Lehrstuhl für
Systemsicherheit

Trusted Channels und ihre Anwendungen

Prof. Dr.-Ing. Ahmad-Reza Sadeghi
& **Marcel Winandy**

Ruhr-Universität Bochum
Horst Görtz Institut für IT-Sicherheit
Lehrstuhl für Systemsicherheit
www.trust.rub.de

Sichere Kommunikation in offenen Netzen

- Dokumentenzugriff im Intra-/Extranet
- e-Commerce, Online-Banking (Eingabe von Passwörtern)
- Migrieren von kryptographischen Schlüsseln (Virtual Data Center)

Sichere Kommunikation in offenen Netzen

- Verschlüsselung der Datenübermittlung
  - TLS/SSL
  - IPSec

- Aber:
  - Spyware, Keylogger
  - Transaktionsgeneratoren

- Lösung dagegen: Trusted Channels

Agenda

- Was ist ein Trusted Channel?
- Security Kernel basierte Realisierung
- Anwendungen von Trusted Channels

Was ist ein Trusted Channel?

„Versagen“ von verschlüsselter Kommunikation

Secure Channel

Schutz der Vertraulichkeit und Integrität der **Daten**

Annahme:

Derjenige, der den Schlüssel kennt, ist der rechtmäßige Empfänger

„Versagen“ von verschlüsselter Kommunikation

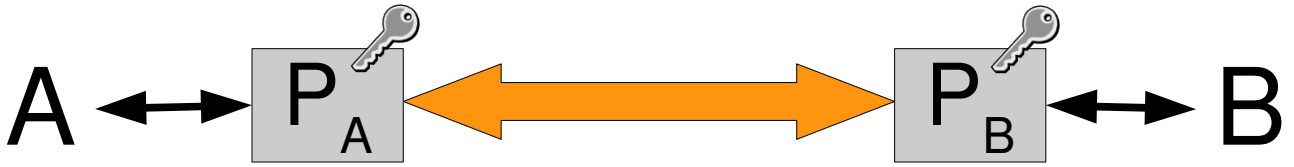
Secure Channel

Schutz der Vertraulichkeit und Integrität der **Daten**

Annahme:

Derjenige, der den Schlüssel kennt, ist der rechtmäßige Empfänger

ABER: Nicht Alice und Bob kommunizieren direkt,
sondern über die Programme auf ihren jeweiligen Computern!



„Versagen“ von verschlüsselter Kommunikation

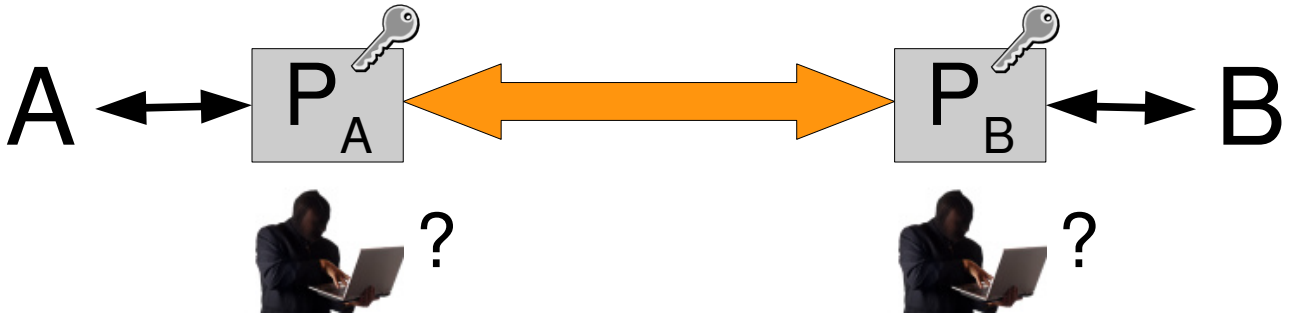
Secure Channel

Schutz der Vertraulichkeit und Integrität der **Daten**

Annahme:

Derjenige, der den Schlüssel kennt, ist der rechtmäßige Empfänger

ABER: Nicht Alice und Bob kommunizieren direkt,
sondern über die Programme auf ihren jeweiligen Computern!



Ausweg: Trusted Channels

Trusted Channel

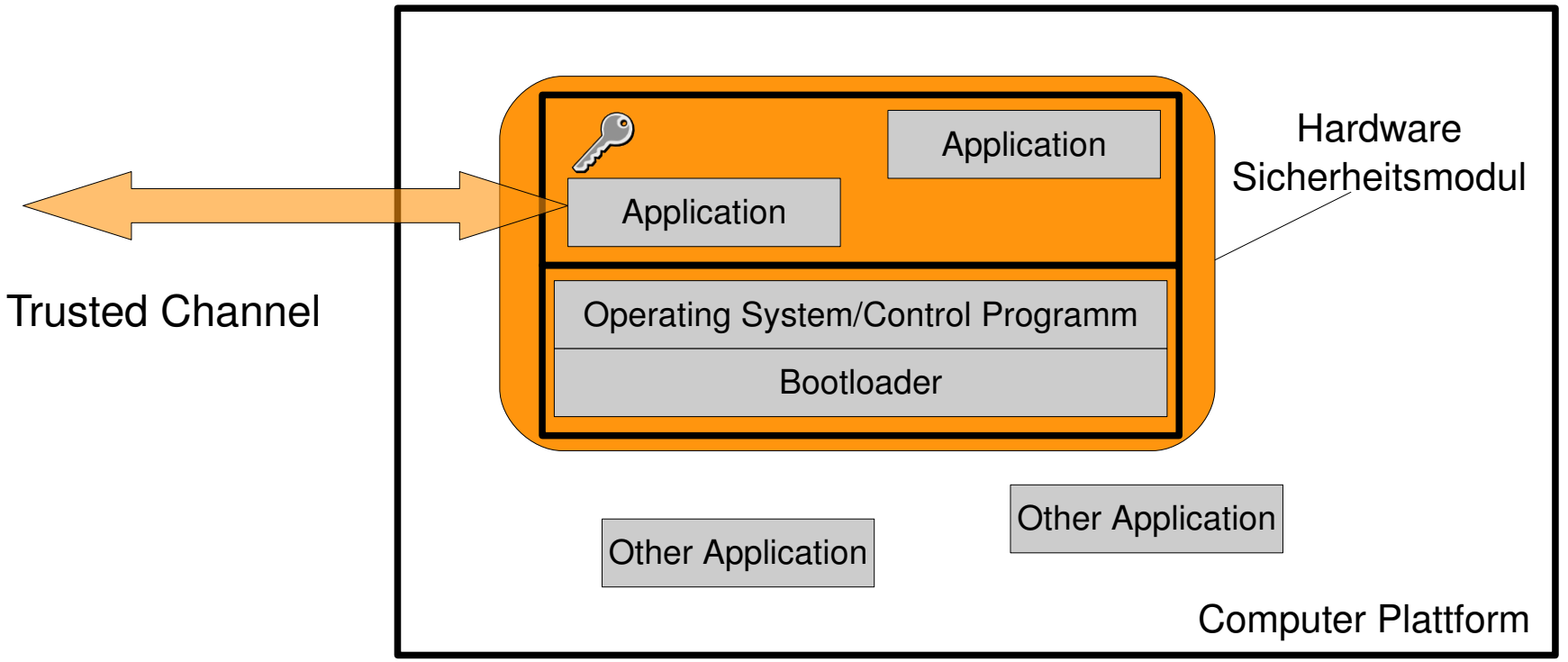
Schutz der Vertraulichkeit und Integrität der **Daten** unter Einbeziehung von **Integritätsinformationen der Endpunkte**

Annahme:

Derjenige, der den Schlüssel kennt und ihn in einer vertrauenswürdigen Ausführungsumgebung speichert und verarbeitet, ist der rechtmäßige Empfänger

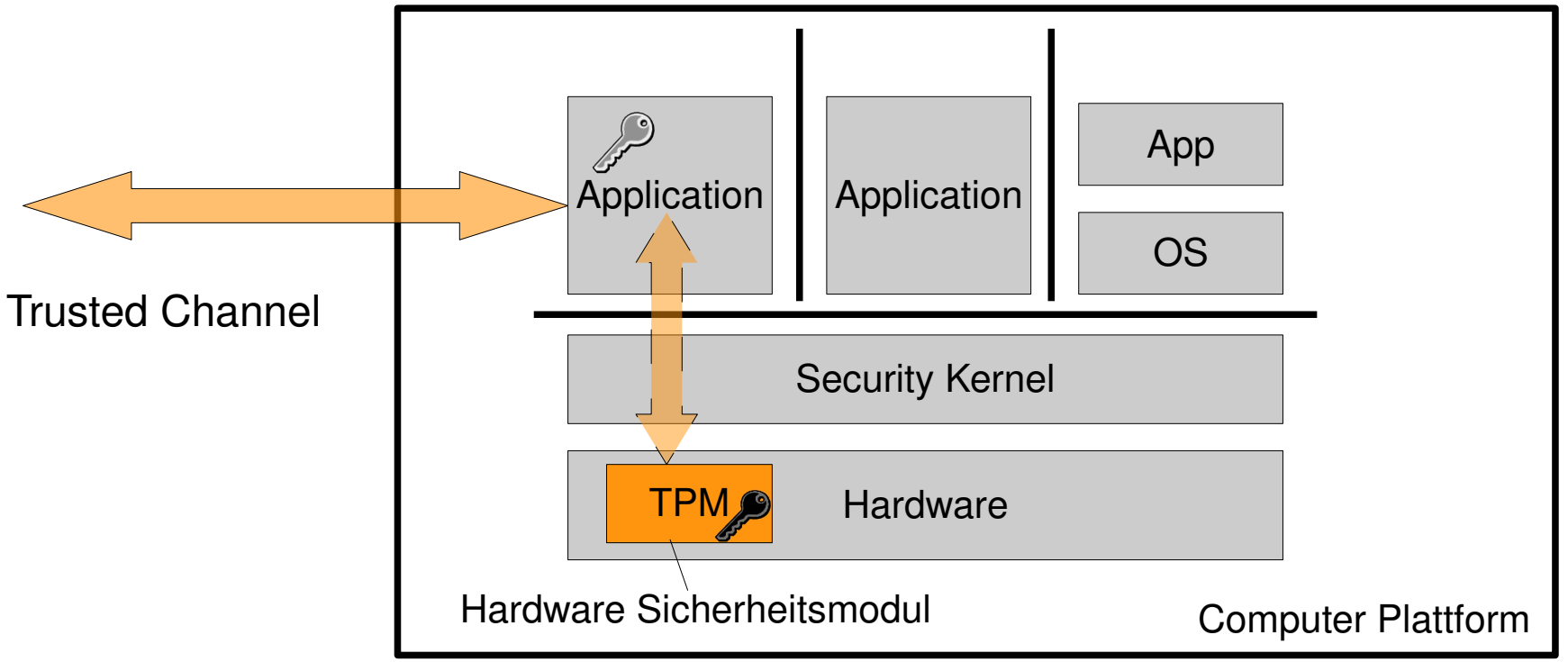
Realisierungsprinzipien (1)

- Secure Coprocessor [z.B. IBM 4758 sowie Smith et al.]
  - Impliziter Trusted Channel
  - Sehr hohe Sicherheit, aber teuer



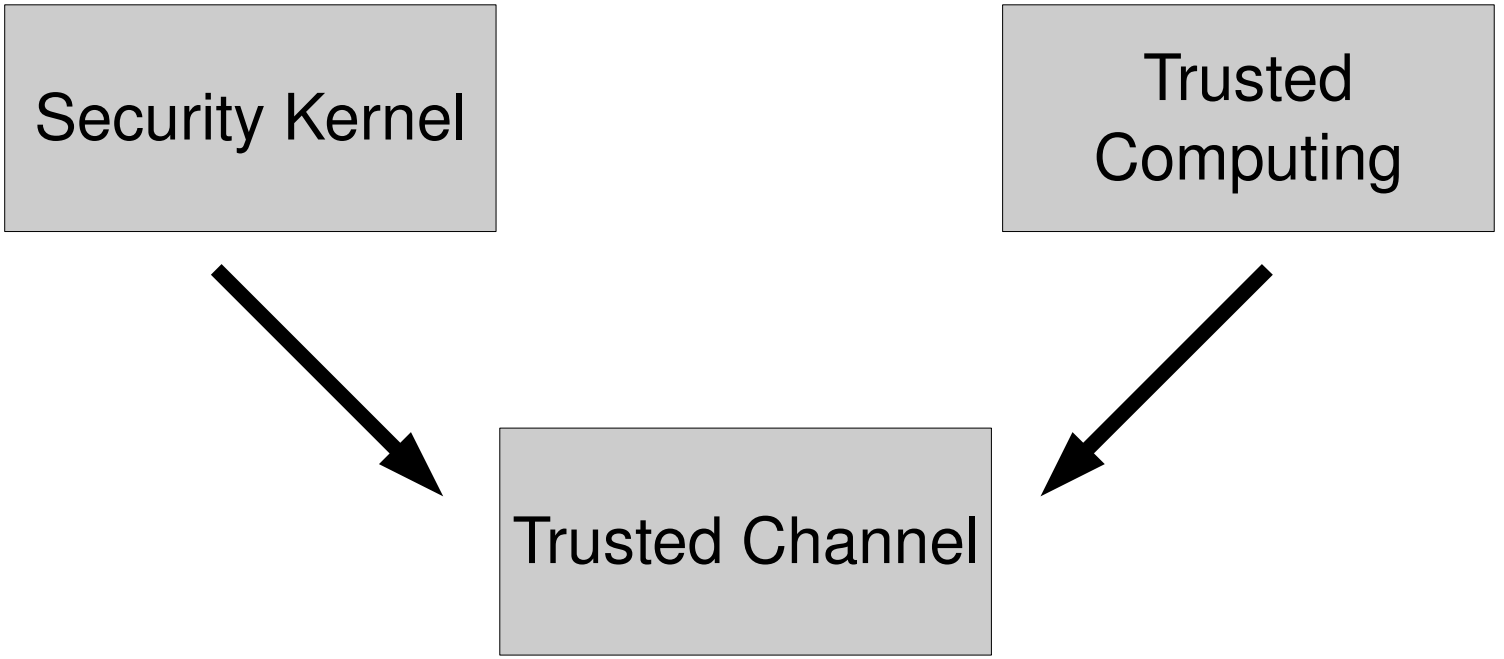
Realisierungsprinzipien (2)

