Mathematical Mesh 3.0 Part IV: Schema Reference

Mesh Schema Reference

<series>draft-hallambaker-mesh-schema

<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

<also>http://mathmesh.com/Documents/draft-hallambaker-mesh-schema.html

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.

[Note to Readers]

Discussion of this draft takes place on the MATHMESH mailing list (mathmesh@ietf.org), which is archived at https://mailarchive.ietf.org/arch/search/?email\_list=mathmesh.

# Introduction

This document describes the data structures of the Mathematical Mesh with illustrative examples. For an overview of the Mesh objectives and architecture, consult the accompanying *Architecture Guide* <norm="draft-hallambaker-mesh-architecture"/>. For information on the implementation of the Mesh Service protocol, consult the accompanying *Protocol Reference* <norm="draft-hallambaker-mesh-protocol"/>

This document has two main sections. The first section presents examples of the Mesh assertions, catalog entries and messages and their use. The second section contains the schema reference. All the material in both sections is generated from the Mesh reference implementation <info="draft-hallambaker-mesh-developer"/>.

Although some of the services described in this document could be used to replace existing Internet protocols including FTP and SMTP, the principal value of any communication protocol lies in the size of the audience it allows them to communicate with. Thus, while the Mesh Messaging service is designed to support efficient and reliable transfer of messages ranging in size from a few bytes to multiple terabytes, the near-term applications of these services will be to applications that are not adequately supported by existing protocols if at all.

# 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

The terms of art used in this document are described in the *Mesh Architecture Guide* <norm="draft-hallambaker-mesh-architecture"/>.

## Related Specifications

The architecture of the Mathematical Mesh is described in the *Mesh Architecture Guide* <norm="draft-hallambaker-mesh-architecture"/>. The Mesh documentation set and related specifications are described in this document.

## Implementation Status

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

# Actors

The Mesh mediates interactions between three principal actors: **Accounts**, **Devices**, and **Services**.

Currently two account types are specified, **user accounts** which belong to an individual user and **group accounts** that are used to share access to confidential information between a group of users. It may prove useful to define new types of account over time or to eliminate the distinction entirely. When active a Mesh account is bound to a Mesh Service. The service to which an account is bound MAY be changed over time but an account can only be bound to a single service at a time.

A Mesh account is an abstract construct that (when active) is instantiated across one or more physical machines called a device. Each device that is connected to an account has a separate set of cryptographic keys that are used to interact with other devices connected to the account and MAY be provisioned with access to the account private keys which MAY or MAY NOT be mediated by the current Mesh Service. A user's Mesh accounts and the devices connected to them constitute that user's Personal Mesh.

A Mesh Service is an abstract construct that is provided by one or more physical machines called Hosts. A Mesh Host is a device that is attached to a service rather than an account.

## Accounts

A Mesh Account is described by a Profile descended from Profile Account and contains a set of Mesh stores. Currently two account profiles are defined:

ProfileUser

Describes a user account.

ProfileGroup

Describes a group account used to share confidential information between a group of users.

Both types of profile specify the following fields:

ProfileSignature

The public signature key used to authenticate the profile itself

AccountAddress

The account name to which the account is currently bound. (e.g. alice@example.com, @alice).

ServiceUdf

If the account is active, specifies the fingerprint of the service profile to which the account is currently bound.

AdministratorSignature

The public signature key used to verify administrative actions on the account. In particular addition of devices to a user account or members to a group account.

AccountEncryption

The public encryption key for the account. All messages sent to the account MUST be encrypted under this key. By definition, all data encrypted under this account is encrypted under this key.

User accounts specify two additional public keys, AccountSignature and AccountAuthentication which allow signature and authentication operations under the account context.

Every account contains a set of catalogs and spools that are managed by the service as directed by the contents of the associated Access catalog.

For example, the personal account profile Alice created in

<include="..\Examples\SchemaAliceProfile.md">

## Device

Every Mesh device has a set of private keys that are unique to that device. These keys MAY be installed during manufacture, installed from an external source after manufacture or generated on the device. If the platform capabilities allow, device private keys SHOULD be bound to the device so that they cannot be extracted or exported without substantial effort.

The public keys corresponding to the device private keys are specified in a ProfileDevice. This MUST contain at least the following fields:

ProfileSignature

The public signature key used to authenticate the profile itself.

Encryption

Public encryption key used as a share contribution to generation of device encryption keys to be used in the context of an account and to decrypt data during the process of connecting to an account.

Authentication

Public authentication key used as a share contribution to generation of device authentication keys to be used in the context of an account and to authenticate the device to a service during the process of connecting to an account.

Signature

Public signature key used as a share contribution to generation of device signature keys to be used in the context of an account.

<include="..\Examples\SchemaAliceDevice2.md">

### Activation

The device private keys are only used to perform cryptographic operations during the process of connecting a device to an account. During that connection process, a threshold key generation scheme is used to generate a second set of device keys bound to the account by combining the base key held by the device with a second device private key provided by the administration device approving the connection of the device to the account. The resulting key is referred to as the device key. The process of combining the base keys with the contributions to form the device keys is called Activation.

<include="..\Examples\SchemaAliceActivationDevice2.md">

The Mesh protocols are designed so that there is never a need to export or escrow private keys of any type associated with a device, neither the base key, nor the device key nor the contribution from the administration device.

