Mathematical Mesh: Application Profiles

Mesh/SSH

<series>draft-hallambaker-mesh-app

<status>informational

<stream>independent

<ipr>trust200902

<author>Phillip Hallam-Baker

<surname>Hallam-Baker

<initials>P. M.

<firstname>Phillip

<organization>Comodo Group Inc.

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

<also>http://prismproof.org/Documents/draft-hallambaker-mesh-app.html

The use of the Mathematical Mesh to manage cryptographic keys for use with Mail and SSH is described. The format of the application profiles is described with examples.

# Introduction

# Definitions

This section presents the related specifications and standard, the terms that are used as terms of art within the documents and the terms used as requirements language.

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in <norm="RFC2119"/>.

## Related Specifications

The related specifications are described in the Mesh Architecture specification <norm="draft-hallambaker-mesh-architecture"/>

## Defined Terms

No terms of art are defined.

## Implementation Status

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

# Mesh Application Profiles

(Pull piece from Mesh Reference to here)

# Catalog Profiles

Catalog profiles are used to synchronize encrypted data sets across devices. The catalog data model is restricted so as to permit a common set of management tools to be used to access and maintain profiles containing different types of data (bookmarks, credentials, contacts, etc.). Catalogs do not contain per device data. A catalog may not be shared with every device in the user’s profile but all the data in a catalog is available to all the devices with which it is shared.

The management operations supported are:

Synchronization

Permit user to add, delete and update entries from multiple devices with minimal surprise. The mechanism is designed to be reasonably robust if network connectivity is lost during an attempted update.

Labelling

Allow entries to be grouped into hierarchical categories defined by the user. An entry may be added to more than one category at once.

Each catalog entry SHOULD contain exactly one timestamp field of time Added, Updated or Deleted. If present, the timestamp entries and the entry identifiers are used to merge catalog profiles that have been updated separately leading to an inconsistent state.

Applications SHOULD specify a timestamp field on every entry unless it is known that update inconsistency cannot occur. For example, when initially populating a catalog.

<include=..\Examples\examples\_catalog.md>

## Credentials

A credentials catalog contains access credentials, typically usernames and passwords, for a set of network resources such as Web sites that do not support the use of Mesh device profile data for authentication.

Mesh/Credential enabled applications SHOULD offer to generate strong passwords for the user if the AutoGenerate field is set to true in the credential profile. Since the use of automatically generated passwords is likely to be inconvenient for users unless all the applications on all the devices they might use support Mesh/Credential profiles, applications MUST NOT automatically generate passwords unless the user has affirmatively indicated that they want to use them.

**Further Work:** Credential entries MAY specify that the credential is restricted to use with certain protocols (Web browsing, SFTP, etc.) and/or certain authentication mechanisms but the precise means of identifying both is not currently defined.

<include=..\Examples\examples\_credentials.md>

## Bookmarks

A bookmarks catalog contains a collection of bookmarks that have been saved for later use. While the ability share bookmarks between groups of users has obvious advantages, at present, the implementation and specification are only written with the use of a single user have been considered.

A bookmark entry contains the URI of the target and a title. If the book mark entry is a HTML resource, the title is taken from the &<title> element in the document header. If network and storage resources permit, catalog entries MAY include a favicon value for easy identification.

**Further Work:** Bookmark entries MAY contain details describing the security properties of the connection to protect against downgrade attack. For example, information from HTTP strict security <norm="RFC6797"/> and key pinning headers <norm="RFC7460"/>.

<include=..\Examples\examples\_bookmarks.md>

## Contacts

A contacts catalog contains a collection of contacts. The ContactEntry object contains the usual fields for describing the person or organization the entry refers to, and means of contact (Internet, Postal).

One significant deviation from existing formats is that the fact that people change names (e.g. marriage) is captured and that means of contact MAY be scoped to a particular organization.

