TeleTrusT EBCA
European Bridge Certificate Authority

TeleTrusT-EBCA "PKI-Workshop"

Berlin, 22.06.2017

# Neue Sicherheitsstandards: TLS 1.3 und S/MIME 4.0

Henrik Koy, Deutsche Bank
Sören Beiler, Net at Work

# Änderungen in TLS 1.3

- Im 20. draft: https://tools.ietf.org/html/draft-ietf-tls-tls13-20
- Signifikante Änderungen im kryptographischen Design: Vertraulichkeit und Integrität der TLS *Handshake* Daten, und der Anwendungsdaten. Neue Schlüsselableitung.
- Schneller Verbindungsaufbau:
  - Verschlüsselte Daten bereits beim Server *Hello* – oder
  - Bereits beim Client *Hello* - im Zero Round Trip Time (0RTT)
- Neue Kryptographie Algorithmen (ECC)
- …

➔ Wird TLS 1.3 auch sich auf PKI Lösungen auswirken?

# Änderungen in S/MIME V4

- draft bis 09.10.2017
- AES-256 GCM oder AES-128 GCM sollen zur Verschlüsselung benutzt werden
- 3DES entfernt, Support nur für bereits verschlüsselte Mails
- SHA-1 & MD5 entfernt
- SHA-512 hinzugefügt
- Einführung von AuthEnvelopedData

# Workshop-Ergebnisse

- **Vorteile: Effizienz auf Serverseite**
  - State of the Art Aplikationen
  - OCSP Spoofing
  - Zertifikatsprofil kann aufgeräumt werden
- **Nachteile:**
  - Interoperabilität bei heterogenen IT Systemen