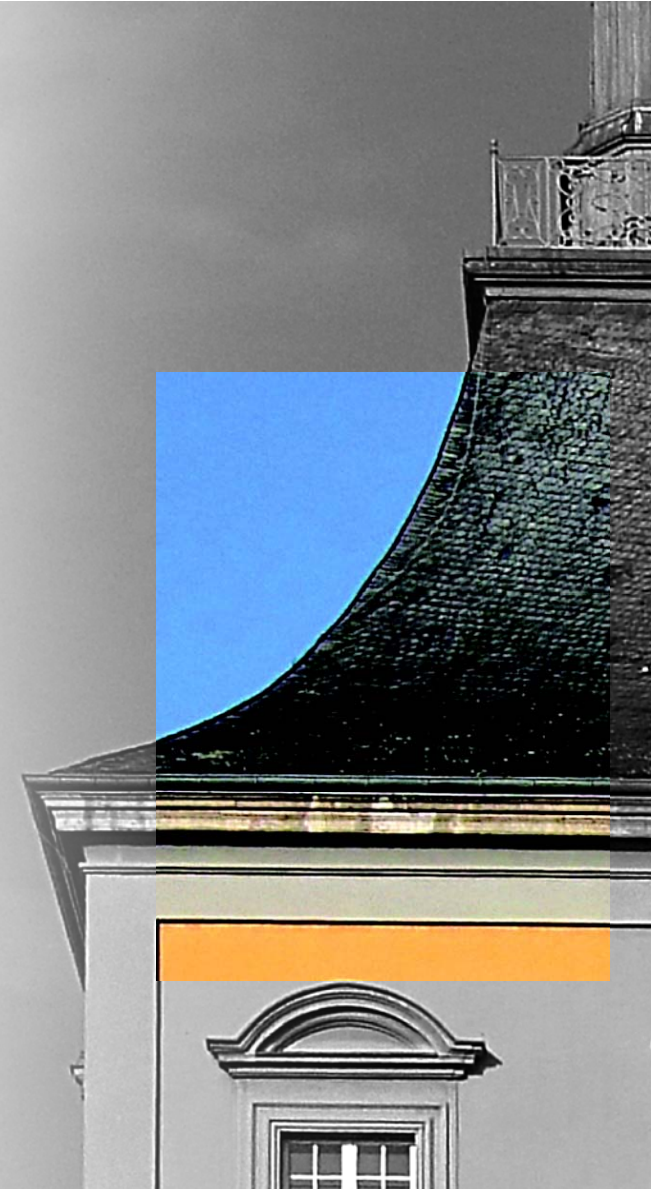


VORLESUNG
NETZWERKSICHERHEIT

SOMMERSEMESTER 2020

MO. 10-12 UHR



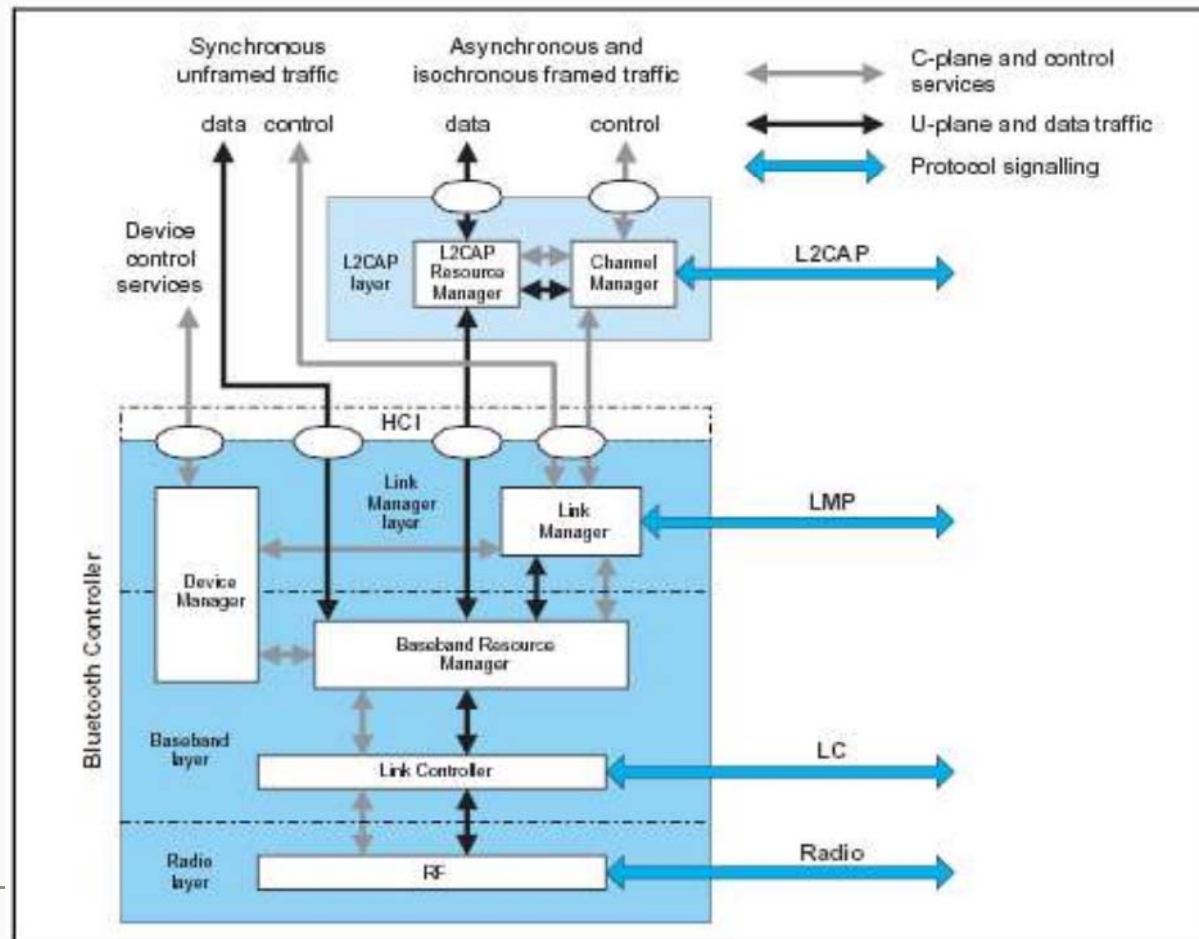
FRAGEN AUS DER LETZTEN WOCH

Welcher Layer1-Standard wird für Bluetooth verwendet?

FRAGEN AUS DER LETZTEN WOCH

7 Application	Anwendungen			
6 Presentation				
5 Session Layer				
4 Transport Layer	SDP	BNEP	RFCOMM	CMTP
3 Network Layer	Logical link control and adaption protocol			
	Host Controller Interface			
2 Data Link Layer	Link Manager Protocol			
	Baseband / Link Controller			
1 Physical Layer	RF / Funk			

FRAGEN AUS DER LETZTEN WOCH



BUGBOUNTY-CHALLENGE

Aktuelle TOP3 (vielen Dank für die Unterstützung):

Platz	Studi	Punkte
1.	Felix	3
1.	Larissa	3
2.	Mario, Marco, Gina	1



KAPITEL 3

PUBLIC-KEY- CRYPTOGRAPHY

Motivation zur kryptographischen Absicherung der Kommunikation:

- Inhalte sind vertraulich und nur für Berechtigte entschlüsselbar
- Daten bei Übermittlung und Speicherung nicht unbemerkt veränderbar
- Sender und Empfänger verifizieren sich gegenseitig als Urheber oder Ziel
- Urheberschaft einer Nachricht nicht abstreitbar



Verschlüsseln & Signieren

ACHTUNG: Nicht alle Ziele immer gleichzeitig erreichbar / gewünscht.