- Security Kernel + Trusted Computing [z.B. Turaya]
  - Expliziter Trusted Channel
  - Mittlere/hohe Sicherheit, COTS möglich

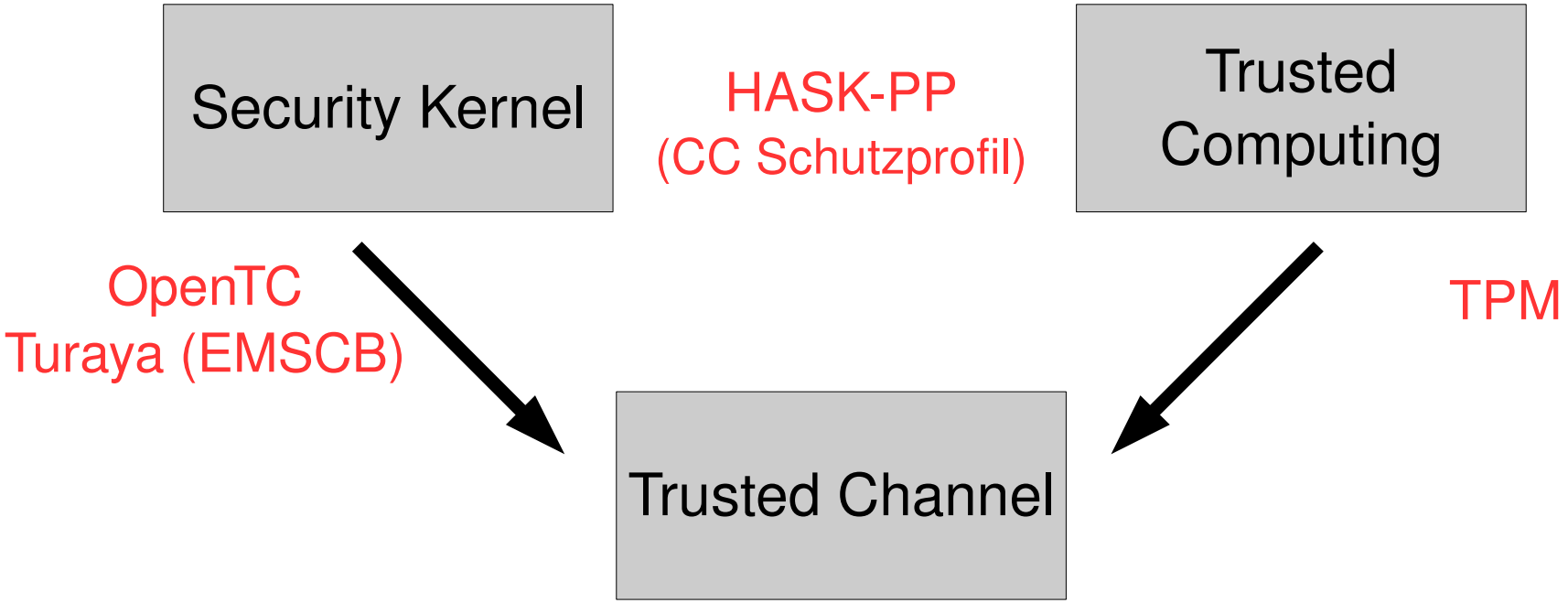


Security Kernel basierte Realisierung

Überblick



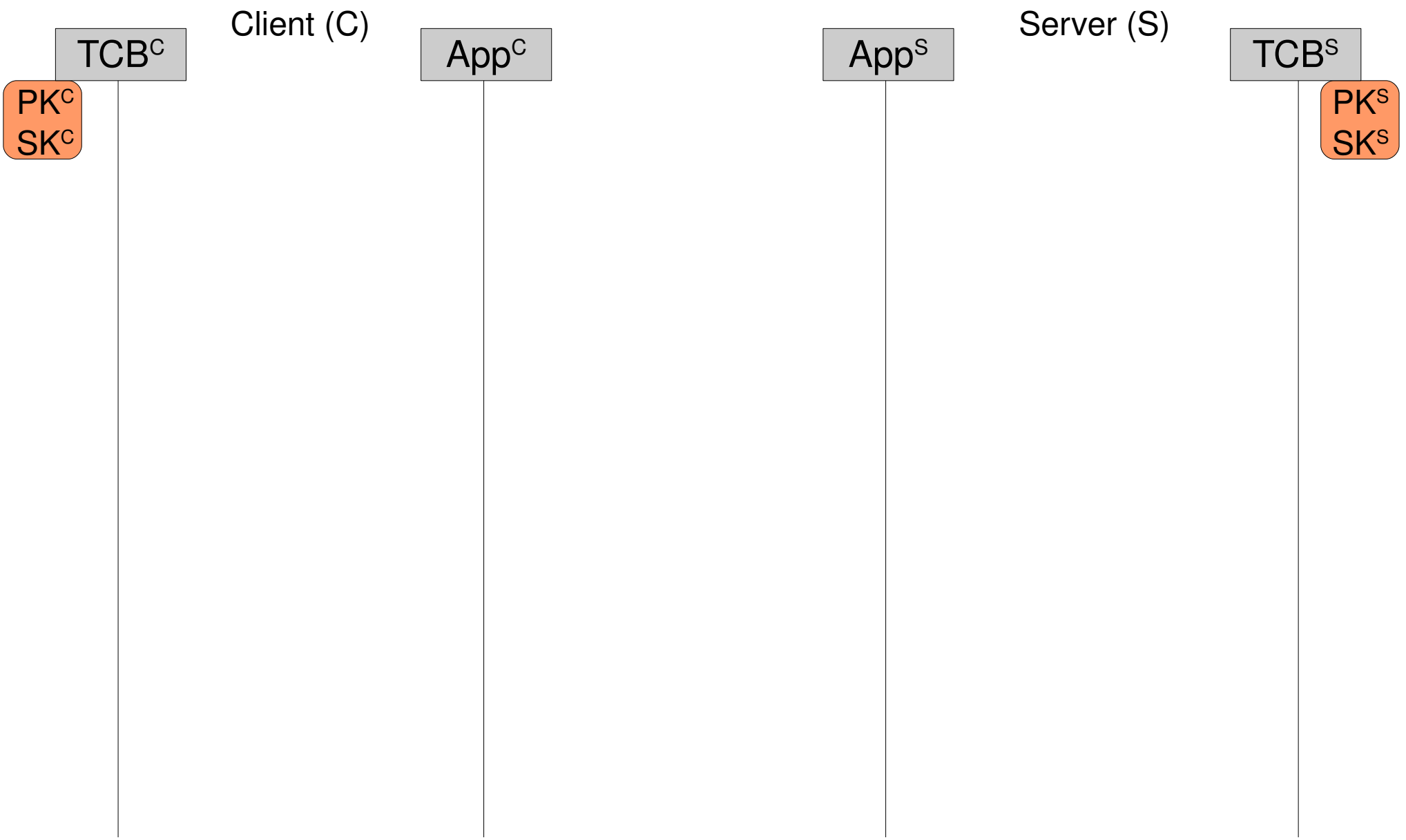
Überblick



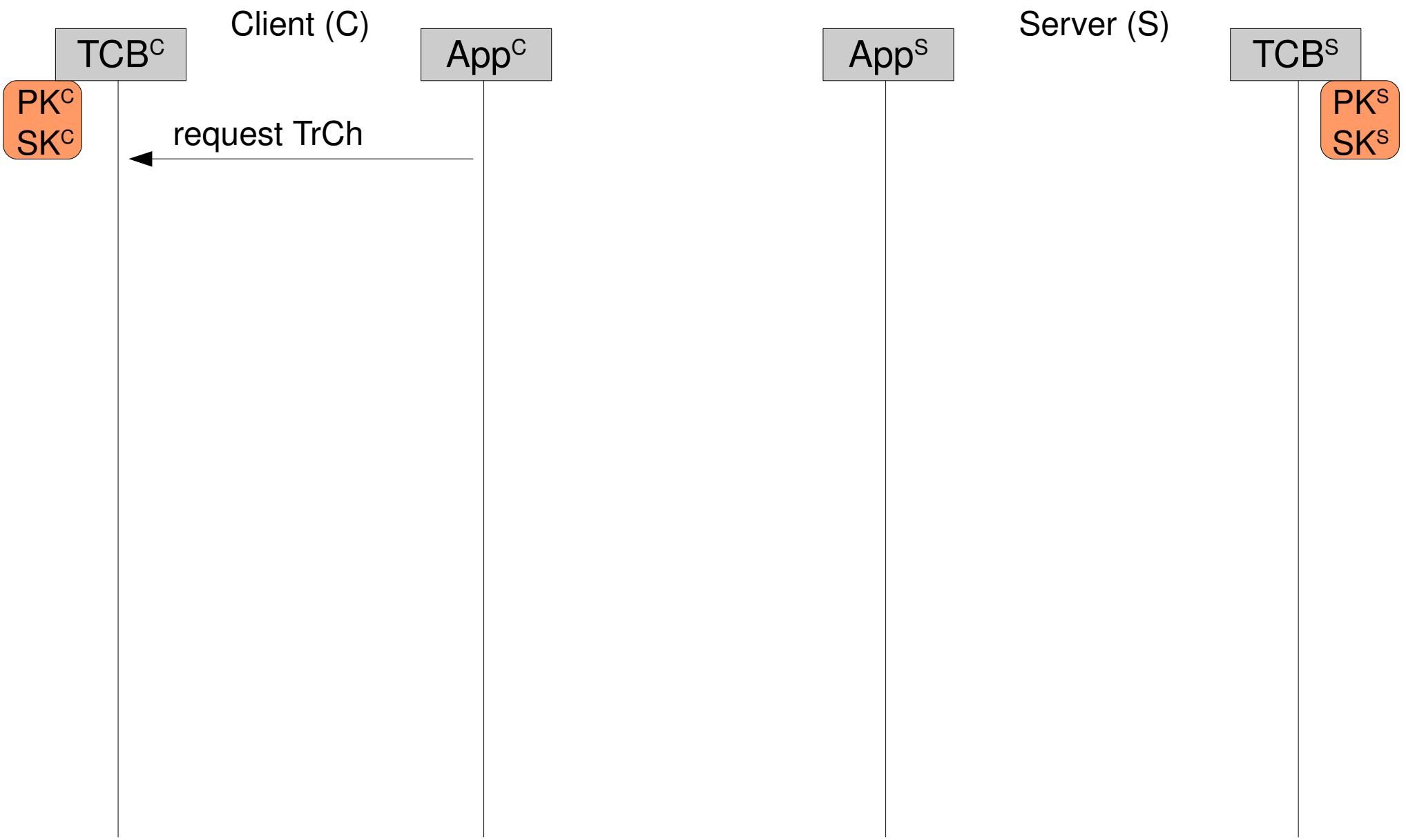
Komponenten und Protokolle

Veröffentlichungen auf internationalen Konferenzen und Workshops
(z.B. WATC 2006, ISC 2007, STC 2007, STC 2008)

