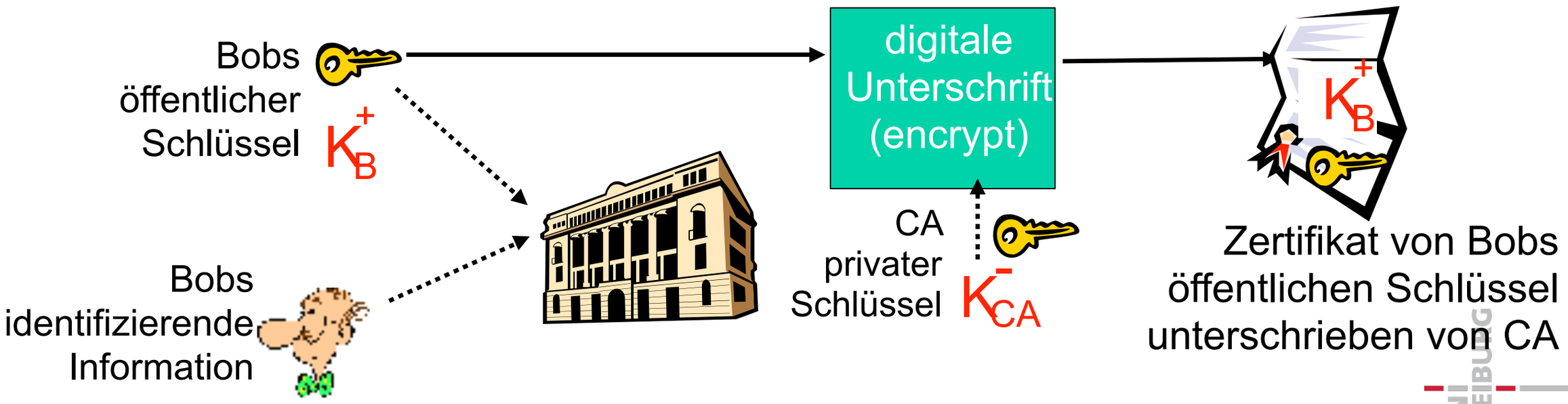
CoNe Freiburg

Public-key Zertifizierung

- Motivation: Trudy spielt Bob einen Pizza-Streich
- Problem:
  - Trudy bestellt per e-mail: „Liebe Pizzeria, schick mir bitte vier Pepperoni-Pizza. vielen Dank Bob“
  - Trudy unterschreibt mit einem privaten Schlüssel
  - Trudy sendet die Bestellung zur Pizzeria
  - Trudy sendet der Pizzeria den öffentlichen Schlüssel, behauptet aber er gehöre Bob
  - Die Pizzeria überprüft die Unterschrift
  - Aber Bob mag gar keine Pepperoni