This approach to device configuration ensures that the keys that are used by the device when operating within the context of the account are entirely separate from those originally provided by the device manufacturer or generated on the device, provided only that the key contributions from the administration device are sufficiently random and unguessable.

### Connection Assertion

The administration device combines the public keys specified in the device profile with the public components of the keys specified in the activation record to calculate the public keys of the device operating in the context of the account. These public keys are then used to create at a ConnectionDevice and a ConnectionService assertion signed by the account administration signature key.

<include="..\Examples\SchemaAliceConnectionDevice2.md">

The ConnectionDevice assertion MAY be used in the same fashion as an X.509v3/PKIX certificate to mediate interactions between devices connected to the same account without the need for interaction with the Mesh service. Thus, a coffee pot device connected to the account can receive and authenticate instructions issued by a voice recognition device connected to that account.

While the ConnectionDevice assertion MAY be used to mediate external interactions, this approach is typically undesirable as it provides the external parties with visibility to the internal configuration of the account, in particular which connected devices are being used on which occasions. Furthermore, the lack of the need to interact with the service means that the service is necessarily unable to mediate the exchange and enforce authorization policy on the interactions.

Device keys are intended to be used to secure communications between devices connected to the same account. All communication between Mesh accounts SHOULD be mediated by a Mesh service. This enables abuse mitigation by applying access control to every outbound and every inbound message.

## Service

Mesh services are described by a ProfileService. This specifies the encryption, and signature authentication keys used to interact with the abstract service.

<include="..\Examples\SchemaProfileService.md">

Since Mesh accounts and services are both abstract constructs, they cannot interact directly. A device connected to an account can only interact with a service by interacted with a device authorized to provide services on behalf of one or more accounts connected to the service. Such a device is called a Mesh Host.

Mesh hosts MAY be managed using the same ProfileDevice and device connection mechanism provided for management of user devices or by whatever other management protocols prove convenient. The only part of the Service/Host interaction that is visible to devices connected to a profile and to hosts connected to other services is the ConnectionHost structure that describes the set of device keys to use in interactions with that specific host.

<include="..\Examples\SchemaConnectionHost.md">

Mesh Services MAY make use of the profile and activation mechanism used to connect devices to accounts to manage the connection of hosts to services. But this is optional. It is never necessary for a device to publish a ProfileHost assertion.

# Catalogs

Catalogs track sets of persistent objects associated with a Mesh Service Account. The Mesh Service has no access to the entries in any Mesh catalog except for the Device and Contacts catalog which are used in device authentication and authorization of inbound messages.

Each Mesh Catalog managed by a Mesh Account has a name of the form:

<prefix>\_<name>

Where <prefix> is the IANA assigned service name. The assigned service name for the Mathematical Mesh is mmm. Thus, all catalogs specified by the Mesh schema have names prefixed with the sequence mmm\_.

The following catalogs are currently specified within the Mathematical Mesh.

Access: mmm\_Access

Describes access control policy for performing operations on the account. The Access catalog is the only Mesh catalog whose contents are readable by the Mesh Service under normal circumstances.

Application: mmm\_Application

Describes configuration information for applications including mail (SMTP, IMAP, OpenPGP, S/MIME, etc) and SSH and for the MeshAccount application itself.

Bookmark: mmm\_Bookmark

Describes Web bookmarks and other citations allowing them to be shared between devices connected to the profile.

Contact: mmm\_Contact

Describes logical and physical contact information for people and organizations.

Credential: mmm\_Credential

Describes credentials used to access network resources.

Device: mmm\_Device

Describes the set of devices connected to the account and the permissions assigned to them

Network: mmm\_Network

Describes network settings such as WiFi access points, IPSEC and TLS VPN configurations, etc.

Member: mmm\_Member

Describes the set of members connected to a group account.

Publication: mmm\_Publication

Describes data published under the account context. The data MAY be stored in the publication catalog itself or on a separate service (e.g. a Web server).

Task: mmm\_CatalogTask

Describes tasks assigned to the user including calendar entries and to do lists.

The Access, and Publication catalogs are used by the service in certain Mesh Service Protocol interactions. The Device and Member catalogs are used to track the connection of devices to a user account and members to a group for administrative purposes. These interactions are further described below.

In many cases, the Mesh Catalog offers capabilities that represent a superset of the capabilities of an existing application. For example, the task catalog supports the appointment tracking functions of a traditional calendar application and the task tracking function of the traditional 'to do list' application. Combining these functions allows tasks to be triggered by other events other than the passage of time such as completion of other tasks, geographical presence, etc.

In such cases, the Mesh Catalog entries are designed to provide a superset of the data representation capabilities of the legacy formats and (where available) recent extensions. Where a catalog entry is derived from input presented in a legacy format, the original data representation MAY be attached verbatim to facilitate interoperability.

## Access

The access catalog mmm\_Access contains a list of access control entries providing authorization to devices authenticated by a particular credential. The access catalog provides information that is necessary for the Mesh Service to act on behalf of the user. It is therefore necessary for the service to be able to decrypt entries in the catalog.

The entries in the catalog have type CatalogedAccess and specify a capability. The following capabilities are defined:

AccessCapability

Authorizes a device authenticated by specified means to request privileged account operations. For example, requesting the status of an account catalog.

CryptographicCapability

Specifies a private key encrypted under the encryption key of the service and criteria specifying the parties authorized to request use of the key.

DataCapability

Authorizes a device authenticated by specified means to obtain a data item.

The Access catalog plays a central role in all operations performed by the service on behalf of the user.