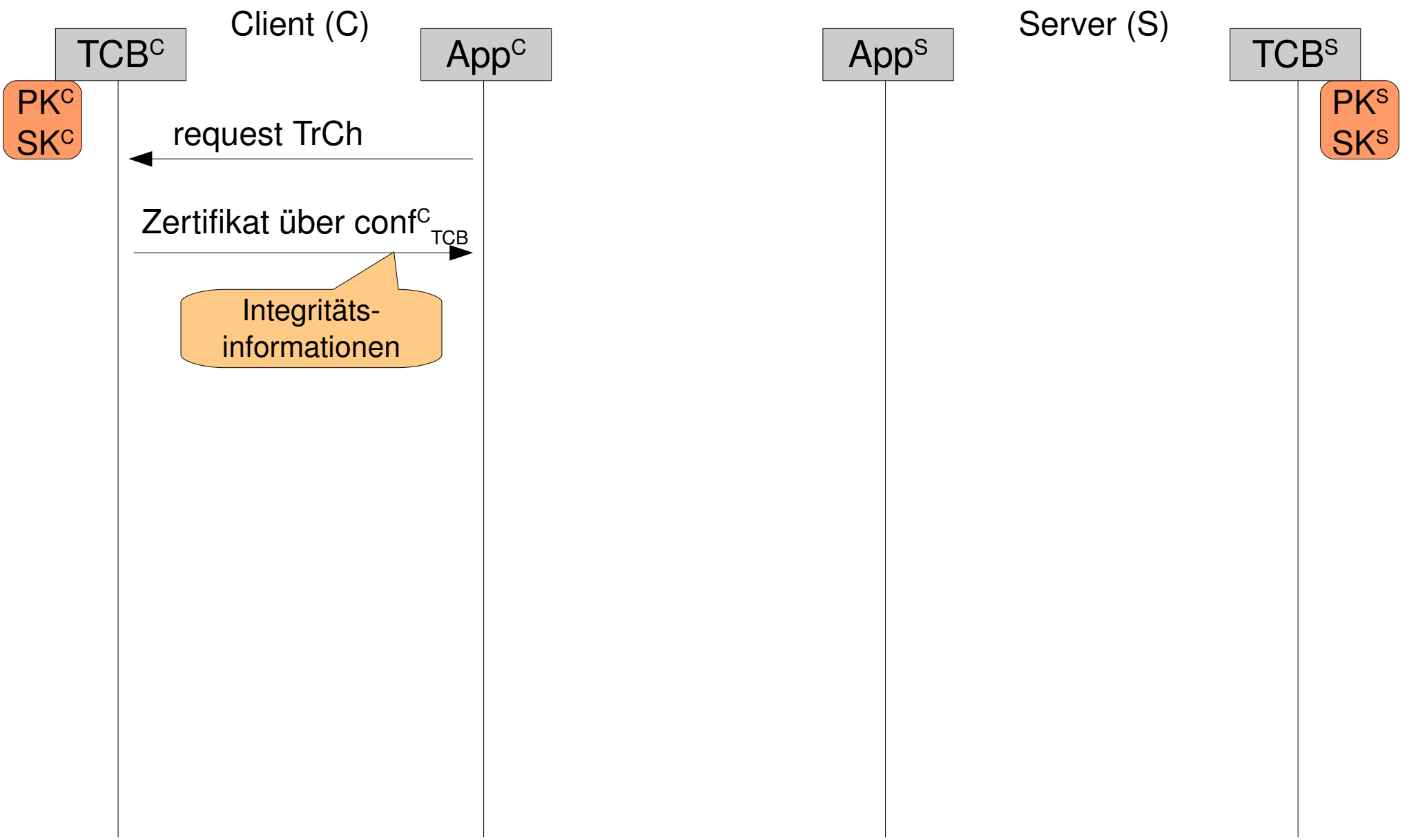
Generisches Trusted Channel Protokoll



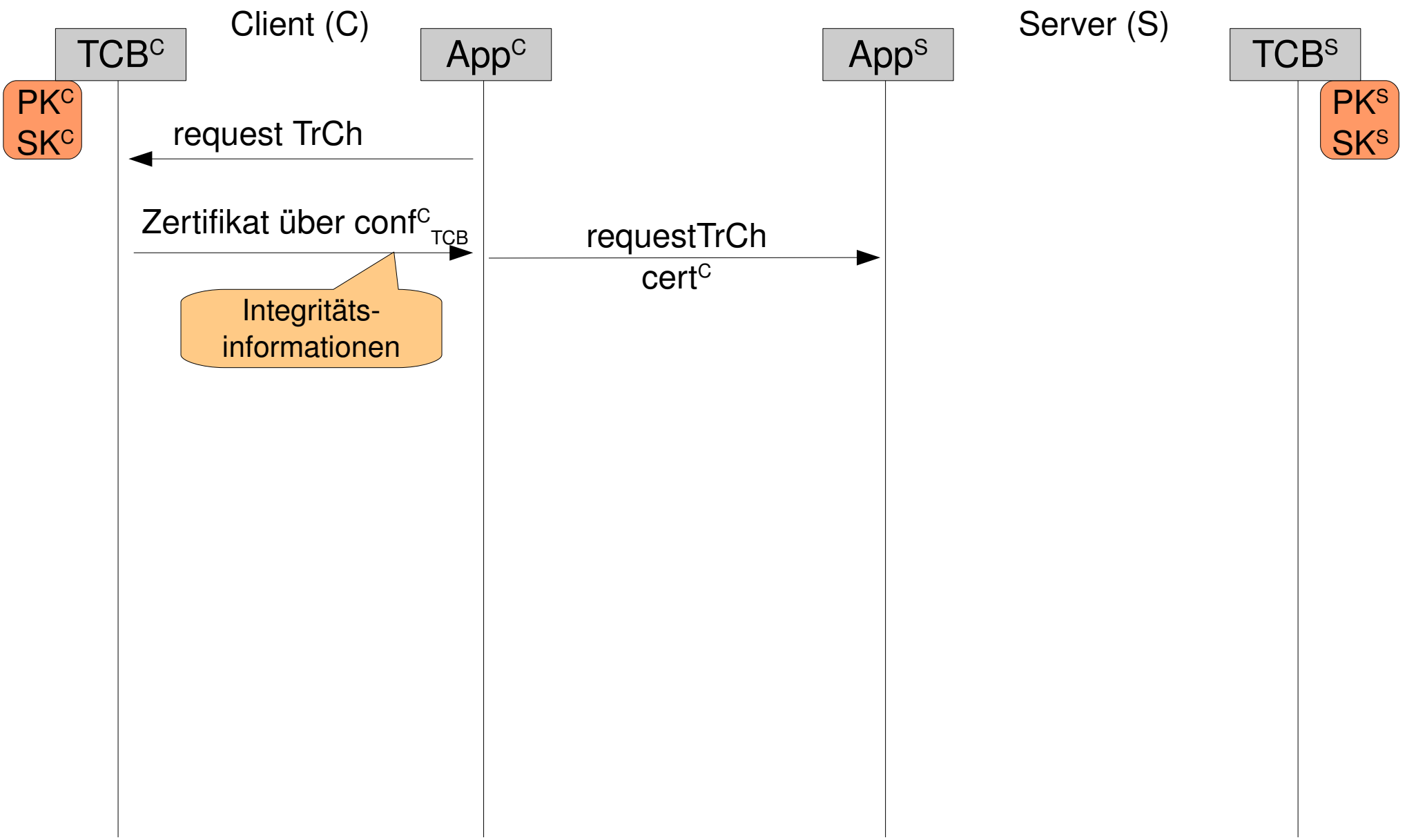
Generisches Trusted Channel Protokoll



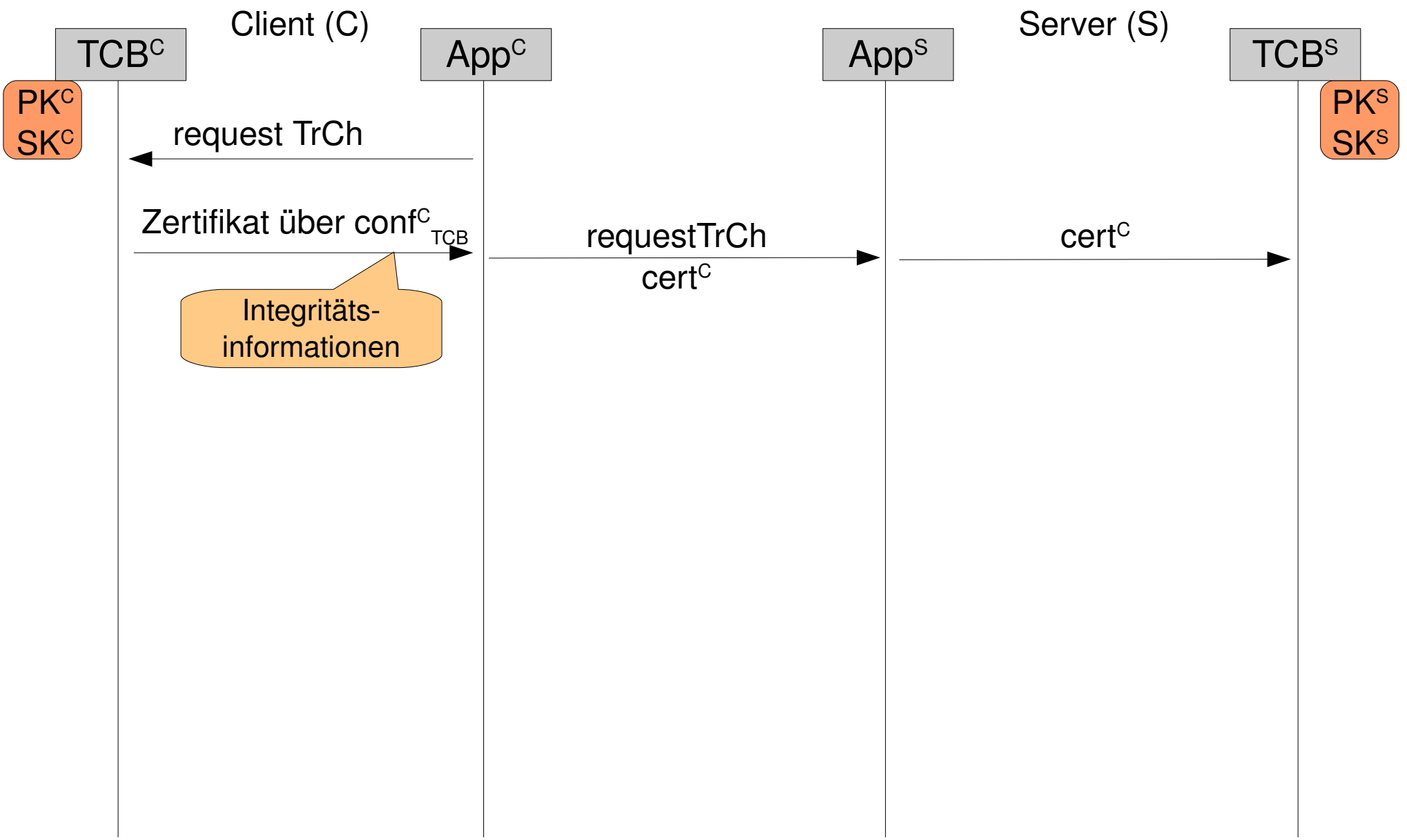
Generisches Trusted Channel Protokoll



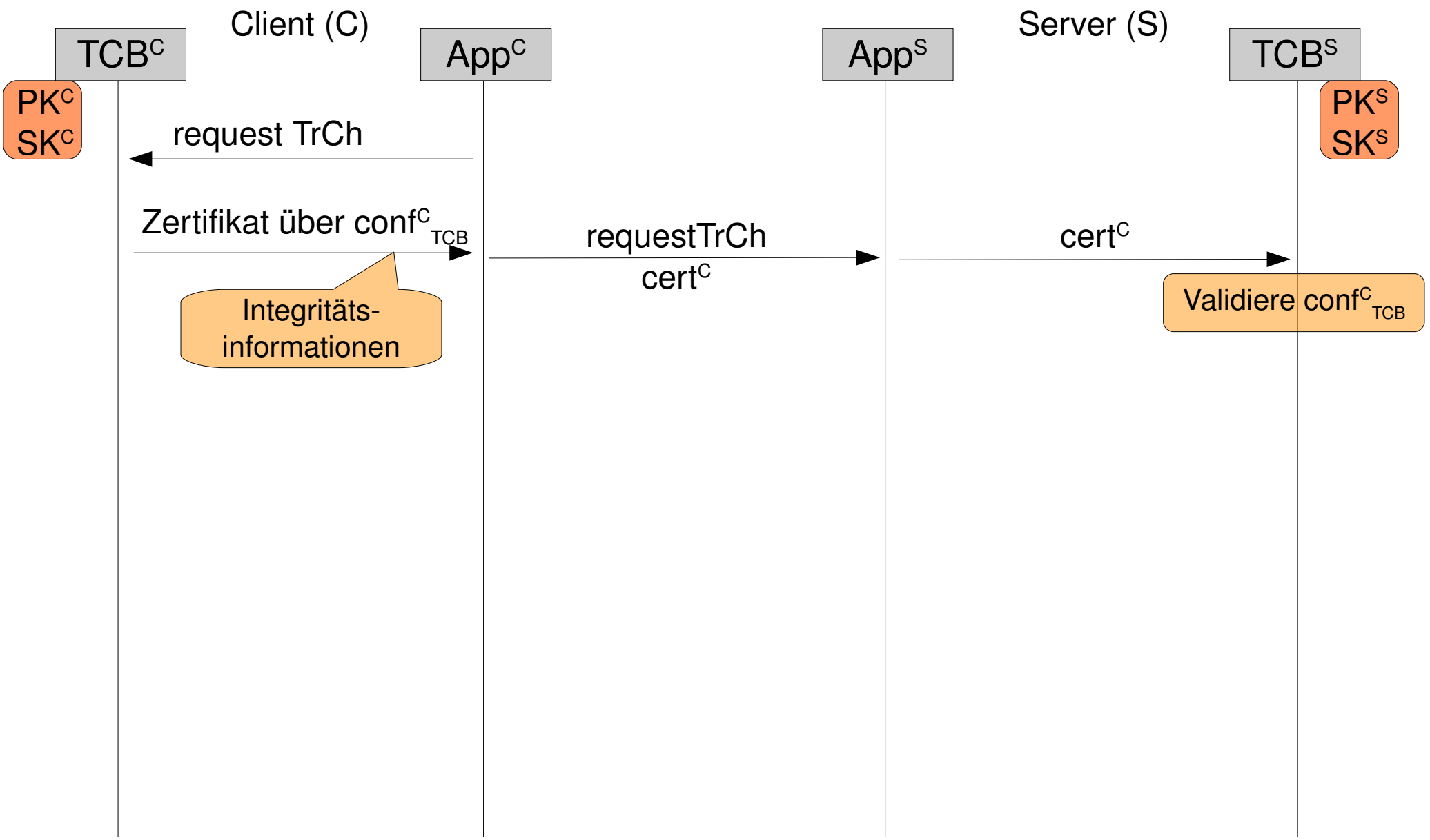
Generisches Trusted Channel Protokoll



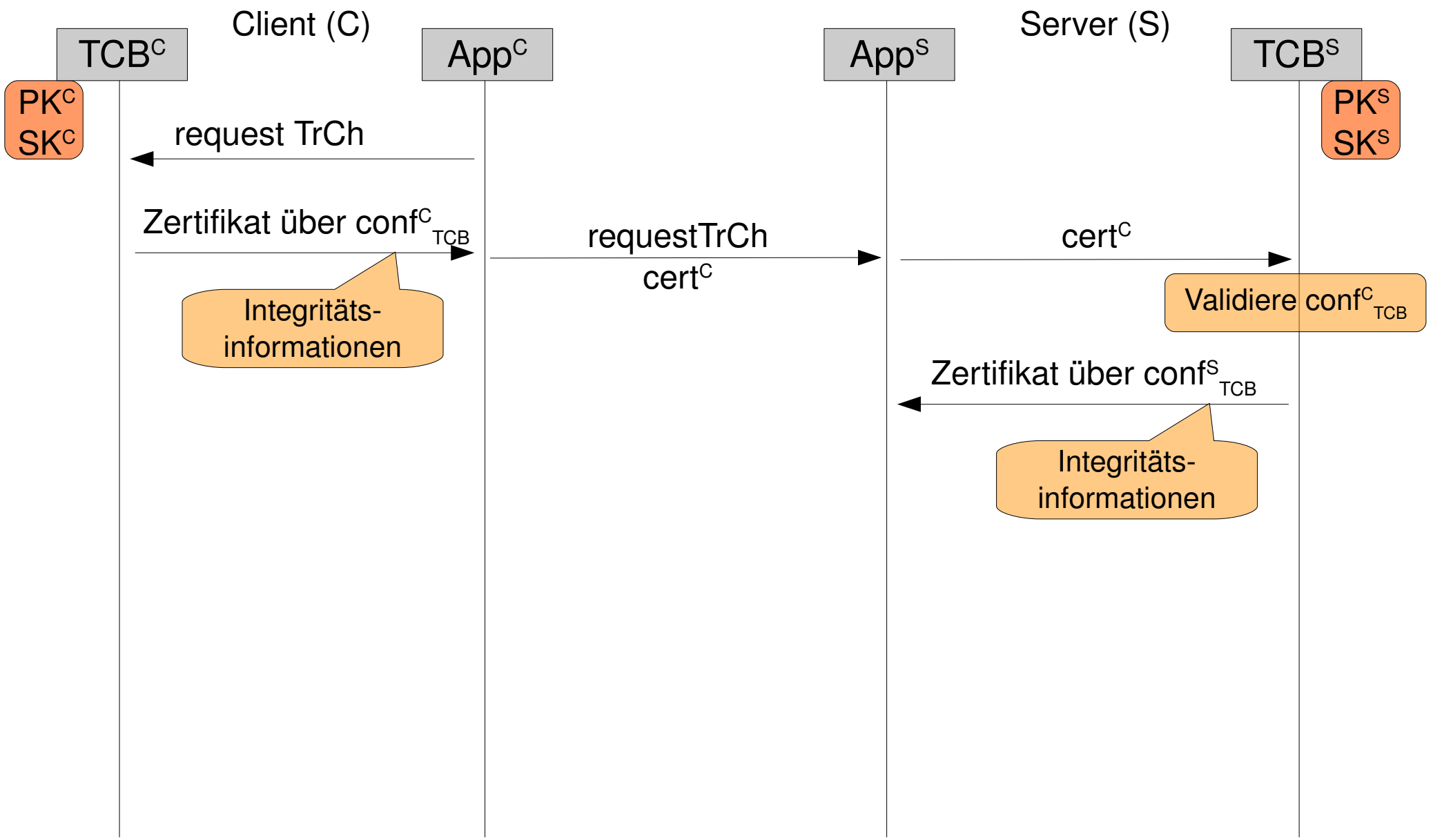
Generisches Trusted Channel Protokoll



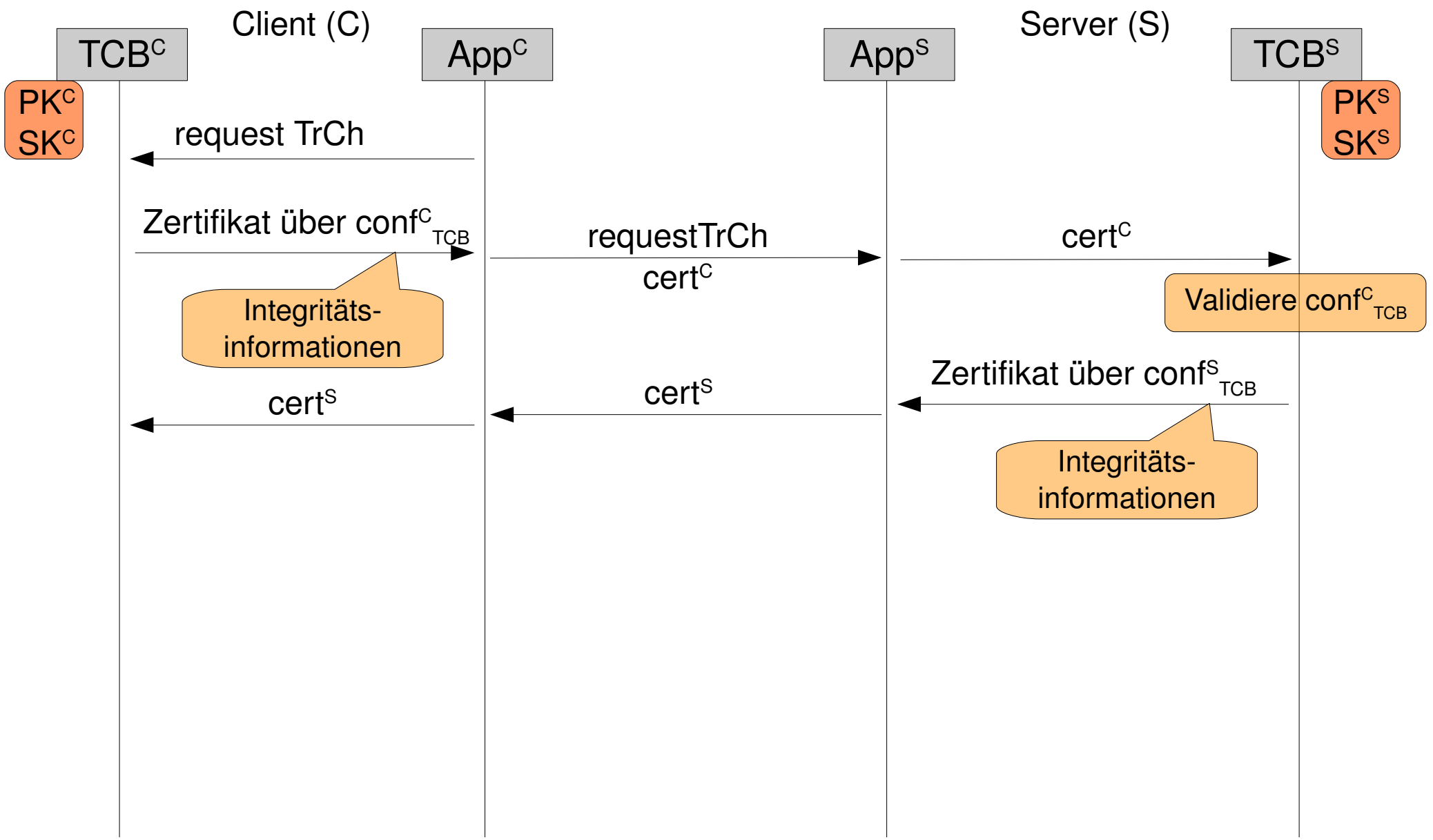
Generisches Trusted Channel Protokoll



