh metadata that allows the date and time of the publication of the Mesh entry to be verified.

### 3.9.2. Message: GetResponse

Reports the success or failure of a Get transaction. If a Mesh entry matching the specified profile is found, containsthe list of entries matching the request.

Inherits: MeshResponse

Inherits: MeshResponse

DataItems: DataItem [0..Many] List of mesh data records matching the request.

PageKey: String (Optional) If non-null, indicates that the number and/or size of the data records returned exceeds either the SearchConstraints specified in the request or internal server limits.

## 3.10. Transaction: Publish

Request: PublishRequest

Request: PublishRequest

Response: PublishResponse

Publish a profile or key escrow entry to the mesh.

### 3.10.1. Message: PublishRequest

Requests publication of the specified Mesh entry.

Inherits: MeshRequest

[No fields]

### 3.10.2. Message: PublishResponse

Reports the success or failure of a Publish transaction.

Inherits: MeshResponse

[No fields]

## 3.11. Transaction: Status

Request: StatusRequest

Request: StatusRequest

Response: StatusResponse

Request the current status of the mesh as seen by the portal to which it is directed.

The response to the status request contains the last signed checkpoint and proof chains for each of the peer portals that have been checkpointed.

[Not currently implemented]

### 3.11.1. Message: StatusRequest

Inherits: MeshRequest

Initiates a status transaction.

[No fields]

### 3.11.2. Message: StatusResponse

Reports the success or failure of a Status transaction.

Inherits: MeshResponse

Inherits: MeshResponse

LastWriteTime: DateTime (Optional) Time that the last write update was made to the Mesh

LastCheckpointTime: DateTime (Optional) Time that the last Mesh checkpoint was calculated.

NextCheckpointTime: DateTime (Optional) Time at which the next Mesh checkpoint should be calculated.

CheckpointValue: String (Optional) Last checkpoint value.

### 3.12. Transaction: ConnectStart

Request: ConnectStartRequest

Request: ConnectStartRequest

Response: ConnectStartResponse

Request connection of a new device to a mesh profile

#### 3.12.1. Message: ConnectStartRequest

Inherits: MeshRequest

Initial device connection request.

SignedRequest: SignedConnectionRequest (Optional) Device connection request signed by thesignature key of the device requesting connection.

AccountID: String (Optional) Account identifier of account to which the device is requesting connection.

#### 3.12.2. Message: ConnectStartResponse

Reports the success or failure of a ConnectStart transaction.

Inherits: MeshRequest

[No fields]

### 3.13. Transaction: ConnectStatus

Request: ConnectStatusRequest

Request: ConnectStatusRequest

Response: ConnectStatusResponse

Request status of pending connection request of a new device to a mesh profile

### 3.13.1. Message: ConnectStatusRequest

Inherits: MeshRequest

Request status information for a pending request posted previously.

AccountID: String (Optional) Account identifier for which pending connection information is requested.

DeviceID: String (Optional) Device identifier of device requesting status information.

### 3.13.2. Message: ConnectStatusResponse

Reports the success or failure of a ConnectStatus transaction.

Inherits: MeshRequest

Inherits: MeshRequest

Result: SignedConnectionResult (Optional) The signed ConnectionResult object.

## 3.14. Transaction: ConnectPending

Request: ConnectPendingRequest

Request: ConnectPendingRequest

Response: ConnectPendingResponse

Request a list of pending requests for an administration profile.

### 3.14.1. Message: ConnectPendingRequest

Inherits: MeshRequest

Specify the criteria for pending requests.

AccountID: String (Optional) The account identifier of the account for which pending connection requests are requested.

SearchConstraints: SearchConstraints (Optional) Constrain the search to a specific time interval and/or limit the number and/or total size of data records returned.

### 3.14.2. Message: ConnectPendingResponse

Reports the success or failure of a ConnectPending transaction.

Inherits: MeshRequest

Inherits: MeshRequest

Pending: SignedConnectionRequest [0..Many] A list of pending requests satisfying the criteria set out in the request.

PageKey: String (Optional) If non-null, indicates that the number and/or size of the data records returned exceeds either the SearchConstraints specified in the request or internal server limits.

## 3.15. Transaction: ConnectComplete

Request: ConnectCompleteRequest

Request: ConnectCompleteRequest

Response: ConnectCompleteResponse

Post response to a pending connection request.

### 3.15.1. Message: ConnectCompleteRequest

Reports the success or failure of a ConnectComplete transaction.

Inherits: MeshRequest

Inherits: MeshRequest

Result: SignedConnectionResult (Optional) The connection result to be posted to the portal. The result MUST be signed by a valid administration key for the Mesh profile.

AccountID: String (Optional) The account identifier to which the connection result is posted.

### 3.15.2. Message: ConnectCompleteResponse

Inherits: MeshRequest

Reports the success or failure of a ConnectComplete transaction.