Every access capability is gated by a specified set of authentication criteria. The following authentication criteria are currently defined:

Device Authentication Key

The service will only perform the operation if the device making the request presents the specified authentication key.

This form of authentication is necessary to restrict access to account operations so that only connected devices can interact with stores, etc.

Account Profile Identifier

The service will only perform the operation if the device making the request presents an authentication key that is credentialed by a connection assertion to the specified account profile.

This form of authentication is necessary to perform administration operations on a group account since it is the account rather than the device that is authorized to perform the operation.

Proof of Knowledge

The service will only perform the operation if proof of knowledge of the identified shared secret is provided.

This form of authentication criteria is used to allow device connection and contact exchange by means of static (i.e. printed) QR codes.

Future: Currently, the set of authentication criteria is limited to direct grants of a single capability to a single specified device or account. This approach may prove to be unnecessarily verbose requiring the same information to be repeated multiple times.

### Access Capability

The access capability permits a specified service operation on the account. Optionally, an access capability MAY specify a Data entry encrypted to a key held by the device.

#### User Device

An access capability is required for every device connected to a user account. Typically, the authentication criteria requires that requests be authenticated by means of the device account authentication key.

If support for future device recovery, the account access log SHOULD specify an access capability for an authentication key that can be obtained from the recovery data (e.g. the Profile authentication key). Otherwise, an out-of-band intervention by the service operator will be required to allow the user to regain the ability to use their account.

Provides the Cataloged Device entry for the device.

// Access capability example.

#### Group administrator

Group account - authentication criteria for admin actions, connection must be issued under the specified account.

Data - contains the share for the account. This is obtained by means of the claim operation.

//

#### Publish device connection profile

Publish device config - authentication criteria is PIN

Obtained by means of the CLAIM operation

#### Publish contact information

//

Publish contact - authentication criteria is PIN

Obtained by means of the CLAIM operation

//

#### Messaging

Messaging - will need more

The current revision of the specification does not address the means by which messaging access rights are granted. This will require a new access capability to be defined.

Contact

Contact messages from the specified subject.

Confirmation

Confirmation messages from the specified subject.

Async

Asynchronous delivery messages (e.g. mail)

Sync

Synchronous delivery messages (e.g. chat)

Presence

Forward presence request.

The following media are defined

Text

Text that MUST NOT contain links or external references

Linked

Text that MAY contain links or external reference

Audio

Audio data (e.g. VOIP, voicemail)

Video

Video data

//

### Cryptographic Capabilities

A Mesh Service can perform cryptographic operations on a private key according to access criteria specified by the user. This capability is used to support use of threshold cryptography to mitigate compromise of a particular device or individual. The splitting of a cryptographic key into two or more parts allows the use of that key to be split into two or more roles.

Note that this approach limits rather than eliminates trust in the service. As with services presenting themselves as 'zero trust', a Mesh service becomes a trusted service after a sufficient number of breaches in other parts of the system have occurred. And the user trusts the service to provide availability of the service.

A Mesh Service MAY also offer to perform private key operations for other purposes. An embargo agent might offer to decrypt data under a private key but only after a specified date and time. An expiry agent might offer to decrypt data but only before a specified date and time. Such services MAY be reserved to the customers of a specified service or provided to the general public. Users of such services MAY combine key services provided by multiple service providers using threshold techniques to achieve separation of roles.

Three service cryptographic operations are currently specified:

Threshold Key Share

A private key share *s*, held by the service is split into key shares *x*, *y* such that *a* = *x* + *y*. One key share is encrypted under a decryption key held by the service. The other is encrypted under a public key specified by the party making the request.

Key Agreement

A private key share s, held by the service is used to calculate the value (*sl* + *c*).*P* where *l*, *c* are integers specified by the requestor and *P* is a point on the curve.

Threshold Signature

A private key share s, held by the service is used to calculate a contribution to a threshold signature scheme.

The implementation of the cryptographic operations described above is described in <norm="draft-hallambaker-threshold"/> and <norm="draft-hallambaker-threshold-sigs"/>.

## Application

The application catalog mmm\_Application contains CatalogEntryApplication entries which describe the use of specific applications under the Mesh Service Account. Multiple application accounts for a single application MAY be connected to a single Mesh Service Account. Each account being specified in a separate entry.

The CatalogEntryApplication entries only contain configuration information for the application as it applies to the account as a whole. If the application requires separate configuration for individual devices, this is specified in the device activation record.

Two applications are currently defined:

Mail

An SMTP email account and associated encryption and signature keys for S/MIME and OpenPGP.

SSH

Secure Shell Client.

Accounts MAY specify multiple instances of each but each application instance is considered as describing a single application account. Thus, if Alice has email accounts alice@example.com and alice@example.net, she will have application entries for each. Accounts connected to Alice's Mesh account may be authorized to use either, both or none of the email accounts.

**Note**: The implementation of these features in the current specification is considered to be a 'proof of concept' rather than a proposed final form. There are many issues that need to be considered when integrating a legacy protocol with extensive deployment into a new platform.

### Mail

Mail configuration profiles are described by one or more CatalogEntryApplicationMail entries, one for each email account connected to the Mesh profile. The corresponding activation records for the connected devices contain information used to provide the device with the necessary decryption information.

Entries specify the email account address(es), the inbound and outbound server configuration and the cryptographic keys to be used for S/MIME and OpenPGP encryption.

