Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 17, 2016

P. Hallam-Baker
Comodo Group Inc.
January 14, 2016

Mathematical Mesh: Client-Service Profiles
draft-hallambaker-mesh-reference-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.

Status of This Memo

This Internet-Draft will expire on July 17, 2016.

Copyright Notice

1. Introduction

NB: The reference material in this document is generated from the schema used to derive the source code. The tool used to create this material has not been optimized to produce output for the IETF documentation format at this time. Consequently the formatting is currently sub-optimal.

2. Definitions

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 RFC 2119 [RFC2119].

3. Use Scenarios

3.1. Create Profile

3.2. Connect Device

3.3. Add Application

3.4. Update Application

3.5. Delete Device

3.6. Key Recovery

4. Architecture

4.1. Data Model

4.1.1. First Class Object

4.1.2. 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.

4.1.3. Record

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

4.1.4. 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.

4.2. Profile Types

Master Profile

Personal Profile

Application Profile

Device Profile

4.3. 03627755Figure SEQ Figure * ARABIC 1: Relationship of Profile TypesFigure SEQ Figure * ARABIC 1: Relationship of Profile TypesMaster 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

4.4. 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

4.5. 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

4.6. Application Profile

Identifier: Randomly chosen

Property: Encrypted Data

5. MeshItem

5.1. MeshItem Transactions

5.2. MeshItem Messages

5.3. MeshItem Structures

5.3.1. Structure: Entry

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

5.3.2. Structure: SignedProfile

Contains a signed profile entry

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

SignedData : JoseWebSignature [0..1]

The signed profile

5.3.3. Structure: SignedDeviceProfile

Contains a signed device profile

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

SignedData : JoseWebSignature [0..1]

The signed profile

5.3.4. Structure: SignedMasterProfile

Contains a signed Personal master profile

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

SignedData : JoseWebSignature [0..1]

The signed profile

5.3.5. Structure: SignedPersonalProfile

Contains a signed Personal current profile

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

SignedData : JoseWebSignature [0..1]

The signed profile

5.3.6. Structure: SignedApplicationProfile

Contains a signed device profile

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

SignedData : JoseWebSignature [0..1]

The signed profile

5.3.7. Structure: EncryptedProfile

Contains an encrypted profile entry

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

EncryptedData :   JoseWebEncryption [0..1]

The signed and encrypted profile

5.3.8. Structure: Profile

Parent class from which all profile types are derrived

Identifier :   String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

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 [0..1]

The time instant the profile was last modified.

NotaryToken :   String [0..1]

A Uniform Notary Token providing evidence that a signature was performed after the notary token was created.

5.3.9. Structure: MasterProfile

Describes the long term parameters associated with a personal profile.

Identifier :   String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

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 [0..1]

The time instant the profile was last modified.

NotaryToken : String [0..1]

A Uniform Notary Token providing evidence that a signature was performed after the notary token was created.

MasterSignatureKey : PublicKey [0..1]

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 POSK which is used to sign device administration application profiles.

5.3.10. Structure: PersonalProfile

Describes the current applications and devices connected to a personal master profile.

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

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 [0..1]

The time instant the profile was last modified.

NotaryToken : String [0..1]

A Uniform Notary Token providing evidence that a signature was performed after the notary token was created.

SignedMasterProfile : SignedMasterProfile [0..1]

The corresponding master profile. The profile MUST be signed by the PMSK.

Devices : SignedDeviceProfile [0..Many]

The set of device profiles connected to the profile. The profile MUST be signed by the DSK in the profile.

Applications : ApplicationProfileEntry [0..Many]

Application profiles connected to this profile.

5.3.11. Structure: ApplicationProfileEntry

Identifier : String [0..1]

The unique identifier of the application

Type : String [0..1]

The application type

Friendly : String [0..1]

Optional friendly name identifying the application.

