Network Time Protocols
Internet-Draft
Intended status: Informational
Expires: 2 September 2026

R. Krishnan
JPMorgan Chase
M. Richardson
Sandelman Software Works Inc
D. Lopez
Telefonica
A. Prasad
Oracle
S. Addepalli
Aryaka
1 March 2026

Hardware-Rooted Attestation for Precision Time Protocol: Scalable Workload Identity and Phased PQC Readiness
draft-ramki-ptp-hardware-rooted-attestation-01

Abstract

This document defines a scalable framework for hardware-rooted cryptographic attestation in the Precision Time Protocol (PTP). Standard PTP security mechanisms rely on symmetric keys, which suffer from identity ambiguity and source non-repudiation failures— vulnerabilities that allow any node possessing the shared secret to impersonate a Grandmaster. To resolve these issues while overcoming the silicon throughput limits of traditional TPMs and the overhead of Post-Quantum Cryptography (PQC), this draft specifies a tiered trust model. A Hardware Root (e.g., TPM) establishes a long-term PQC identity, while a workload identity management plane (e.g., SPIFFE/SPIRE) manages the frequent rotation of short-lived operational keys. These keys perform amortized signing of PTP message batches via Merkle Trees, ensuring wire-speed synchronization and irrefutable provenance for regulated environments.

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 2 September 2026.

Table of Contents

1. Introduction

Precise, auditable time provenance is a cornerstone for regulated environments, including financial services, distributed ledgers, and sovereign AI. However, standard PTP security (IEEE 1588-2019) faces three critical architectural challenges:

1. *The Identity and Non-Repudiation Problem:* Current PTP security relies largely on symmetric keys (HMAC-SHA256). Because the Grandmaster (GM) and all Slaves share the same secret, any compromised node can forge time messages appearing to originate

from the GM. This lack of source non-repudiation makes it impossible to irrefutably audit time provenance or defend against "insider" clock spoofing.

2. *The Throughput Gap:* Hardware Security Modules (TPMs) are "slow-path" silicon, often constrained to tens-to-hundreds of asymmetric operations per second — insufficient for high-performance PTP profiles that may require sustained high-frequency signing.
3. *The PQC Payload Problem:* Post-Quantum Cryptographic (PQC) signatures (e.g., ML-DSA) are significantly larger than standard PTP message MTUs, introducing fragmentation risks and unacceptable processing jitter if applied per-packet.

This draft introduces a *Transitive and Amortized Attestation* model. Amortization, in this context, refers to spreading the cost of a single cryptographic signature across many PTP messages by signing only the root of their Merkle hash tree. By anchoring an automated software control plane in hardware silicon, we resolve the identity ambiguity of symmetric keys while maintaining wire-speed performance.

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.

2. Architecture: The Tiered Trust Model

Trust is distributed across three functional layers to bridge the gap between "Slow-but-Secure" hardware and "Fast-and-Precise" network timing.

2.1. Tier 1: Hardware Root (Immutable Identity)

The Root of Trust (RoT) is a hardware component (e.g., TPM 2.0, HPE iLO 7, or SmartNIC SRoT) containing a non-exportable Identity Key. This key MUST be asymmetric and SHOULD be PQC-compatible (e.g., ML-DSA). This establishes an irrefutable "Silicon Identity" that cannot be cloned, addressing the fundamental weakness of symmetric shared secrets.

2.2. Tier 2: Control Plane (Workload Orchestration)

To manage the lifecycle of cryptographic material without manual intervention, the PTP daemon is treated as a managed workload under workload identity management frameworks such as *SPIFFE/SPIRE*. * *Attestation:* The host identity management plane (e.g., HPE OneView, Keylime verifier/registrar) MUST verify the RoT’s identity and platform state (PCRs) before authorizing key issuance. The interaction between the host identity management plane and the workload identity management plane for attesting the workload identity agent is described in {{GEO-FENCE}}. * *Delegation:* Upon successful attestation, the Workload identity management plane (e.g., SPIFFE/SPIRE) issues short-lived SVIDs and ephemeral *Operational Keys* which use standard non-PQC cryptography. This "Transitive Attestation" binds the high-speed software/NIC key to the immutable hardware identity.

2.3. Tier 3: Data Plane (Amortized Execution)

High-frequency signing is offloaded to the Data Plane using the *Operational Keys* in software or a hardware offload such as SmartNIC. * *Merkle Batching:* PTP messages are hashed into a Merkle Tree. A single signature on the Merkle Root provides cryptographic integrity and non-repudiation proof for the entire batch of PTP events. A batch is flushed and transmitted to the receiver when either the configured batch size N is reached or a maximum latency timer T expires, whichever comes first. This amortization makes large PQC signatures feasible within the PTP ecosystem.

3. Scalable Attestation Mechanism

3.1. Solving Source Non-Repudiation

By utilizing asymmetric operational keys certified by the Hardware Root, a Verifier can irrefutably prove that a batch of PTP messages originated from a specific physical device. In this model, a compromised Slave has no access to the private key required to forge a GM’s signature, fixing the identity ambiguity inherent in current symmetric PTP profiles.

