Adapting NTS to PTP

Douglas Arnold, Meinberg-USA

Martin Langer, Ostfalia University of Applied Sciences

Rainer Bermbach, Ostfalia University of Applied Sciences

ITSF 2020, November 3-5

Agenda

Ostfalia University of Applied Sciences

MEINBERG The Synchronization Experts.

- Securing PTP
- TLS-based NTS key exchange
- NTS for unicast PTP
- NTS for multicast PTP
- Advantages of NTS for secured PTP
- Next steps
- Summary

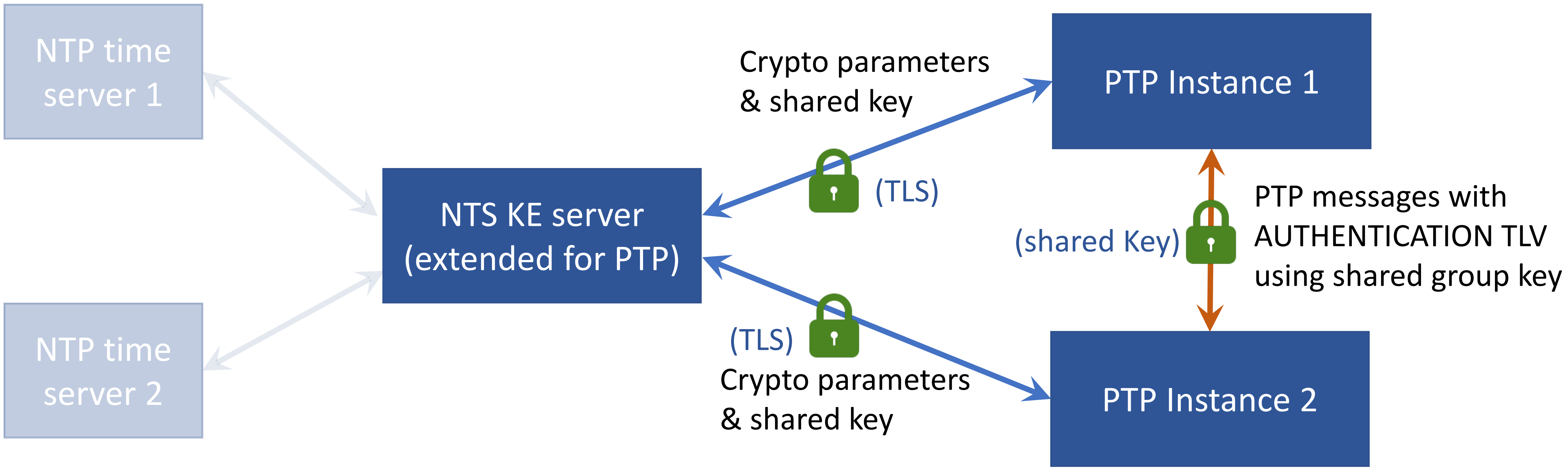
Securing PTP

- IEEE 1588-2019 defines AUTHENTICATION TLV
  - Facilitates message integrity (ICV over whole PTP message)
  - Key management system needed
- NTS (RFC 8915) defines robust cryptographic security for NTP
  - Replaces outdated Autokey mechanism
  - Key Management based on Transport Layer Security (TLS)
- Commercial timeservers support PTP and NTP
  - Using the same key management scheme is efficient for product developers and network operators
  - TLS key management is already part of most networks and network appliances

→ **Why not extend NTS Key Management for PTP?**

TLS-based NTS Key Exchange

- Principle Topology for Multicast and Unicast PTP


NTP time server 1
NTP time server 2
NTS KE server (extended for PTP)
Crypto parameters & shared key
(TLS)
PTP Instance 1
(TLS)
Crypto parameters & shared key
PTP Instance 2
(shared Key)
PTP messages with AUTHENTICATION TLV using shared group key

