Options for Cryptographic protection of PTP

Doug Arnold

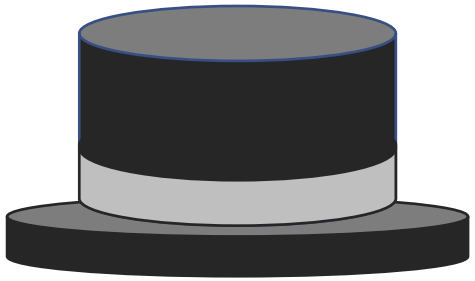
ITSF 2021

Agenda

- Need to secure network time transfer
- PTP security
- Key management options
- Comparison

Timing network vulnerabilities

- Device failures
- GNSS
  - Interference (intentional or not)
  - Spoofing
  - System failure
- Network level interference
  - Propagation delay asymmetry
  - Malicious interference (hacking)



Man in the middle attacks

Compromised switch might go undetected if only timing affected

- Leased line
- Network operators in different department from timing engineers

Healthy switch

Compromised switch

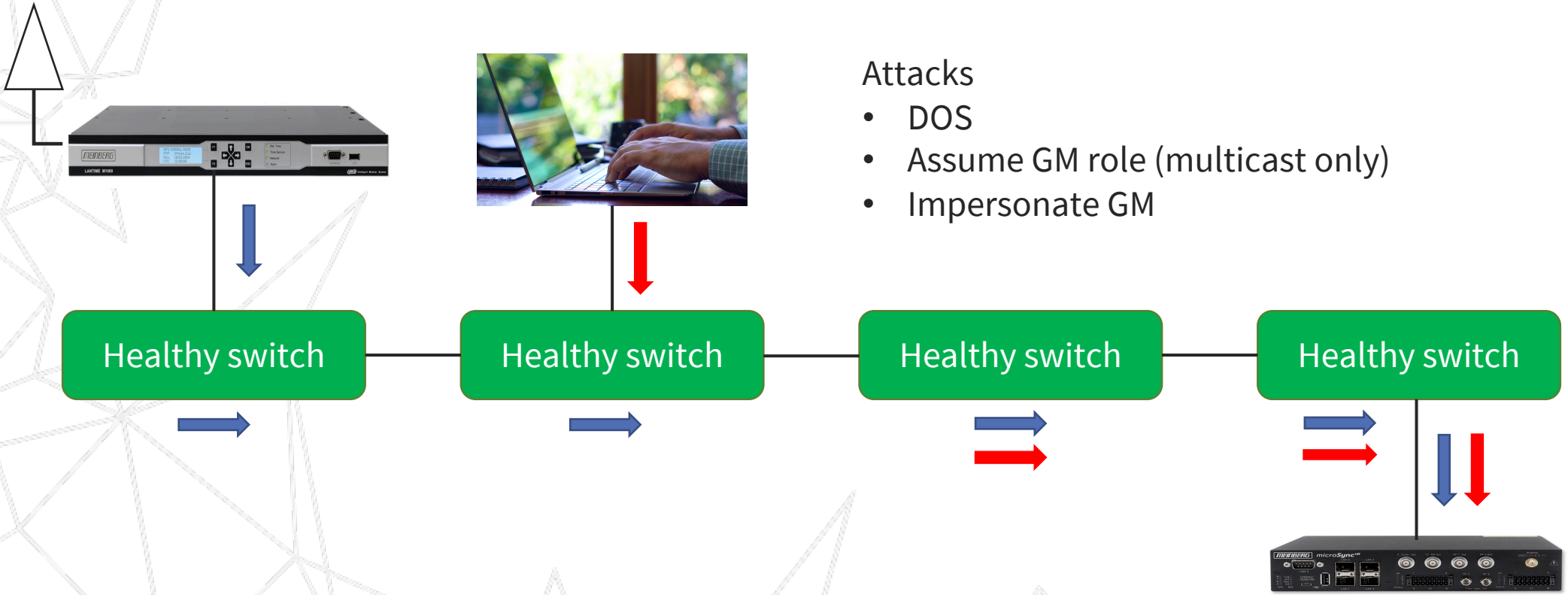
Healthy switch

Healthy switch

Delay attack

Altering message

Rogue node attacks



Attacks
- DOS
- Assume GM role (multicast only)
- Impersonate GM

Attacker does not need to take over a device, just gain access to the network!