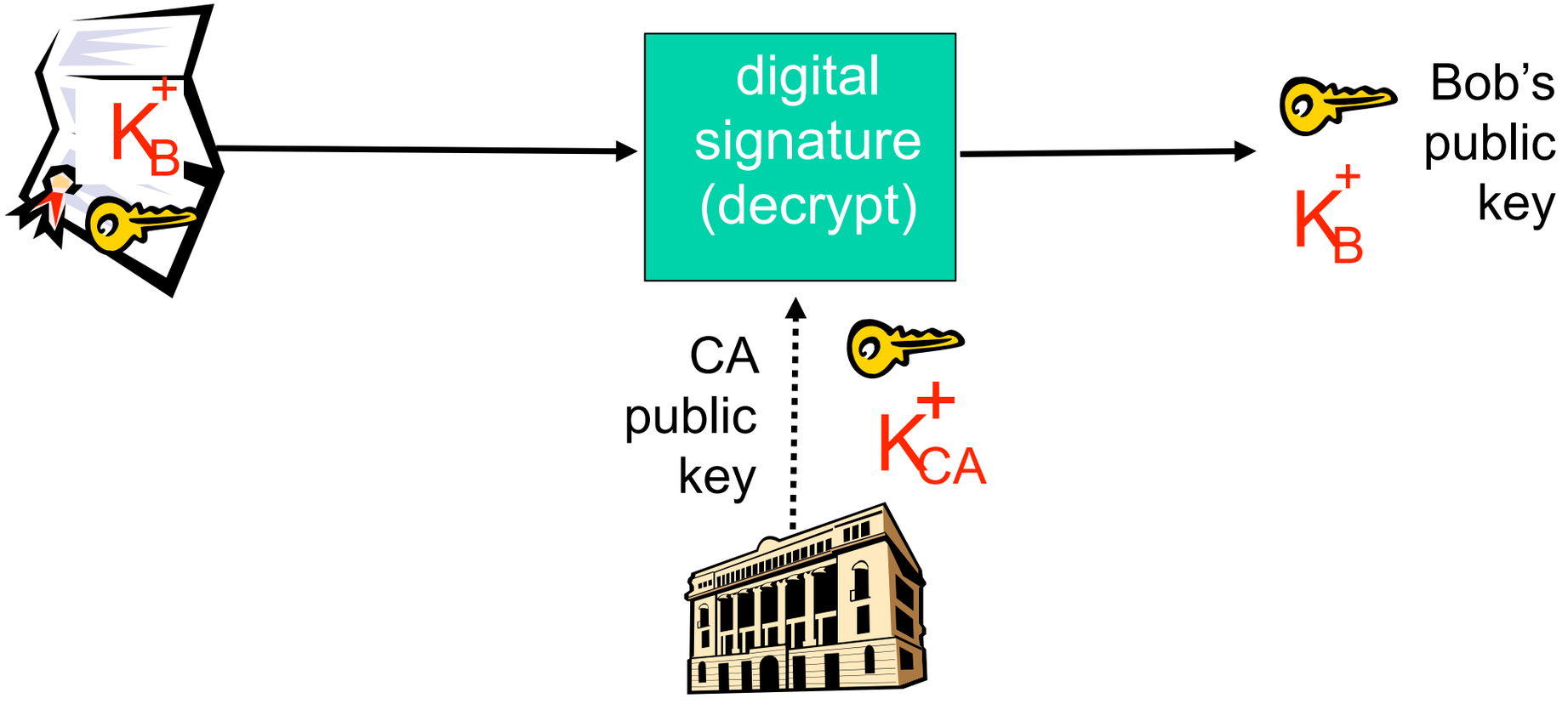
Zertifizierungsstelle
Certification Authorities (CA)

- Zertifizierungsstelle (Certification authority – CA): verknüpft öffentlichen Schlüssel mit der Entität (Person, Service, Router) E
- E registriert seinen öffentlichen Schlüssel mit CA
  - E „beweist seine Identität“ der Zertifizierungsstelle
  - CA erzeugt eine Zertifizierungsverknüpfung von E mit seinem öffentlichen Schlüssel
  - Zertifikat mit E‘s öffentlichen Schlüssel wird von der CA digital unterschrieben:
    - „Das ist der öffentliche Schlüssel von E“



Zertifizierungsstelle
Certification Authorities (CA)

- Wenn Alice Bobs öffentlichen Schlüssel möchte
  - erhält Bobs Zertifikat
  - wendet CA's öffentlichen Schlüssel auf Bobs Zertifikat an
    - Alice erhält Bobs öffentlichen Schlüssel



CoNe Freiburg

Zertifikate

- Hauptstandard X.509 (RFC 2459)
- Zertifikat enthält
  - Name des Ausstellers (Issuer name)
  - Name der Entität, Adresse, Domain-Name, etc.
  - Öffentlicher Schlüssel der Entität
  - Digitale Unterschrift (unterschrieben mit dem geheimen Schlüssel des Ausstellers)
- Public-Key Infrastruktur (PKI)
  - Zertifikate und Zertifizierungsstellen