SignID : String [0..Many]

List of devices authorized to sign application profiles

DecryptID : String [0..Many]

List of devices authorized to read private parts of application profiles

5.3.12. Structure: DeviceProfile

Describes a mesh device.

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

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 [0..1]

The time instant the profile was last modified.

NotaryToken : String [0..1]

A Uniform Notary Token providing evidence that a signature was performed after the notary token was created.

Description : String [0..1]

Description of the device

DeviceSignatureKey : PublicKey [0..1]

Key used to sign certificates for the DAK and DEK. The fingerprint of the DSK is the UniqueID of the Device Profile

DeviceAuthenticationKey : PublicKey [0..1]

Key used to authenticate requests made by the device.

DeviceEncryptiontionKey : PublicKey [0..1]

Key used to pass encrypted data to the device such as a DeviceUseEntry

5.3.13. Structure: DevicePrivateProfile

Private portion of device encryption profile.

DeviceSignatureKey : Key [0..1]

Private portion of the DeviceSignatureKey

DeviceAuthenticationKey : Key [0..1]

Private portion of the DeviceAuthenticationKey

DeviceEncryptiontionKey : Key [0..1]

Private portion of the DeviceEncryptiontionKey

5.3.14. Structure: ApplicationProfile

Parent class from which all application profiles inherit.

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

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 [0..1]

The time instant the profile was last modified.

NotaryToken : String [0..1]

A Uniform Notary Token providing evidence that a signature was performed after the notary token was created.

EncryptedData : JoseWebEncryption [0..1]

Encrypted application data

5.3.15. Structure: PasswordProfile

Stores usernames and passwords

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

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 [0..1]

The time instant the profile was last modified.

NotaryToken : String [0..1]

A Uniform Notary Token providing evidence that a signature was performed after the notary token was created.

EncryptedData : JoseWebEncryption [0..1]

Encrypted application data

5.3.16. Structure: PasswordProfilePrivate

Entries : PasswordEntry [0..Many]

[TBS]

5.3.17. Structure: PasswordEntry

Username password entry for a single site

Sites : String [0..Many]

DNS name of site *.example.com matches www.example.com etc.

Username : String [0..1]

Case sensitive username

Password : String [0..1]

Case sensitive password.

5.3.18. Structure: MailProfile

Public profile describes mail receipt policy. Private describes Sending policy

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

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 [0..1]

The time instant the profile was last modified.

NotaryToken :   String [0..1]

A Uniform Notary Token providing evidence that a signature was performed after the notary token was created.

EncryptedData :   JoseWebEncryption [0..1]

Encrypted application data

EncryptionPGP :   PublicKey [0..1]

The current OpenPGP encryption key

EncryptionSMIME :   PublicKey [0..1]

The current S/MIME encryption key

5.3.19. Structure: MailProfilePrivate

Describes a mail account configuration

Private profile contains connection settings for the inbound and outbound mail server(s) and cryptographic private keys. Public profile may contain security policy information for the sender.

EmailAddress :   String [0..1]

The RFC822 Email address. [e.g. "alice@example.com"]

ReplyToAddress :   String [0..1]

The RFC822 Reply toEmail address. [e.g. "alice@example.com"]

When set, allows a sender to tell the receiver that replies to this account should be directed to this address.

DisplayName : String [0..1]

The Display Name. [e.g. "Alice Example"]

AccountName : String [0..1]

The Account Name for display to the app user [e.g. "Work Account"]

Inbound : Connection [0..Many]

The Inbound Mail Connection(s). This is typically IMAP4 or POP3

If multiple connections are specified, the order in the sequence indicates the preference order.

Outbound : Connection [0..Many]

The Outbound Mail Connection(s). This is typically SMTP/SUBMIT

If multiple connections are specified, the order in the sequence indicates the preference order.

Sign : PublicKey [0..Many]

The public keypair(s) for signing and decrypting email.

If multiple public keys are specified, the order indicates preference.

Encrypt : PublicKey [0..Many]

The public keypairs for encrypting and decrypting email.