<include=..\Examples\examples\_contacts.md>

## Calendar

It is generally acknowledged that representation of calendar information is a ‘difficult’ problem. Since it is the author’s experience that such problems almost invariably arise from an attempt to make use of an inadequate data model, the format for exchange of calendar information is currently undefined.

**Further Work**: Two major causes of difficulty are the use of local time zones and daylight savings, the definition of which are capricious at best. When a recurring meeting is specified it is vital that the time zone in which the meeting is to recur is specified explicitly. Attempts to normalize meetings to a single time zone will inevitably fail when the definition of time changes between the time the meeting is called and the meeting is held.

Another major limitation in existing formats is the lack of understanding that when the user travels, at least some part of their context for scheduling also changes. It should be possible to integrate all parts of the user’s schedule to offer alerts and reminders appropriate to their current location.

# Mail

Mesh Mail profiles serve two distinct purposes:

* To provision a user’s devices with the credentials, network configuration and cryptographic keys necessary to support use of mail and end-to-end mail security enhancements.
* To publish necessary information for use by mail senders.

While the principle focus of Mesh/Mail is to support exchange of mail over SMTP protocol, any infrastructure that provides a mechanism for publishing a recipient’s public keys for use by senders can, at least in principle, also publish information describing the user’s mail capabilities including the ability to support new messaging protocols.

The use of end-to-end secure protocols requires the generation and use of at least one public key pair for signature and encryption. Best current practices require the use of separate keypairs for signature and encryption and if practical separate signature keys for each device.

Since S/MIME and OpenPGP as currently specified do not support the use of Proxy Re-Encryption (recryption) to enable separate the use of separate decryption keys for each device, a single encryption keypair is used. A mail profile must therefore contain an encrypted copy of the corresponding decryption key for each device.

**Further Work:** Support Signal etc. At present the profiles are not differentiated on a per device level. It is likely that it would be useful to specify that certain devices are to carry a complete copy of the user’s mail while others should only carry messages from the last few weeks or months. It is also likely that it would be useful to be able to mark certain selections as being likely to be most useful offline.

<include=..\Examples\examples\_mail.md>

# SSH

The Secure Shell (SSH) transport layer protocol <norm="RFC4253"/> is widely used as a mechanism for securing access to remote hosts. In addition to providing a terminal connection to a remote host, SSH also supports file transfer and remote access (VPN) functionality. It is also used to provide remote procedure call (RPC) capabilities in applications such as Git.

While SSH permits a high level of security to be achieved, achieving a high security configuration requires a considerable degree of attention to detail. Numerous ‘how to’ guides found on the Internet advise the user to engage in many unsafe practices. These include:

* Using a single private key for authentication for every machine to be used as a client.
* Emailing a copy of the authentication key to yourself to transfer it to a new machine. (Alternatively use of insecure FTP, copying the data to /temp, etc.)

Of equal concern was the fact that none of the guides mentioned any form of maintenance activity such as deleting authentication keys for a decommissioned device or performing a rekey operation in the case that a device is compromised.

Configuring SSH securely is a non-trivial task because SSH is the tool through which the administrator will be connecting to secure their system. This is a bootstrap problem: It is easy to solve the problem of SSH configuration once we have SSH configured for use. To enable SSH access to a machine without creating an insecure path first is not a trivial matter.

A Mesh/SSH profile contains three sets of information:

* A set of the user’s public authentication keys. This is used to generate auth\_hosts files and equivalents to enable the user to access machines.
* A set of hosts known to the user. This is encrypted as it shows the machines that the user at least is likely to visit. This is used to generate known\_hosts files and equivalents to enable the user to authenticate hosts.
* A set of device key entries. The entry for each host is encrypted. This is used to create the private key file(s) for the user on each of their devices.

<include=..\Examples\examples\_ssh.md>

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

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

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

# Acknowledgements

Your name could appear here.

# Security Considerations

[This is just a sketch for the present.]

# IANA Considerations

[TBS list out all the code points that require an IANA registration]