Ostfalia
University of
Applied Sciences

NTS4PTP

Network Time Security for the Precision Time Protocol

Update Report of the Draft

Martin Langer, Rainer Bermbach

IETF NTP working group, June 22, 2021

Agenda

Ostfalia
University of
Applied Sciences

- Goals and Features
- Protocol Overview
- Draft Status

NTS4PTP
Goals

Ostfalia
University of
Applied Sciences

- We need a security solution for PTP
  - PTPv2.1 provides an AUTHENTICATION TLV
  - The key management system is out of scope
- Idea: Using NTS as a key management system for PTP
  - Then we have one NTS-KE server, which supports NTP and PTP
- We want a solution for all PTP functionalities and modes
  - Not easy and very different to NTP

NTS4PTP
Features

Ostfalia University of Applied Sciences

- NTS4PTP defines two approaches:
  - Group-based approach (GrBA): for PTP multicast and mixed multicast/unicast
  - Ticket-based approach (TiBA): for PTP unicast only (scalable)

- We have extended the NTS-KE protocol to support PTP

- We have defined the NTS Time Server Registration (NTS-TSR) protocol
  - The communication between time server (PTP grantor) and NTS-KE server
  - Therefore, the NTS-KE server can run the NTS-KE and NTS-TSR protocol (depending on the ALPN)
    - Necessary to be able to distinguish messages