Asymmetrische Kryptographie

- Benötigt Schlüsselpaar
 - Öffentlicher Schlüssel
 - Privater Schlüssel
 - Öffentlicher Schlüssel von privatem Schlüssel abgeleitet
- Bekannte Algorithmen
 - DH (Diffie-Hellman; Schlüsseltausch)
 - ElGamal (ElGamal; Verschlüsseln & Signieren)
 - RSA (Rivest; Shamir; Adleman; Verschlüsseln & Signieren)
- Quiz: Wer ist auf dem Foto?

Absicherung von Kommunikation

- TLS (SSL)
- GnuPG
- S/MIME

Absicherung von Softwareinstallation

- GnuPG

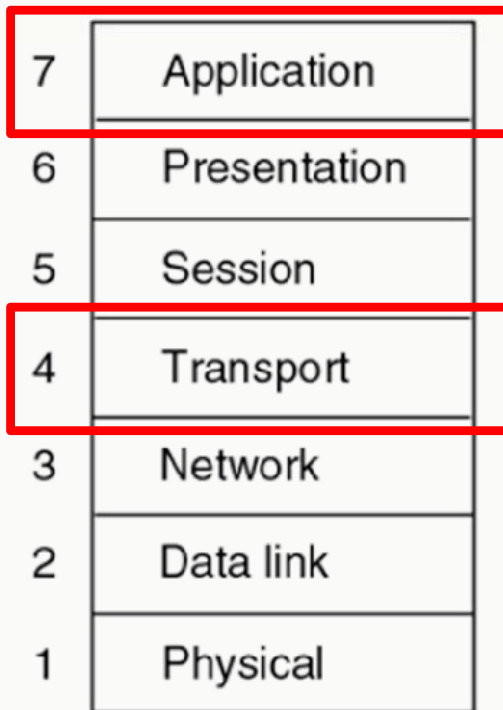
Hintergrund

- Public Key Cryptography Standards (PKCS)

TRANSPORT LAYER SECURITY (TLS)

TRANSPORT LAYER SECURITY (TLS)

OSI



Was meint Transport Layer Security?

- Absicherung der Transportschicht?
 - Absicherung durch darunterliegende Schichten
- Absicherung durch die Transportschicht?
 - Absicherung der darüber liegenden Schichten

Vorgänger: Secure Sockets Layer (SSL)

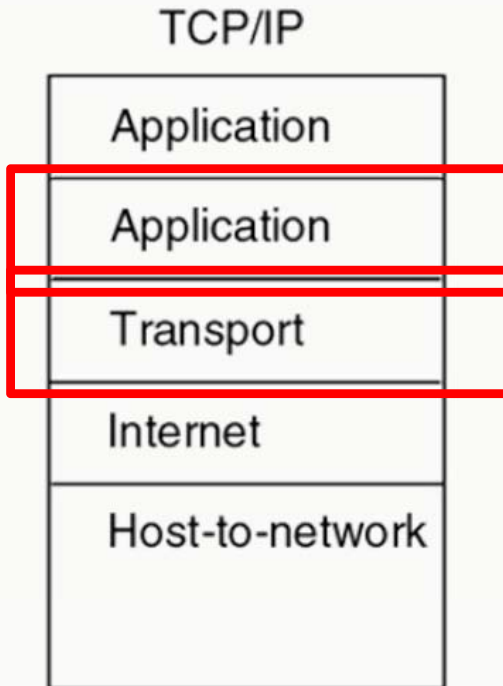
 Eigene Schicht im Protokollstapel

Ziel: Absicherung der Anwendungsschicht

- OSI Layer 5/6 (Sitzungs- und Darstellungsschicht)

TRANSPORT LAYER SECURITY (TLS)

TLS im TCP/IP – Protokollstapel



- Betrachtung von TLS als Anwendung
- "Tunnel" von Anwendungsprotokollen durch TLS
- Bekannte Beispiele:
 - HTTP over TLS (HTTPS)
 - SMTP over TLS (SMTPS)
 - FTP over TLS (FTPS)