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

Note that the inbound and outbound server configuration does not specify the access credentials to be used to access the service. These are specified in the Credential catalog.

Future: The mail application should support automated means of credentialling the public key including obtaining an X.509v3 certificate or uploading the key to a key service.

### SSH

SSH configuration profiles are described by CatalogEntryApplicationSSH entries. The corresponding activation records for the connected devices contain the contributions used to derive the private keys.

A user may have separate SSH configurations for separate purposes within a single Mesh Account. This allows a system administrator servicing multiple clients to maintain separate SSH profiles for each of her customers allowing credentials to be easily (and verifiably) revoked at contract termination.

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

Future: The SSH application is only used to track the SSH client private key which is the same for all of a user's devices. This approach is obviously not ideal from the point of view of cryptographic hygiene: we would much prefer to specify a different client key for every device.

Future: The present specification only manages client keys. In the context of managing IoT devices, the ability to manage service keys is highly desirable.

## Bookmark

The bookmark catalog mmm\_bookmark contains CatalogEntryBookmark entries which describe Web bookmarks and other citations allowing them to be shared between devices connected to the profile.

The fields currently supported by the Bookmarks catalog are currently limited to the fields required for tracking Web bookmarks. Specification of additional fields to track full academic citations is a work in progress.

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

## Contact

The contact catalog mmm\_contact contains CatalogEntryContact entries which describe the person, organization or location described.

The fields of the contact catalog provide a superset of the capabilities of vCard <info="RFC2426"/>.

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

The Contact catalog is typically used by the MeshService as a source of authorization information to perform access control on inbound and outbound message requests. For this reason, Mesh Service SHOULD be granted read access to the contacts catalog by providing a decryption entry for the service.

## Credential

The credential catalog mmm\_credential contains CatalogEntryCredential entries which describe credentials used to access network resources.

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

Only username/password credentials are stored in the credential catalog. If public key credentials are to be used, these SHOULD be managed as an application profile allowing separate credentials to be created for each device.

## Device

The device catalog mmm\_Device contains CatalogEntryDevice entries which describe the devices connected to the account and the permissions assigned to them.

Each device connected to a Mesh Account has an associated CatalogEntryDevice entry that includes the activation and connection records for the account. These records are described in further detail in section ???.

## Network

The network catalog contains CatalogEntryNetwork entries which describe network settings, IPSEC and TLS VPN configurations, etc.

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

## Publication

[Note, this catalog is obsolete, the functions provided by this catalog are being merged with the Access catalog]

The publication catalog mmm\_Publication contains CatalogEntryPublication entries which describe content published through the account.

If the data being published is small, it MAY be specified in the CatalogEntryPublication entry itself as enveloped data. Otherwise a link to the external content is required.

The Publication catalog is currently used to publish two types of data:

Contact

Used in the Static QR Code Contact Exchange interaction.

Profile Device

Used in the Preconfigured Device Connection interaction.

The interactions using this published data are described in <norm="draft-hallambaker-mesh-protocol"/>.

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

## Task

The Task catalog mmm\_Task contains CatalogEntryTask entries which describe tasks assigned to the user including calendar entries and to do lists.

The fields of the task catalog currently reflect those offered by the iCalendar specification <info="RFC5545"/>. Specification of additional fields to allow task triggering on geographic location and/or completion of other tasks is a work in progress.

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

# Spools

Spools are DARE Containers containing an append only list of messages sent or received by an account. Three spools are currently defined:

Inbound

Messages sent to the account. These are encrypted under the account encryption keys of the sender and receiver that were current at the time the message was sent.

Outbound

Messages sent from the account. These are encrypted under the account encryption keys of the sender and receiver that were current at the time the message was sent.

Local

Messages sent from the account for internal use. These are encrypted under the encryption key of the intended recipient alone. This is either the account administration encryption key or a device encryption key.

Every Mesh Message has a unique message identifier. Messages created at the beginning of a new messaging protocol interaction are assigned a random message identifier. Responses to previous messages are assigned message identifiers formed from the message identifier to which they respond by means of a message digest function.

Every Mesh Message stored in a spool is encapsulated in an envelope which bears a unique identifier that is formed by applying a message digest function to the message identifier. Each stored message has an associated state which is initially set to the state Initial and MAY be subsequently altered by one or more MessageComplete messages subsequently appended to the spool. The allowable message states depending upon the spool in question.

## Outbound

The outbound spool stores messages that are to be or have been sent and MessageComplete messages reporting changes to the status of the messages stored on the spool.

Messages posted to the outbound spool have the state Initial, Sent, Received or Refused:

Initial

The initial state of a message posted to the spool.

Sent

The Mesh Service of the sender has delivered the message to the Mesh Service of the recipient which accepted it.

Received

The Mesh Service of the sender has delivered the message to the Mesh Service of the recipient and the recipient has acknowledged receipt.

Refused

The Mesh Service of the sender has delivered the message to the Mesh Service of the recipient which refused to accept it.

MessageComplete messages are only valid when posted to the spool by the service.

## Inbound

The inbound spool stores messages that have been received by the Mesh service servicing the account and MessageComplete messages reporting changes to the status of the messages stored on the spool.

Messages posted to the outbound spool have the state Initial, Read:

Initial

The initial state of a message posted to the spool.

Read

The message has been read.

A message previously marked as read MAY be returned to the unread state by marking it as being in the Initial state.

