Betriebssysteme und Sicherheit

Signatursysteme

WS 2012/2012

Dr.-Ing. Elke Franz
Elke.Franz@tu-dresden.de

Überblick

1 Prinzip digitaler Signatursysteme

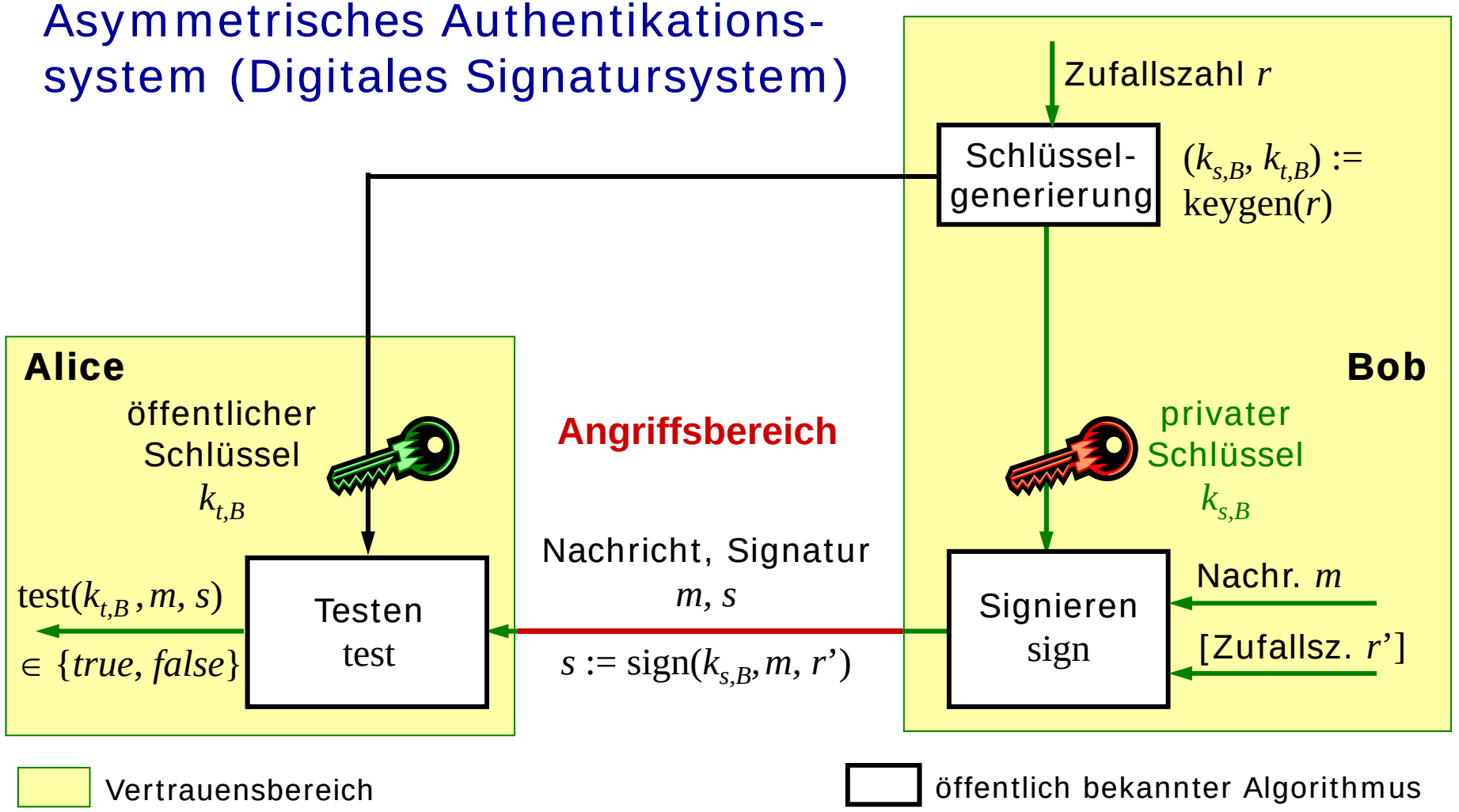
2 Vergleich symmetrische / asymmetrische Authentikation

3 Schlüsselzertifikate

4 Regelungen zum Einsatz digitaler Signaturen

5 Beispiel: RSA als Signatursystem

Asymmetrisches Authentikations-system (Digitales Signatursystem)



2 Vergleich symmetrische / asymmetrische Authentikation

	Symmetrische Authentikationssysteme (MAC)	Asymmetrische Authentikationssysteme (Digitale Signatursysteme)
Schlüssel	Geheimer Schlüssel, einem Paar von Kommunikationspartner zugeordnet	Schlüsselpaar: privater Signaturschlüssel und öffentlicher Testschlüssel
Prüfung	MAC für empfangene Daten berechnen und mit empfangenem MAC vergleichen	Testalgorithmus erforderlich
Schutzziele	Integrität	Integrität Zurechenbarkeit