NTS4PTP
Features

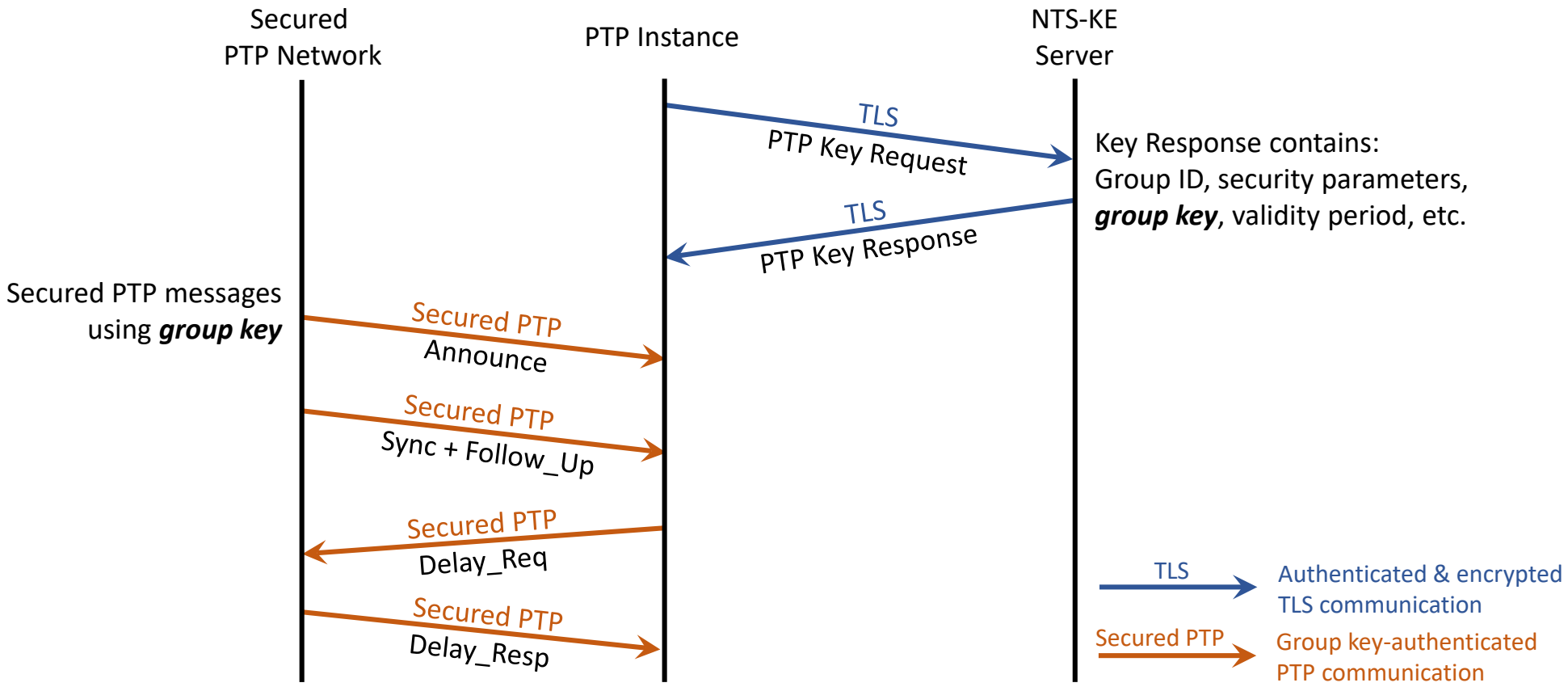
Ostfalia
University of
Applied Sciences

- More features:
  - Group- and E2E security
  - Cyclic key update process
    - Without interruption of PTP communication
    - Simple group control
  - PTP grantor and algorithm negotiation for unicast connections

NTS4PTP
Protocol Overview – Group-Based Approach

Ostfalia University of Applied Sciences

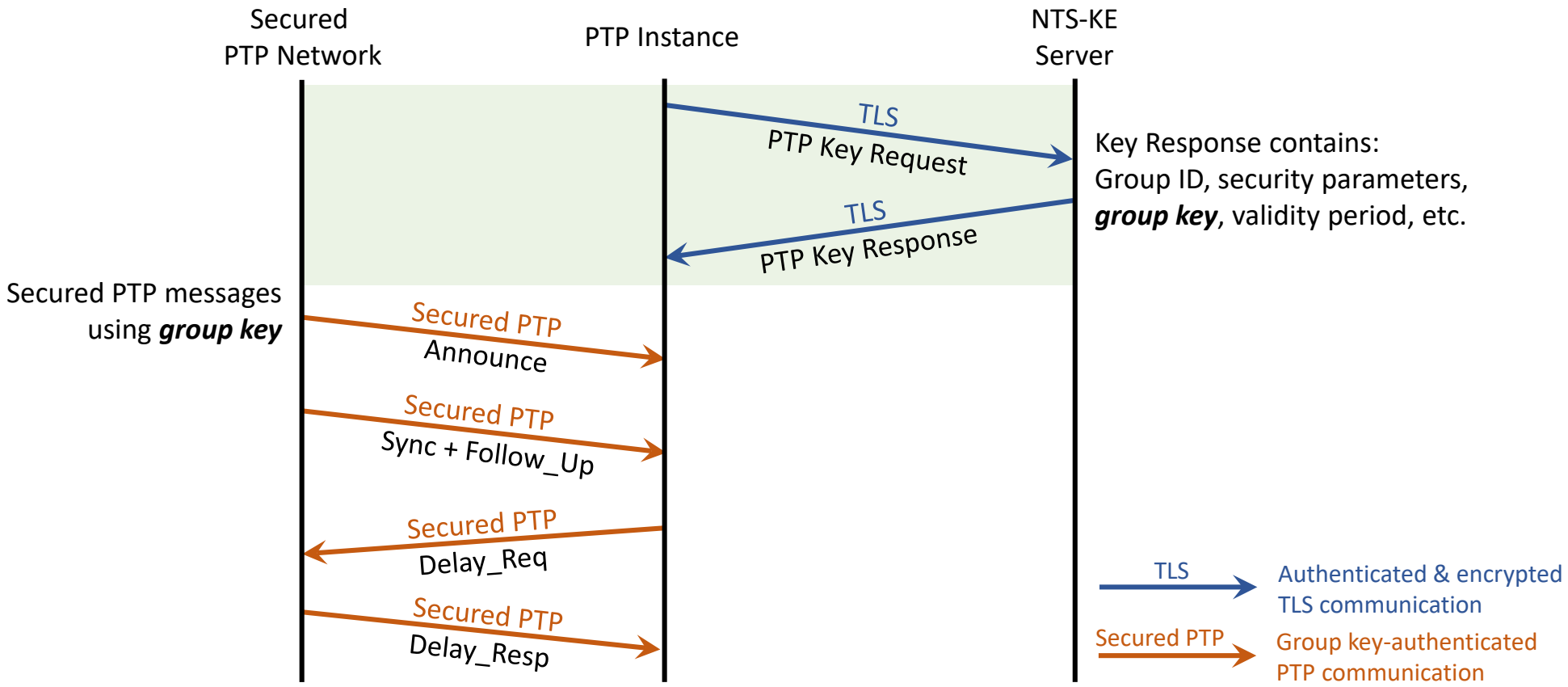
- Same procedure for every PTP instance of the group



