Ostfalia
University of
Applied Sciences

Extending Network Time Security for PTP

Martin Langer, Ostfalia University of Applied Sciences

Rainer Bermbach, Ostfalia University of Applied Sciences

Douglas Arnold, Meinberg-USA

WSTS 2021, March 30 – April 01

Agenda

- Need for Secure PTP
  - Authentication TLV
  - Key Management Options
- Network Time Security (NTS)
  - NTS for PTP
  - Principle Key Distribution Sequence
  - NTS for Multicast
  - NTS for Unicast
  - Advantages
- Summary

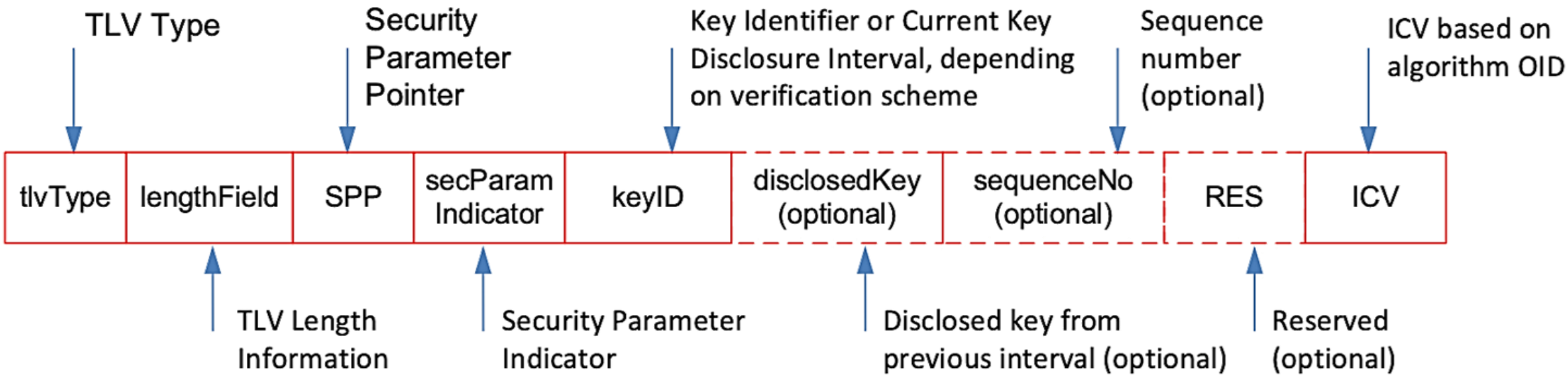
Need for Secure PTP

- Why secure PTP?
  - Many network operators want secure versions of protocols - Even behind a firewall (for example HTTPS instead of HTTP)
  - PTP can traverse leased lines
  - PTP provided as a service in data centers with many organizations present
    - For example, financial exchanges

- Security for different PTP modes
  - Multicast
  - Mixed multicast/unicast (hybrid)
  - Unicast

Authentication TLV

- Defined in IEEE 1588-2019 to enable message authentication
  - However, standard has little information on automated key management



Key Management Options

- Manual key management
- Automatic key management
  - GDOI & TESLA
  - Now NTS

- NTS… supports PTP and NTP
  - Using the same key management scheme is efficient for product developers and network operators

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

Network Time Security (NTS)

- NTS defines robust cryptographic security for NTP
  - RFC 8915 since October 2020
  - Replaces unsecure Autokey mechanism
  - Key Management based on Transport Layer Security (TLSv1.3)

- General NTS features
  - Authentication and message integrity
  - Good scalability and tracking protection
  - Fast cryptography (symmetric keys) and key freshness
  - Minimizes the influence on the synchronization accuracy