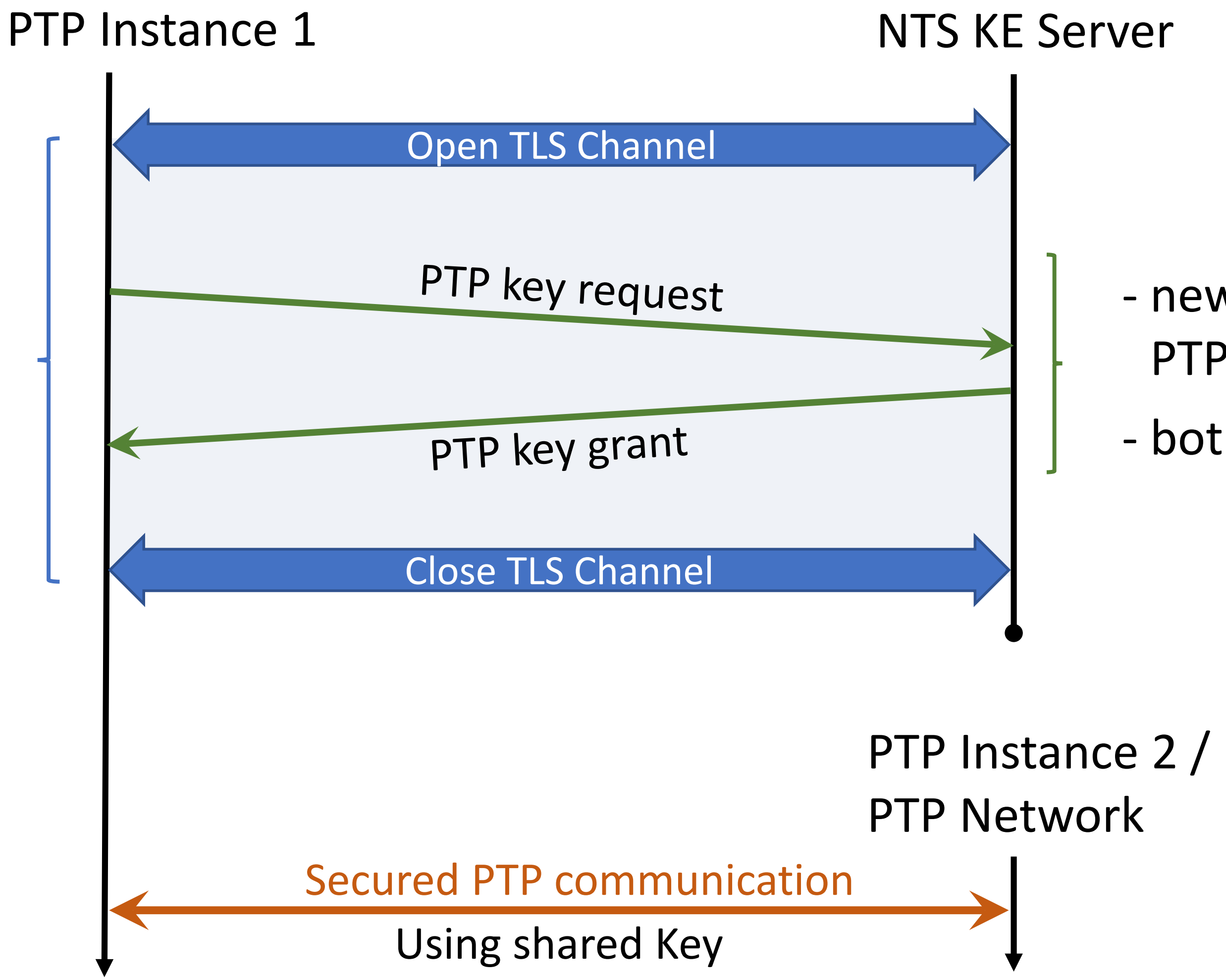
Note: - unlike NTP servers PTP ports are stateful
- so NTS cookies are not needed

Principle Key Distribution Sequence

TLS handshake:

1. Initiated by PTP Instance
2. Establish secure Communication Channel
3. Authenticate KE server and PTP Instance

See RFC 8446 for details



- new NTS messages for PTP key exchange
- both Unicast and Multicast

Principle Key Distribution

Loose time synchronization is necessary in advance

Algorithms and parameters

- Chosen by the KE server (Unicast/Multicast)
- PTP instances must support them or can’t join