If multiple public keys are specified, the order indicates preference.

5.3.20. Structure: NetworkProfile

Describes the network profile to follow

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

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 [0..1]

The time instant the profile was last modified.

NotaryToken : String [0..1]

A Uniform Notary Token providing evidence that a signature was performed after the notary token was created.

EncryptedData : JoseWebEncryption [0..1]

Encrypted application data

5.3.21. Structure: NetworkProfilePrivate

Describes the network profile to follow

Sites : String [0..Many]

DNS name of sites to which profile applies *.example.com matches www.example.com etc.

DNS :   Connection [0..Many]

DNS Resolution Services

Prefix :   String [0..Many]

DNS prefixes to search

CTL :   Binary [0..1]

Certificate Trust List giving WebPKI roots to trust

WebPKI :   String [0..Many]

List of UDF fingerprints of keys making up the trust roots to be accepted for Web PKI purposes.

5.3.22. Structure: EscrowEntry

Contains escrowed data

Identifier :   String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

EncryptedData :   JoseWebEncryption [0..1]

[TBS]

5.3.23. Structure: OfflineEscrowEntry

Contains data escrowed using the offline escrow mechanism.

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

EncryptedData : JoseWebEncryption [0..1]

[TBS]

5.3.24. Structure: OnlineEscrowEntry

Contains data escrowed using the online escrow mechanism.

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

EncryptedData : JoseWebEncryption [0..1]

[TBS]

5.3.25. Structure: EscrowedKeySet

A set of escrowed keys.

PrivateKeys : Key [0..Many]

The escrowed keys.

5.3.26. Structure: Connection

Describes network connection parameters for an application

ServiceName : String [0..1]

DNS address of the server

Port : Integer [0..1]

TCP/UDP Port number

Prefix : String [0..1]

DNS service prefix as described in [RFC6335]

Security : String [0..Many]

Describes the security mode to use. Valid choices are Direct/Upgrade/None

UserName : String [0..1]

Username to present to the service for authentication

Password : String [0..1]

Password to present to the service for authentication

URI : String [0..1]

Service connection parameters in URI format

Authentication :   String [0..1]

List of the supported/acceptable authentication mechanisms, preferred mechanism first.

TimeOut :   Integer [0..1]

Service timeout in seconds.

Polling :   Boolean [0..1]

If set, the client should poll the specified service intermittently for updates.

5.3.27. Structure: EncryptedData

Container for JOSE encrypted data and related attributes.

Data :   Binary [0..1]

[TBS]

5.3.28. Structure: SignedData

Container for JOSE signed data and related attributes.

Data :   Binary [0..1]

[TBS]

5.3.29. Structure: PublicKey

Container for public key pair data

UDF :   String [0..1]

UDF fingerprint of the key

X509Certificate :   Binary [0..1]

List of X.509 Certificates

X509Chain :   Binary [0..Many]

X.509 Certificate chain.

X509CSR :   Binary [0..1]

X.509 Certificate Signing Request.

5.3.30. Structure: ConnectionRequest

ParentUDF :   String [0..1]

[TBS]

Device :   SignedDeviceProfile [0..1]

[TBS]

BlockToken :   String [0..1]

[TBS]

5.3.31. Structure: ConnectionResult

ParentUDF :   String [0..1]

[TBS]

Device :   SignedDeviceProfile [0..1]

[TBS]

BlockToken : String [0..1]

[TBS]

Result : String [0..1]

[TBS]

5.3.32. Structure: SignedConnectionRequest

Contains a signed connection request

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

SignedData : JoseWebSignature [0..1]

The signed profile

5.3.33. Structure: SignedConnectionResult

Contains a signed connection request

Identifier : String [0..1]

Globally unique identifier that remains constant for the lifetime of the entry.

SignedData : JoseWebSignature [0..1]

The signed profile

6. MeshProtocol

6.1. MeshProtocol Transactions

6.1.1. Transaction: Hello

- o

  * 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.