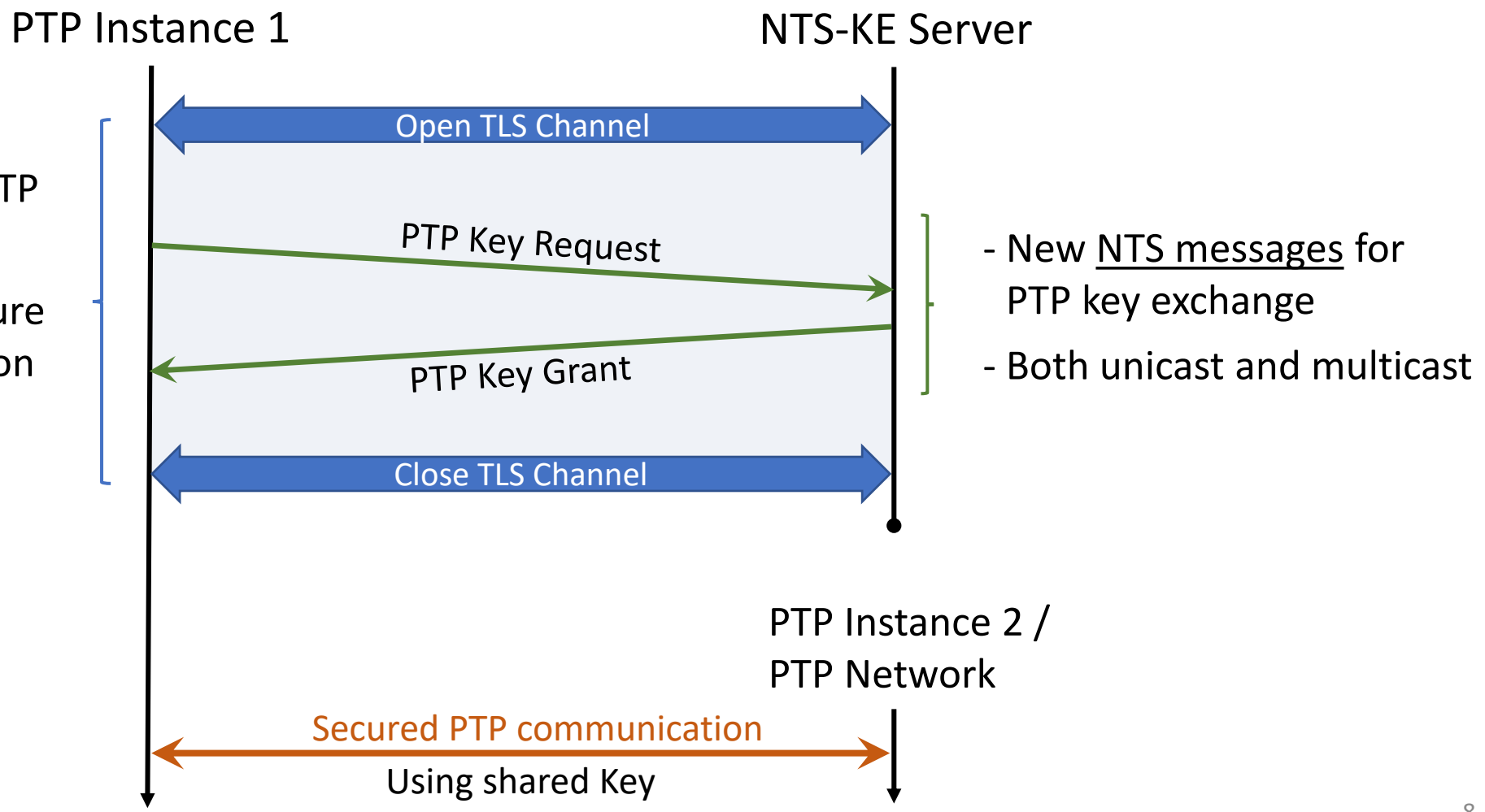
NTP: *Network Time Protocol*

NTS for PTP

- Specification process is ongoing (IEEE 1588 security subcommittee)
- New NTS Messages for PTP
- Provides key freshness and group control

- Secured PTP modes:
  - Multicast / hybrid
    - Definition of security groups
    - Group-of-2 (Go2) unicast (subgroups)
  - Unicast with unicast negotiation