TRANSPORT LAYER SECURITY (TLS)

Historie

- 1994 SSLv1 (Netscape)
- 1995 SSLv2 (Netscape)
- 1996 SSLv3 (Netscape / Microsoft)
- 1999 TLSv1 (IETF Standard: RFC 2246)
- 2006 TLSv1.1 (RFC 4346)
- 2008 TLSv1.2 (RFC 5246)
- 2018 TLSv1.3 (RFC 8446)

TRANSPORT LAYER SECURITY (TLS)

Historie

- 1994 SSLv1 (Netscape)
- 1995 SSLv2 (Netscape)
- 1996 SSLv3 (Netscape / Microsoft)
- 1999 TLSv1 (IETF Standard: RFC 2246)
- 2006 TLSv1.1 (RFC 4346)
- 2008 TLSv1.2 (RFC 5246)
- 2018 TLSv1.3 (RFC 8446)

TLSv1 Updates:

- RFC 2712
- RFC 2817
- RFC 2818
- RFC 3268
- RFC 3546
 - Erweiterungen (z.B. SNI)
- RFC 5746
- RFC 6176
 - Prohibiting SSLv2
- RFC 7465
- RFC 7507
- RFC 7919

TRANSPORT LAYER SECURITY (TLS)

Historie

- 1994 SSLv1 (Netscape)
- 1995 SSLv2 (Netscape)
- 1996 SSLv3 (Netscape / Microsoft)
- 1999 TLSv1 (IETF Standard: RFC 2246)
- 2006 TLSv1.1 (RFC 4346)
- 2008 TLSv1.2 (RFC 5246)
- 2018 TLSv1.3 (RFC 8446)

TLSv1.1 Updates:

- RFC 4366
- RFC 4680
- RFC 4681
- RFC 5746
- RFC 6176
 - Prohibiting SSLv2
- RFC 7465
- RFC 7507
- RFC 7919

TRANSPORT LAYER SECURITY (TLS)

Historie

- 1994 SSLv1 (Netscape)
- 1995 SSLv2 (Netscape)
- 1996 SSLv3 (Netscape / Microsoft)
- 1999 TLSv1 (IETF Standard: RFC 2246)
- 2006 TLSv1.1 (RFC 4346)
- 2008 TLSv1.2 (RFC 5246)
- 2018 TLSv1.3 (RFC 8446)

TLSv1.2 Updates:

- RFC 5746
- RFC 5878
- RFC 6176
 - Prohibiting SSLv2
- RFC 7465
 - Prohibiting RC4
- RFC 7507
- RFC 7568
 - Deprecating SSLv3
- RFC 7627
- RFC 7685
- RFC 7905
- RFC 7919
- RFC 8447

TRANSPORT LAYER SECURITY (TLS)

Historie

- 1994 SSLv1 (Netscape)
- 1995 SSLv2 (Netscape)
- 1996 SSLv3 (Netscape / Microsoft)
- 1999 TLSv1 (IETF Standard: RFC 2246)
- 2006 TLSv1.1 (RFC 4346)
- 2008 TLSv1.2 (RFC 5246)
- 2018 TLSv1.3 (RFC 8446)

TLSv1.3 Updates:

- Bisher keine

Aufbau

- TLS definiert **zwei** eigene Schichten
 - Kontrollschicht
 - TLS Handshake Protocol
 - TLS Cipher Spec. Protocol
 - TLS Alert Protocol
 - TLS Application Data Protocol
 - Nutzdatenschicht
 - TLS Record Protocol