## Local

The local spool stores messages that are used for administrative functions. In normal circumstances, only administrator devices and the Mesh Service require access to the local spool.

The local spool is used to store MessagePin messages used to notify administration devices that a PIN code has been registered for some purpose and RespondConnection messages used to inform a device of the result of a connection request.

The local spool is used in a device connection operation to provide a device with the activation and connection records required to access the service as an authorized client. Servicing these requests requires that the service be able to access messages stored in the spool by envelope id.

Messages posted to the outbound spool have the states Initial, Closed:

Initial

The initial state of a message posted to the spool.

Closed

The action associated with the message has been completed.

Future: Redefining the role of the Local spool would allow the Claim/PollClaim operations used in device connection to be eliminated and greater consistency achieved between the device connection interactions.

# Cryptographic Operations

The Mesh makes use of various cryptographic operations including threshold operations. For convenience, these are gathered here and specified as functions that are referenced by other parts of the specification.

## Key Derivation from Seed

Mesh Keys that derived from a seed value use the mechanism described in <norm="draft-hallambaker-mesh-udf"/>. Use of the keyname parameter allows multiple keys for different uses to be derived from a single key. Thus escrow of a single seed value permits recovery of all the private keys associated with the profile.

The keyname parameter is a string formed by concatenating identifiers specifying the key type, the actor that will use the key and the key operation:

## Message Envelope and Response Identifiers.

Every Mesh message has a unique Message Identifier MessageId. The MakeID() function is used to calculate the value of Envelope Identifier and Response identifier from the message identifier as follows:

<include="..\Examples\SchemaCode2.md">

Where the values of content are given as follows:

<include="..\Generated\MeshConstantsIdentifierDerrivation.md">

For example:

<include="..\Examples\SchemaMessageIds.md">

## Proof of Knowledge of PIN

Mesh Message classes that are subclasses of MessagePinValidated MAY be authenticated by means of a PIN. Currently two such messages are defined: MessageContact used in contact exchange and RequestConnection message used in device connection.

The PIN codes used to authenticate MessagePinValidated messages are UDF Authenticator strings. The type code of the identifier specifies the algorithm to be used to authenticate the PIN code and the Binary Data Sequence value specifies the key.

The inputs to the PIN proof of knowledge functions are:

PIN: string

A UDF Authenticator. The type code of the identifier specifies the algorithm to be used to authenticate the PIN code and the Binary Data Sequence value specifies the key.

Action: string

A code determining the specific action that the PIN code MAY be used to authenticate. By convention this is the name of the Mesh message type used to perform the action.

Account: string

The account for which the PIN code is issued.

ClientNonce: binary

Nonce value generated by the client using the PIN code to authenticate its message.

PayloadDigest: binary

The PayloadDigest of a DARE Envelope that contains the message to be authenticated. Note that if the envelope is encrypted, this value is calculated over the ciphertext and does not provide proof of knowledge of the plaintext.

The following values of Action are currently defined:

<include="..\Generated\MeshConstantsPinActionCodes.md">

These inputs are used to derive values as follows:

<include="..\Examples\SchemaCode3.md">

<include="..\Examples\SchemaPINFunction.md">

Where MAC(data, key) is the message authentication code algorithm specified by the value of alg.

When an administrative device issues a PIN code, a Message PIN is appended to the local spool. This has the MessageId PinId and specifies the value saltedPIN in the field of that name.

When PIN code authentication is used, a message of type MessagePinValidated specifies the values ClientNonce, PinWitness and PinId in the fields of those names. These values are used to authenticate the inner message data specified by the AuthenticatedData field.

## EARL

The UDF Encrypted Authenticated Resource Locator mechanism is used to publish data and provide means of authentication and access through a static identifier such as a QR code.

This mechanism is used to allow contact exchange by means of a QR code printed on a business card and to connect a device to an account using a static identifier printed on the device in the form of a QR code.

In both cases, the information is passed using the EARL format described in <norm="draft-hallambaker-mesh-udf"/>.

# Mesh Assertions

Mesh Assertions are signed DARE Envelopes that contain one of more claims. Mesh Assertions provide the basis for trust in the Mathematical Mesh.

Mesh Assertions are divided into two classes. Mesh Profiles are self-signed assertions. Assertions that are not self-signed are called declarations. The only type of declaration currently defined is a Connection Declaration describing the connection of a device to an account.

<figuresvg="../Images/SchemaProfilesConnections.svg">Profiles And Connections

## Encoding

The payload of a Mesh Assertion is a JSON encoded object that is a subclass of the Assertion class which defines the following fields:

Identifier

An identifier for the assertion.

Updated

The date and time at which the assertion was issued or last updated

NotaryToken

An assertion may optionally contain one or more notary tokens issued by a Mesh Notary service. These establish a proof that the assertion was signed after the date the notary token was created.

Conditions

A list of conditions that MAY be used to verify the status of the assertion if the relying party requires.

The implementation of the NotaryToken and Conditions mechanisms is to be specified in <norm="draft-hallambaker-mesh-notary"/> at a future date.

Note that the implementation of Conditions differs significantly from that of SAML. Relying parties are required to process condition clauses in a SAML assertion to determine validity. Mesh Relying parties MAY verify the conditions clauses or rely on the trustworthiness of the provider.

The reason for weakening the processing of conditions clauses in the Mesh is that it is only ever possible to validate a conditions clause of any type relative to a ground truth. In SAML applications, the relying party almost invariably has access to an independent source of ground truth. A Mesh device connected to a Mesh Service does not. Thus the types of verification that can be achieved in practice are limited to verifying the consistency of current and previous statements from the Mesh Service.