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

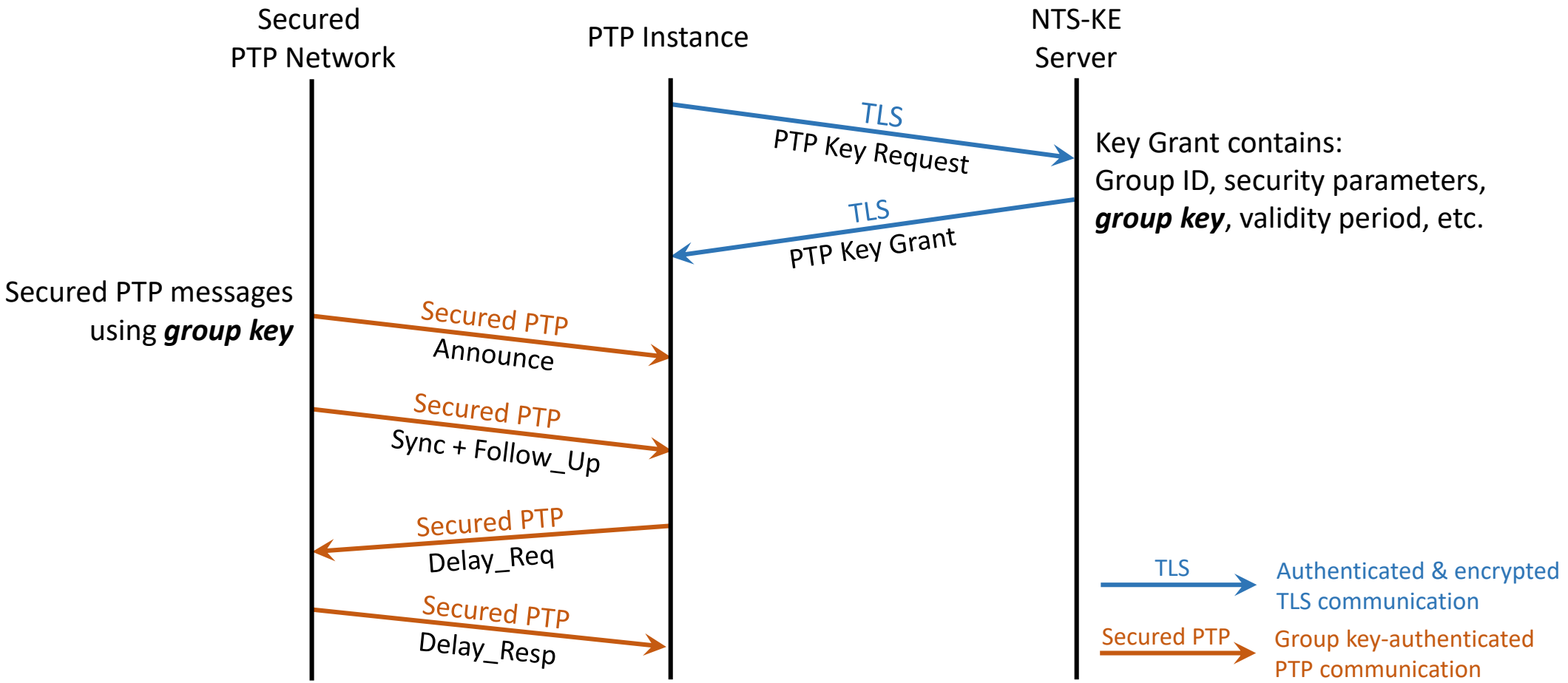
NTS for Multicast & Group-of-2 PTP

- Advantages
  - Easy group-based PTP communication
  - Immediate PTP message generation/verification by using group key
  - Also supports Transparent Clocks
  - No changes to PTPv2.1 messages necessary

- Security Association for Multicast
  - Algorithms and parameters chosen by NTS-KE server
  - Group number (PTP domain & profile) identifies the group
  - PTP network can also be divided in multiple security subgroups (Group-of-2)
    - A Group-of-2 allows multicast as well as unicast connections