Key refresh

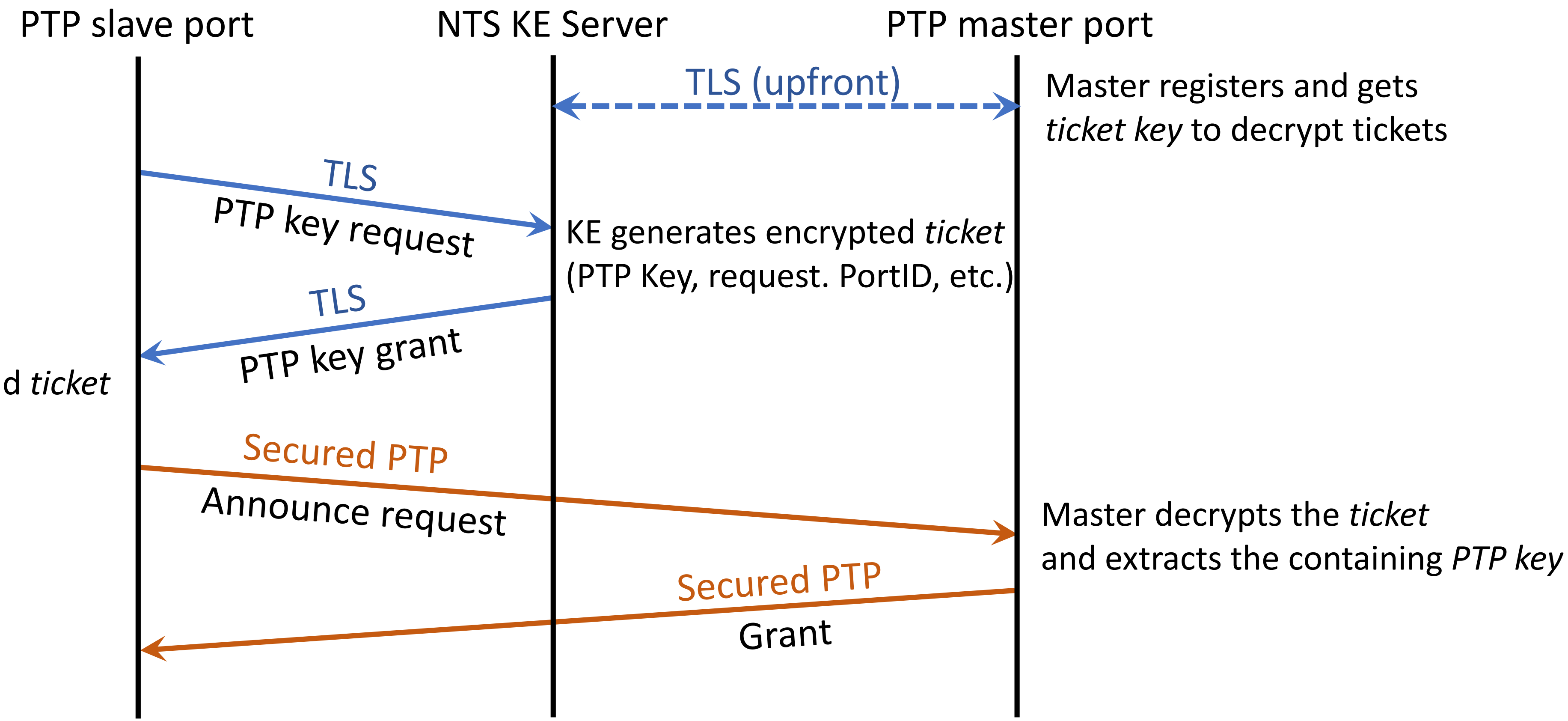
- Key request messages transmitting times randomized to prevent overload at KE server
- PTP instances accept messages with previous key for some time after key change to accommodate network delays

Two new NTS message types

- PTP key request contains e.g. Unicast flag, target PortID/GroupID, algorithms, etc.
- PTP key grant contains e.g. Security Associations, key, validity period, etc.

Start-Up for Unicast PTP

Upfront: - PTP master registers with the NTS KE server
- Master is being authenticated and commits security parameters



PTP slave port

NTS KE Server

PTP master port

TLS (upfront)

Master registers and gets *ticket key* to decrypt tickets

TLS

PTP key request

KE generates encrypted *ticket* (PTP Key, request. PortID, etc.)

TLS

PTP key grant

Secured PTP

Announce request

Master decrypts the *ticket* and extracts the containing *PTP key*

Secured PTP

Grant

PTP key grant:
contains *PTP key* and *ticket*

Announce request:
contains *ticket*

NTS for Unicast PTP

Identification

- PortIDs of master and slave ports identify communication partners
- Note: Many unicast pairs in a PTP network might have the same domain number and SdoId

Ticket system

- Separate symmetric key (ticket key) between master and KE server
- Only KE server and master can encrypt/decrypt this ticket
- Ticket contains: PTP Key, requesting slave (PortID), validity period, etc.
- Slave forwards this ticket to the master via PTP signaling message
- Master decrypts and extracts ticket content