NTS4PTP
Protocol Overview – Group-Based Approach

Ostfalia University of Applied Sciences

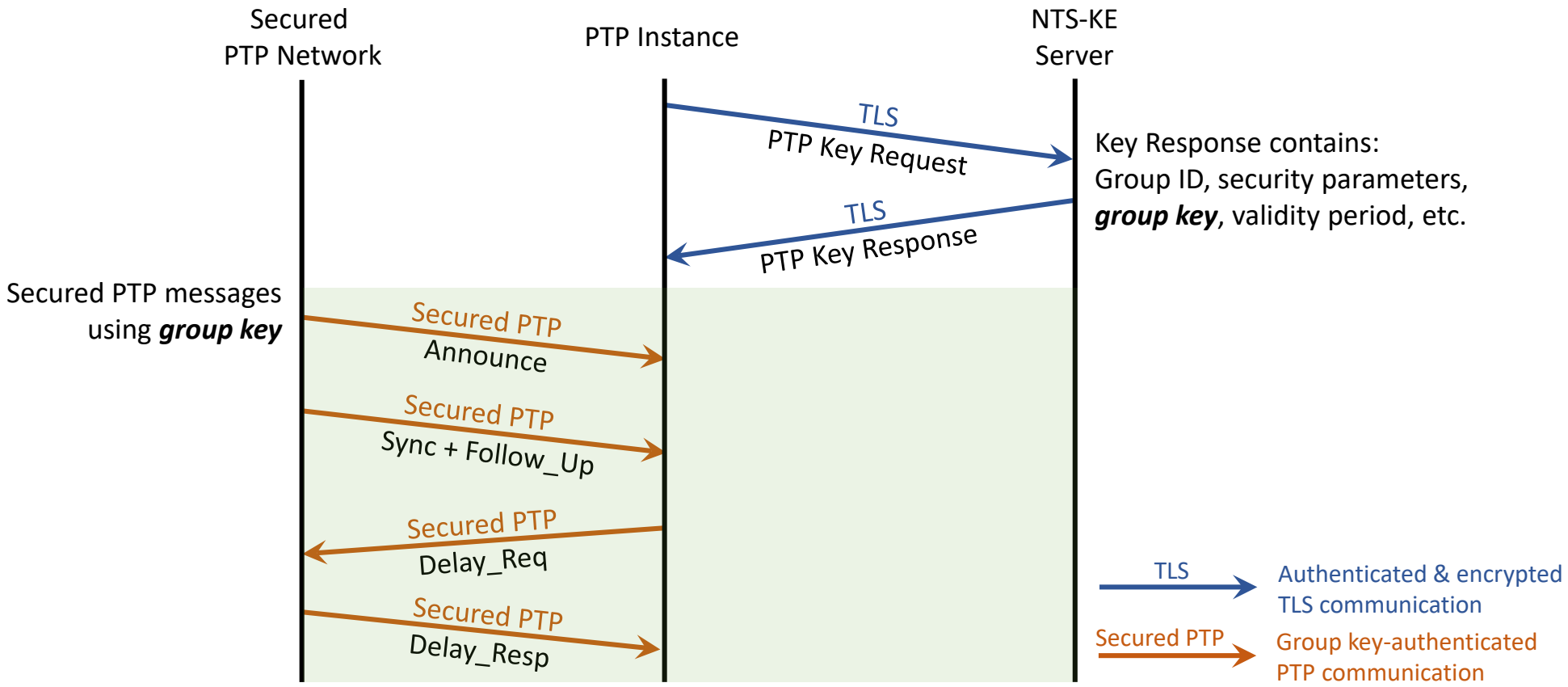
- Same procedure for every PTP instance of the group