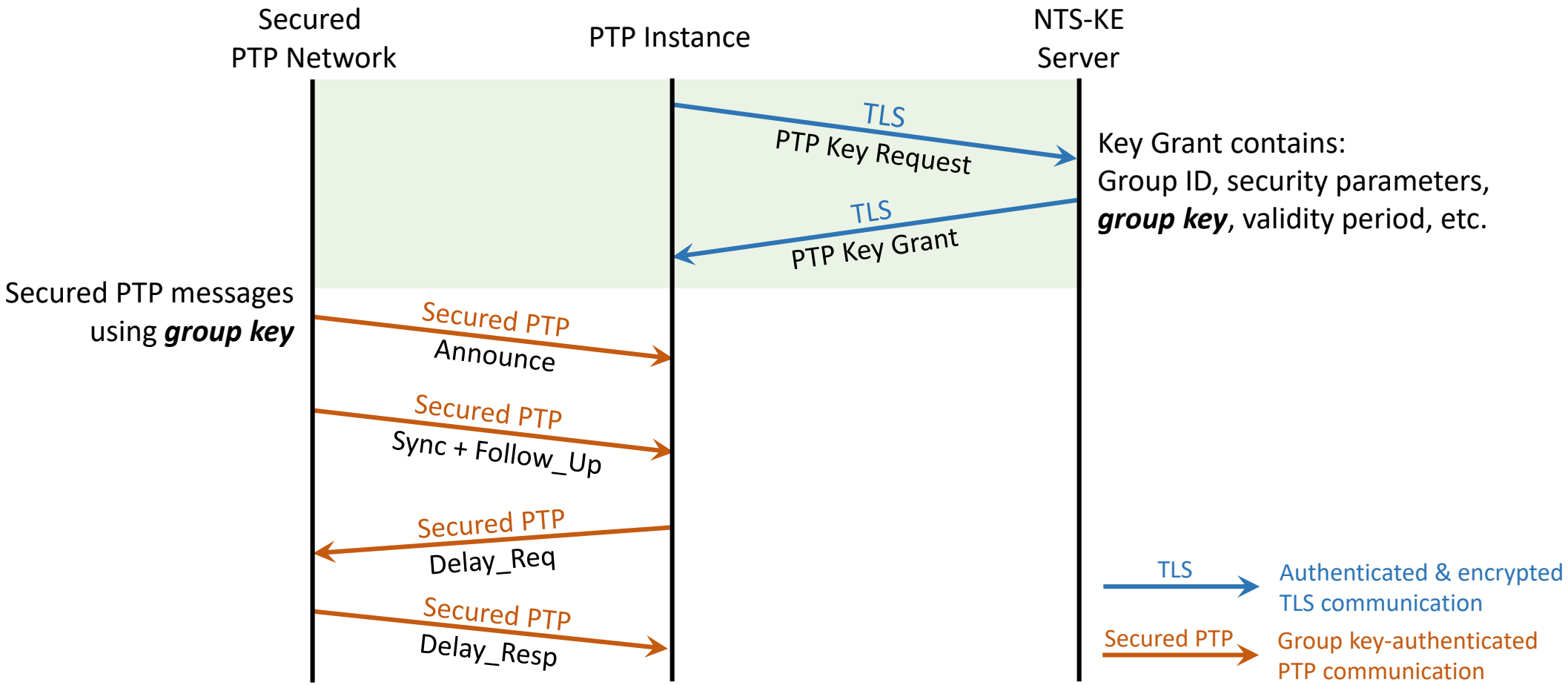
NTS for Multicast & Group-of-2 PTP

- Same procedure for every PTP instance of the group



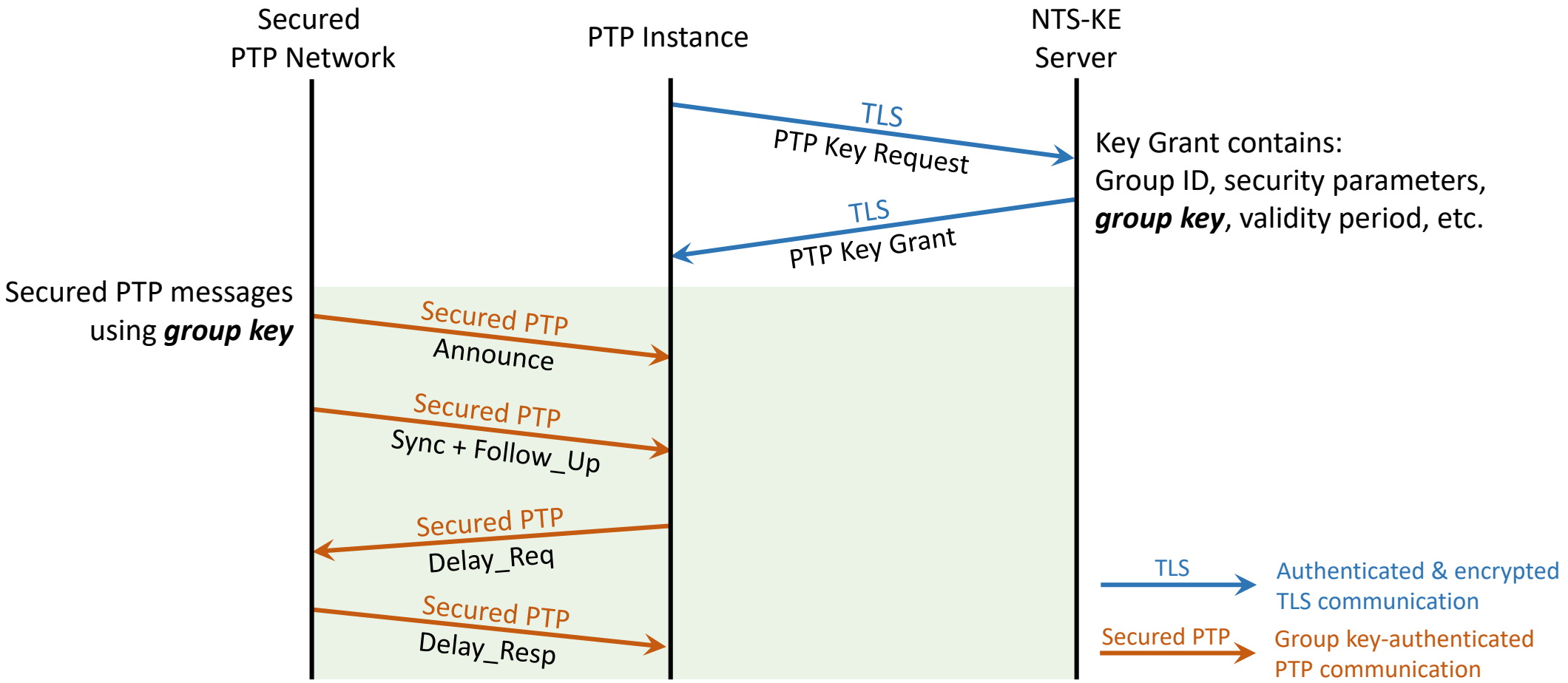
NTS for Multicast & Group-of-2 PTP

