Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 10 December 2025

N. Elkins
Inside Products, Inc.
M. Ackermann
BCBS Michigan
A. Deshpande
Google
T. Pecorella
University of Florence

8 June 2025

Registration Protocol for Performance and Diagnostic Metrics
draft-elkins-pdmv2-registration-00

Abstract

This document specifies a registration protocol for use with Performance and Diagnostic Metrics version 2 (PDMv2). This registration process enables endpoints to communicate supported policies and capabilities in advance of measurement sessions, simplifying setup and enhancing security. The protocol defines a set of commands, responses, and message formats, and proposes integration with the Diameter Base Protocol (RFC6733) as the transport and authentication mechanism.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://ameyand.github.io/PDMv2/draft-elkins-ippm-encrypted-pdmv2.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-elkins-pdmv2-registration/.

Discussion of this document takes place on the IP Performance Measurement Working Group mailing list (mailto:ippm@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ippm/. Subscribe at https://www.ietf.org/mailman/listinfo/ippm/.

Source for this draft and an issue tracker can be found at https://github.com/ameyand/PDMv2.

Status of This Memo

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

This Internet-Draft will expire on 10 December 2025.

Copyright Notice

Table of Contents

1. Introduction

Performance and Diagnostic Metrics (PDM) defined in [RFC8250] allow for enhanced diagnostics of packet delay and network behavior. PDMv2 builds upon this by requiring prior registration of participating endpoints to negotiate policies, authentication, and encryption modes.

A robust registration mechanism allows Clients, Servers, and Analyzers to declare their role, supported cipher suites, and address ranges. This draft defines such mechanisms.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terminology

* Authentication Server (AS): Manages endpoints (Client, Server, Analyzer). Holds the policies and roles. Assists in creating cryptographic keys.

* Client: An Endpoint Node which initiates a session with a listening port on another Endpoint Node and sends PDMv2 data.

* Server: An Endpoint Node which has a listening port and sends PDMv2 data to another Endpoint Node.

* Analyzer: An Endpoint Node which analyzes PDMv2 metrics.

Note: a Client may act as a Server (have listening ports).

* Public and Private Keys: A pair of keys that is used in asymmetric cryptography. If one is used for encryption, the other is used for decryption. Private Keys are kept hidden by the source of the key pair generator, but Public Key is known to everyone. pkX (Public Key) and skX (Private Key). Where X can be, any client or any server.

* Pre-shared Key (PSK): A symmetric key. Uniformly random bitstring, shared between any Client or any Server or a key shared between an entity that forms client-server relationship. This could happen through an out-of band mechanism: e.g., a physical meeting or use of another protocol.

* Session Key: A temporary key which acts as a symmetric key for the whole session.

4. Use of Diameter

Diameter [RFC6733] defines a framework for AAA services, and is extensible for different applications through extensions. Given the requirements of PDMv2 registration protocol, the use of a standard-based AAA system seems to be logical.

[RFC6733] defines various entities that can be mapped to the PDMv2 entities (client, server, analyzer, Authentication Server). In the Diameter terminology, the Authentication Server could be mapped to a 'Proxy Agent', which can enforce policy rules, e.g., preventing the clients from requesting a connection to a server.

All the other entities can be configured as Diameter 'Peers', with specific application TLVs describing their operations.

Note: The use of Diameter in the PDMv2 context will require the definition of an application specific to PDMv2, specific AVP, and message formats. The decision to use Diameter will also need to be validated through a Proof of Concept.

5. Protocol Flow

The PDMv2 registration protocol will proceed in the following steps.

Step 1: Registration of Organization

Step 2: Optionally, registration of allowed Organization partners

Step 3: Registration of Server, Client, and Analyzer

Step 4: Registration of Session Partners (which Clients are allowed to connect to which Servers)

Step 5: PDMv2 data flow between Client and Server.

Registration SHOULD be done in a session before the data session containing PDMv2. Otherwise, there will be a delay at the start of the session.

After-the-fact (or real-time) data analysis of PDMv2 flow may occur by network diagnosticians or network devices. If analysis is to be done in real-time, that is while the session is still active, only the Client or Server may have an Analyzer role.

5.1. Architecture and Participants

Registration involves the following entities:

* Client

*Server

* Analyzer

* Authentication Server (AS)

The AS authenticates and registers nodes. Registration occurs over TLS-secured Diameter communication channels.

5.2. Registration Commands

The following are needed for PDMv2 registration. An equivalent needs to be found in Diameter. If one is not found, then enhancements to Diameter will be suggested.

* RegisterOrganization

* RegisterClient

* RegisterServer

* RegisterConnection

* RegisterAnalyzer

* CreateMasterSecret

Each command includes supported policies and cipher suites. The Authentication Server responds with corresponding Reply messages or Error codes.

5.2.1. RegisterClient Command

Fields:

RecordType: "RegisterClient"

OrganizationalEntity: Organization or Individual

PoliciesSupported: Encrypted, Unencrypted, SignOnly

CipherSuitesSupported: List of cipher suite identifiers

AddressRange: /64, /128, or other

RegisterAllMyAddresses: Yes/No

The client software may detect its active interfaces and addresses (e.g., using ipconfig/ifconfig) to populate this information.

5.2.2. RegisterOrganization Command

Fields:

RecordType: "RegisterOrganization"

PoliciesSupported: Encrypted, Unencrypted, SignOnly

CipherSuitesSupported: List

Organizations declare policies and optionally allow group registrations under their prefix.

5.3. Security Considerations

PDMv2 registration should be encrypted via TLS. Authentication Server certificates must be validated. Authentication tokens and cipher suite preferences must be verified to avoid spoofing or downgrade attacks.

5.4. Privacy Considerations

Exposure of IPv6 address ranges and policy information poses a privacy risk. Clients should restrict registration to trusted Authentication Server and avoid over-broad address registration.

5.5. IANA Considerations

This draft requests allocation of a new Diameter application ID for "PDMv2 Registration."

6. 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>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <https://www.rfc-editor.org/rfc/rfc6733>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8250] Elkins, N., Hamilton, R., and M. Ackermann, "IPv6 Performance and Diagnostic Metrics (PDM) Destination Option", RFC 8250, DOI 10.17487/RFC8250, September 2017, <https://www.rfc-editor.org/rfc/rfc8250>.

Authors' Addresses

Nalini Elkins
Inside Products, Inc.
United States
Email: nalini.elkins@insidethestack.com

Michael Ackermann
BCBS Michigan
United States
Email: mackermann@bcbsm.com

Ameya Deshpande
Google
India
Email: ameyanrd@gmail.com

Tommaso Pecorella
University of Florence
Italy
Email: tommaso.pecorella@unifi.it