NTS4PTP
Protocol Overview – Group-Based Approach

Ostfalia University of Applied Sciences

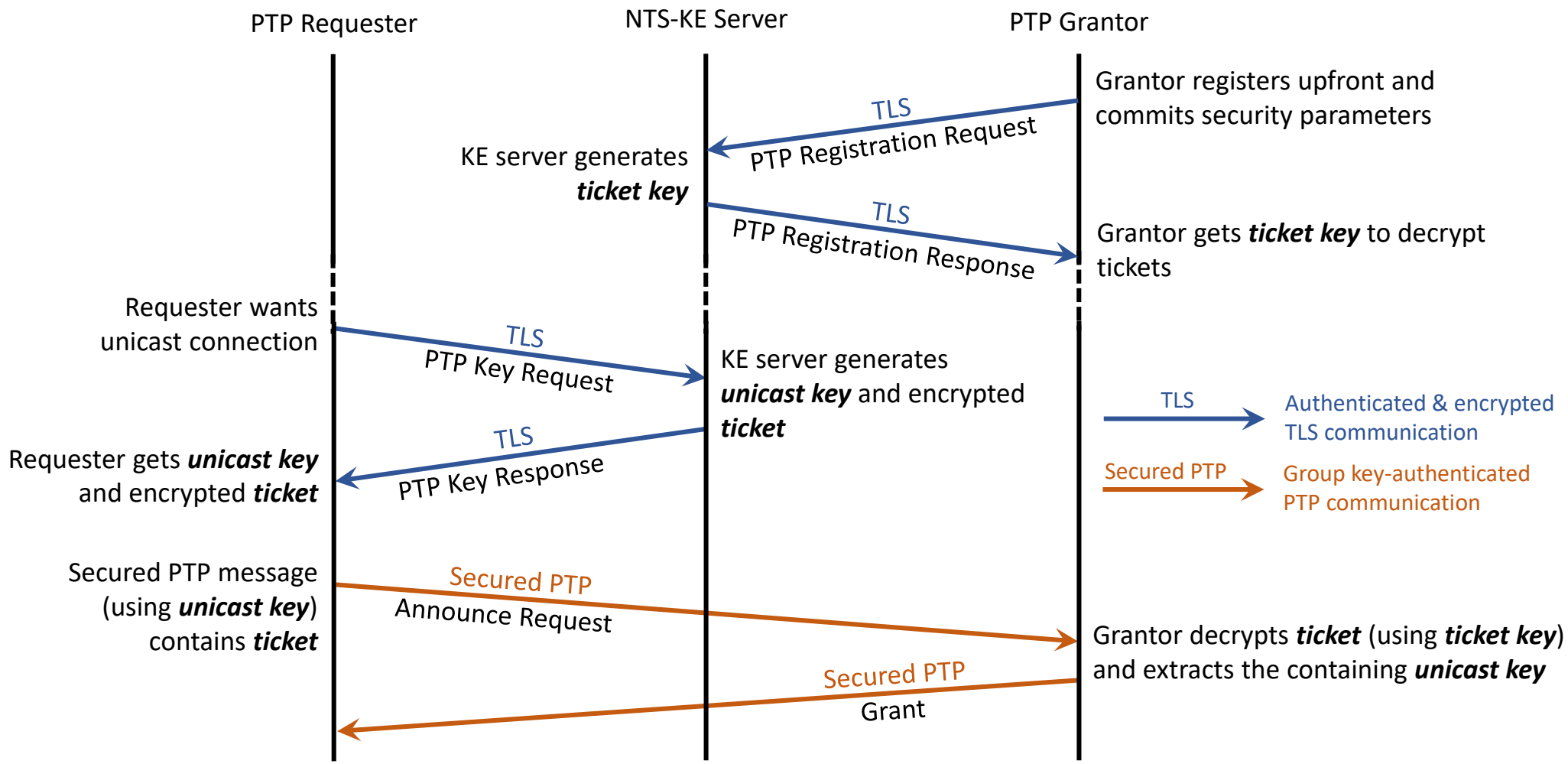
- Same procedure for every PTP instance of the group



