gematik

TLS 1.3

Transport Layer Security

Mike Kurtze
Gematik | Senior Software Engineer
mike.kurtze@gematik.de

Was ist TLS 1.3 (Transport Layer Security)

- **TLS**: Verschlüsselungsprotokoll zur Authentifizierung und Datenverschlüsselung zwischen zwei Kommunikationspartnern (Server, Computer und Anwendungen)

- **Vorteil**: Server und Client tauschen keine geheimen Informationen aus, die unverschlüsselt sind.

- **TLS 1.2** (RfC 5246, 2008, IETF):
  - Derzeit am weitesten angewendet
  - Updates (5746, 5878, 6176, 7465, 7507, 7568, 7627, 7685, 7905, 7919, 8447)

- **TLS 1.3** (RfC8446, 2018, IETF):
  - Sicherheit wurde verbessert (ältere und unsichere Algorithmen wurden entfernt)
  - Performance wurde verbessert (einige Handshake-Messages wurden entfernt)

Vertraulichkeit: sensible Daten müssen verschlüsselt übertragen werden.

AES

Symmetrische Algorithmen: sensible Daten werden mit AES verschlüsselt.

Schlüssellänge wird per Handshake ausgehandelt.

RSA/DHE/ECDHE

Asymmetrische Algorithmen: Berechnung des symmetrischen Keys.

Server und Client besitzen ihr eigenes asymmetrisches Schlüsselpaar.

Integrität: Daten dürfen nicht verändert werden.

SHA-256/384

Hashwertberechnung: für Schlüsselableitung (HKDF) und Prüfsummenberechnung (HMAC)

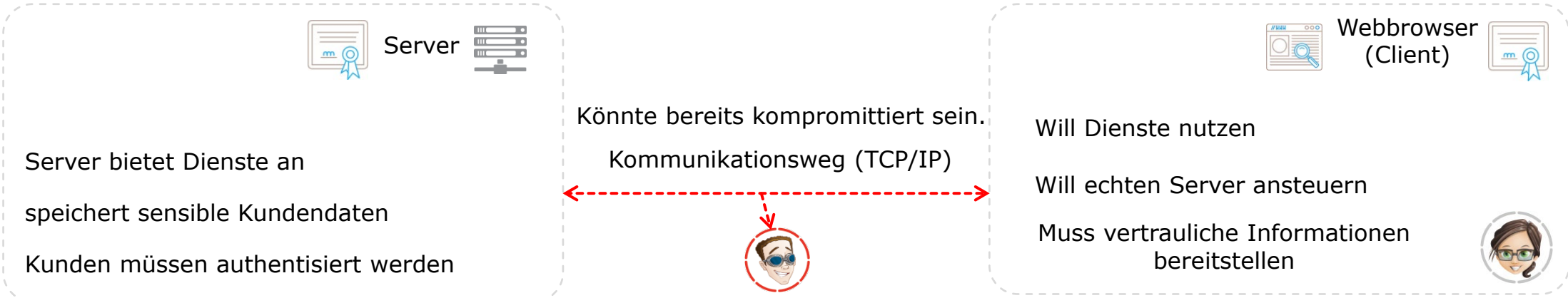
Pkcs#1

Digitale Signatur: Server und Client (optional) signieren Messages (Certificate Verify)

Authentizität: Kommunikationspartner muss vertrauenswürdig sein

Digitale Zertifikat: Server und Client authentisieren sich über Zertifikate und public Keys.

Frage: Wie können beide Seiten sich gegenseitig vertrauen und eine TLS-Verbindung aufbauen!



Handshake-Message: Client-Hello

TLS 1.2: ~~TLS-ECDHE_ECDSA_WITH_AES_256_GCM_SHA284~~

- Neue CipherSuites (5): TLS_AES_256_GCM_SHA384

  Vorherige Ciphersuites werden nicht mehr unterstützt.

- Extension - Supported Groups: Welche EC-Kurven werden unterstützt? (z.B. secp256r1, secp384r1) (5 ECDHE, 5 DHE)

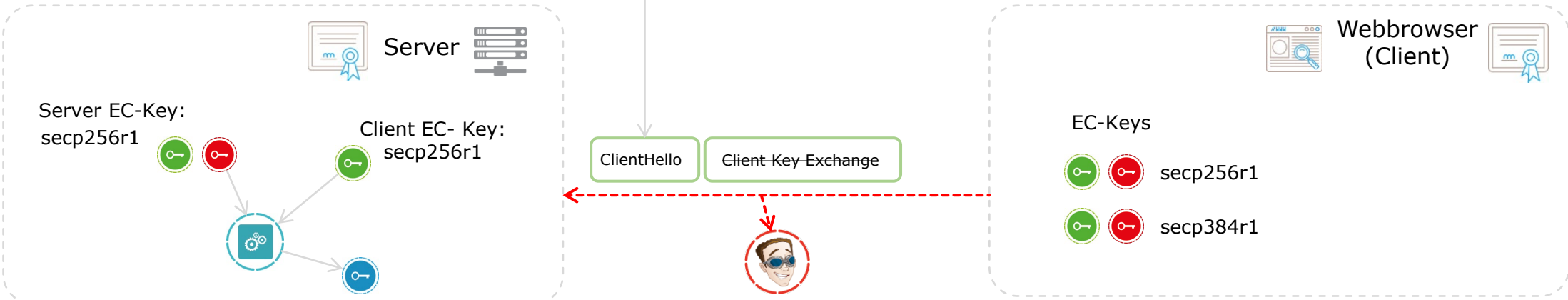
- Extension - Signature Algorithm: Welche Signaturalgorithmen werden zur Prüfung des Servers unterstützt?