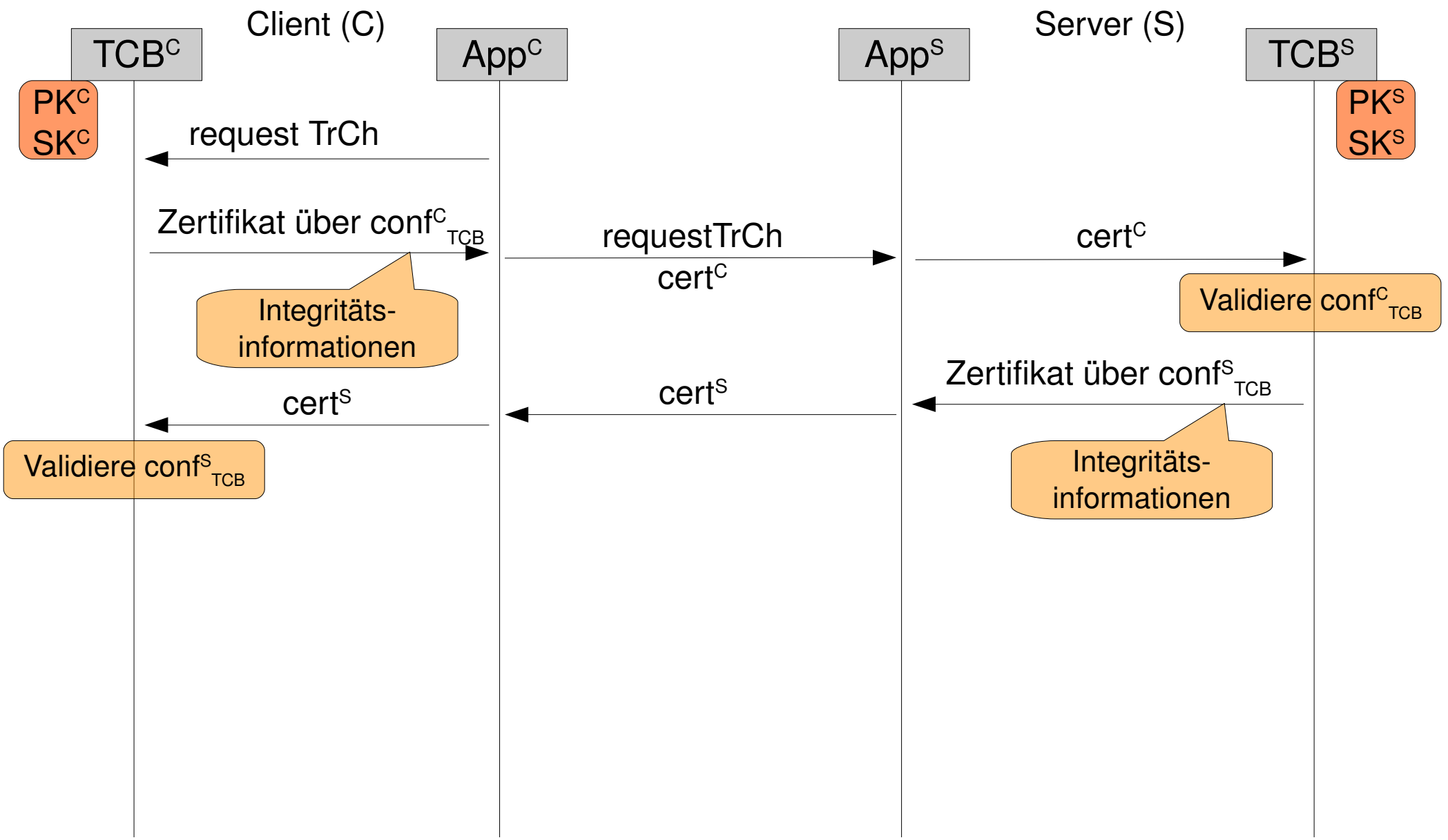
Generisches Trusted Channel Protokoll



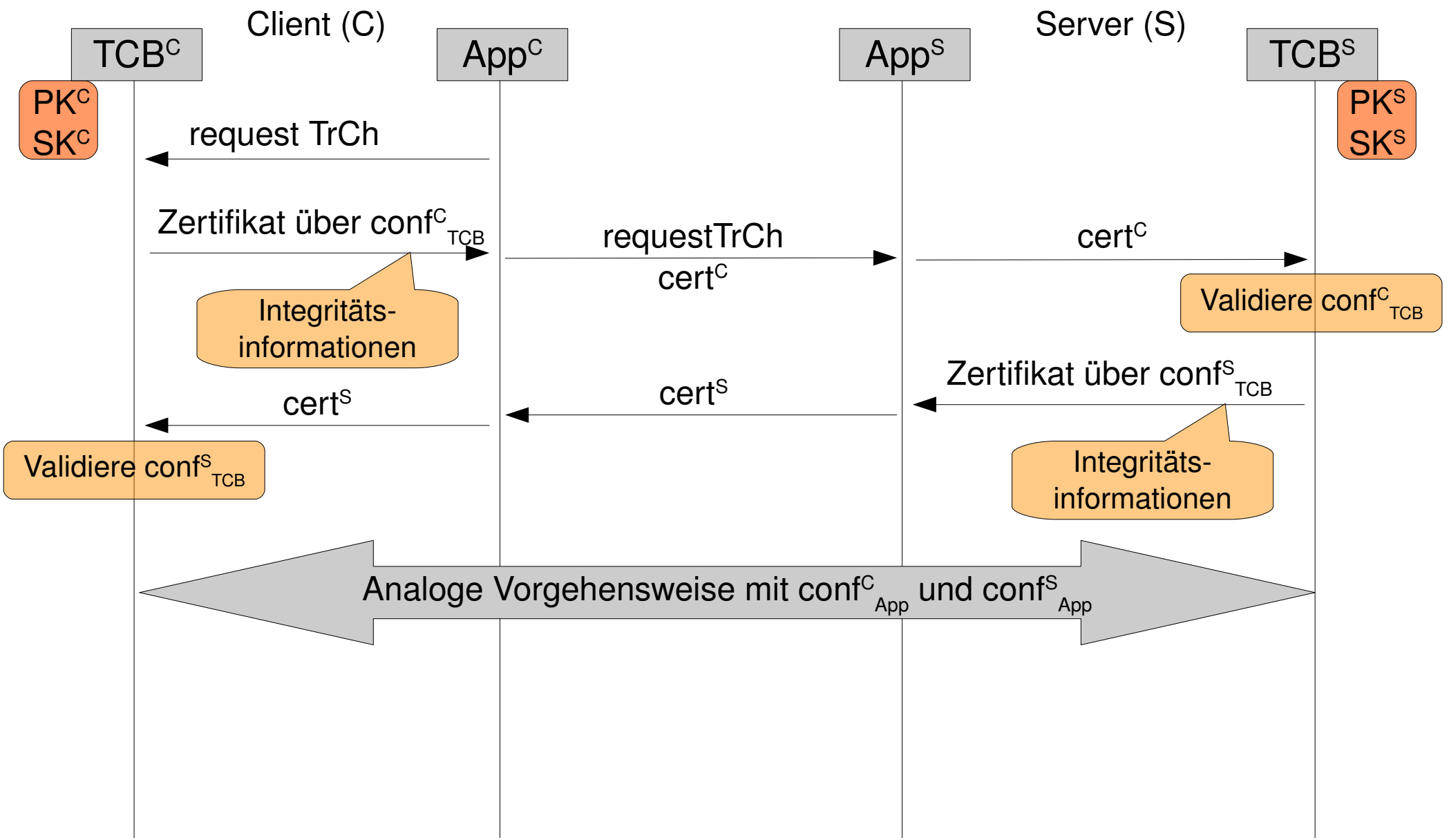
Generisches Trusted Channel Protokoll



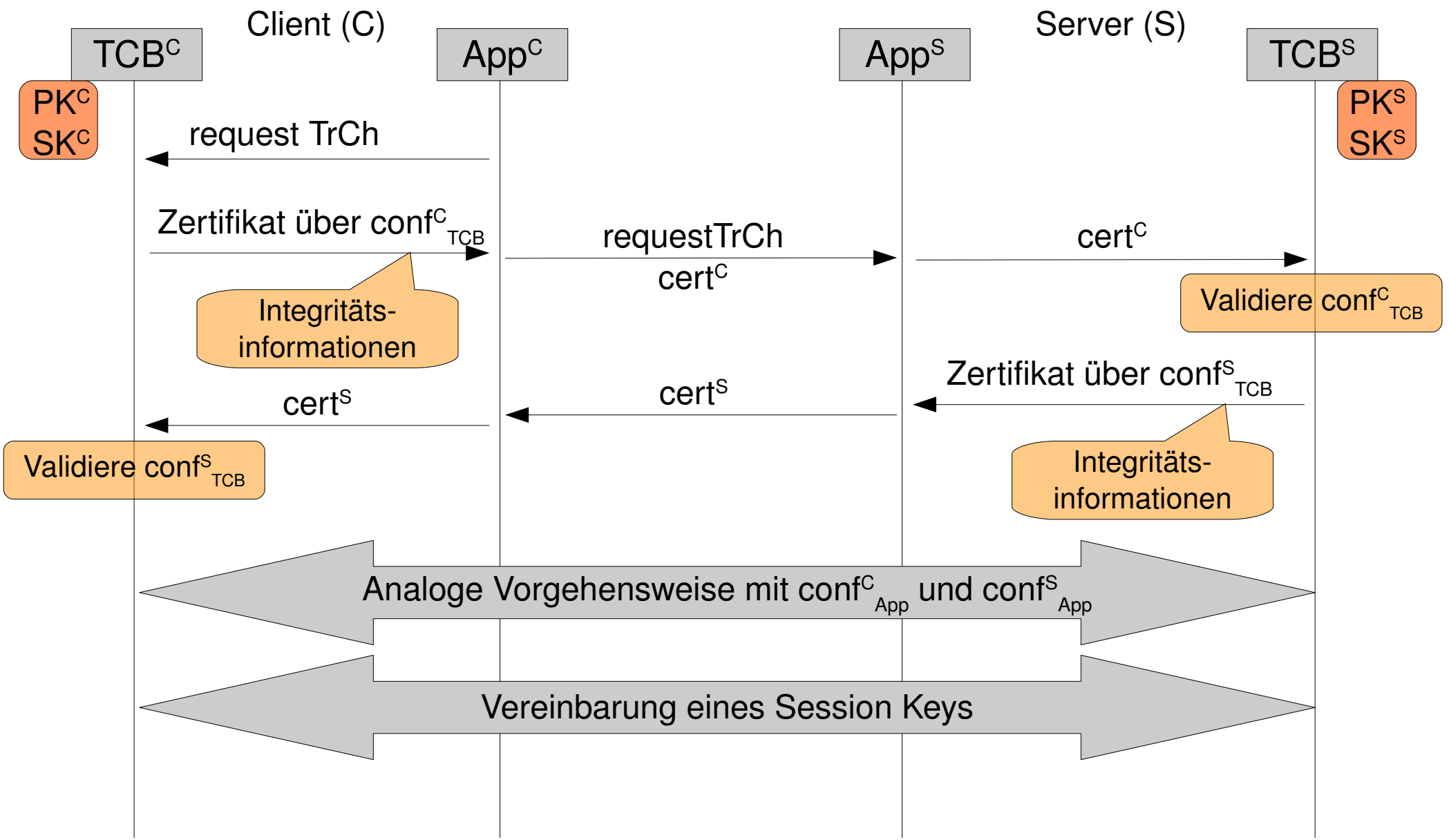
Generisches Trusted Channel Protokoll



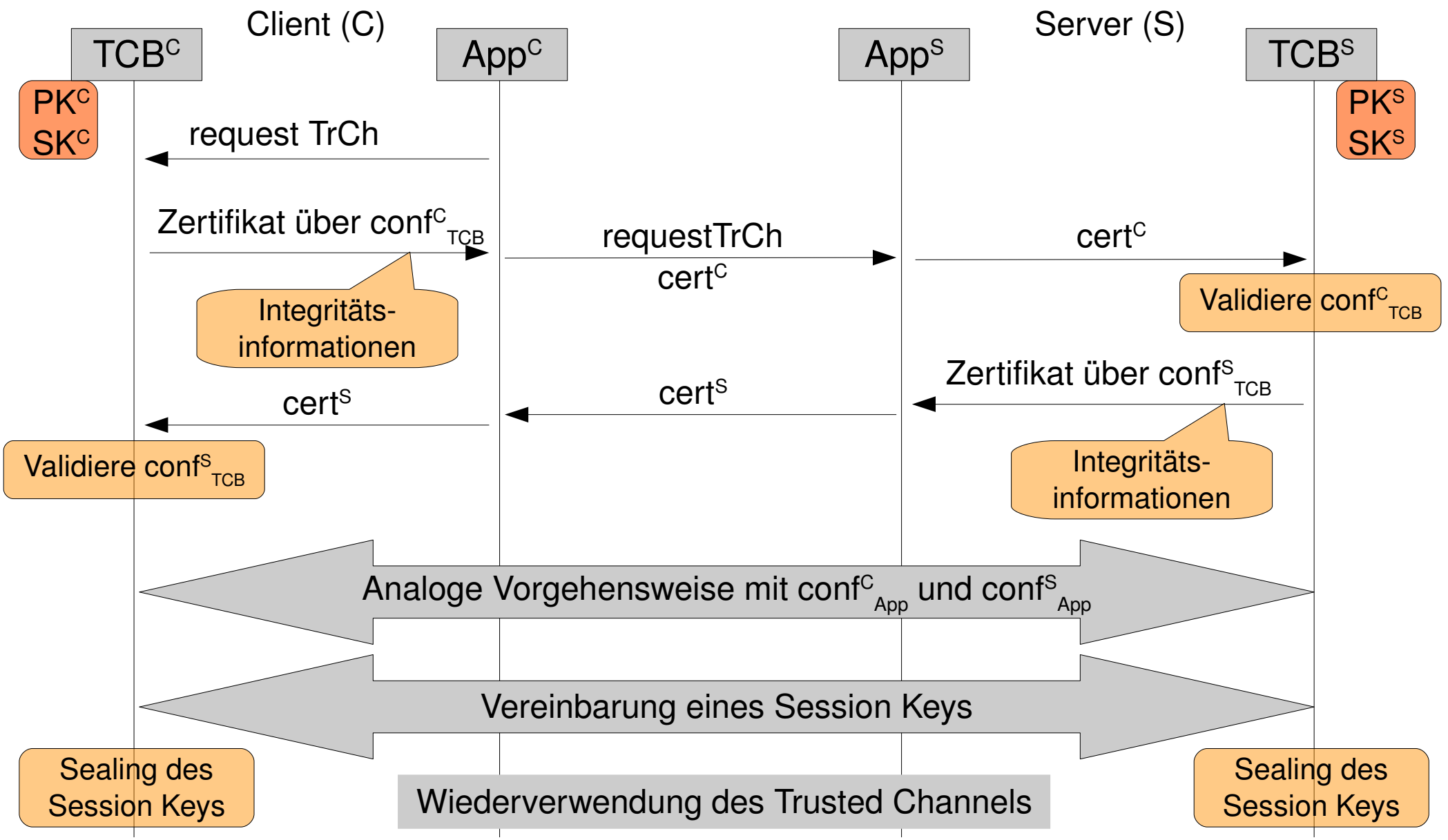
Generisches Trusted Channel Protokoll



Generisches Trusted Channel Protokoll



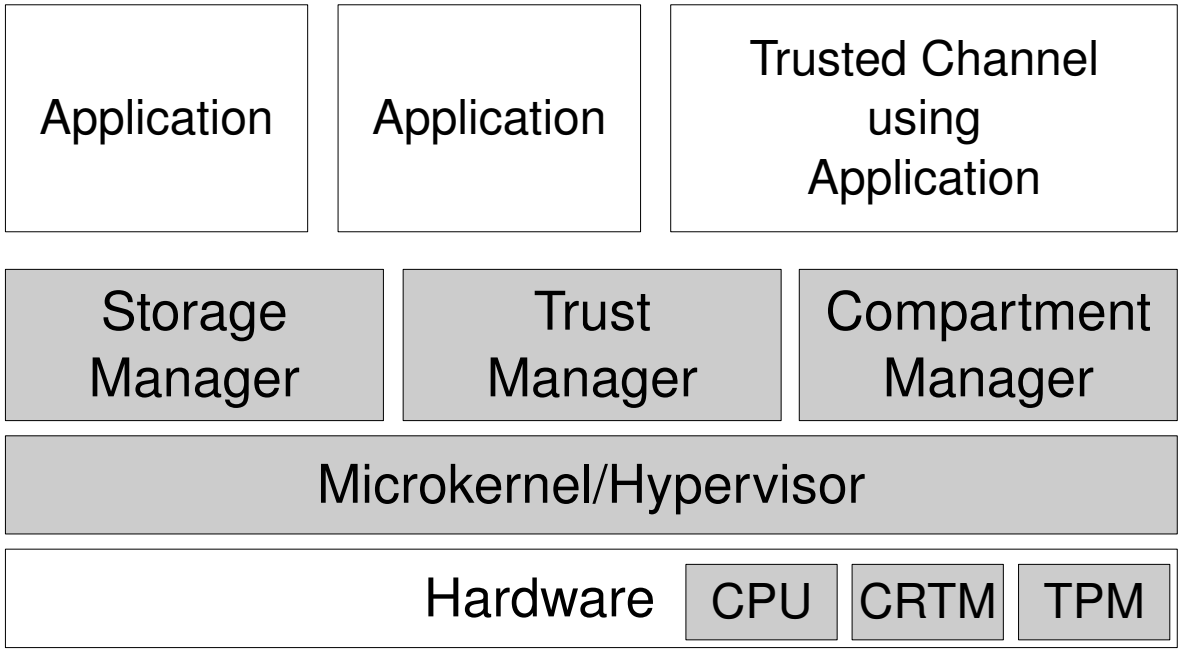
Generisches Trusted Channel Protokoll



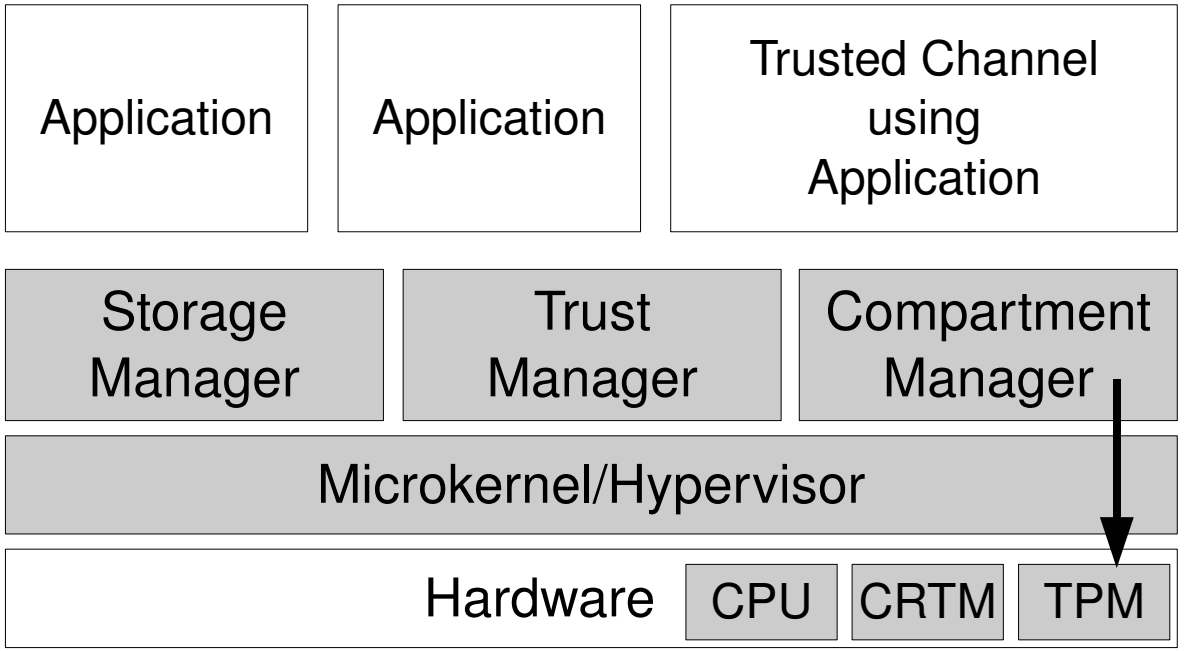
Trusted Channel Implementierungen