TLS HANDSHAKE PROTOCOL

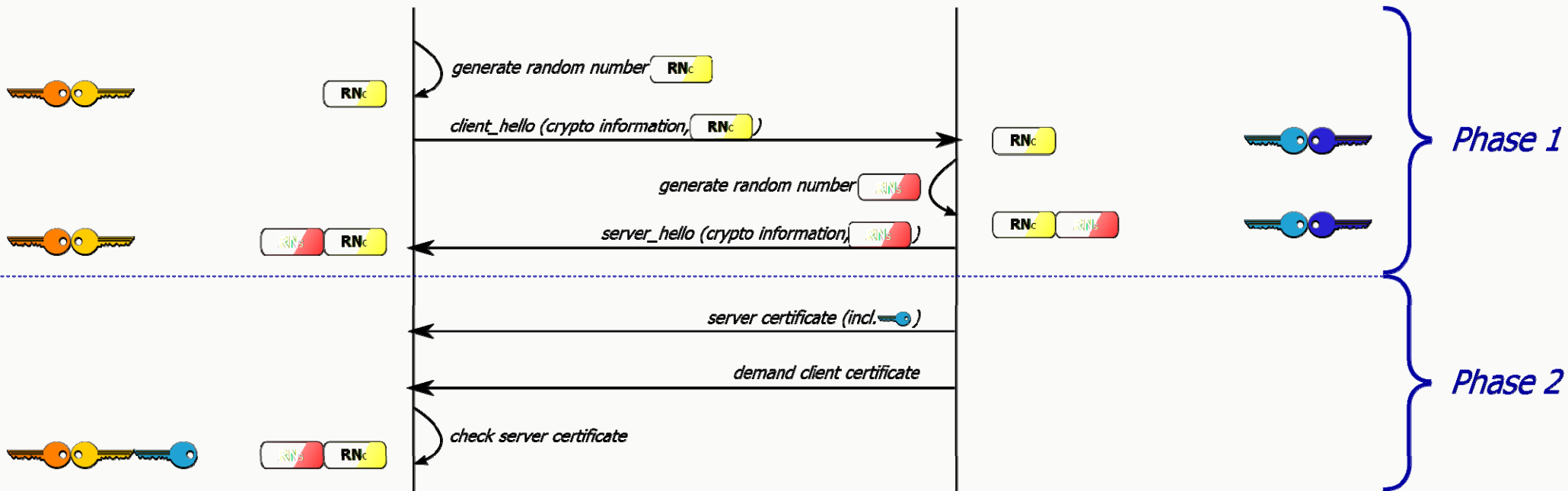
- Ablauf

- Cipher Auswahl / Abstimmung
 - **ACHTUNG:** Es gibt auch NULL-Encryption
 - Schlüsselaustausch für asymmetrische Verschlüsselung
 - Serverauthentifikation
 - Clientauthentifikation
- } Authentifikation mittels X509v3 Zertifikat

