IETF 106

20 November 2019

Security in the IEEE 1588 Draft Revision

Karen O'Donoghue

odonoghue@isoc.org

Basic Timeline

- 2008: 1588 version 2 published with Annex K
- 2013: PAR for 1588 revision approved
- 2013: Security subcommittee of 1588 started working
  - 2014: Security requirements for time protocols published in the IETF (RFC 7384)
- 2019 (November): Approved for publication by the IEEE Standards Board

IEEE 1588 Security Approach

- IEEE 1588 security includes security mechanisms and guidance that can be used together or individually.
- Individual mechanisms are optional.
- The specific mechanisms chosen will vary by application and environment.
  - Future profile development

IEEE 1588 Security: Multi-pronged Approach

- PTP Integrated Security Mechanisms (Prong A)
- External Transport Security Mechanisms (Prong B)
- Architecture Guidance (Prong C)
- Monitoring and Management Guidance (Prong D)

PTP Integrated Security Mechanism (Prong A)

8499 **16.14 PTP integrated security mechanism (optional)**

8500 **16.14.1 General**

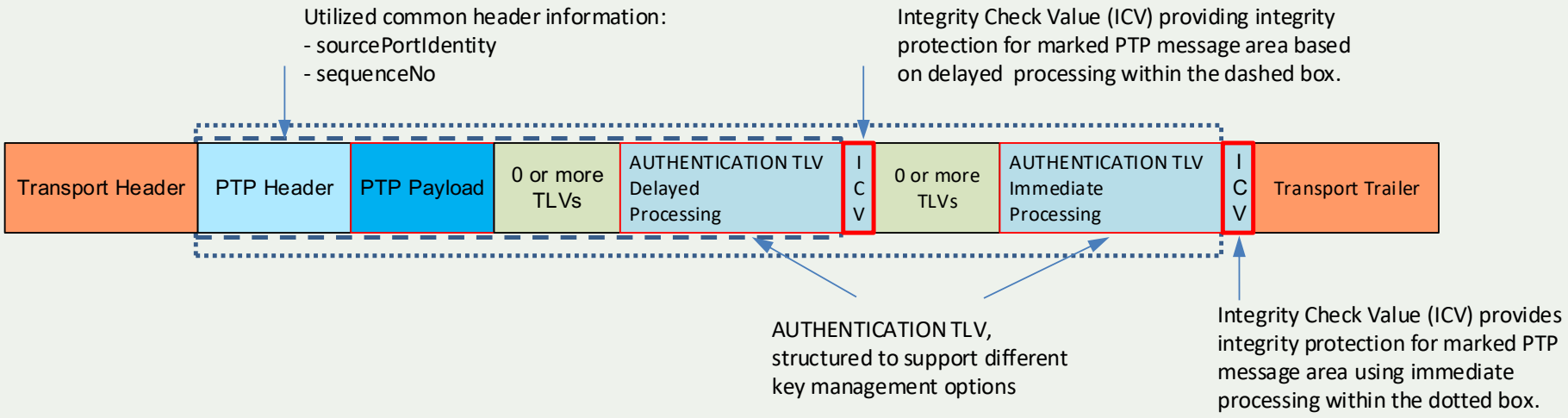
8501 This option specifies a security extension to PTP. The PTP security extension provides source authentication,
8502 message integrity, and replay attack protection for PTP messages within a PTP domain. See Annex S for a more
8503 comprehensive discussion on security. The PTP security extension is realized by two basic mechanisms:

- PTP Security extension provides:
  - source authentication,
  - message integrity, and
  - replay attack protection

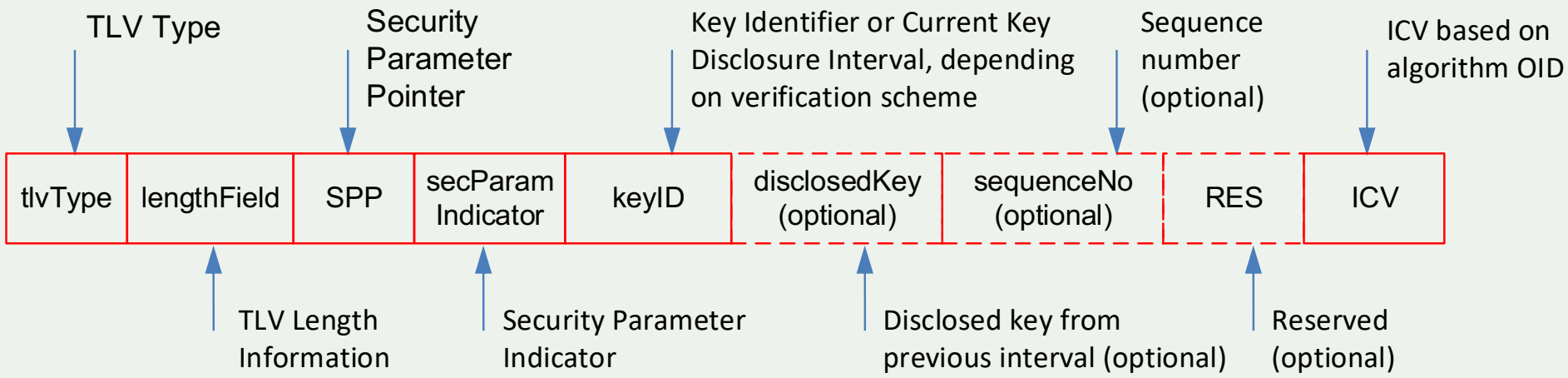
- Definition of an AUTHENTICATION TLV and the associated processing rules

PTP Integrated Security Mechanism (Prong A) -- PTP Packet

- TLV definition and processing rules (normative but optional)
- Information on example key management schemes (informative)
  - Future specification of specific key management schemes in IETF



PTP Integrated Security Mechanism (Prong A) – The AUTHENTICATION TLV



External Transport Security Mechanisms (Prong B)

- MACSec
  - Based on IEEE 802.1AE Media Access Control (MAC) Security
  - Integrity protection between two IEEE 802 ports
  - Key management is manual or based on MACsec Key Agreement (MKA) specified in IEEE 802.1X-2010.

- IPSec
  - Base architecture defined in IETF RFC 4301
  - Node authentication and key exchange defined in RFC 7296
  - Integrity checking and encryption of data defined in RFC 4303

Architecture Guidance (Prong C)

- Redundancy
  - Redundant timing systems
  - Redundant PTP grandmasters
  - Redundant paths

Monitoring and Management Guidance (Prong D)

- Definition of parameters in IEEE 1588 data sets that can be monitored to detect security problems
- A recommendation to not use unsecure management protocols including IEEE 1588 native management

… and Best Practices!