

EAP-PPT

Privacy Preserving Network Access

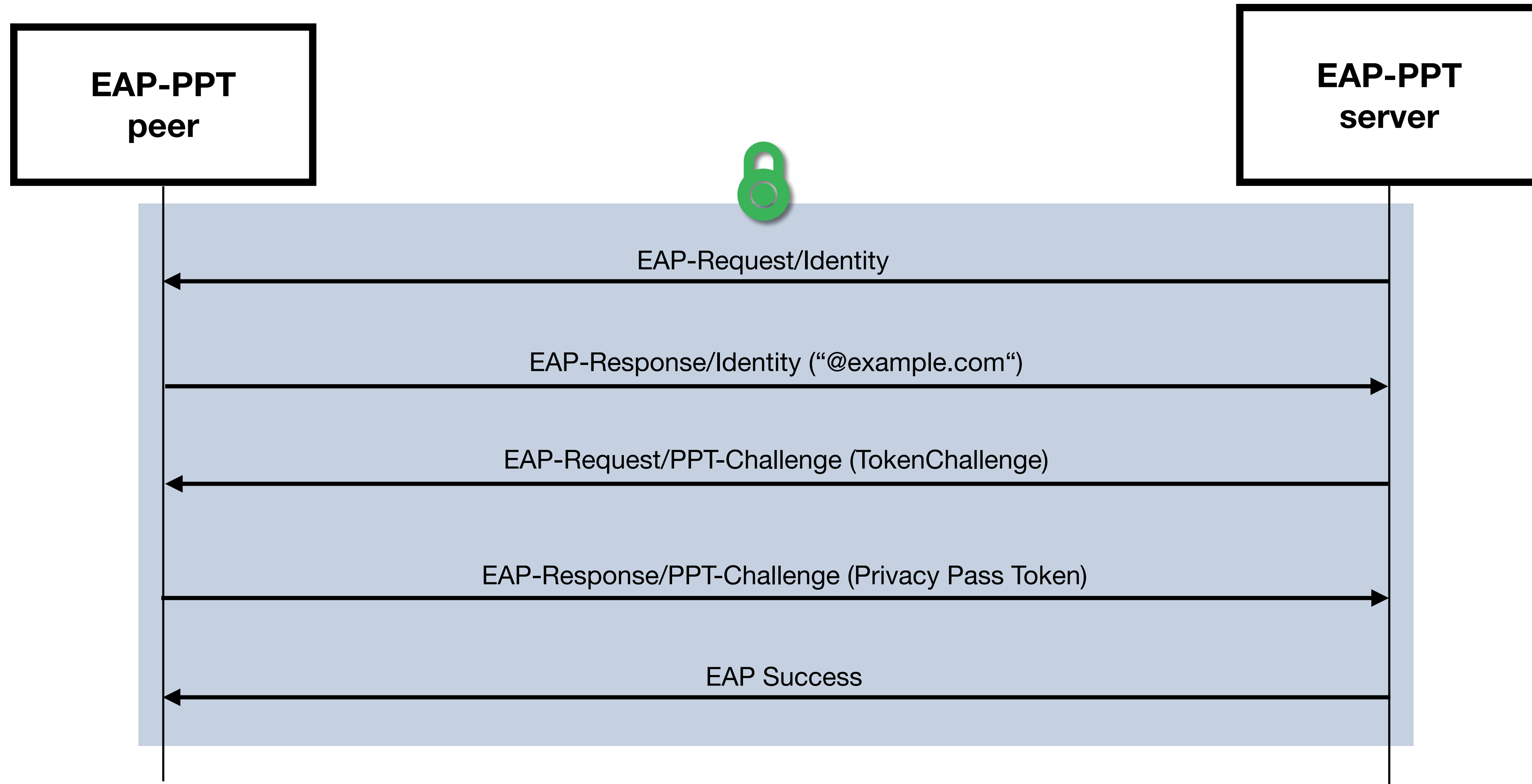
Paresh Sawant, Bart Brinckman

EMU, IETF 121 Dublin, November 2024

Recap

- EAP-PPT - EAP Using Privacy Pass Token
 - Peer authentication using Privacy Pass Token inside secure Tunnel
 - Privacy Pass Token - product of Privacy Pass WG
- Objectives -
 - Anonymous network access
 - Privacy protection against -
 - Active and passive attackers
 - Network Service Providers
 - Identity Providers
 - Venue owners, enterprises, educational institutions

EAP-PPT



Feedback from IETF 120

- Inability to generate Key Material (No Cryptographic Binding)
- Areas of Privacy implications
 - Outer EAP Identity
 - TLS session resumption
 - Client authentication during TLS handshake
- Absence of Channel Binding
- Lack of details on deployment considerations

EAP-PPT - draft 01

- Key material generation using TLS exporter interface (RFC7505)
- Channel Binding
- Specifications to protect privacy in -
 - Outer Identity
 - TLS Session Resumption
 - Client Authentication during TLS handshake
- Deployment considerations
 - Public and Private deployments
 - Federated deployment

Q&A