Secure Transport for PCEP

draft-ietf-pce-pceps

IETF91 – Honolulu

Diego R. Lopez - Telefónica (diego.r.lopez@telefonica.com)
Oscar González de Dios – Telefónica (oscar.gonzalezdedios@telefonica.com)
Qin Wu – Huawei (sunseawq@huawei.com)
Dhruv Dhody – Huawei (dhruv.ietf@gmail.com)

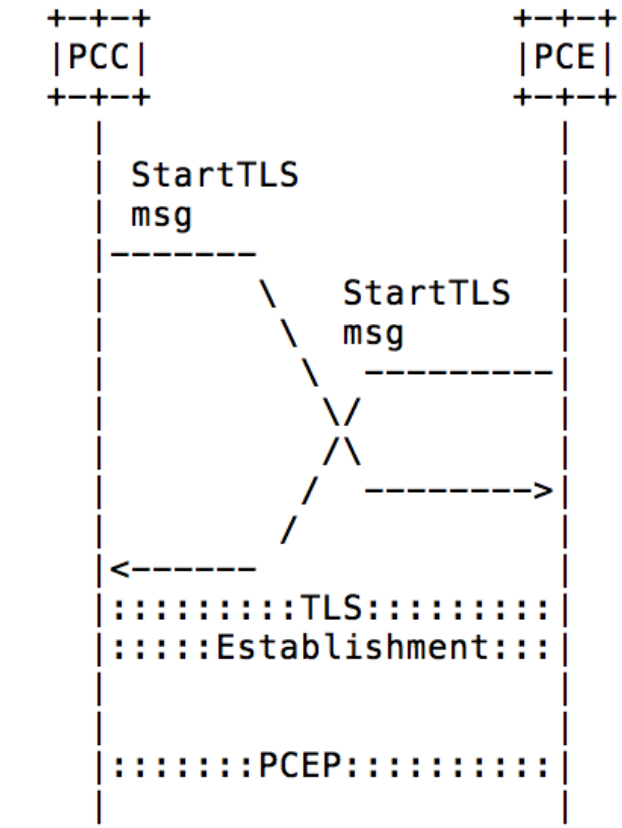
The Goals

- Secure PCEP exchanges
  - Peer authentication and authorization
  - Data exchange integrity
  - Data exchange confidentiality
- Do not require change to current PCEP implementations
- Do not preclude future extensions
- Allow emerging applications

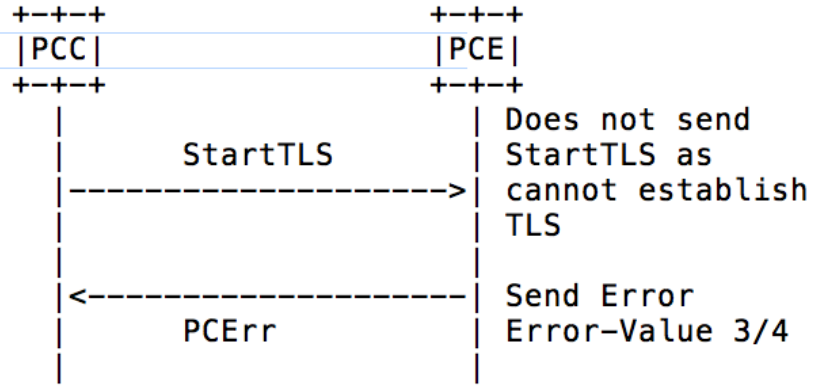
The Changes

- Introduce the StartTLS message
  - As the mechanism to start TLS on a PCE connection
    - Very much following the LDAP model
    - Aligned with the discussion with Transport Area
  - Simple format, just Message-Type
  - Must be the first message (prior to Open)
    - Impacts RFC5440
    - Necessary to guarantee security
- No impact on existing implementations
  - Peer not supporting StartTLS signal an unknown message
- Dedicated error management

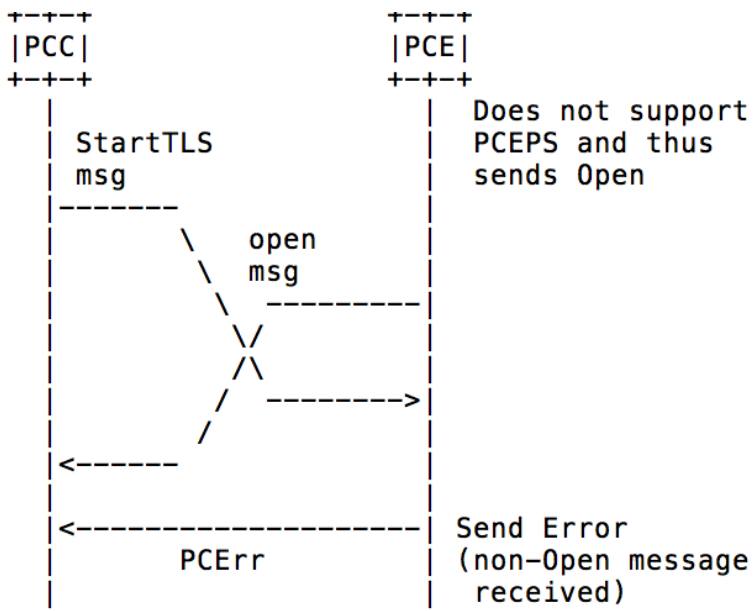
The Flows



Both PCEP Speakers support PCEPS



Both PCEP Speaker support PCEPS, but cannot establish TLS



One PCEP Speaker does not support PCEPS

The (still) Open Issues

- Align with discovery mechanisms
  - As the I-Ds on them evolve
- Concrete message and error types
- Go for direct operational evidence
  - Implementation
  - Experimental deployment
  - Gain experience with security mechanisms
    - TLS profile
    - Peer identification
    - DANE applicability