- Same procedure for every PTP instance of the group



NTS for Multicast & Group-of-2 PTP

- Same procedure for every PTP instance of the group



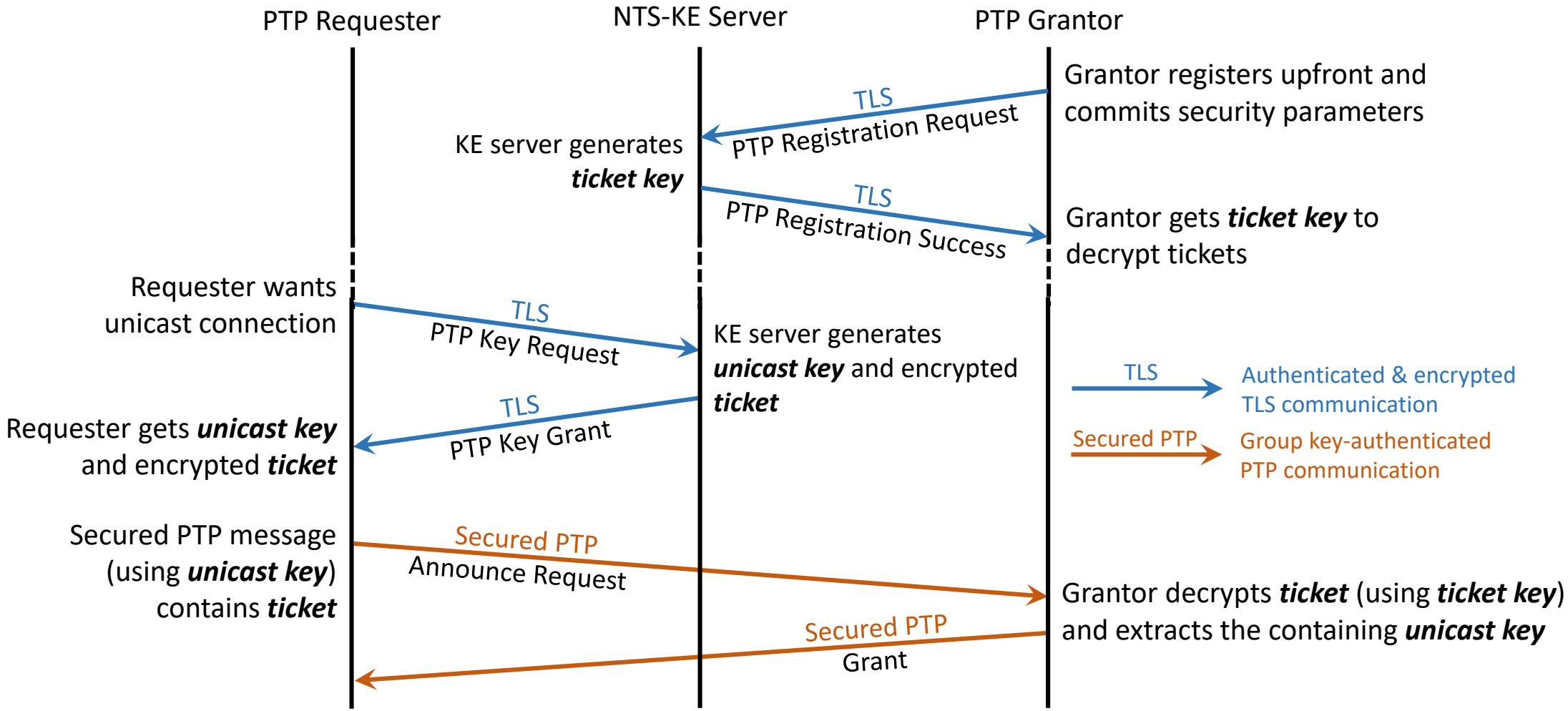