- Einbettung in TLS/SSL
  - Attestierung der Plattformkonfiguration im TLS-Handshake
  - Gasmi et al. (STC 2007), Armknecht et al. (STC 2008)
- Anwendungsspezifisch
  - Bindung eines Schlüssels an die Plattformkonfiguration (Sealing)
  - DRM: Asokan et al. (ISC 2007), vTPM: Sadeghi et al. (ISC 2008)

Security Kernel Komponenten für Trusted Channels

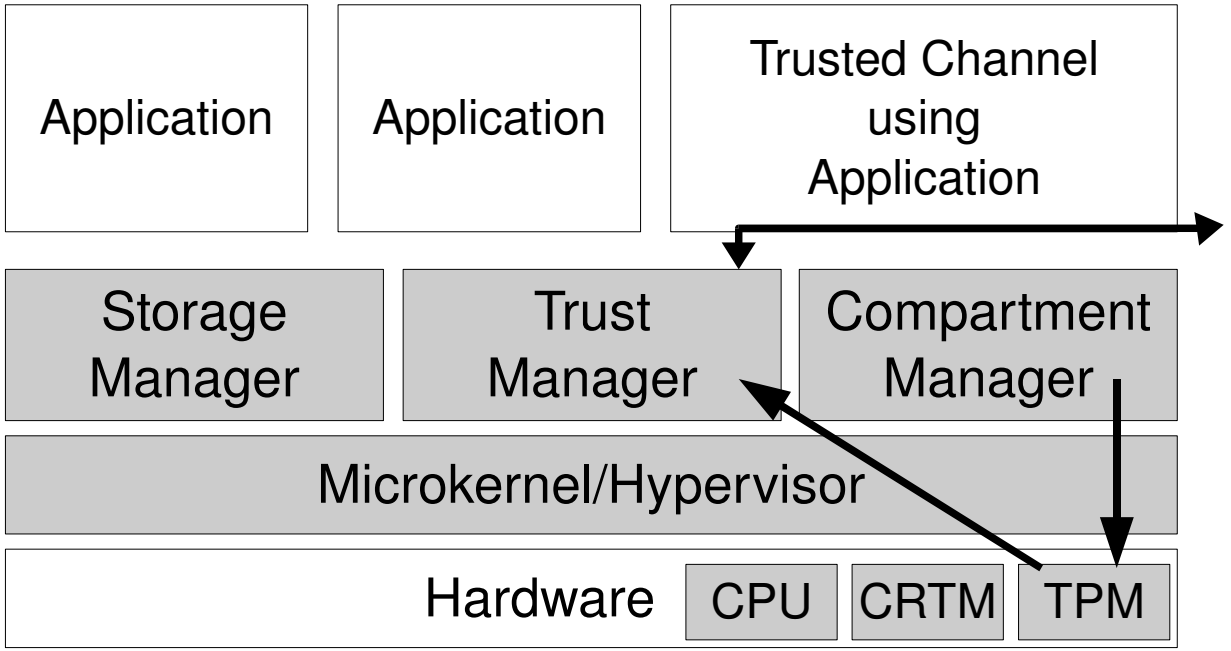


Security Kernel Komponenten für Trusted Channels



Compartment Manager:
Integritätsprüfwerte ermitteln