## Mesh Profiles

Mesh Profiles perform a similar role to X.509v3 certificates but with important differences:

* Profiles describe credentials, they do not make identity statements
* Profiles do not expire, there is therefore no need to support renewal processing.
* Profiles may be modified over time, the current and past status of a profile being recorded in an append only log.

Profiles provide the axioms of trust for the Mesh PKI. Unlike in the PKIX model in which all trust flows from axioms of trust held by a small number of Certificate Authorities, every part in the Mesh contributes their own axiom of trust.

It should be noted however that the role of Certificate Authorities is redefined rather than eliminated. Rather than making assertions whose subject is represented by identities which are inherently mutable and subjective, Certificate Authorities can now make assertions about immutable cryptographic keys.

Every Profile MUST contain a SignatureKey field and MUST be signed by the key specified in that field.

A Profile is valid if and only if:

* There is a SignatureKey field.
* The profile is signed under the key specified in the SignatureKey field.

A profile has the status current if and only if:

* The Profile is valid
* Every Conditions clause in the profile is understood by the relying party and evaluates to true.

## Mesh Connections

A Mesh connection is an assertion describing the connection of a device or a member to an account.

Mesh connections provide similar functionality to 'end-entity' certificates in PKIX but with the important proviso that they are only used to provide trust between a device connected to an account and the service to which that account is bound and between the devices connected to an account.

A connection is valid with respect to an account with profile *P* if and only if:

* The profile *P* is valid
* The AuthorityUdf field of the connection is consistent with the UDF of *P*
* The profile is signed under the key specified in the AdministrationKey field of *P*.
* Any conditions specified in the profile are met

A connection has the status current with respect to an account with profile if and only if:

* The connection is valid with respect to the account with profile *P*.
* The profile P is current.

A device is authenticated with respect to an account with profile P if and only if:

* The connection is valid with respect to the account with profile *P*.
* The device has presented an appropriate proof of knowledge of the DeviceAuthentication key specified in the connection.

## Device Preconfiguration

The DevicePreconfiguration record provides a means of bundling all the information used to preconfigure a device for use in the Mesh. This comprises:

* The Enveloped ProfileDevice.
* A ConnectionDevice assertion credentialing the device to the configuration provider Mesh Service.
* A ConnectionService assertion credentialing the device to the configuration provider Mesh Service.
* The secret seed used to create the ProfileDevice data.

The DevicePreconfiguration record MAY be used as the means of preconfiguring devices to allow connection to a user's account profile using the Preconfigured/Static QR Code device connection interaction.

For example, Alice's coffee pot was preconfigured for connection to a Mesh account at the factory and the following DevicePreconfiguration record created:

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

The use of the publication mechanism in device connection is discussed further in <norm="draft-hallambaker-mesh-protocol"/>.

# Architecture

The Mesh architecture has four principal components:

Mesh Account

A collection of information (contacts, calendar entries, inbound and outbound messages, etc.) belonging to a user who uses the Mesh to management.

Mesh Device Management

The various functions that manage binding of devices to a Mesh to grant access to information and services bound to that account.

Mesh Service

Provides network services through which devices and other Mesh users may interact with a Mesh Account.

Mesh Messaging

An end to end secure messaging service that allows short messages (less than 32KB) to be exchanged between Mesh Accounts and between the Mesh devices connected to a particular account.

The separation of accounts and services as separate components is a key distinction between the Mesh and earlier Internet applications. A Mesh account belongs to the owner of the Mesh and not the Mesh Service Provider which the user may change at any time of their choosing.

A Mesh Account May be active or inactive. By definition, an active Mesh account is serviced by exactly one Mesh Service, an inactive Mesh account is not serviced by a Mesh Service. A Mesh Service Provider MAY offer a backup service for accounts hosted by other providers. In this case the backup provider is connected to the account as a Mesh device, thus allowing the backup provider to maintain a copy of the stores contained in the account and facilitating a rapid transfer of responsibility for servicing the account should that be desired. The use of backup providers is described further in <norm="draft-hallambaker-mesh-discovery"/>.

## Mesh Account

Mesh Accounts contains all the stateful information (contacts, calendar entries, inbound and outbound messages, etc.) related to a particular persona used by the owner.

By definition a Mesh Account is active if it is serviced by a Mesh Service and inactive otherwise. A Mesh user MAY change their service provider at any time. An active Mesh Account is serviced by exactly one Mesh Service at once but a user MAY register a 'backup' service provider to their account in the same manner as adding an advice. This ensures that the backup service is pre-populated with all the information required to allow the user to switch to the new provider without interruption of service.

Each Mesh account is described by an Account Profile. Currently separate profile Account Profile are defined for user accounts and group accounts. It is not clear if this distinction is a useful one.

### Account Profile

A Mesh account profile provides the axiom of trust for a mesh user. It contains a Master Signature Key and one or more Administration Signature Keys. The unique identifier of the master profile is the UDF of the Master Signature Key.

An Account Profile MUST specify an EscrowEncryption key. This key MAY be used to escrow private keys used for encryption of stored data. They SHOULD NOT be used to escrow authentication keys and MUST NOT be used to escrow signature keys.