NTS for Unicast PTP

- Modified approach
  - Using a ticket based solution to transmit security parameters

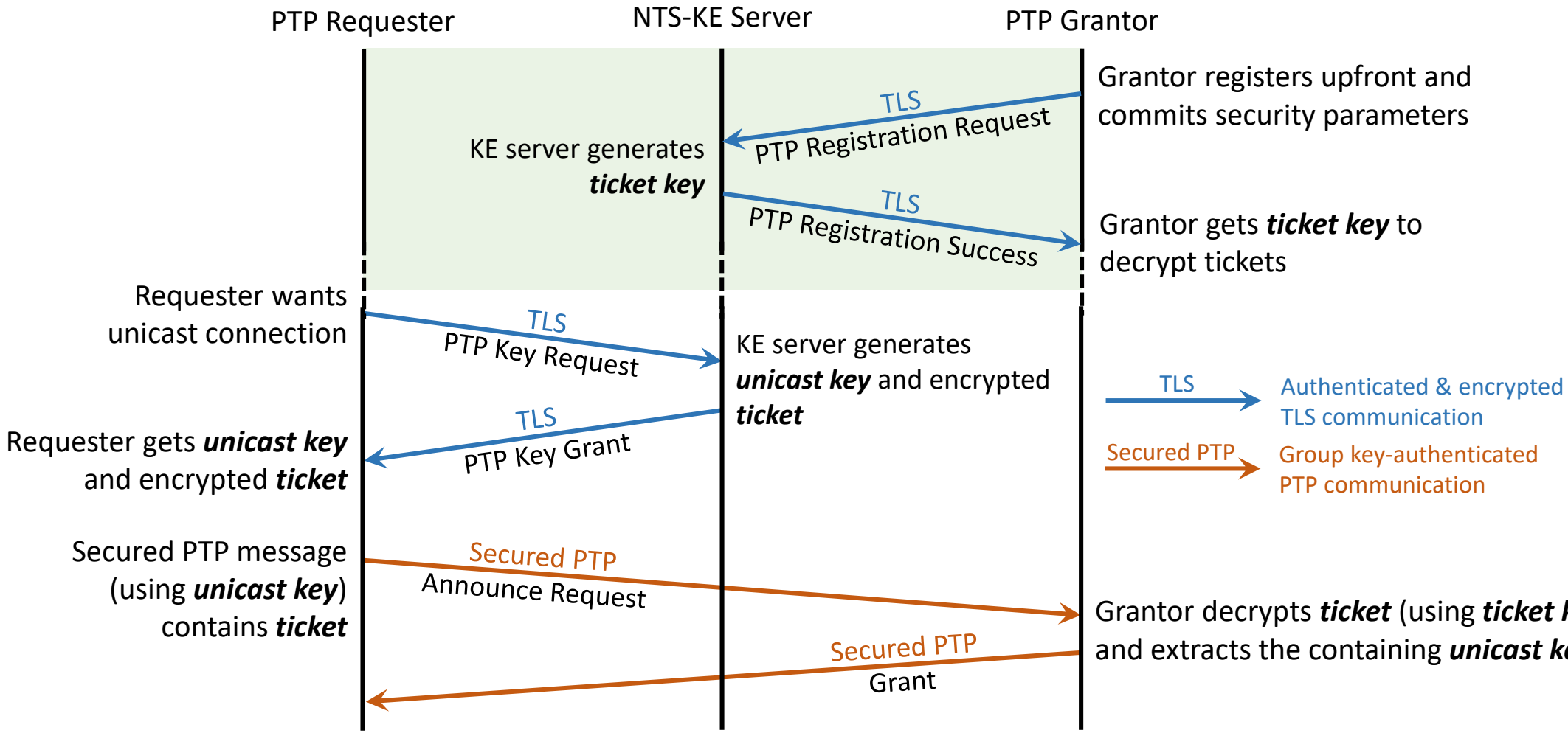
  →Scales better than Group-of-2 approach