CoNe Freiburg

SSL: Secure Sockets Layer

- Weit verbreitetes Sicherheitsprotokoll
  - Unterstützt durch alle Browser und Web-Server
  - https
  - Jährlich Transaktionen im Wert von Zigmilliarden Euro über SSL
- 1993 entworfen von Netscape
- Aktueller Name
  - TLS: transport layer security, RFC 2246
- Gewährleistet
  - Vertraulichkeit (Confidentiality)
  - Nachrichtenintegrität (Integrity)
  - Authentifizierung

UNI FREIBURG

CoNe Freiburg

SSL: Secure Sockets Layer

- Ursprüngliche Motivation
  - Web E-Commerce Transaktionen
  - Verschlüsselung (Credit-Karte)
- Web-server Authentifizierung
  - Optional Client Authentifizierung
- Kleinstmöglicher Aufwand für Einsteiger
- In allen TCP Anwendungen verfügbar
  - Secure socket interface

CoNe Freiburg

Zumeist: Symmetrische Codes

- DES – Data Encryption Standard: Block
- 3DES – Triple strength: Block
- RC2 – Rivest Cipher 2: Block
- RC4 – Rivest Cipher 4: Stream

- Auch Public-Key-Verschlüsselung
  - RSA

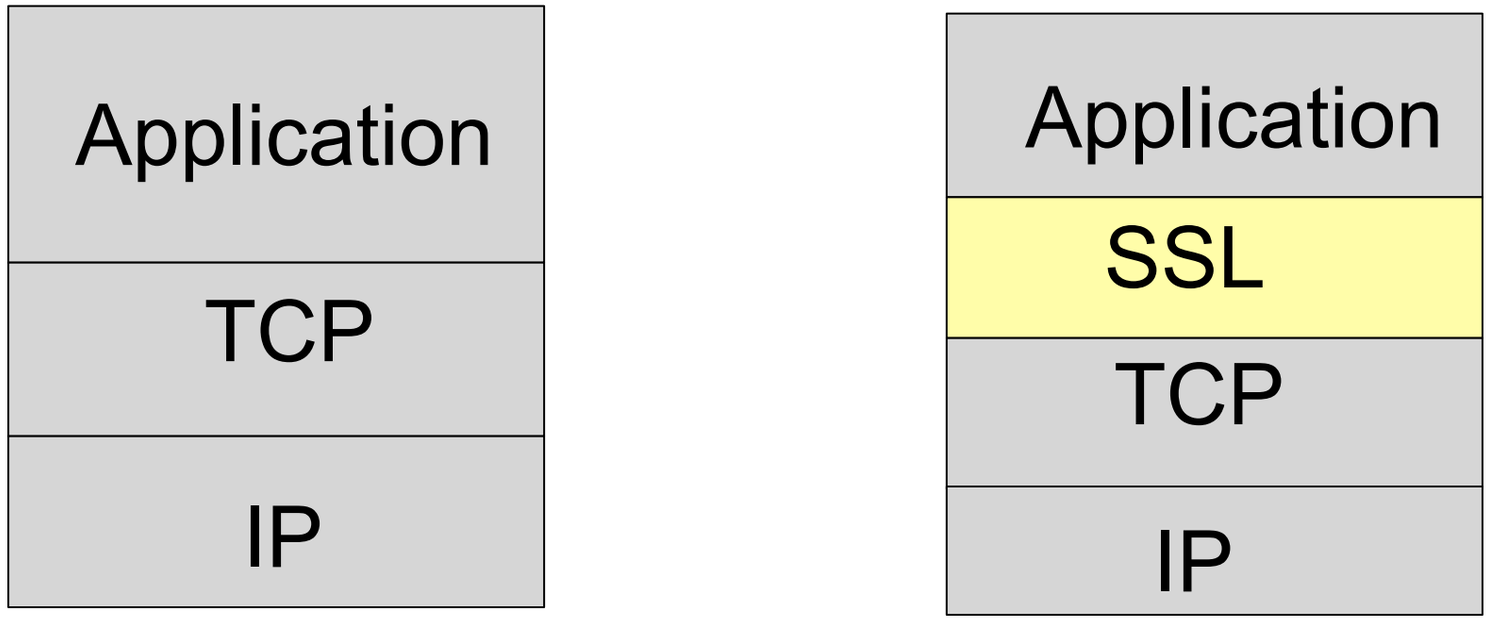
UNI FREIBURG

CoNe Freiburg

SSL Cipher Suite

- Cipher Suite
  - Public-key Algorithmus
  - Symmetrische Verschlüsselungsalgorithmus
  - MAC Algorithmus
- SSL unterstützt mehrere Kodierungsverfahren
- Verbindungsvereinbarung (Negotiation)
  - Client und Server einigen sich auf ein Kodierungsverfahren
- Client bietet eine Auswahl an
  - Server wählt davon eines

SSL and TCP/IP



Normale Anwendung

Anwendung mit SSL

- SSL stellt eine Programm-Interface für Anwendungen zur Verfügung
- C and Java SSL Bibliotheken/Klassen verfügbar

CoNe Freiburg

SSL: Handshake (1)

- Ziel
  - Server Authentifizierung
  - Verbindungsvereinbarung:
    - Einigung auf gemeinsames kryptographische Verfahren
  - Schlüsselaustausch
  - Client Authentifizierung (optional)

SSL: Handshake (2)

- Client sendet
  - Liste unterstützter Krypto-Algorithmen
  - Client nonce (salt)