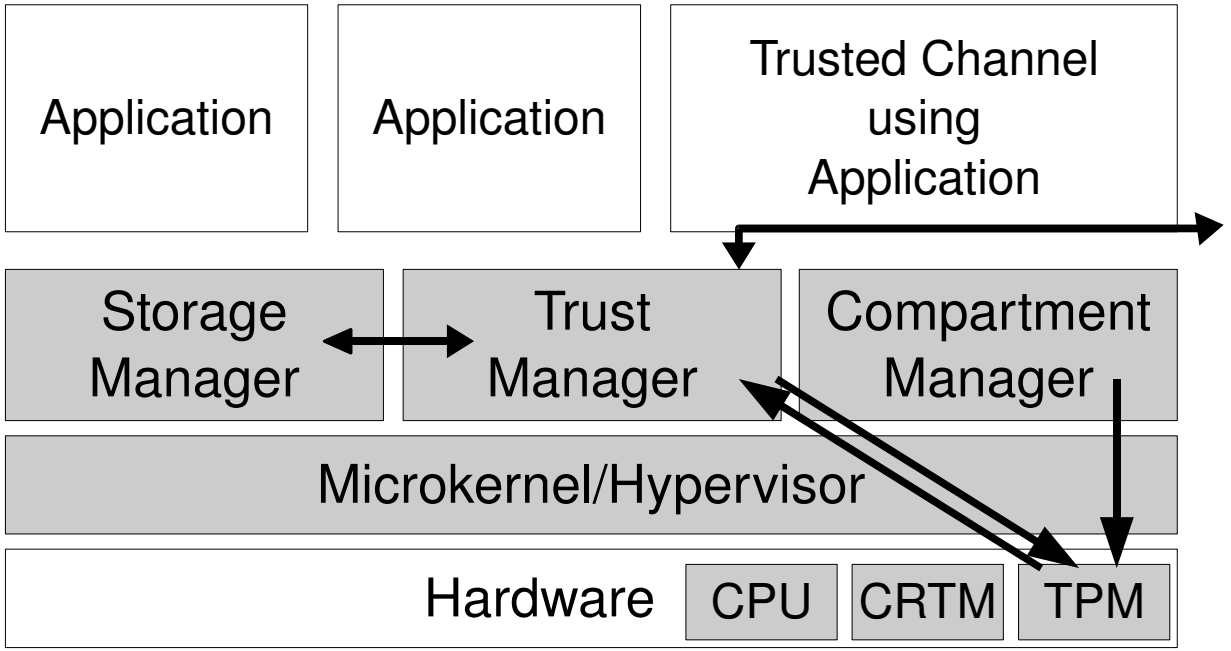
Security Kernel Komponenten für Trusted Channels



Compartment Manager:
Integritätsprüfwerte ermitteln

Trust Manager:
Attestierung durchführen,
Session Key empfangen

Security Kernel Komponenten für Trusted Channels



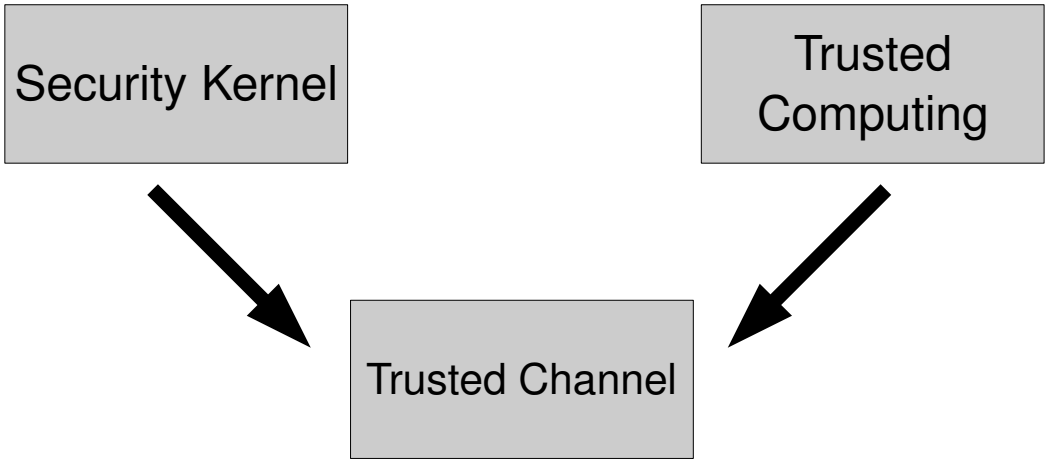
Compartment Manager:
Integritätsprüfwerte ermitteln

Trust Manager:
Attestierung durchführen,
Session Key empfangen

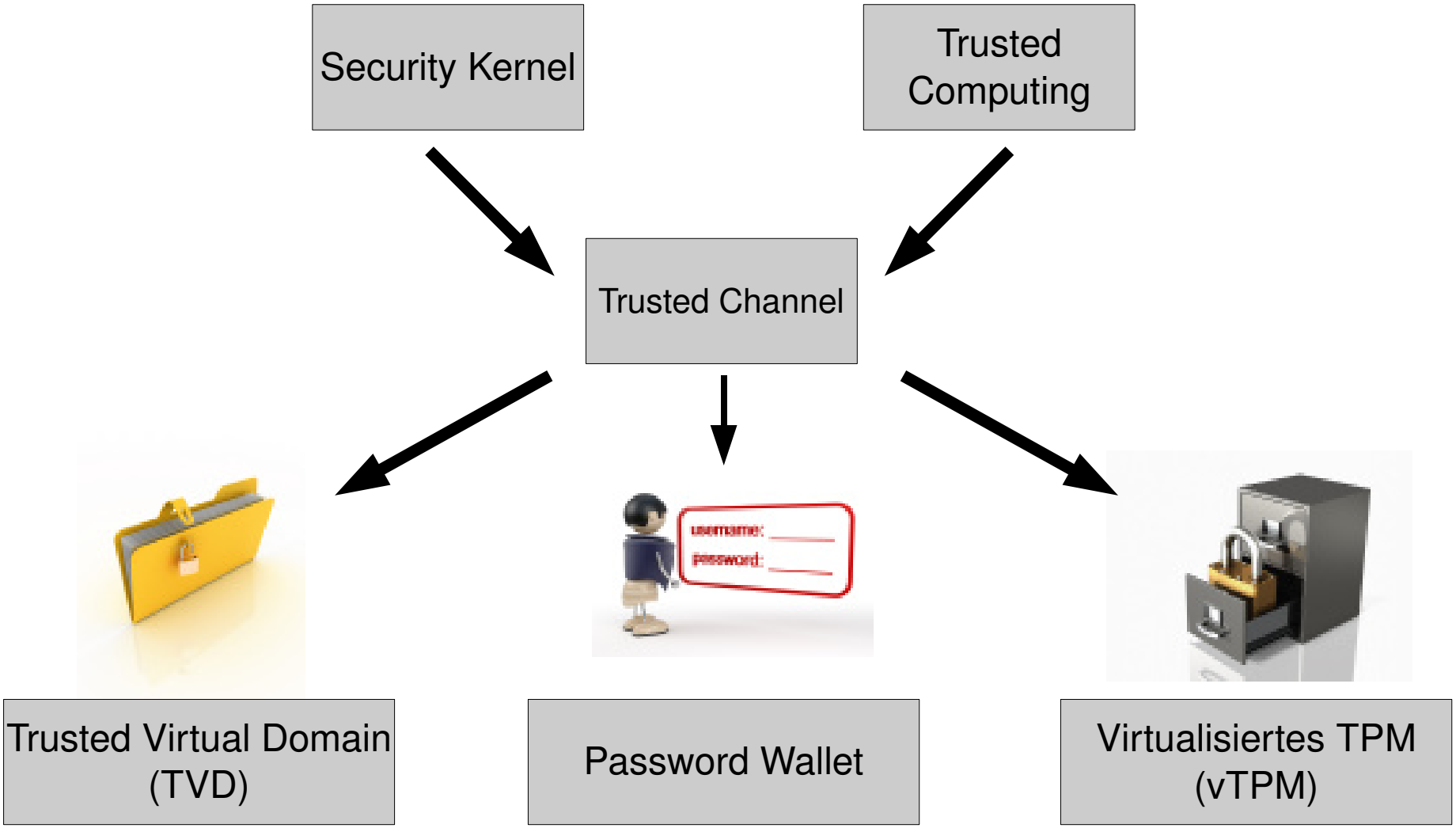
Storage Manager:
Persistente Speicherung
von Session Keys