A user should not need to replace their account profile unless they intend to establish a separate identity. To minimize the risk of disclosure, the Profile Signature Key is only ever used to sign updates to the account profile itself. This allows the user to secure their Profile Signature Key by either keeping it on hardware token or device dedicated to that purpose or by using the escrow mechanism and paper recovery keys as described in this document.

#### Creating a ProfileMaster

Creating a ProfileMaster comprises the steps of:

1. Creating a Master Signature key.
2. Creating an Online Signing Key
3. Signing the ProfileMaster using the Master Signature Key
4. Persisting the ProfileMaster on the administration device to the CatalogHost.
5. (Optional) Connecting at least one Administration Device and granting it the ActivationAdministration activation.

#### Updating a ProfileMaster

Updating a ProfileMaster comprises the steps of:

1. Making the necessary changes.
2. Signing the ProfileMaster using the Master Signature Key
3. Persisting the ProfileMaster on the administration device to the CatalogHost.

## Device Management

Device management allows a collection of devices belonging to a user to function as a single personal Mesh.

The device management functions are principally concerned with the catalog containing the entries describing the connected devices.

### The Device Catalog

Each Mesh Account has a Device Catalog CatalogDevice associated with it. The Device Catalog is used to manage the connection of devices to the Personal Mesh and has a CatalogEntryDevice for each device currently connected to the catalog.

Each Administration Device MUST have access to an up-to-date copy of the Device Catalog in order to manage the devices connected to the Mesh. The Mesh Service protocol MAY be used to synchronize the Device Catalog between administration devices in the case that there is more than one administration device.

The CatalogEntryDevice contains fields for the device profile, device private and device connection.

### Mesh Devices

The principle of radical distrust requires us to consider the possibility that a device might be compromised during manufacture. Once consequence of this possibility is that when an administration device connects a new device to a user's personal Mesh, we cannot put our full trust in either the device being connected or the administration device connecting it.

This concern is resolved by (at minimum) combining keying material generated from both sources to create the keys to be used in the context of the user's personal Mesh with the process being fully verified by both parties.

Additional keying material sources could be added if protection against the possibility of compromise at both devices was required but this is not supported by the current specifications.

A device profile provides the axiom of trust and the key contributions of the device. When bound to an account, the base keys specified in the Device Profile are combined with the key data provided in the Activation device to construct the keys the device will use in the context of the account.

<figuresvg="../Images/SchemaProfileDeviceKeys.svg">Mapping of Device Profile and Device Private to Device Connection Keys.

Unless exceptional circumstances require, a device should not require more than one Device profile even if the device supports use by multiple users under different accounts. But a device MAY have multiple profiles if this approach is more convenient for implementation.

#### Creating a ProfileDevice

Creating a ProfileDevice comprises the steps of:

1. Creating the necessary key
2. Signing the ProfileDevice using the Master Signature Key

Once created, a ProfileDevice is never changed. In the unlikely event that any modification is required, a completely new ProfileDevice MUST be created.

#### Connection to a Personal Mesh

Devices are only connected to a personal Mesh by an administration device. This comprises the steps of:

1. Generating the PrivateDevice keys.
2. Creating the ConnectionDevice data from the public components of the ProfileDevice and PrivateDevice keys and signing it using the administration key.
3. Creating the Activations for the device and signing them using the administration key.
4. Creating the CatalogEntryDevice for the device and adding it to the CatalogDevice of the Personal Mesh.
5. If the Personal Mesh has accounts that are connected to a Mesh Service, synchronizing the CatalogEntryDevice to those services.

These steps are usually performed through use of the Mesh Protocol Connection mechanism. However, Mesh clients MAY support additional mechanisms as circumstances require provided that the appropriate authentication and private key protection controls are provided.

## Mesh Services

A Mesh Service provides one or more Mesh Hosts that support Mesh Accounts through the Mesh Web Service Protocol.

Mesh Services and Hosts are described by Service Profiles and Host Profiles. The means by which services manage the hosts through which they provide service is outside the scope of this document.

As with a Device connected to a Mesh Account, a the binding of a Host to the service it supports is described by a connection record:

<figuresvg="../Images/SchemaProfileService.svg">Service Profile and Delegated Host Assertion.

The credentials provided by the ProfileService and ProfileHost are distinct from those provided by the WebPKI that typically services TLS requests. WebPKI credentials provide service introduction and authentication while a Mesh ProfileHost only provides authentication.

Unless exceptional circumstances require, a service should not need to revise its Service Profile unless it is intended to change its identity. Service Profiles MAY be countersigned by Trusted Third Parties to establish accountability.

## Mesh Messaging

Mesh Messaging is an end-to-end secure messaging system used to exchange short (<32KB) messages between Mesh devices and services. In cases where exchange of longer messages is required, Mesh Messaging MAY be used to provide a control plane to advise the intended message recipient(s) of the type of data being offered and the means of retrieval (e.g an EARL).

All communications between Mesh accounts takes the form of a Mesh Message carried in a Dare Envelope. Mesh Messages are stored in two spools associated with the account, the SpoolOutbound and the SpoolInbound containing the messages sent and received respectively.

This document only describes the representation of the messages within the message spool. The Mesh Service protocol by which the messages are exchanged between devices and services and between services is described in <norm="draft-hallambaker-mesh-protocol"/>.

### Message Status

As previously described in section ###, every message stored in a spool has a specified state. The range of allowable states is defined by the message type. New message states MAY be defined for new message types as they are defined.