- Server
  - wählt Algorithmen von der Liste
  - sendet zurück: Wahl + Zertifikat + Server Nonce
- Client
  - verifiziert Zertifikat
  - extrahiert Servers öffentlichen Schlüssel
  - erzeugt pre_master_secret verschlüsselt mit Servers öffentlichen Schlüssel
  - sendet pre_master_secret zum Server
- Client und Server
  - berechnen unabhängig die Verschlüsselungs- und MAC-Schlüssel aus pre_master_secret und Nonces
- Client sendet ein MAC von allen Handshake-Nachrichten
- Server sendet ein MAC von allen Handshake-Nachrichten

CoNe Freiburg

SSL Verbindung

handshake: ClientHello

handshake: ServerHello

handshake: Certificate

handshake: ServerHelloDone

handshake: ClientKeyExchange

ChangeCipherSpec

handshake: Finished

Ab hier ist alles verschlüselt

ChangeCipherSpec

handshake: Finished

application_data

application_data

Alert: warning, close_notify

TCP Fin folgt

CoNe Freiburg

Schlüsselherstellung

- Client Nonce, Server Nonce und pre-master secret werden in Pseudozufallsgenerator gegeben
  - Ausgabe: Master Secret
- Master Secret und neue Nonces werden in anderen Pseudozufallsgenerator mit Ausgabe: “key block”
- Key block:
  - Client MAC key
  - Server MAC key
  - Client encryption key
  - Server encryption key
  - Client initialization vector (IV)
  - Server initialization vector (IV)

UNI FREIBURG

CoNe Freiburg

Fortsetzung folgt..

- Wir werden in den Schichten des Internets noch weitere Sicherheitsprotokolle kennenlernen:
  - VPN
  - IPsec
  - WEP

Sicherheit in Rechnernetzwerken

- Spielt eine Rolle in den Schichten
  - Bitübertragungsschicht
  - Sicherungsschicht
  - Vermittlungsschicht
  - Transportschicht
  - Anwendungsschicht
- Was ist eine Bedrohung (oder ein Angriff)?
- Welche Methoden gibt es?
  - Kryptographie
- Wie wehrt man Angriffe ab?
  - Beispiel: Firewalls

CoNe Freiburg

Was ist eine Bedrohung?