Networks attacks and mitigation

Attack type	Mitigation tactics
Delay attack	Redundant GMs on different paths Heuristic rules for delay values
DOS	Identified and blocked by switches
False GM	Cryptography
Impersonate GM	Cryptography
Altered messages	Cryptography

Cryptographic scheme must:

- protect message → PTP AUTHENTICATION TLV
- verify source
- Refresh keys periodically

} Automated key management protocol

AUTHENTICATION TLV

Defined in IEEE 1588-2019 (subclause 16:14)
Can be appended to any PTP message

0x8009	6 + ICV size	0x00 – 0xFF	0x00	ICV
tlvType for AUTHENTICATION TLV	TLV length in octets	Security Parameter Pointer(SPP) points to a specific algorithm, parameters, and key(s)	Security Parameter Indicator: flags indicate presence of optional fields (not included when SPI = 0x00	Integrated Check Value (ICV) : i.e. Hash code

Present in all PTP TLVs

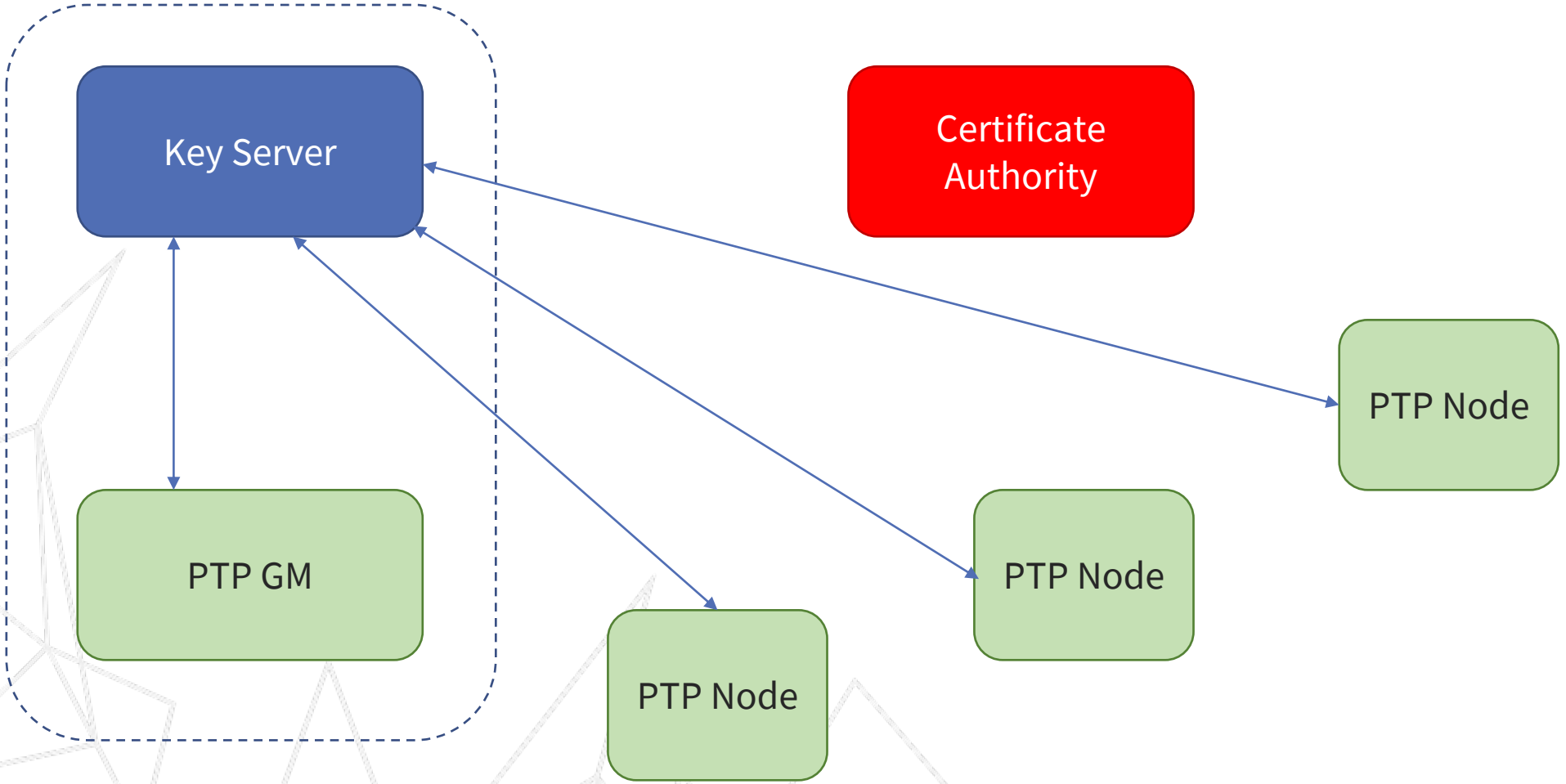
Optional fields:

- Disclosed key
- Sequence number
- Reserved

Principles of automated key management

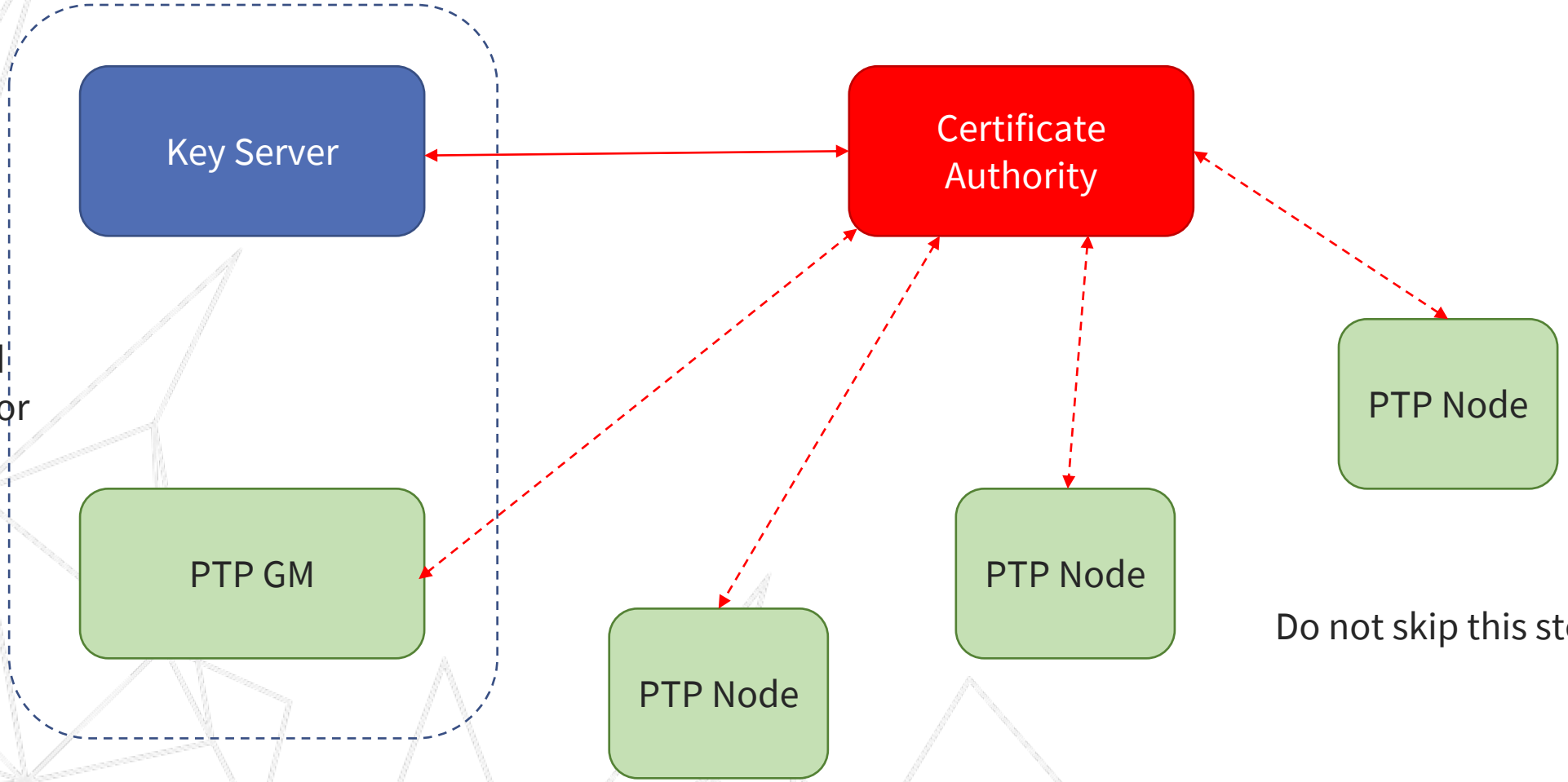
Key server
And GM
Optionally
integrated

PTP devices
obtain keys from
key server
Protected by
standard security
mechanism



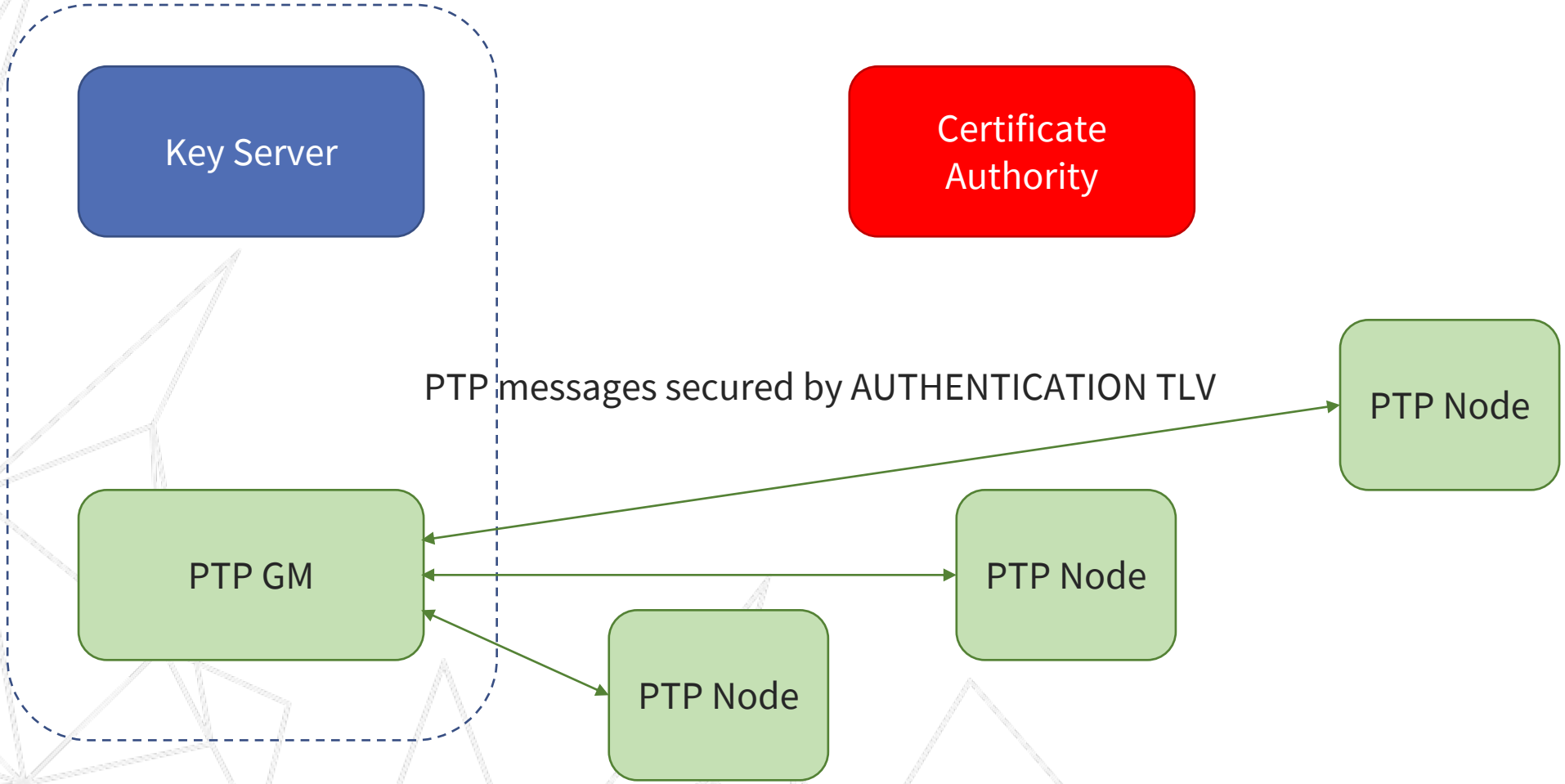
Principles of automated key management

Each key refresh cycle: Either all PTP nodes authenticated by key server or all nodes authenticate each other



Do not skip this step!

Principles of automated key management



GDOI (Group Domain of Interaction)

- All nodes in a group share a group key
  - All nodes periodically check in to key server to obtain group key
  - Key has finite lifetime
  - Shared secret is the biggest weakness
- Uses IPsec sessions secure key exchange
- Good choice for:
  - Multicast PTP
  - PTP networks with on path support
  - Networks already using IPsec
- Standards
  - RFC 6407 (protocol definition)
  - IEC 62351-9 (application to power grid)
  - IEEE P1588d (draft amendment for use with PTP)