NTS4PTP

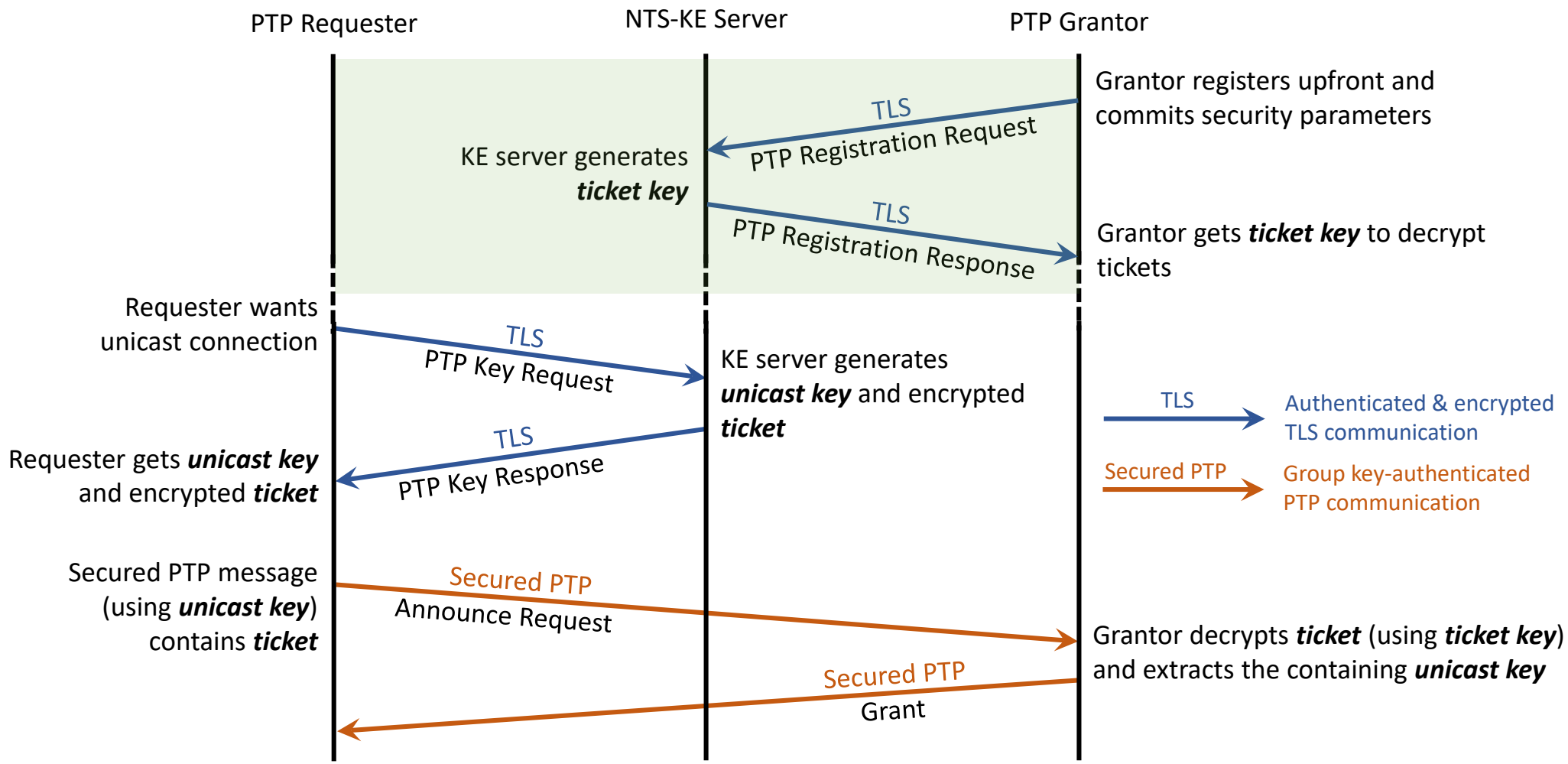
Protocol Overview – Ticket-Based Approach