3.2. Amortized PQC Readiness

PQC adoption is phased to ensure that data-plane performance is never compromised: 1. *Identity Layer:* RECOMMENDED to use PQC-capable hardware roots (Identity Key) today to secure the long-term device identity. 2. *Control Layer:* RECOMMENDED to use PQC-signed workload identities (e.g., SPIFFE/SPIRE SVIDs) to protect the distribution and rotation of keys. 3. *Data Layer:* MAY use classical asymmetric

algorithms (e.g., Ed25519) for the Merkle Root today, transitioning to PQC as specialized hardware acceleration becomes pervasive.

4. Signed Token Structure (CBOR)

The amortized token provides the "Batch Proof" for a set of N consecutive sequence IDs between a single sender <-> receiver pair. The token is created by the signing entity (GM or boundary clock) at batch flush time and validated by the receiver. The signature field (key 7) covers the canonical CBOR encoding of fields 1 through 6.

```
; Amortized Signed Token (CBOR map)
{
  1 : uint,         ; version (e.g., 2)
  2 : uint,         ; batch_size (N)
  3 : bstr,         ; Merkle Root Hash
  4 : uint,         ; First SequenceID in batch
  5 : bstr,         ; Operational Key ID / Certificate Thumbprint
  6 : bstr,         ; nonce (verifier-issued)
  7 : bstr          ; signature over fields 1-6 (PQC recommended)
}
```

5. Security Considerations

5.1. Integrity vs. Network Jitter

PQC signatures are computationally heavy. Performing these on every packet would introduce variable jitter into the PTP timing loop. The amortized Merkle approach ensures that the timing-sensitive hardware timestamping remains asynchronous from the heavy cryptographic signing process.

5.2. Symmetric Key Obsolescence

Symmetric-key PTP security is insufficient for regulated time provenance due to the lack of source non-repudiation. This draft provides the blueprint for transitioning to asymmetric hardware-rooted keys as the only viable path to meaningful identity in multi-tenant or untrusted fabrics.

5.3. Network Path Asymmetry

Attestation provides proof of Identity, Integrity, and Residency. It does not protect against physical network delay or path asymmetry. This mechanism MUST be used in conjunction with PTP’s native delay measurement mechanisms.

6. IANA Considerations

This document requests IANA to create a new registry named "PTP Amortized Attestation TLV Types" under an appropriate PTP-related registry group. The registry MUST define the following fields for each entry:

* *TLV Type:* A unique unsigned integer identifier.
* *Name:* A descriptive name (e.g., PTP_AMORTIZED_ATTESTATION_TLV).
* *Reference:* The RFC or specification defining the TLV.

Initial allocations in this registry are defined in this document. Future allocations SHALL follow the Specification Required policy as defined in {{!RFC8126}}.

7. References

7.1. Normative References

[IEEE1588] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE 1588-2019, 2019.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, https://www.rfc-editor.org/info/rfc8949 (https://www.rfc-editor.org/info/rfc8949).

[FIPS204] NIST, "Module-Lattice-Based Digital Signature Standard (ML-DSA)", FIPS 204, 2024.

[SPIFFE] SPIFFE Project, "Secure Production Identity Framework for Everyone (SPIFFE) Specification", https://github.com/spiffe/spiffe (https://github.com/spiffe/spiffe).

[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/info/rfc2119 (https://www.rfc-editor.org/info/rfc2119).

[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/info/rfc8174 (https://www.rfc-editor.org/info/rfc8174).

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, https://www.rfc-editor.org/info/rfc8126 (https://www.rfc-editor.org/info/rfc8126).

7.2. Informative References

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and

W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, https://www.rfc-editor.org/info/rfc9334 (https://www.rfc-editor.org/info/rfc9334).

[GEO-FENCE] Krishnan, R., et al., "Verifiable Geo-Fence for Workload Identity", Work in Progress, Internet-Draft, draft-lkspa-wimse-verifiable-geo-fence, https://github.com/ramkri123/ietf-tpm-geofencing/blob/master/draft-lkspa-wimse-verifiable-geo-fence.md (https://github.com/ramkri123/ietf-tpm-geofencing/blob/master/draft-lkspa-wimse-verifiable-geo-fence.md).

[HPE-ILO7] HPE, "HPE iLO 7 Security Whitepaper", https://www.hpe.com (https://www.hpe.com).

Authors' Addresses

Ramki Krishnan
JPMorgan Chase
Email: ramkri123@gmail.com

Michael Richardson
Sandelman Software Works Inc
Email: mcr+IETF@sandelman.ca

Diego R. Lopez
Telefonica
Email: diego.r.lopez@telefonica.com

A Prasad
Oracle
Email: a.prasad@oracle.com

Srinivasa Addepalli
Aryaka
Email: srinivasa.addepalli@aryaka.com