- Identification
  - Address information (e.g. PortID, IP, MAC) of grantor and requester identifies communication partners
  - Note: Many unicast pairs in a PTP network might have the same PTP domain number and Profile (SdoId)

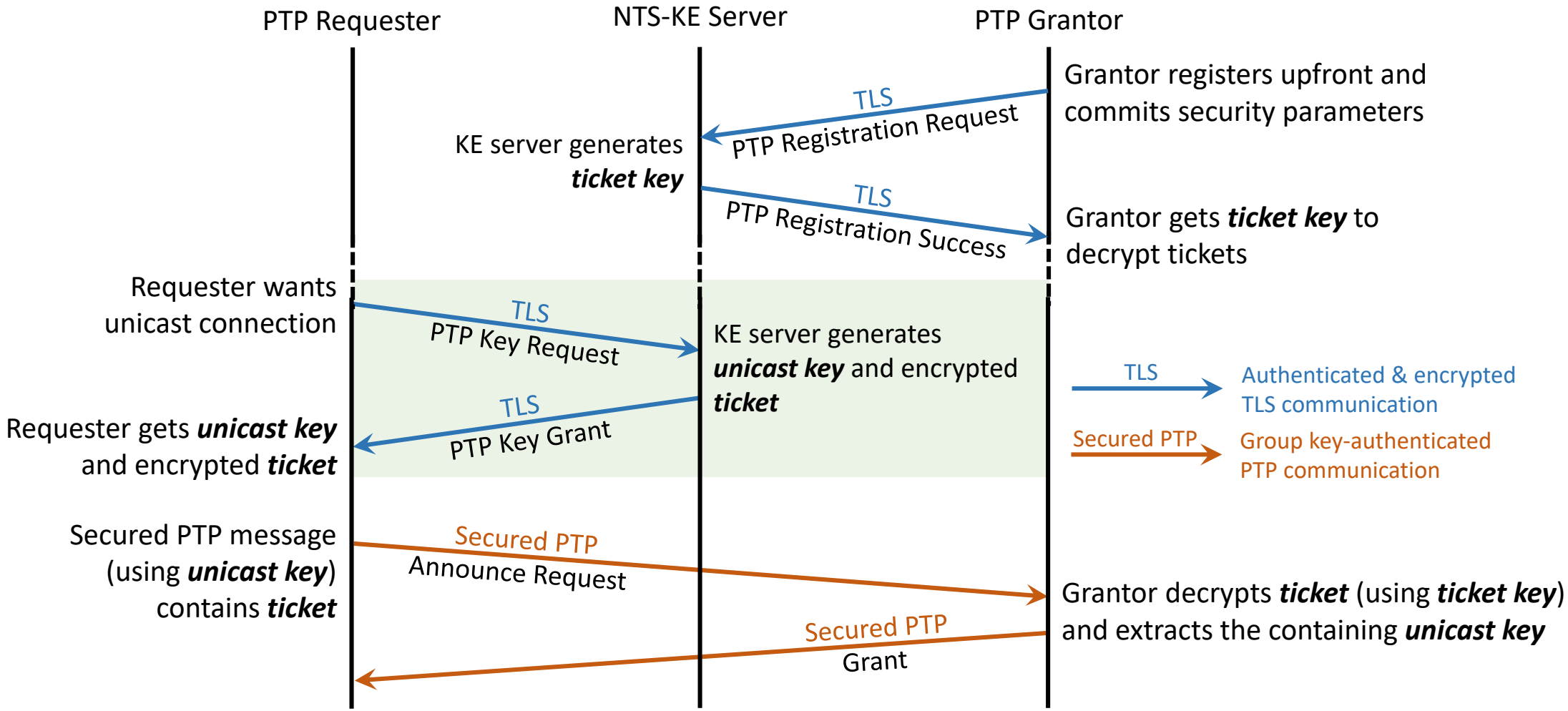
NTS for Unicast PTP



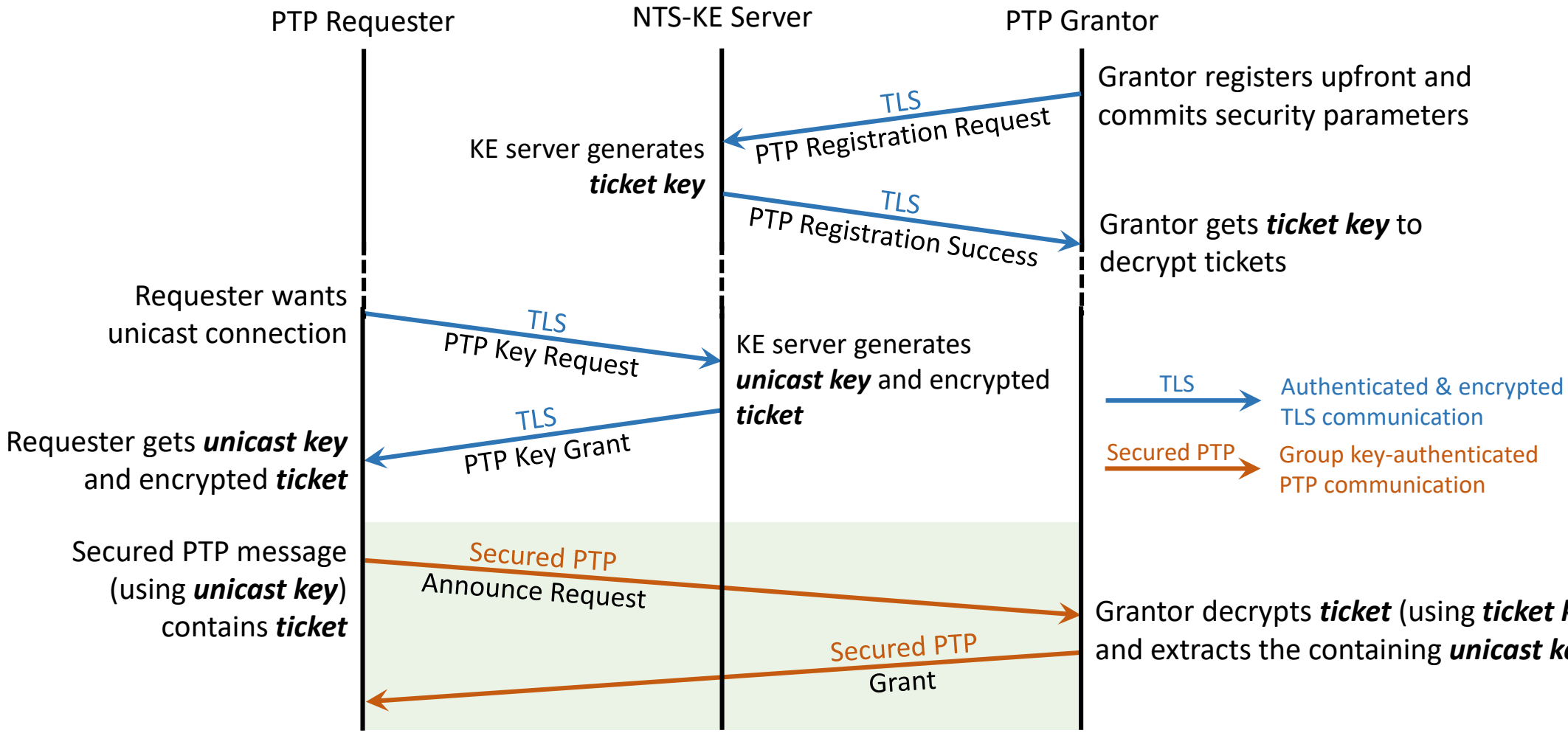
NTS for Unicast PTP



NTS for Unicast PTP



NTS for Unicast PTP



Advantages of NTS for Secured PTP

- Easy to implement, multicast & Group-of-2 even easier
- 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 (hardware)

Ostfalia
University of
Applied Sciences

MEINBERG
The Synchronization Experts.

Thank you for your attention

For more information contact
Martin Langer: mart.langer@ostfalia.de
Douglas Arnold: doug.arnold@meinberg-usa.com