Anwendungen von Trusted Channels

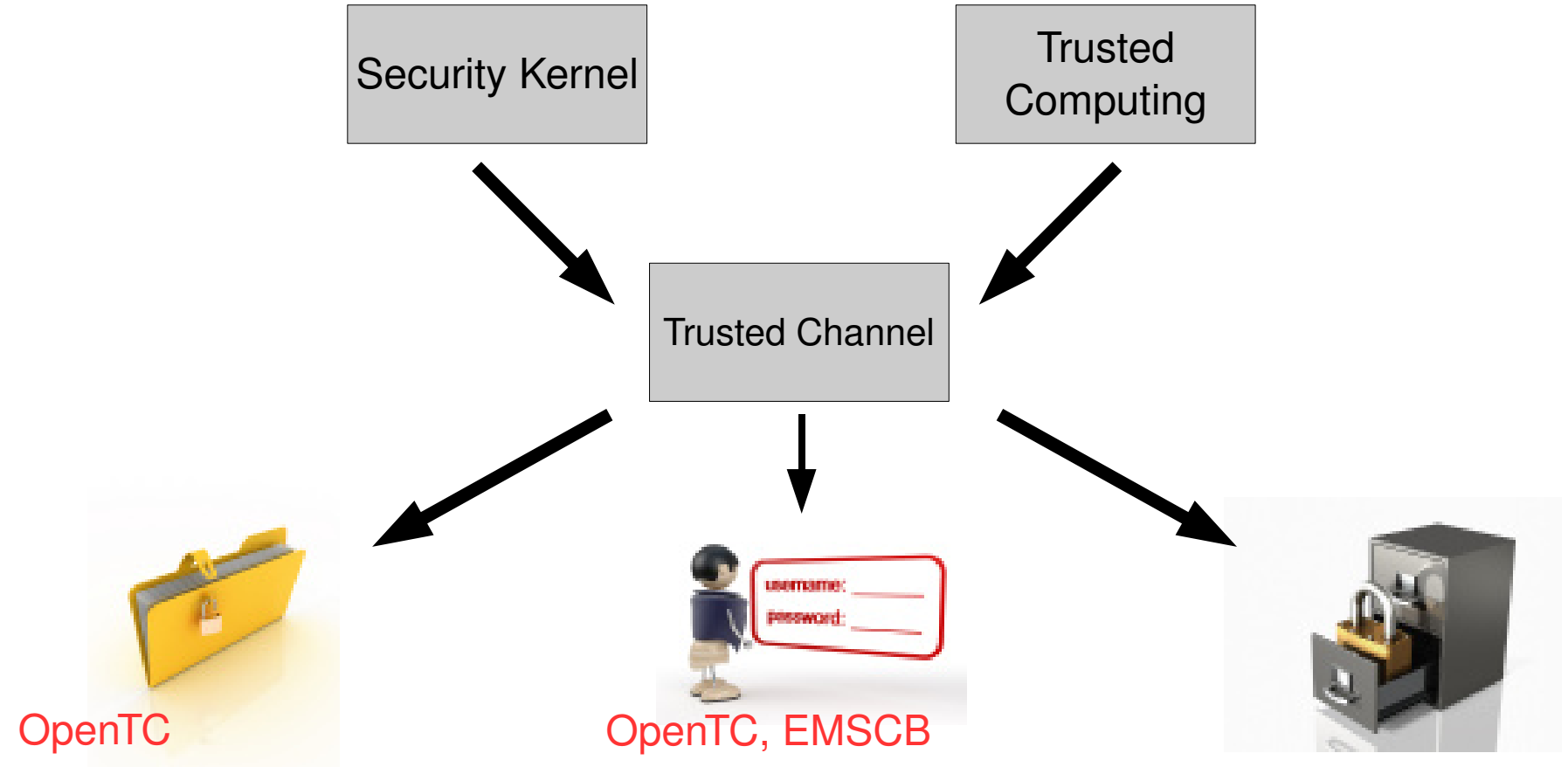
Überblick



Überblick

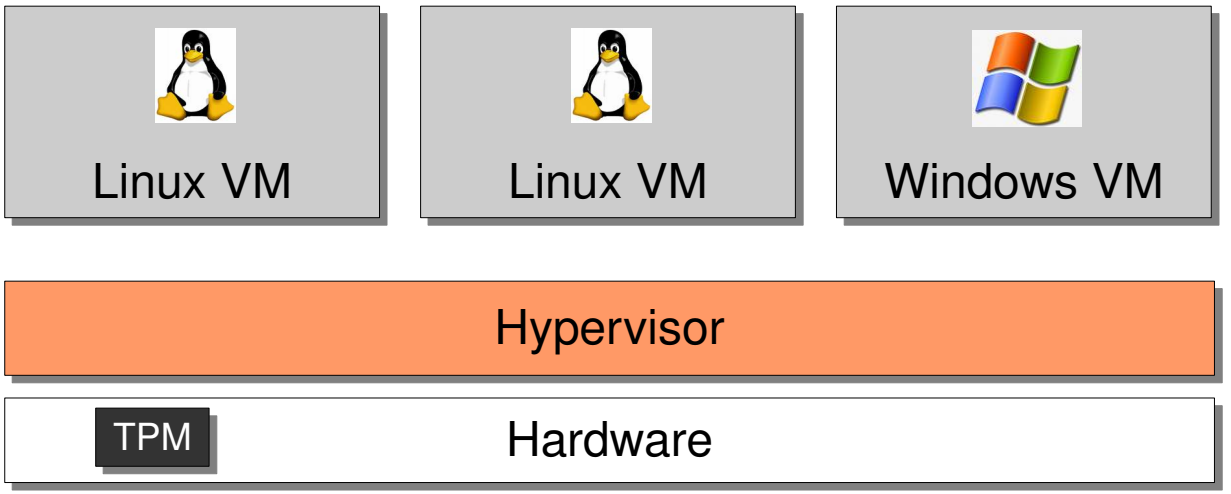

Security Kernel
Trusted Computing
Trusted Channel
username:
password:
Trusted Virtual Domain (TVD)
Password Wallet
Virtualisiertes TPM (vTPM)

Überblick


Security Kernel
Trusted Computing
Trusted Channel
OpenTC
OpenTC, EMSCB
Trusted Virtual Domain (TVD)
Password Wallet (TruWallet)
Virtualisiertes TPM (vTPM)
Journal of Computer Science (demnächst)
Gajek et al. (ARES 2007)
Sadeghi et al. (ISC 2008)

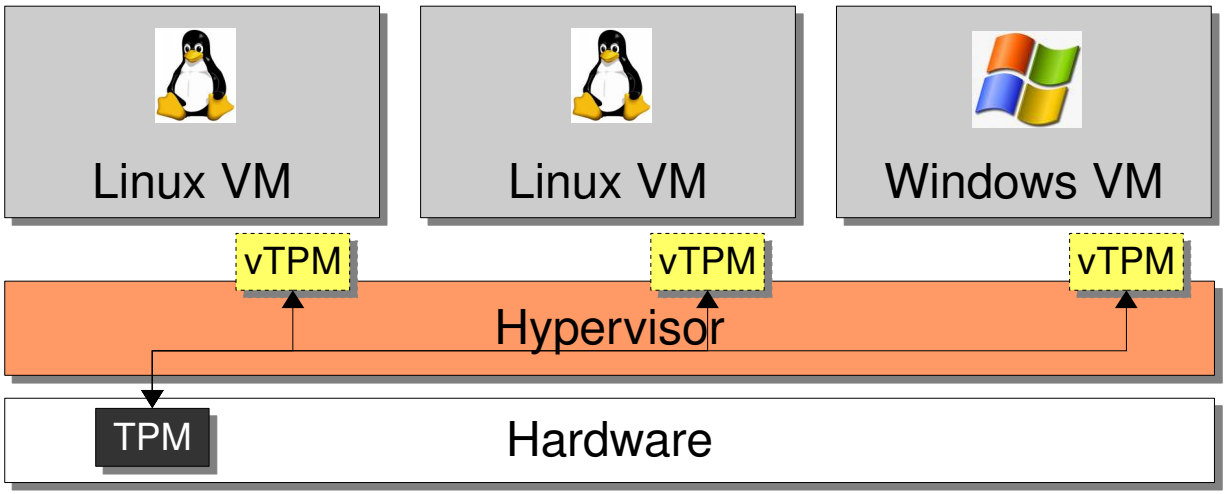
Beispiel: vTPM

- Jede Virtuelle Maschine (VM) benötige TPM
- Aber nur ein physikalisches TPM vorhanden



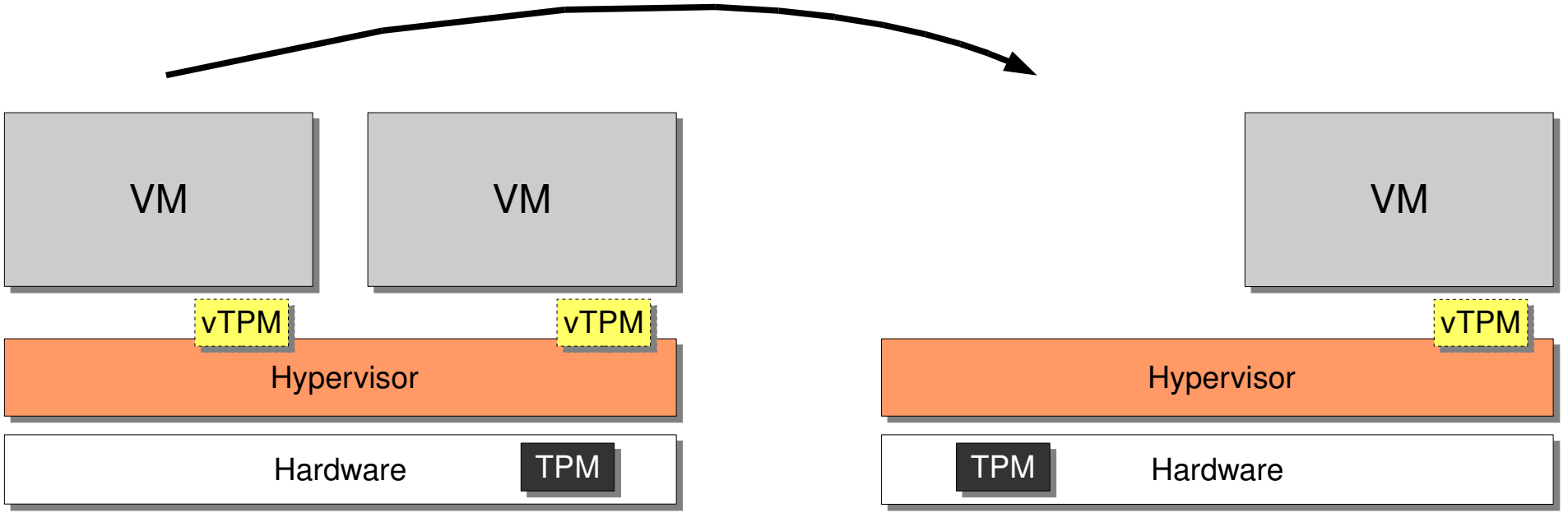
Beispiel: vTPM

- Virtualisierung des TPM: vTPM
  - Emulation in Software, wird aber an VM und TPM gebunden
  - Basierend auf Arbeiten von IBM (Berger et al. 2006)



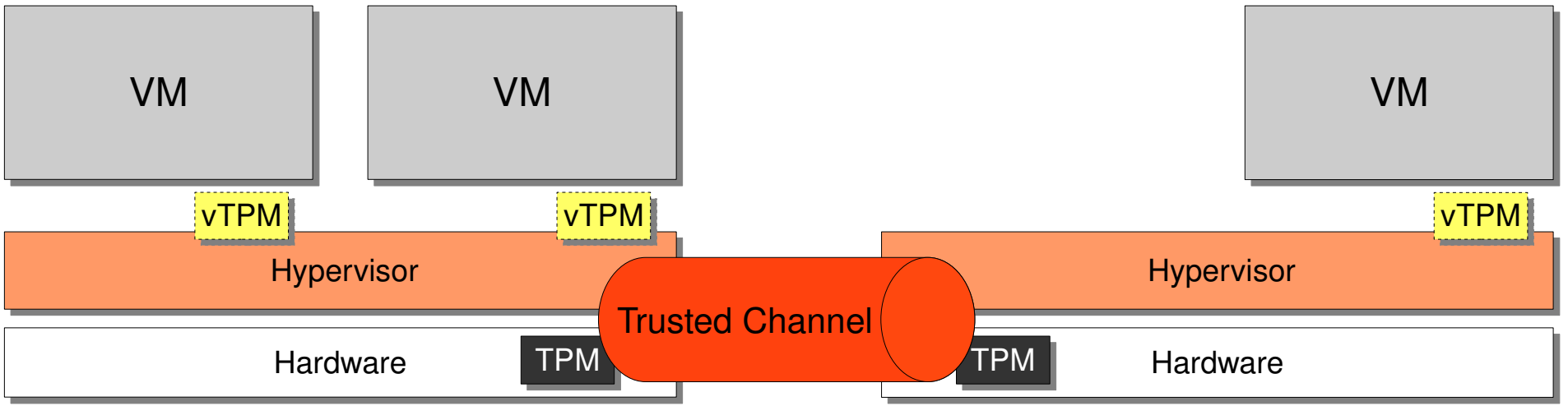
Migration eines vTPM

- Sichere Migration
  (Vertraulichkeit, Integrität, Authentizität)
- Neubindung des vTPM an Ziel-TPM