- Extension - Key_share: Public Keys für EC-Kurven, welche Client unterstützt.

  Oder „*Pre_shared_keys*“ für Wiederaufnahme der Verbindung.

- Extension Supported_Version: TLS 1.3 (0x0304)

Client-Hello
Protocolversion 0x0303
CipherSuites
Supported Groups
SignatureAlgorithm
Key_share
Supported_Version
Random, LegacySessionID, LegacyCompression, …



Handshake-Message: Server-Hello

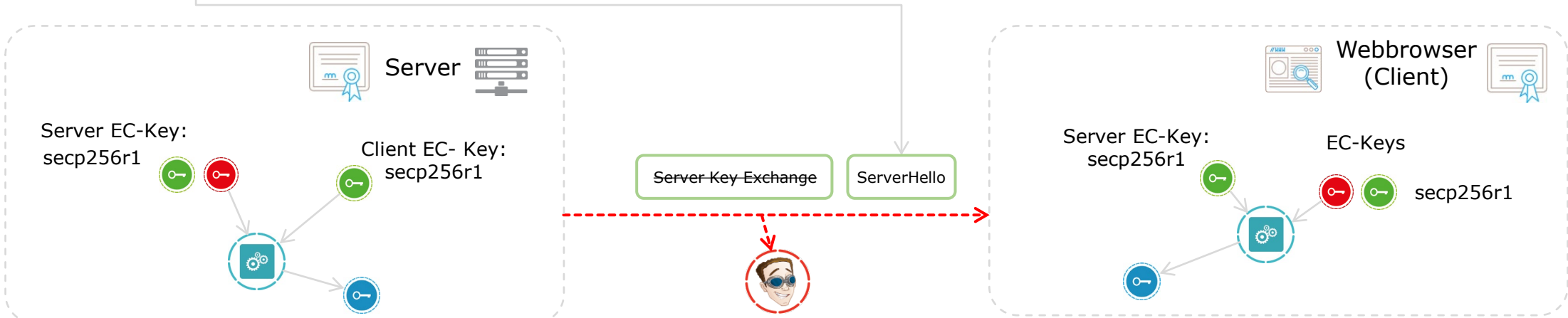
Server-Hello
Protocolversion
CipherSuite
Key_share
supported_Version
...

ChipherSuite:

Server wählt Cipher aus Liste vom Client.

Extension Key_share:

Public Key für EC-Kurve, vom Server generiert.



Handshake-Messages: Encrypted Extension und Certificate Request

gematik

Certificate Request (Optional)
signature_algorithm
certificate_authorities
...

Encrypted Extension
Server_name
client_certificate_type
server_certificate_type
...

- Encrypted extension:

  server_name: Server muss seinen Namen hinterlegen

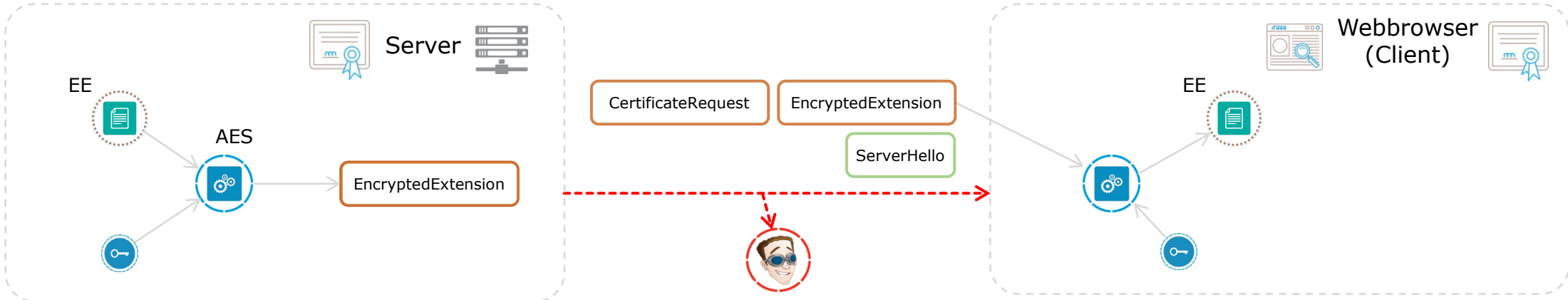
  client_certificate_type: welchen Typ kann der Client anbieten

  server_certificate_type: welchen Typ vom Server kann der Client verarbeiten.