Ostfalia University of Applied Sciences



NTS4PTP
Protocol Overview – Ticket-Based Approach

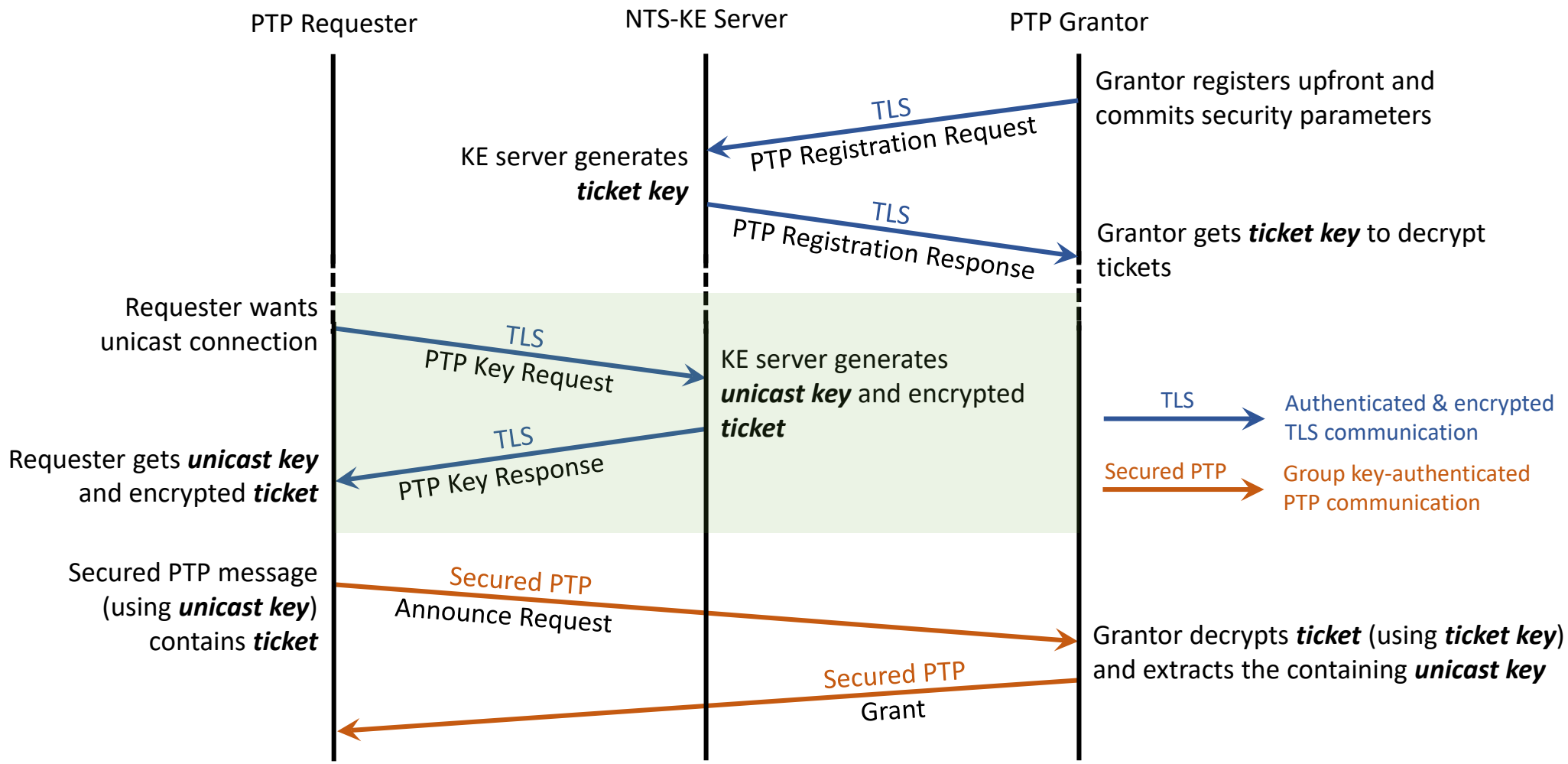
Ostfalia University of Applied Sciences



NTS4PTP

Protocol Overview – Ticket-Based Approach

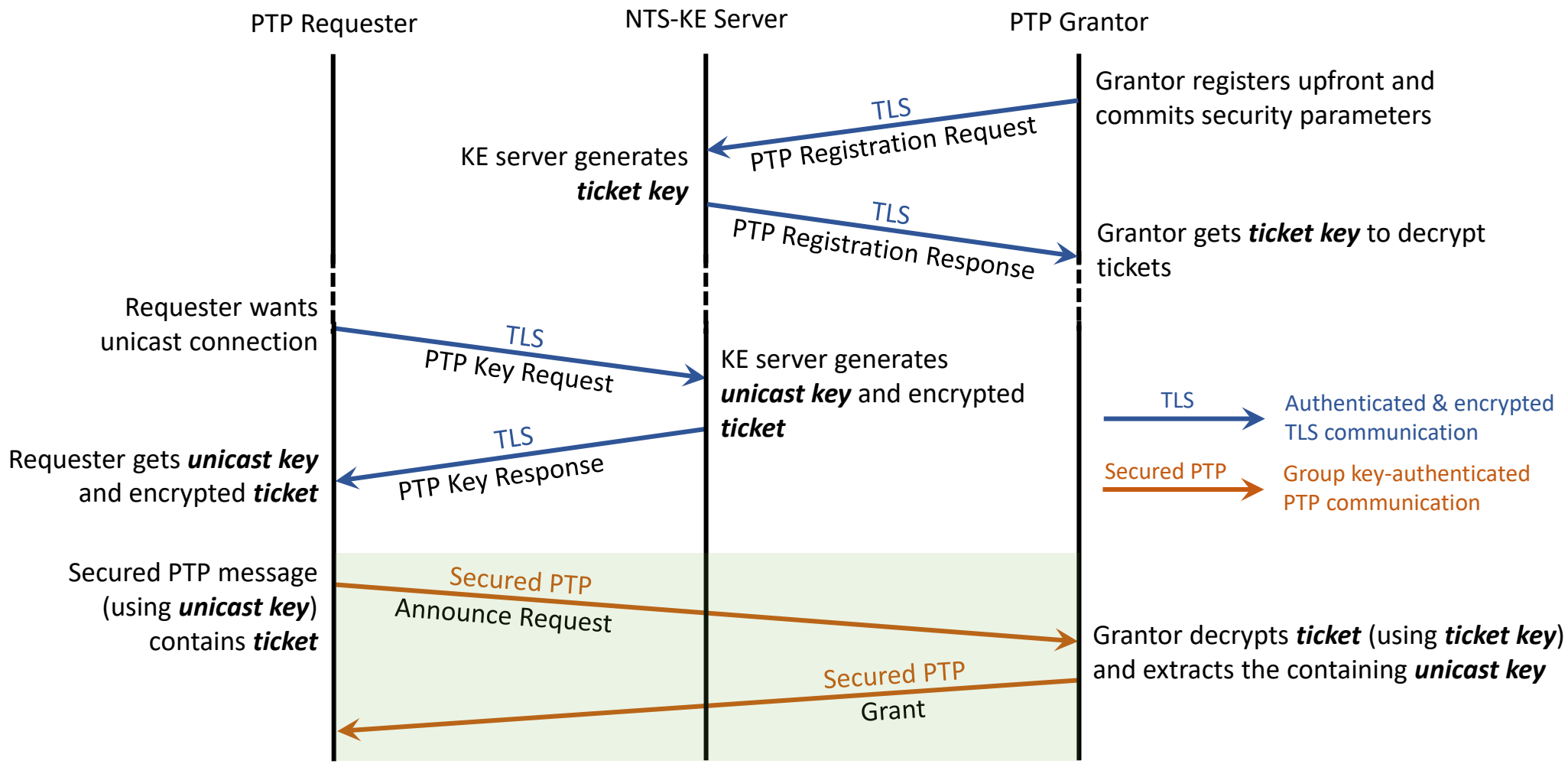
Ostfalia University of Applied Sciences



NTS4PTP

Protocol Overview – Ticket-Based Approach

Ostfalia University of Applied Sciences



NTS4PTP
Draft Status

Ostfalia University of Applied Sciences

- Current version: *draft-langer-ntp-nts-for-ptp-01*

- Next update in 6 to 8 weeks

- The following version contains many changes
  - NTS messages were simplified
  - Key rotation process has been optimized
  - Clarifications and text improvements
  - Preparation for PoC implementation underway
    - possible integration into Linux PTP for initial tests

Ostfalia
University of
Applied Sciences

Thank you for your attention!

Martin Langer, Rainer Bermbach

Ostfalia University of Applied Sciences,
Wolfenbüttel, Germany