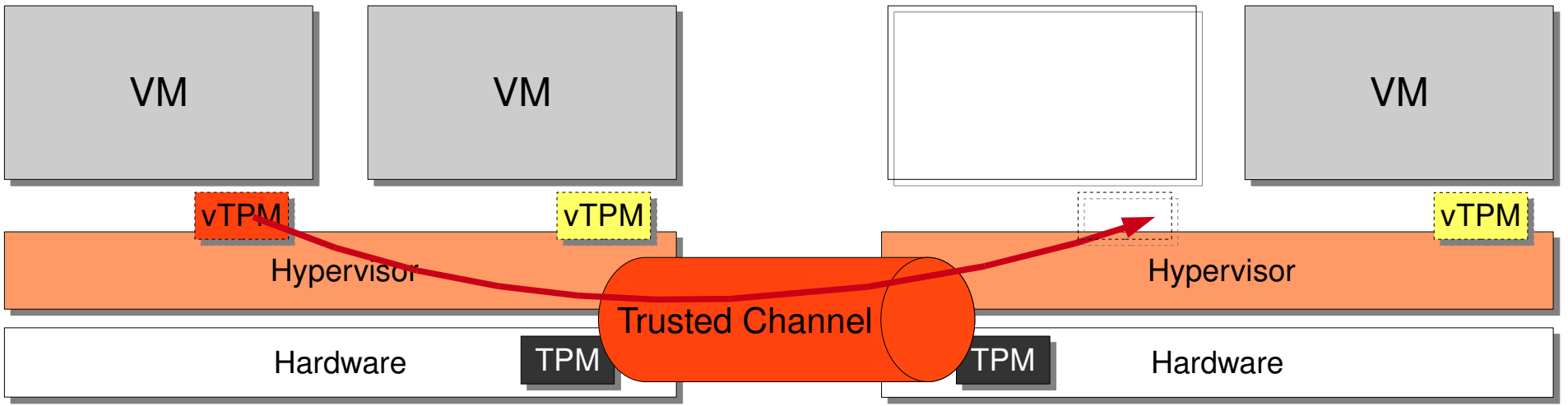
Trusted Channel basierte Migration

- Quell-Plattform fordert Trusted Channel an
  - Schlüssel wird an Konfiguration der Zielplattform gebunden
  - Wiederverwendbar für mehrere Migrationen



Trusted Channel basierte Migration

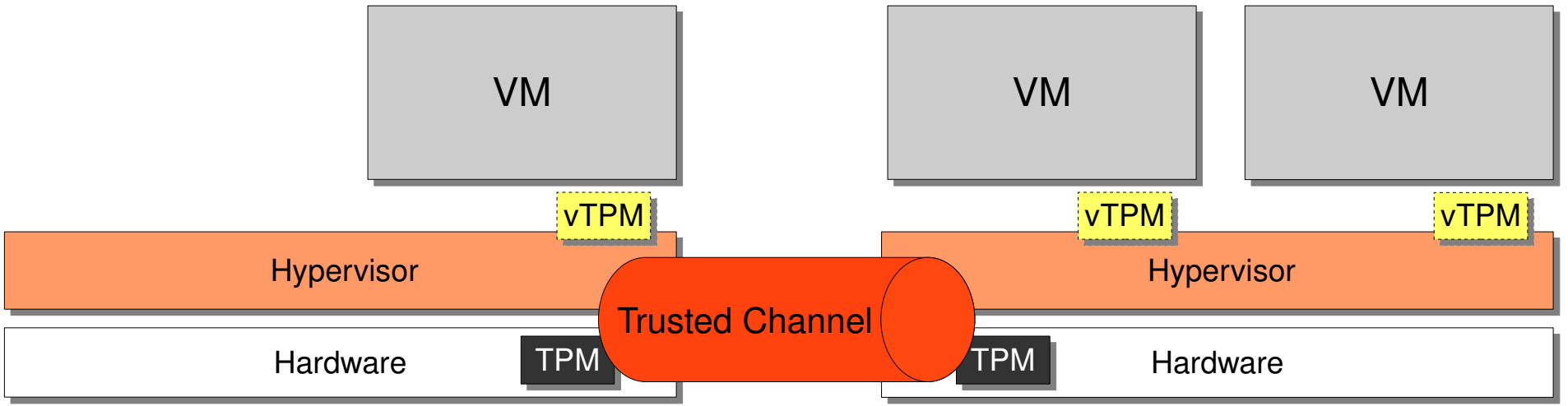
- Quell-Plattform fordert Trusted Channel an
  - Schlüssel wird an Konfiguration der Zielplattform gebunden
  - Wiederverwendbar für mehrere Migrationen



Übertragung des TPM Zustands (Register, Schlüssel, etc.) via Trusted Channel

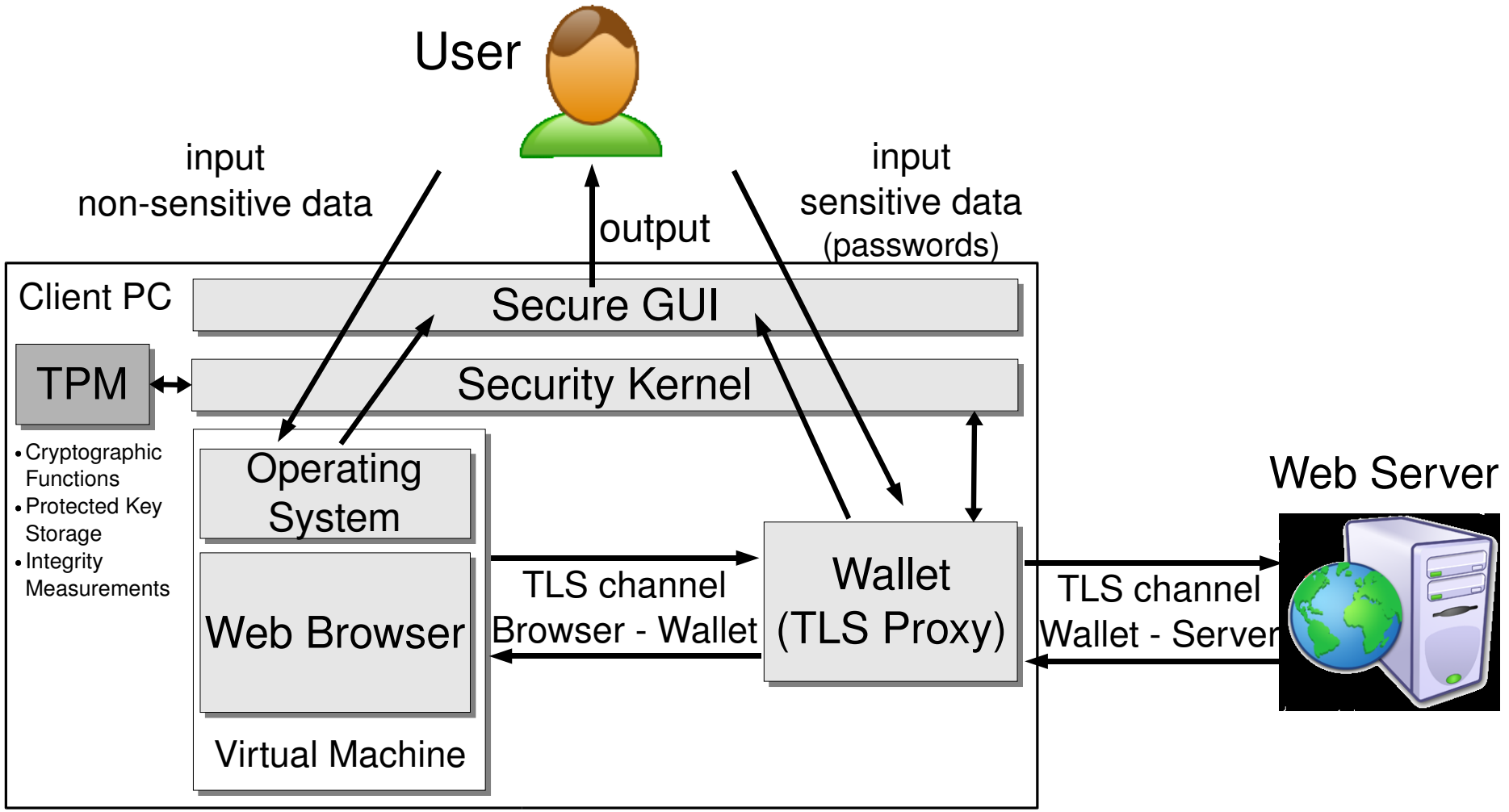
Trusted Channel basierte Migration

- Quell-Plattform fordert Trusted Channel an
  - Schlüssel wird an Konfiguration der Zielplattform gebunden
  - Wiederverwendbar für mehrere Migrationen

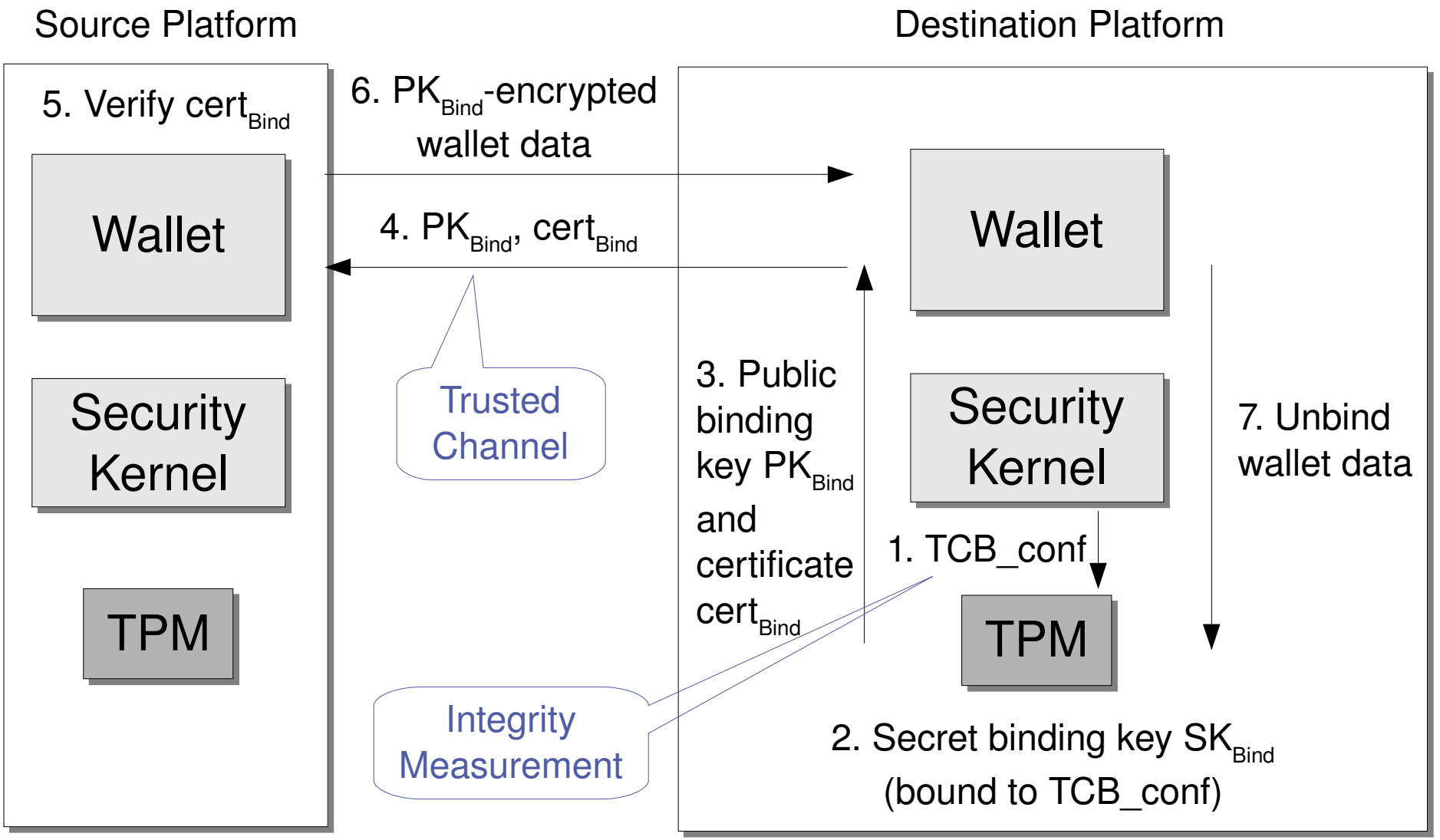


Übertragung des TPM Zustands (Register, Schlüssel, etc.) via Trusted Channel

Beispiel: TruWallet



Migration des Wallets



Zusammenfassung

- Secure Channels (Krypto) allein reicht nicht!
- Trusted Channels beziehen Integrität der Endpunkte ein
- Realisierung mittels Security Kernel
  - Eingebettet in TLS/SSL
  - Anwendungsspezifisch
- Diverse Anwendungsszenarien
  - Virtual Data Center (TVD, vTPM), e-Commerce (Wallet)
- Prototypen basierend auf Microkernel und Xen-Hypervisor
  - Turaya (www.emscb.de)
  - OpenTC (www.opentc.net)

Zentrale Erkenntnis

- Kryptographie allein reicht nicht
- Integrität der Endpunkte wichtig

Trusted Channels =
Kryptographie + Betriebssystemsicherheit

Lehrstuhl für
Systemsicherheit

Vielen Dank!

Marcel Winandy

Ruhr-Universität Bochum
marcel.winandy@trust.rub.de