- Definition:
  - Eine Bedrohung eines Rechnernetzwerks ist jedes mögliche Ereignis oder eine Folge von Aktionen, die zu einer Verletzung von Sicherheitszielen führen kann
  - Die Realisierung einer Bedrohung ist ein Angriff
- Beispiel:
  - Ein Hacker erhält Zugang zu einem geschlossenen Netzwerk
  - Veröffentlichung von durchlaufenden E-Mails
  - Fremder Zugriff zu einem Online-Bankkonto
  - Ein Hacker bringt ein System zum Absturz
  - Jemand agiert unautorisiert im Namen anderer (Identity Theft)

UNI FREIBURG

Sicherheitsziele

- Vertraulichkeit:
  - Übertragene oder gespeicherte Daten können nur vom vorbestimmten Publikum gelesen oder geschrieben werden
  - Vertraulichkeit der Identität der Teilnehmer: Anonymität
- Datenintegrität
  - Veränderungen von Daten sollten entdeckt werden
  - Der Autor von Daten sollte erkennbar sein
- Verantwortlichkeit
  - Jedem Kommunikationsereignis muss ein Verursacher zugeordnet werden können
- Verfügbarkeit
  - Dienste sollten verfügbar sein und korrekt arbeiten
- Zugriffskontrolle
  - Dienste und Informationen sollten nur autorisierten Benutzern zugänglich sein

Angriffe

- Maskierung (Masquerade)
  - Jemand gibt sich als ein anderer aus
- Abhören (Eavesdropping)
  - Jemand liest Informationen, die nicht für ihn bestimmt sind
- Zugriffsverletzung (Authorization Violation)
  - Jemand benutzt einen Dienst oder eine Resource, die nicht für ihn bestimmt ist
- Verlust oder Veränderung (übertragener) Information
  - Daten werden verändert oder zerstört
- Verleugnung der Kommunikation
  - Jemand behauptet (fälschlicherweise) nicht der Verursacher von Kommunikation zu sein
- Fälschen von Information
  - Jemand erzeugt (verändert) Nachrichten im Namen anderer
- Sabotage
  - Jede Aktion, die die Verfügbarkeit oder das korrekte Funktionieren der Dienste oder des Systems reduziert

CoNe Freiburg

Bedrohungen und Sicherheitsziele

Sicherheits-ziele	Bedrohungen						
	Mas-kierung	Abhören	Zugriffs-ver-letzung	Verlust oder Verän-derung (über-tragener) information	Verleug-nung der Kommuni-kation	Fäl-schen von Infor-mation	Sabotage (z.B. Überlast)
Vertraulichkeit	x	x	x				
Datenintegrität	x		x	x		x	
Verantwort-lichkeit	x		x		x	x	
Verfügbarkeit	x		x	x			x
Zugriffs-kontrolle	x		x			x	

Terminologie der Kommunikationssicherheit

- Sicherheitsdienst
  - Ein abstrakter Dienst, der eine Sicherheitseigenschaft zur erreichen sucht
  - Kann mit (oder ohne) Hilfe kryptografischer Algorithmen und Protokolle realisiert werden, z.B.
    - Verschlüsselung von Daten auf einer Festplatte
    - CD im Safe
- Kryptografischer Algorithmus
  - Mathematische Transformationen
  - werden in kryptografischen Protokollen verwendet
- Kryptografisches Protokoll
  - Folge von Schritten und auszutauschenden Nachrichten um ein Sicherheitsziel zu erreichen

CoNe Freiburg

Sicherheitsdienste

- Authentisierung
  - Digitale Unterschift: Das Datum ist nachweislich vom Verursacher
- Integrität
  - Sichert ab, dass ein Datum nicht unbemerkt verändert wird
- Vertraulichkeit
  - Das Datum kann nur vom Empfänger verstanden werden
- Zugriffskontrolle
  - kontrolliert, dass nur Berechtigte Zugang zu Diensten und Information besitzen
- Unleugbarkeit
  - beweist, dass die Nachricht unleugbar vom Verursacher ist

UNI FREIBURG

CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG

Systeme II

3. Sicherheit

Thomas Janson°, Kristof Van Laerhoven*, Christian Ortolf°
Folien: Christian Schindelhauer°
Technische Fakultät
°: Rechnernetze und Telematik, *: Eingebettete Systeme
Albert-Ludwigs-Universität Freiburg
Version 29.04.2015

UNI FREIBURG