Workgroup: Network Working Group
Internet-Draft:
draft-hallambaker-mesh-platform
Published: 27 July 2020
Intended Status: Informational
Expires: 28 January 2021
Authors: P. M. Hallam-Baker

Mathematical Mesh: Platform Configuration

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. This document describes how Mesh profiles are stored for application access on Windows, Linux and OSX platforms.

This document is also available online at http://prismproof.org/Documents/draft-hallambaker-mesh-platform.html.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 28 January 2021.

Table of Contents

1. Introduction

This document describes recommended platform specific configuration for Mathematical Mesh applications. The use of common conventions for storage of profiles and private keys allows mesh enabled applications to interoperate on the same machine.

Protecting private key material from disclosure to other processes presents complex and difficult technical challenges. Ensuring that a key is properly erased from storage before memory is released relies on a complex series of assumptions about memory management at the compiler, operating system and the platform level.

For maximum security, the use of private key storage facilities provided by the platform is preferred.

2. Definitions

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

2.1. Requirements Language

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2.2. Defined Terms

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

2.3. Related Specifications

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

2.4. Implementation Status

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

3. Mesh Content

The catalogs and spools associated with a user's Mesh profiles and accounts are stored in Dare Containers.

This section describes the conventions used to describe

3.1. Directory Layout

host.dare The CatalogHost container with entries for each Mesh

-udf>.dcat` The CatalogDevice container for the Mesh with -udf>

-udf>/ Directory containing catalogs for the account -udf>

-udf>/CatalogApplication.dcat The applications catalog for the account -udf>

-udf>/CatalogContact.dcat The contacts catalog for the account -udf>

3.1.1. CatalogHost

A catalog of DeviceConnection, AdminConnection and PendingConnection entries describing Mesh connections for the device on which the container is hosted.

PendingConnection Describes a pending request to join a Mesh. This entry **SHOULD** be deleted once the request is either completed, refused or has expired.

DeviceConnection Describes a non-administrative connection to a Mesh

AdminConnection Describes a connection with full administration privileges to a Mesh

3.1.2. CatalogDevice

Holds the CatalogEntryDevice entries that describe all the devices connected to the Mesh whose UDF fingerprint matches the filename.

3.1.3. CatalogApplication

Holds application information that is shared across all the administration devices connected to an account.

3.1.4. CatalogContact

Holds the contact information corresponding to the account.

3.1.5. CatalogRecrypt

Holds recryption entries to be provisioned to a recryption service associated with the account. The entries are encrypted under the public encryption key of the service and indexed under the UDF of the corresponding decryption key.

3.2. Container Locking

A combination of file access protections and system locks are used to prevent container data being corrupted through conflicting concurrent access.

*Since Dare Containers are append only, the scope for read/write conflict is limited to actions that cause the end of file marker to change. It is thus only necessary for processes to acquire a lock on the file when:

*Reading the file to update the last position in the file.

*Writing to the file to append an object.

A single system-wide names MUTEX is used.

To write to the container, a process **MUST** acquire the named read MUTEX, performs the write operation and releases it.

A process reading the container **SHOULD NOT** acquire the container MUTEX to determine that the end of file marker is greater than zero or that the end of file marker has moved. A process **MUST** acquire the container MUTEX to update the value of the end of file marker so as to ensure that any pending write operation has completed.

The single lock approach was chosen in preference to more sophisticated approaches involving multiple concurrent read locks because the time to acquire the lock is typically greater than the time required to update the end of file position.

4. Platform Specific Bindings

4.1. Windows

4.2. OSX

4.3. Linux

5. IANA Considerations

None

6. Acknowledgements

TBS

7. 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, <https://www.rfc-editor.org/rfc/rfc2119>.

8. Informative References

[draft-hallambaker-mesh-architecture]
Hallam-Baker, P., "Mathematical Mesh 3.0 Part I: Architecture Guide", Work in Progress, Internet-Draft, draft-hallambaker-mesh-architecture-13, 9 March 2020, <https://tools.ietf.org/html/draft-hallambaker-mesh-architecture-13>.

[draft-hallambaker-mesh-developer]
Hallam-Baker, P., "Mathematical Mesh: Reference Implementation", Work in Progress, Internet-Draft, draft-hallambaker-mesh-developer-09, 23 October 2019, <https://tools.ietf.org/html/draft-hallambaker-mesh-developer-09>.