→ Allows the master to verify and generate secured PTP messages

NTS for Multicast PTP

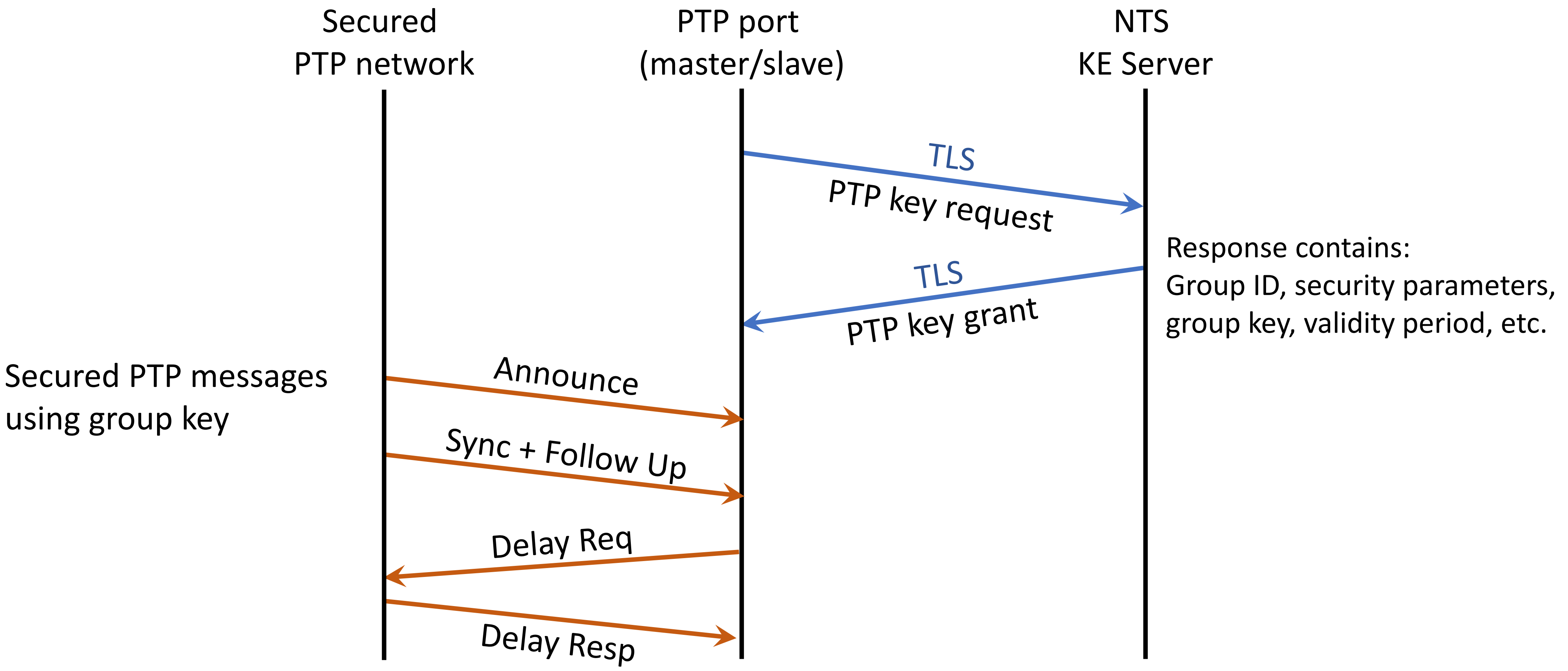
- PTP standard proposes GDOI or TESLA for key exchange
  - GDOI: towards IPsec and rarely available
  - TESLA: complex and can be broken by delay attacks

- NTS Key Exchange: allows easy group-based PTP communication
  - No changes to PTPv2.1 messages necessary
  - Immediate PTP message generation/verification by using group key
  - Also supports Transparent Clocks
  - Security Association for Multicast
    - Algorithms and parameters chosen by KE server
    - Group number identifies the group

GDOI: *Group Domain of Interpretation* protocol
TESLA: *Timed Efficient Stream Loss-tolerant Authentication* protocol

Start-Up for Multicast PTP

- PTP master registers (upfront) with the NTS KE server
- Same procedure for every PTP instance of the group



Response contains:
Group ID, security parameters, group key, validity period, etc.

Secured PTP messages using group key

Advantages of NTS for secured PTP

- Easy to implement
- Secured by standard TLS security procedure
- Cyclic update process
  - Ensures key freshness
  - Without interruption of PTP communication
  - Simple group control

- Symmetric Keys
  - Fast, One Step mode possible

- But…
  - Group key-based approaches generally are vulnerable to compromised PTP nodes

Next Steps

- Address source authentication
- More details on TLS handshake
- More details on key request and grant messages
- Building a Proof-of-Concept-Implementation
- Results from test
- Consideration of the chicken-egg problem (time sync / security)

Summary

- NTS can be adapted for use with PTP
- Simpler than TESLA or GDOI key management schemes
- Key exchange based on commonly deployed TLS standard
- Commercial timeservers support PTP and NTP
  - Using the same key management scheme is efficient for product developers and network operators
  - TLS is already part of most networks and network appliances
- Secure solution for unicast and multicast PTP

Ostfalia
University of
Applied Sciences

MEINBERG
The Synchronization Experts.

Thank you for your attention

For more information contact

Douglas Arnold: doug.arnold@meinberg-usa.com

Martin Langer: mart.langer@ostfalia.de