- Certificate Request:

  Server kann Identifizierung des Clients anfordern.

  Kann Liste der unterstützen Signaturalgorithmen angeben.



Handshake-Messages: Server Certificate und Server Certificate Verify

gematik

Server Certificate
List of x.509v3 Certificates

Certificate Verify
Signature Algorithm
Signature

Server Certificate:

Zertifikat vom Server im X.509v3-Format und deren Herausgeber

Muss zum Signaturalgorithmus im Client-Hello passen.

Server Certificate Verify:

Daten: Hashwert über Messages (*Transcript Hash*)

Text: „*TLS 1.3, Server CertificateVerify*„

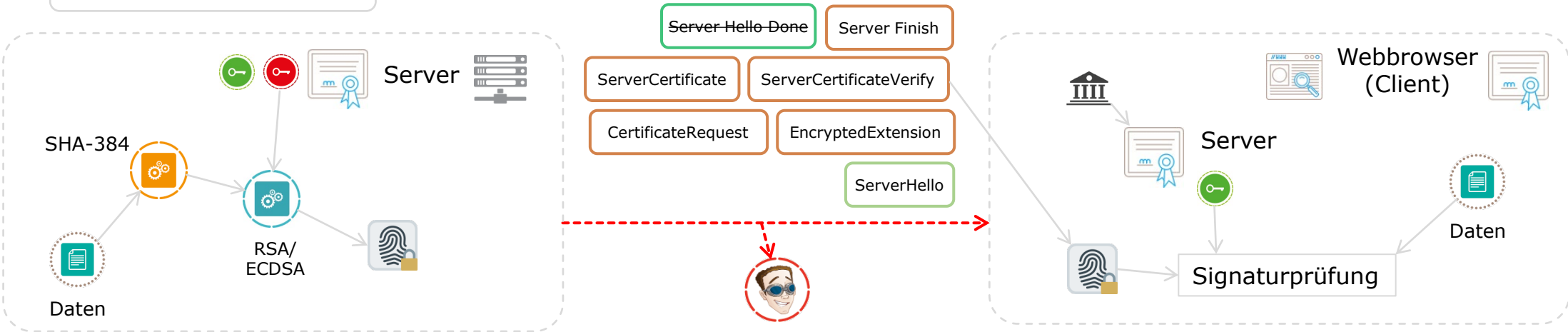
Signatur: PKCS#1-Signatur über Daten

Extension - Signature Algorithm

RSASSA-PKCS1-v1_5

RSASSA-PSS

ECDSA und EdDSA



Client Certificate:

Zertifikat vom Server im X.509v3-Format und deren Herausgeber

Public Key wird separat angegeben

Client Certificate Verify:

Daten

Hashwert über Messages (*Transcript Hash*)

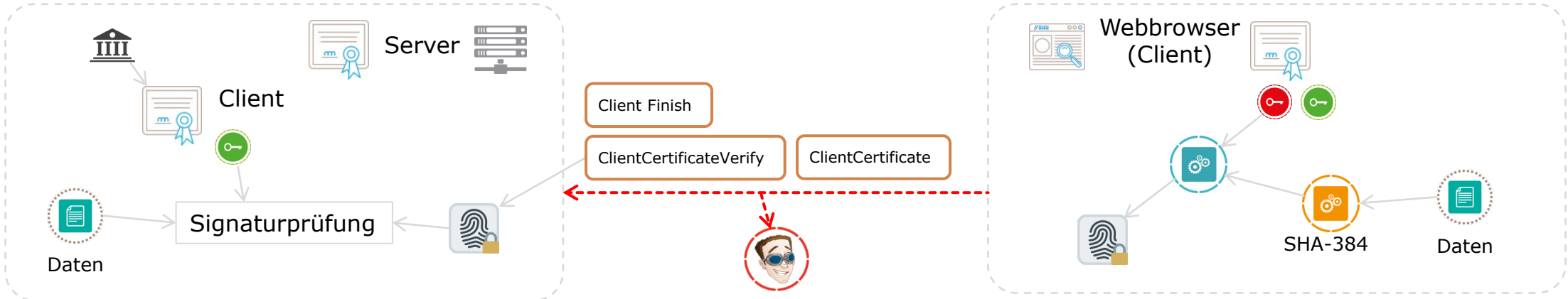
Text: *„TLS 1.3, Client CertificateVerify„*

Signatur

PKCS#1-Signatur über Daten

Certificate Verify
Optional
Signature Algorithm
Signature

Client Certificate
Optional
List of x.509v3 Certificates



- **iX 8/2018:** „Die Neuerungen in TLS 1.3, Supersicher“ (Filipe Pereira Martins, Anna Kobylinska)
- **RfC 8446:** https://datatracker.ietf.org/doc/html/rfc8446
- **The New Illustrated TLS Connection:** https://tls13.ulfheim.net/
- **TLS 1.3 Performance Part 5:**

  https://www.wolfssl.com/tls-1-3-performance-part-5-client-server-authentication/