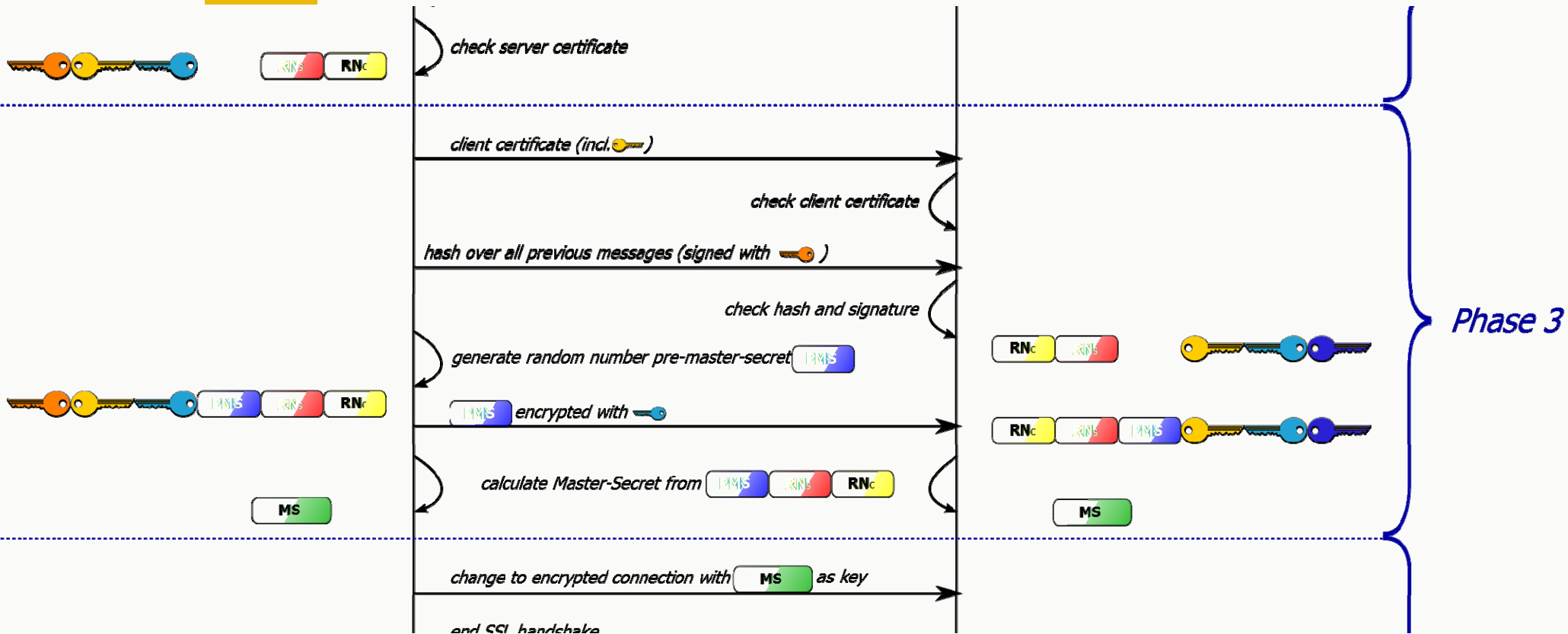
TLS HANDSHAKE PROTOCOL

public key client 
private key client  **Client**

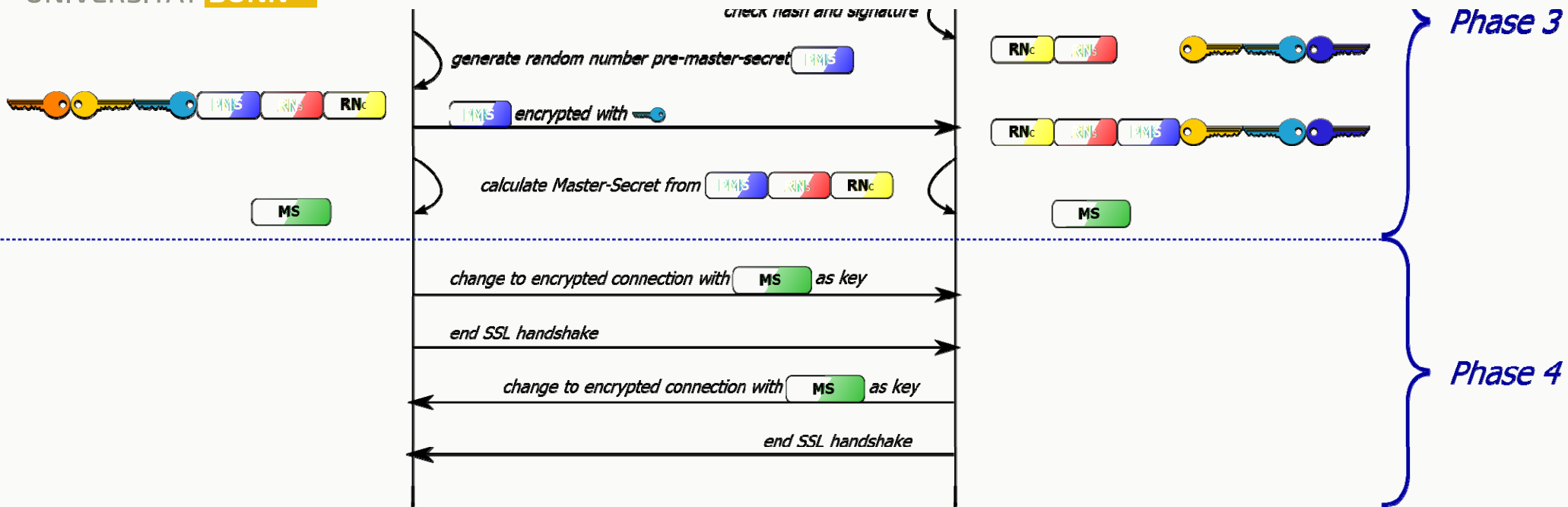
Server  public key server
 private key server