6.1.2. Transaction: ValidateAccount

- o

  * 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.

6.1.3. Transaction: CreateAccount

- o

  * Request: CreateRequest

  * Response: CreateResponse

Request creation of a new mesh 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.

6.1.4. Transaction: Publish

- o

  * Request: PublishRequest

  * Response: PublishResponse

Publish a profile or key escrow entry to the mesh.

6.1.5. Transaction: Get

- o

  * Request: GetRequest

  * Response: GetResponse

Search for data in the mesh that matches a set of keys.

6.1.6. Transaction: GetRecords

- o

  * Request: GetRequest

  * Response: GetRecordsResponse

6.1.7. Transaction: Transfer

- o

  * Request: TransferRequest

  * Response: TransferResponse

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

[Not currently implemented]

6.1.8. Transaction: Status

- o

  * 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]

6.1.9. Transaction: ConnectStart

- o

  - Request: ConnectStartRequest

  - Response: ConnectStartResponse

Request connection of a new device to a mesh profile

6.1.10. Transaction: ConnectStatus

- o

  - Request: ConnectStatusRequest

  - Response: ConnectStatusResponse

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

6.1.11. Transaction: ConnectPending

- o

  - Request: ConnectPendingRequest

  - Response: ConnectPendingResponse

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

6.1.12. Transaction: ConnectComplete

- o

  - Request: ConnectCompleteRequest

  - Response: ConnectCompleteResponse

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

6.2. MeshProtocol Messages

6.2.1. Message: MeshRequest

[None]

6.2.2. Message: MeshResponse

[None]

6.2.3. Message: HelloRequest

[None]

6.2.4. Message: HelloResponse

Version : Version [0..1]

Enumerates the protocol versions supported

Alternates : Version [0..Many]

Enumerates alternate protocol version(s) supported

6.2.5. Message: ValidateRequest

Account : String [0..1]

Account name requested

Reserve : Boolean [0..1]

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.

6.2.6. Message: ValidateResponse

Valid : Boolean [0..1]

[TBS]

Minimum : Integer [0..1]

[TBS]

InvalidCharacters : String [0..1]

A list of characters from the requested account that the service does not accept in account names.

Reason : String [0..1]

Text explaining the reason an account name was rejected.

6.2.7. Message: CreateRequest

Account : String [0..1]

Account name requested

6.2.8. Message: CreateResponse

[None]

6.2.9. Message: PublishRequest

[None]

6.2.10. Message: PublishResponse

[None]

6.2.11. Message: GetRequest

Identifier : String [0..1]

Lookup by profile ID

Account : String [0..1]

Lookup by Account ID

KeyValues : KeyValue [0..Many]

List of KeyValue pairs specifying the conditions to be met

NotBefore : DateTime [0..1]

[TBS]

NotOnOrAfter : DateTime [0..1]

[TBS]

Multiple : Boolean [0..1]

If true return multiple responses if available

6.2.12. Message: GetResponse

[None]

6.2.13. Message: GetRecordsResponse

DataItems :   DataItem [0..Many]

List of mesh data records matching the request.

6.2.14. Message: TransferRequest

NotBefore :   DateTime [0..1]

Until :   DateTime [0..1]

After :   String [0..1]

MaxEntries :   Integer [0..1]

MaxBytes :   Integer [0..1]

6.2.15. Message: TransferResponse

[None]

6.2.16. Message: StatusRequest

[None]

6.2.17. Message: StatusResponse

LastWriteTime :   DateTime [0..1]

Time that the last write update was made to the Mesh

LastCheckpointTime :   DateTime [0..1]

Time that the last Mesh checkpoint was calculated.

NextCheckpointTime : DateTime [0..1]

Time at which the next Mesh checkpoint should be calculated.

CheckpointValue : String [0..1]

Last checkpoint value.