Anforderungen an die Schlüssel

- Direkter Schlüsselaustausch nicht ausreichend für Zurechenbarkeit

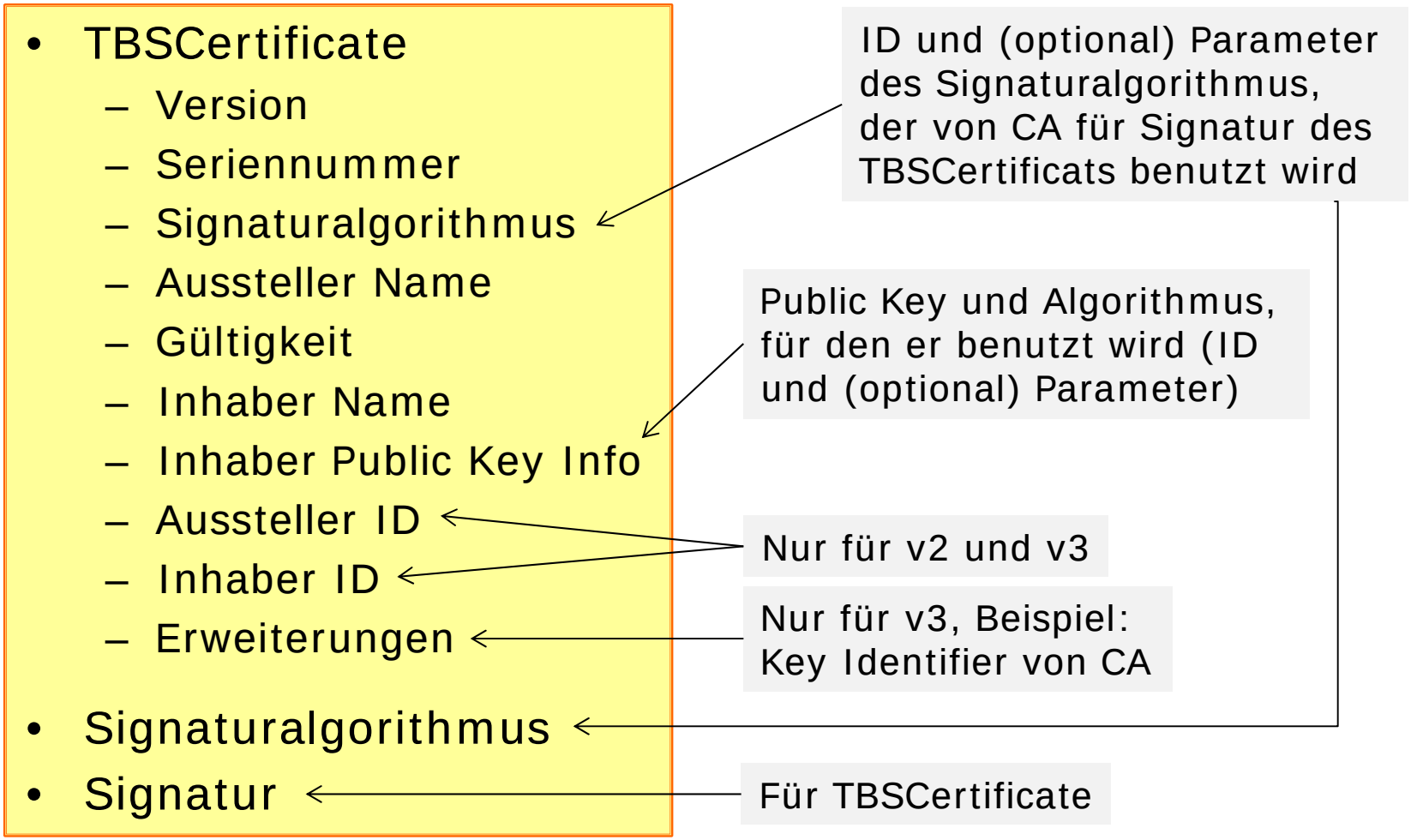
- Notwendig für Zurechenbarkeit:

  Bestätigung der Zuordnung des öffentlichen Testschlüssels zum jeweiligen Teilnehmer mittels Schlüsselzertifikat, ausgestellt von Zertifizierungsinstanz (*certification authority CA*)

- Verbreitetes Format für Schlüsselzertifikat: X.509
  - Erstmals 1988 veröffentlicht, aktuell in Version 3 (X.509v3)
  - Standard der ITU-T für Public-Key Infrastructure:
    http://www.itu.int/rec/T-REC-X.509
  - RFC 5280
  - Sperrlisten für Zertifikate