TLS HANDSHAKE PROTOCOL



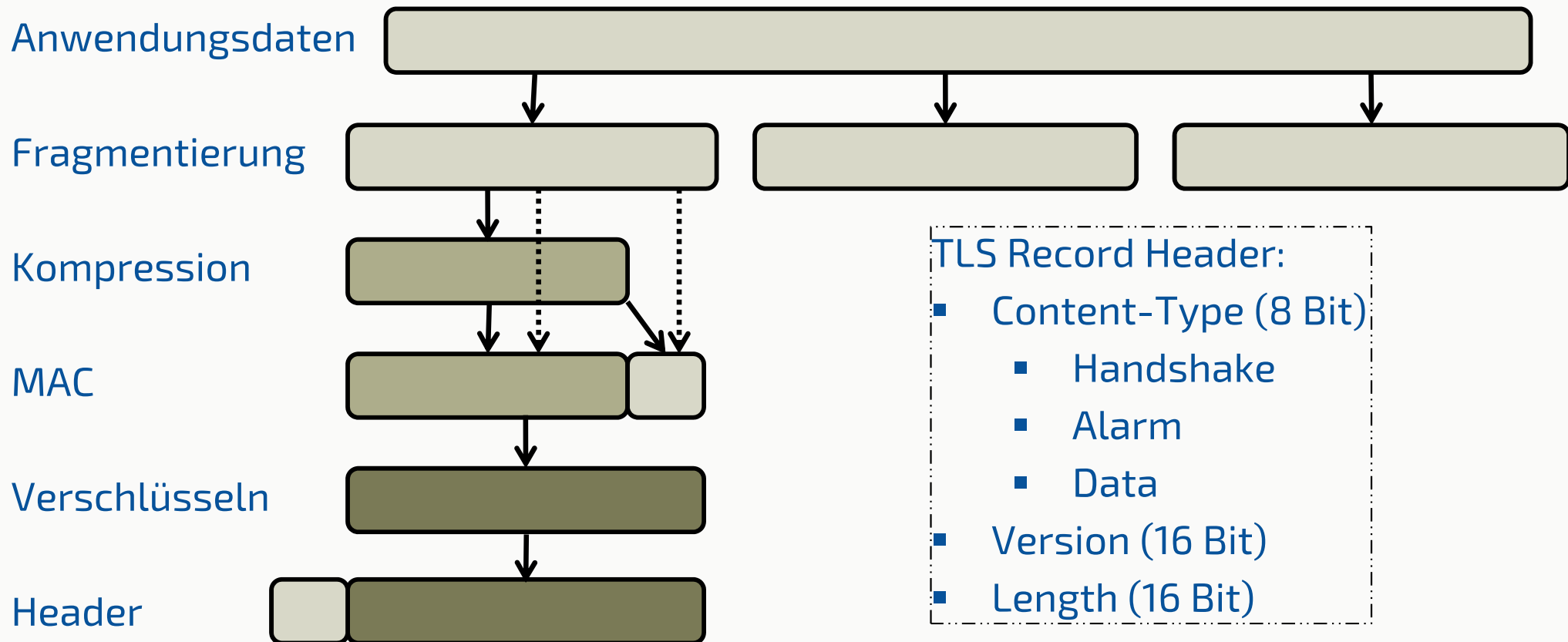
TLS HANDSHAKE PROTOCOL



X509V3 (ISO/IEC 9594-8)