[No fields]

### 3.16. Transaction: Transfer

Request: TransferRequest

Request: TransferRequest

Response: TransferResponse

Perform a bulk transfer of the log between the specified transaction identifiers. Requires appropriate authorization

[Not currently implemented]

#### 3.16.1. Message: TransferRequest

Request a bulk transfer of the log between the specified transaction identifiers. Requires appropriate authorization

Inherits: MeshRequest

Inherits: MeshRequest

SearchConstraints: SearchConstraints (Optional) Constrain the search
to a specific time interval and/or limit the number and/or total size of data records returned.

#### 3.16.2. Message: TransferResponse

Inherits: MeshResponse

Reports the success or failure of a Transfer transaction. If successful, contains the list of Mesh records to be transferred.

DataItems: DataItem [0..Many] List of mesh data records matching the
request.

PageKey: String (Optional) If non-null, indicates that the number and/or size of the data records returned exceeds either the SearchConstraints specified in the request or internal server limits.

## 4. Assets

### 4.1. Data

### 4.2. Credentials

### 4.3. Reputation

#### 4.3.1. Outbound Messaging Abuse ()

## 5. Risks

### 5.1. Confidentiality

Is a regulatory requirement GDPR/HIPPA

#### 5.1.1. Privacy

Stronger requirement, given data but with restrictions on use

Unintended use within an organization may put it in default

GDPR

HIPPA

### 5.2. Integrity

Modification of data enables control breaches

### 5.3. Availability

#### 5.3.1. Data loss

Loss of the pictures of the kids at 5

#### 5.3.2. Partial data survivability

Where they buried Aunt Agatha's jewelry but not where they buried Aunt Agatha.

### 5.4. Inbound Messaging Abuse (Spam)

## 6. Threats

### 6.1. End point Compromise

6.2.

# 7. Controls

## 7.1. Cryptographic

### 7.1.1. Triple lock

#### 7.1.1.1. Transport Security

Traffic analysis protection

#### 7.1.1.2. Message Security

Access control

Authentication / Integrity

#### 7.1.1.3. Data Level Security

Data Confidentiality

Non-Repudiation

### 7.1.2. Key Protection

Use of platform provided facilities to bind private keys in the Device profile to the device is highly desirable. Ideally, private keys should be protected against extraction by hardware techniques presenting a high degree of resistance.

#### 7.1.2.1. Windows

Use encrypted key store

Preferably use BitLocker

#### 7.1.2.2. OSX

Use Key Ring

#### 7.1.2.3. iOS

Use ???

#### 7.1.2.4. Linux

Use the DBUS mechanism

#### 7.1.2.5. Android

Hope and prayers.

### 7.1.3. Key and Nonce Generation

Use strong mechanisms as described in RFC???

Use of key co-generation as described in part 8 is advised

### 7.1.4. Key Escrow and Recovery

Master profile keys should be escrowed

Escrow strategies for DARE should take account of the fact that users
may want some but not all their data assets to survive them.

### 7.1.5. Profile Verification

Check that the device credential has been signed by an administration
device and that the administration device was properly authorized by
the master profile.

Device catalog MUST be signed by the admin device.

Future ? provide protection against rollback attacks.

### 7.1.6. Identity Validation

See the separate document on the trust model

### 7.1.7. Trust Broker Accountability

Cert transparency type techniques

## 7.2. Mesh Messaging

### 7.2.1. Ingress Control

Every message is subject to access control

Mesh Services should perform abuse filtering on inbound mail

Mesh Services MUST apply user specified ingress control as specified
in their contacts catalog.

### 7.2.2. Egress Control

Some applications may require egress control

For example, classified environments

Mail too stupid to send

### 7.2.3. Security Signal

Confirmation messages requiring payments

Need Accountability

Need to know the source of the accountability assertions

Should be distinguished from sender controlled part of a message

#### 7.2.3.1. Brand

If messages are being sent on behalf of a corporate entity, this should be signaled to both sender and receiver

Sender ? remind them that they are speaking on behalf of another party

Receiver ? establish who is speaking by the familiar technique.

### 7.2.4. Accountability

Authentication and consequences

## 8. Security Considerations

This document comprises the security considerations for the use and implementation of the Mathematical Mesh.

## 9. IANA Considerations

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

## 10. Acknowledgements

## 11. References

### 11.1. Normative References

[draft-hallambaker-mesh-architecture]
Hallam-Baker, P., "Mathematical Mesh Part I: Architecture Guide", draft-hallambaker-mesh-architecture-06 (work in progress), August 2018.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.

### 11.2. Informative References

[draft-hallambaker-mesh-developer]
Hallam-Baker, P., "Mathematical Mesh: Reference Implementation", draft-hallambaker-mesh-developer-07 (work in progress), April 2018.

### 11.3. URIs

[1] http://mathmesh.com/Documents/draft-hallambaker-mesh-security.html

Author's Address

Phillip Hallam-Baker

Email: phill@hallambaker.com