3 Schlüsselzertifikate

- Aufbau eines X.509-Zertifikats [RFC 5280]



Notwendige Rahmenbedingungen

- Rechtliche Regelungen für Anerkennung digitaler Signaturen notwendig
- EU Richtlinie 1999/93/EG
- Deutschland:
  - Signaturgesetz (SigG)
    - Fassung vom 16.05.2001, letzte Änderung am 17.7.2009
    - Schaffung von Rahmenbedingungen für den Einsatz elektronischer Signaturen
    - Anforderungen an Zertifizierungsdiensteanbieter, Produkte für qualifizierte elektronische Signaturen, Prüf- und Bestätigungsstellen
  - Signaturverordnung (SigV)
    - Fassung vom 16.11.2001, letzte Änderung am 15.11.2010
    - Ergänzende Einzelregelungen

Elektronische Signaturen entsprechend SigG

- Elektronische Signaturen
  - Daten in elektronischer Form, die anderen elektronische Daten beigefügt sind und zur Authentifizierung dienen
- Fortgeschrittene elektronische Signaturen

  Zusätzliche Forderungen:
  - ausschließlich dem Signaturschlüssel-Inhaber zugeordnet
  - können nur mit Mitteln erzeugt werden, die unter seiner Kontrolle sind
  - ermöglichen die Identifizierung des Signaturschlüsselinhabers
  - nachträgliche Änderungen der Daten erkennbar
- Qualifizierte elektronische Signaturen

  Zusätzliche Forderungen:
  - Erstellung basierend auf gültigem qualifizierten Zertifikat
  - Erzeugt mit sicherer Signaturerstellungseinheit

4 Regelungen zum Einsatz digitaler Signaturen

- Elektronische Signaturen könnten auch gescannte Unterschriften sein
- Digitale Signatursysteme für fortgeschrittene und qualifizierte elektronische Signaturen erforderlich
- Qualifizierte elektronische Signaturen entsprechen herkömmlichen Signaturen in der elektronischen Welt

- Zuständige Behörde in Deutschland: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
  http://www.bundesnetzagentur.de/
  - Beaufsichtigung der notwendigen Infrastruktur
  - Beaufsichtigung der Zertifizierungsdiensteanbieter
  - Akkreditierung (Gütezeichen)
  - Wurzelzertifikat
  - Übersicht geeigneter Algorithmen und zugehöriger Parametern für Schlüsselerzeugung, zum Hashen und für Erzeugung und Prüfung von Signaturen

4 Regelungen zum Einsatz digitaler Signaturen

- Geeignete Algorithmen für Erzeugen und Prüfen von digitalen Signaturen

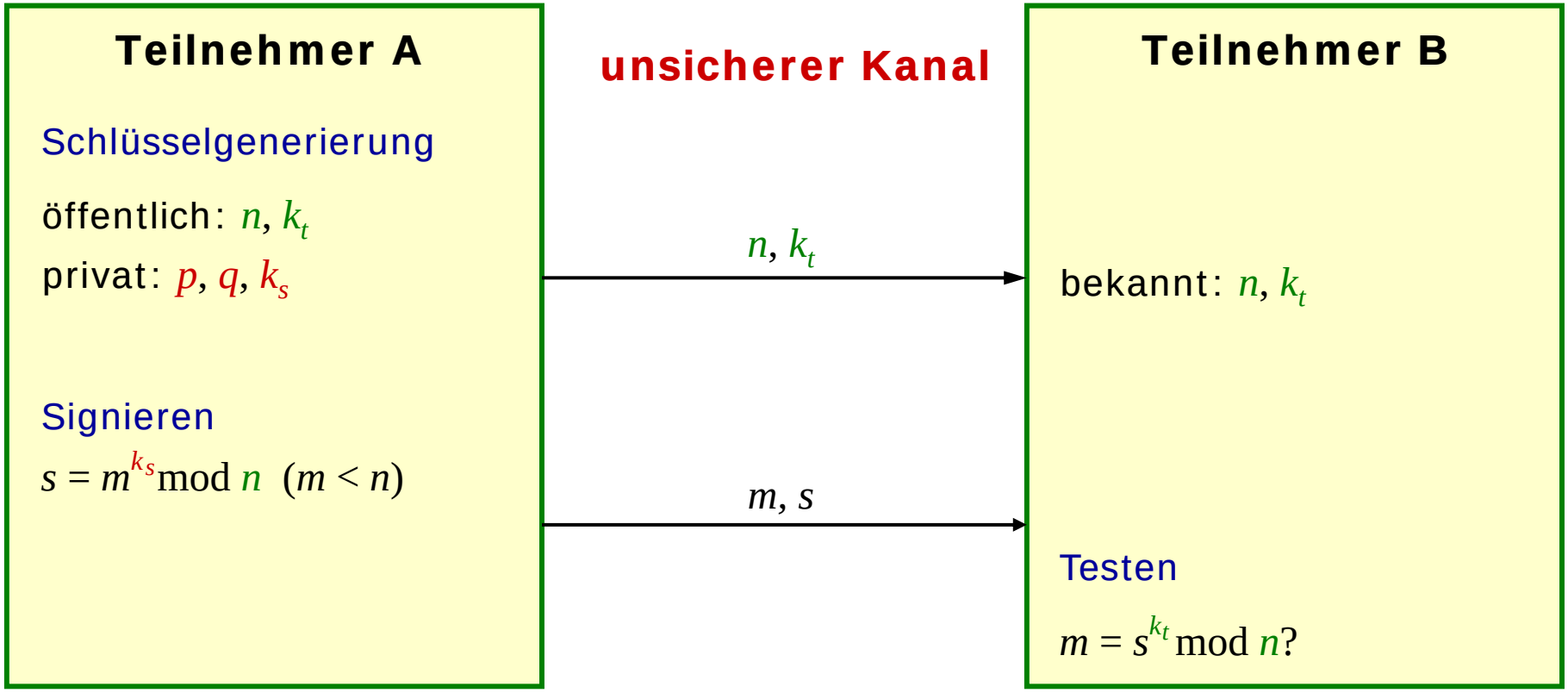
  (veröffentlicht von der Bundesnetzagentur am 18.1.2012 im Bundesanzeiger Nr. 10, Seite 243)