- ITU-T-Standard für Public-Key-Infrastrukturen
 - ITU = Internationale Fernmeldeunion der Vereinten Nationen
 - ITU-T = Standardisierungs-Einheit der ITU
 - X = „Data networks and open system communications“
- Spezifizierte Datentypen
 - Public-Key-Zertifikat
 - Attributzertifikat
 - Certificate Revocation List (CRL)
 - Attribute Certificate Revocation List (ACRL)

TLS RECORD PROTOCOL



Viele Standards, die heutiges Cryptographieumfeld prägen

- ITU-T (Vereinte Nationen)
 - X509-Zertifikate
- IEEE 802
 - 802.1X – Authentifikation am Ethernet-Port
- RSA Security Inc. Public-Key-Cryptography-Standard (PKCS)
 - 15 Standards und Definitionen für Public-Key-Crypto
- Request for Comments (RFC)
 - Organisationsübergreifende Veröffentlichung von Standards (bzw. Entwürfen und Updates)

PUBLIC-KEY-CRYPTOGRAPHY-STANDARDS

- PKCS#1 – RSA public key crypto
- ~~PKCS#2 – RSA encryption of message digests~~ Merged in PKCS#1
- PKCS#3 – Diffie-Hellman key agreement
- ~~PKCS#4 – RSA key syntax~~ Merged in PKCS#1
- PKCS#5 – Password based cryptography specification
- PKCS#6 – Extended certificate syntax
- PKCS#7 – Cryptographic message syntax
- PKCS#8 – Private key information syntax

- PKCS#9 – Selected attribute types
- PKCS#10 – Certification request standard
- PKCS#11 – Crypto token interface (cryptoki)
- PKCS#12 – Personal information exchange syntax
- PKCS#13 – Elliptic curve cryptography
- PKCS#14 – Pseudo random number generation
- PKCS#15 – Cryptographic token information format

PKCS#1 – RSA PUBLIC KEY CRYPTOGRAPHY

RFCs:

- | | | |
|------------|-------------|---------------|
| ▪ RFC 2313 | Version 1.5 | März 1998 |
| ▪ RFC 2437 | Version 2.0 | Oktober 1998 |
| ▪ RFC 3447 | Version 2.1 | Februar 2003 |
| ▪ RFC 8017 | Version 2.2 | November 2016 |

Definitionen:

- RSA Schlüsseltypen für öffentliche und private Schlüssel
 - Öffentlicher Schlüssel:
 - n : modulus
 - e : öffentlicher exponent
 - Privater Schlüssel
 - n : modulus
 - d : privater exponent
- “Multi-prime” RSA (ab PKCS#1 v2.1):
 - Modulus ist das Produkt von mehr als zwei Primfaktoren

Definitionen:

- Umwandlung von Datentypen (Integer \leftrightarrow Octet-String Primitive)
 - I2OSP
 - OS2IP
- Ver- und Entschlüsselung (Primitive und Operationen)
 - RSAEP $((n, e), m)$ mit m = Nachricht (Integer)
 - RSADP (K, c) mit K = privater Schlüssel & Parameter zur Erzeugung
- Signatur und Verifikation (Primitive und Operationen)
 - RSASP1 (K, m)
 - RSASV1 $((n, e), s)$

PKCS#1 – VERWENDET ASN.1

PKCS#1 sieht für die Repräsentation von Schlüsseln das ASN.1-Format vor:

- Abstract Syntax Notation One (ASN.1) – ITU-T-Standard (gemeinsam mit ISO)
- Definiert Repräsentation von
 - Schlüsseln (öffentlich/privat)
 - Zertifikatanfragen (CSR)
 - Zertifikaten
- Darstellungs-/Übertragungsformate:
 - DER
 - CER
 - PEM (nicht Teil von ASN.1) – oft Base64 encoded DER

Privacy Enhanced Mail
(definiert durch IETF)

- RFC 7468
- Encoding von
kryptografischem
Material