6.2.18. Message: ConnectStartRequest

SignedRequest : SignedConnectionRequest [0..1]

AccountID : String [0..1]

6.2.19. Message: ConnectStartResponse

SignedConnectionResult : String [0..1]

6.2.20. Message: ConnectStatusRequest

AccountID : String [0..1]

DeviceID : String [0..1]

6.2.21. Message: ConnectStatusResponse

Result : SignedConnectionResult [0..1]

6.2.22. Message: ConnectPendingRequest

AccountID : String [0..1]

6.2.23. Message: ConnectPendingResponse

Pending : SignedConnectionRequest [0..Many]

6.2.24. Message: ConnectCompleteRequest

Result : SignedConnectionResult [0..1]

AccountID : String [0..1]

6.2.25. Message: ConnectCompleteResponse

[None]

6.3. MeshProtocol Structures

6.3.1. Structure: Version

Major : Integer [0..1]

Major version number of the service protocol. A higher

Minor : Integer [0..1]

Minor version number of the service protocol.

Encodings : Encoding [0..Many]

Enumerates alternative encodings (e.g. ASN.1, XML, JSON-B) if supported by the server

URI : String [0..Many]

The preferred URI for this service. This MAY be used to effect a redirect in the case that a service moves.

6.3.2. Structure: Encoding

ID : String [0..Many]

The IANA encoding name

Dictionary : String [0..Many]

For encodings that employ a named dictionary for tag or data compression, the name of the dictionary as defined by that encoding scheme.

6.3.3. Structure: KeyValue

Key : String [0..1]

[TBS]

Value : String [0..1]

[TBS]

7. Portal

7.1. Portal Transactions

7.2. Portal Messages

7.3. Portal Structures

7.3.1. Structure: PortalEntry

Created : DateTime [0..1]

Time the pending item was created.

Modified : DateTime [0..1]

Time the pending item was last modified.

7.3.2. Structure: Account

Entry containing the UniqueID is Account[Name]-[Portal] Indexed by [Name], [UserProfileUDF] [Most recent open]

Created : DateTime [0..1]

Time the pending item was created.

Modified : DateTime [0..1]

Time the pending item was last modified.

AccountID : String [0..1]

Assigned account identifier, e.g. 'alice@example.com'. Account names are not case sensitive.

UserProfileUDF : String [0..1]

Fingerprint of associated user profile

Status : String [0..1]

Status of the account, valid values are 'Open', 'Closed', 'Suspended'

7.3.3. Structure: AccountProfile

Created : DateTime [0..1]

Time the pending item was created.

Modified : DateTime [0..1]

Time the pending item was last modified.

AccountID : String [0..1]

Assigned account identifier, e.g. 'alice@example.com'. Account names are not case sensitive.

UserProfileUDF : String [0..1]

Fingerprint of associated user profile

Status : String [0..1]

Status of the account, valid values are 'Open', 'Closed', 'Suspended'

Profile : SignedPersonalProfile [0..1]

[TBS]

7.3.4. Structure: ConnectionsPending

Object containing the list of currently pending device connection requests for the specified account. Unique-ID is ConnectionsPending-[UserProfileUDF]

Created : DateTime [0..1]

Time the pending item was created.

Modified : DateTime [0..1]

Time the pending item was last modified.

AccountID : String [0..1]

Assigned account identifier, e.g. 'alice@example.com'. Account names are not case sensitive.

UserProfileUDF : String [0..1]

Fingerprint of associated user profile

Status : String [0..1]

Status of the account, valid values are 'Open', 'Closed', 'Suspended'

Requests : SignedConnectionRequest [0..Many]

List of pending requests

8. Security Considerations

TBS

8.1. Confidentiality

8.2. Integrity

8.3. Service

9. IANA Considerations

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

10. Acknowledgements

11. Normative References

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

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, DOI 10.17487/RFC6335, August 2011.

Author's Address

Phillip Hallam-Baker
Comodo Group Inc.

Email: philliph@comodo.com