  – RSA
    - Anforderungen an Parameter n bis Ende 2018:

      Mindestlänge 1976 Bit,

      Empfohlene Länge 2048 Bit
  – DSA
  – DSA-Varianten, basierend auf elliptischen Kurven:
    - EC-DSA
    - EC-KDSA, EC-GDSA
    - Nyberg-Rueppel-Signaturen

RSA als Signatursystem (unsichere Variante)



5 Beispiel: RSA als Signatursystem

- Passive Angriffe auf RSA als Signatursystem
  - Angreifer: Wahl einer Signatur, Berechnung der zugehörigen Nachricht mit $m = s^{k_t} \bmod n$
  - Existentielles Brechen damit möglich
  - Forderung: sinnvolle Texte dürfen sich nur mit sehr geringer Wahrscheinlichkeit ergeben
  - Angriff wird zusätzlich erschwert durch Verwendung einer Hashfunktion (zur Verhinderung aktiver Angriffe)

5 Beispiel: RSA als Signatursystem

Aktive Angriffe

- Grundlage: RSA ist Homomorphismus bzgl. Multiplikation
- Angreifer
  - beobachtet Signaturen s_1, s_2 für Nachrichten m_1, m_2
  - berechnet Signatur $s_3 = s_1 s_2 \bmod n$ für Nachricht $m_3 = m_1 m_2 \bmod n$ (m_3 jedoch nicht frei wählbar)

Aktiver Angriff von Davida (selektiv)

- Ziel: Signatur für *gewählte* Nachricht m_3
- Angreifer
  - wählt m_1 und berechnet $m_1^{-1} \bmod n$
  - berechnet $m_2 = m_3 m_1^{-1} \bmod n$
  - lässt m_1 und m_2 signieren → erhält s_1, s_2
  - berechnet $s_3 = s_1 s_2 \bmod n$

5 Beispiel: RSA als Signatursystem

Verbesserter aktiver Angriff von Moore (selektiv)

- Ziel: Signatur für *gewählte* Nachricht m_2
- Angreifer
  - wählt $r \in Z_n^*$, berechnet $r^{-1} \bmod n$
  - berechnet $m_1 = m_2 r^{k_t} \bmod n$
  - lässt m_1 signieren → erhält s_1
  - berechnet $s_2 = s_1 r^{-1} \bmod n$

- Anwendung der Angriffe auf RSA als Konzelationssystem möglich

5 Beispiel: RSA als Signatursystem

Anmerkung: Blinde Signaturen mit RSA

- Ausnutzen des Angriffs von Moore
- Empfänger der Signatur möchte Text unterschreiben lassen, ohne dass der Signierer den Text erfährt
- Anwendung z.B. für digitale Zahlungssysteme

- Ziel: blinde Signatur für Nachricht m_2
- Teilnehmer
  - wählt $r \in Z_n^*$, berechnet $r^{-1} \bmod n$
  - „blendet“ m_2 durch Multiplikation mit r^{k_t}: $m_1 = m_2 r^{k_t} \bmod n$
  - lässt m_1 signieren → erhält s_1
  - berechnet $s_2 = s_1 r^{-1} \bmod n$