NTS for 4 PTP

- Adaption of Network Time Security (NTS) defined for NTP
- Based on research at Ostfalia University of Applied Sciences
  - Langer, M., Heine, K., Sibold, D., and R. Bermbach, "A Network Time Security Based Automatic Key Management for PTPv2.1", 2020 IEEE 45th Conference on Local Computer Networks (LCN), Sydney, Australia, November 2020
- Key exchange protected by Transport Layer Security (TLS)
- Two operation modes:
  - Group key mode for multicast PTP and/or on path support
  - Ticket system for unicast PTP: allows GM to manage multiple PTP slaves with same key (that slaves do not know)
  - GM to key server interface defined allows them to be separate nodes
- Good Choice for:
  - Products that support both unicast and multicast PTP
  - Networks that already include TLS
- Standards
  - IETF: draft-langer-ntp-nts-for-ptp-02

NTS for 4 Unicast PTP

- Adaption of Network Time Security (NTS) defined for NTP
- Key exchange protected by Transport Layer Security (TLS)
- Designed to be as similar to NTS for NTP as possible
  - Covers only unicast PTP
  - Uses cookies transported as a TLV on PTP messages
- Good Choice for:
  - Products that support both NTP and unicast and PTP
  - Networks that contain both NTP and PTP
  - Networks that already include TLS
- Standards
  - draft-gerstung-nts4uptp-03

Comparison

	Base Security Technology	Strengths	Weaknesses
GDOI	IPsec	• Published standards • Used in power industry to secure other protocols • Group key efficient for multicast and on path support	• Inefficient for large number of unicast associations • Shared secret (group key)
NTS4PTP	TLS	• Efficient for both multicast and unicast	• Standardization uncertain* • Shared secret (group key
NTS4UPTP	TLS, NTS	• Easy to integrate with NTS for NTP	• Standardization uncertain* • Unicast only

* One of the NTS4PTP/NTS4UPTP proposals may be abandoned, or proposal may be merged

Thank you for your attention

Doug Arnold

doug.arnold@meinberg-usa.com