By default, messages are appended to a spool in the Initial state, but a spool entry MAY specify any state that is valid for that message type.

The state of a message is changed by appending a completion message to the spool as described in <norm="draft-hallambaker-mesh-protocol"/>.

Services MAY erase or redact messages in accordance with local site policy. Since messages are not removed from the spool on being marked deleted, they may be undeleted by marking them as read or unread. Marking a message deleted MAY make it more likely that the message will be removed if the sequence is subsequently purged.

### Four Corner Model

A four-corner messaging model is enforced. Mesh Services only accept outbound messages from devices connected to accounts that it services. Inbound messages are only accepted from other Mesh Services. This model enables access control at both the outbound and inbound services

<figuresvg="../Images/ArchFourCorner.svg">Four Corner Messaging Model

The outbound Mesh Service checks to see that the request to send a message does not violate its acceptable use policy. Accounts that make a large number of message requests that result in complaints SHOULD be subject to consequences ranging from restriction of the number and type of messages sent to suspending or terminating messaging privileges. Services that fail to implement appropriate controls are likely to be subject to sanctions from either their users or from other services.

<figuresvg="../Images/ArchOutboundAccessControl.svg">Performing Access Control on Outbound Messages

The inbound Mesh Service also checks to see that messages received are consistent with the service Acceptable Use Policy and the user's personal access control settings.

Mesh Services that fail to police abuse by their account holders SHOULD be subject to consequences in the same fashion as account holders.

<figuresvg="../Images/ArchInboundAccessControl.svg">Performing Access Control on Inbound Messages

### Traffic Analysis

The Mesh Messaging protocol as currently specified provides only limited protection against traffic analysis attacks. The use of TLS to encrypt communication between Mesh Services limits the effectiveness of naïve traffic analysis mechanisms but does not prevent timing attacks unless dummy traffic is introduced to obfuscate traffic flows.

The limitation of the message size is in part intended to facilitate use of mechanisms capable of providing high levels of traffic analysis such as mixmaster and onion routing but the current Mesh Service Protocol does not provide support for such approaches and there are no immediate plans to do so.

# Publications

Static QR codes MAY be used to allow contact exchange or device connection. In either case, the QR code contains an EARL providing the means of locating, decrypting and authenticating the published data.

The use of EARLs as a means of publishing encrypted data and the use of EARLs for location, decryption and authentication is discussed in <norm="draft-hallambaker-mesh-dare"/> .

## Profile Device

## Contact Exchange

When used for contact exchange, the envelope payload is a CatalogedContact record.

Besides allowing for exchange of contact information on a business card, a user might have their contact information printed on personal property to facilitate return of lost property.

# Schema

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

# Security Considerations

The security considerations for use and implementation of Mesh services and applications are described in the Mesh Security Considerations guide <norm="draft-hallambaker-mesh-security"/>.

# IANA Considerations

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

# Acknowledgements

A list of people who have contributed to the design of the Mesh is presented in <norm="draft-hallambaker-mesh-architecture"/>.

# Appendix A: Example Container Organization (not normative)

The means by which profiles are stored on devices is outside the scope of the specification. Only catalogs that are required to be shared between machines by means of accounts need to be standardized.

## Device

Host Catalog: Host.dare

Catalog of all the Mesh Profiles that the user has registered with the device and the latest version of the device profile for this device.

MeshCatalog: [UDF-Mesh].dcat

Catalog containing the Account Entries for the Mesh [UDF-Mesh].

Account Catalogs: [UDF-Account]/mmm\_Device.dcat

The device catalog associated with the specified account

Account Catalogs: [UDF-Account]/[Catalog name].dcat

The set of account catalogs that are shared verbatim between the devices connected to the account.

### Creating a new Mesh

* Create new Mesh Profile, Device Profile, Add to Host Catalog
* Create MeshCatalog

### Adding an Account

* Create new Account Profile, Add to MeshCatalog
* Create new Account Device Catalog
* For each device to be added to the account: Create Account Connection Assertion, add to Account Device Catalog.

### Adding a Device

* Create a Device Connection Assertion.
* For each account the device is to be added to: Create Account Connection Assertion, add to Account Device Catalog.

## Service

Master Catalog

Catalog of all services on machine

Service Catalog

Catalog of accounts in the service.

### Creating a Service

* Create a Service Description, add to Master Catalog

### Adding an Account

* Create the account entry, add to Service Catalog
* Create the Account Directory

# Appendix: Privilege Minification

Multiple admin device model

Transition to a new service.

As is obvious to anyone of ordinary skill in the art of practicing threshold cryptography, threshold techniques MAY be employed to further minimize the privileges granted to individual devices.

* Divide administration operations between the device and the service
* Divide administration operations between administration devices

# Appendix Adding a device

(This needs to be moved into the architecture section and replace stale description.)

To add a device to the system we need to create the cataloged device

ActivationDevice provisions the keys to be used to bind the device to the account. These are keys that are only used by the device within the account context. Note however that since the AD record is encrypted to the device profile, the manufacturer could decrypt it. Thus we do not want to put any sensitive data into AD

ActivationAccount provisions the account keys and rights to the device

ApplicationEntries has a list of Application activations for the specific device. Each activation has a public and a private part. This allows provisioning of device specific key pairs and present the public part in the unencrypted part. The encrypted part is encrypted under the device account key.

# Appendix B: Standard Device Configurations

## Recovery Device

## Administration Device

## Web Device

## Messaging Device