Grundlagen der entfernten Authentifizierung und Autorisierung: Kerberos

Proseminar Konzepte von Betriebssystem-Komponenten
Sommersemster 2010

Florian Lukas
florian.lukas@e-technik.stud.uni-erlangen.de

23. Juni 2010

Motivation

Ausgangspunkt:

Typisches Firmen oder Universitäts-Szenario:

- Verschiedene Dienste
  (Login, NFS, HTTP, SSH, Drucker, ...)
- **Verteilte Rechner**
  (Desktops, Server, VPN-Clients, ...)
- **Mehrere Benutzer**
  (Mitarbeiter, Studenten, Admins, Programme, ...)

Motivation

Ziel:

- **Zugriffskontrolle** (wer darf was)
- **einheitliches, zentrales User-Management**
- **Single-Sign-On** (nur ein Login für alle Dienste)

Inhalt

Grundlagen

Grundlegende Unterscheidung zwischen

- Authentifizierung
- Autorisierung

Authentifizierung

Feststellen und Überprüfen der Identität eines Benutzers

Nachweis der Identität durch

- Passwort
- Zertifikate
- Smart-Card
- Biometrische Merkmale (Fingerabdruck, ...)

Autorisierung

Überprüfung und Vergabe von Zugriffrechten eines (authentifizierten) Benutzers

Meist dienstspezifisch, z.B.

- **Dateizugriffsrechte** (UNIX mode bits, ACLs)
- **Erlaubte Operationen** (GRANT Befehl in SQL)
- **...**

Sichere Kommunikation

Ziel:

Sichere Kommunikation zwischen A (Benutzer) und B (Dienst)

Ansatz:

- Verteilung symmetrischer Schlüssel
- Verschlüsselung aller Kommunikation mit diesem Schlüssel

Probleme

- Vorverteilung von symmetrischen Schlüsseln skaliert sehr schlecht:
  N Teilnehmer brauchen N(N-1)/2 Schlüssel
- **Replay-Angriff:** Nachrichten werden abgefangen und später wiederholt
- **Suppress-Replay-Angriff:** Nachrichten werden verzögert

Entfernte Authentifizierung

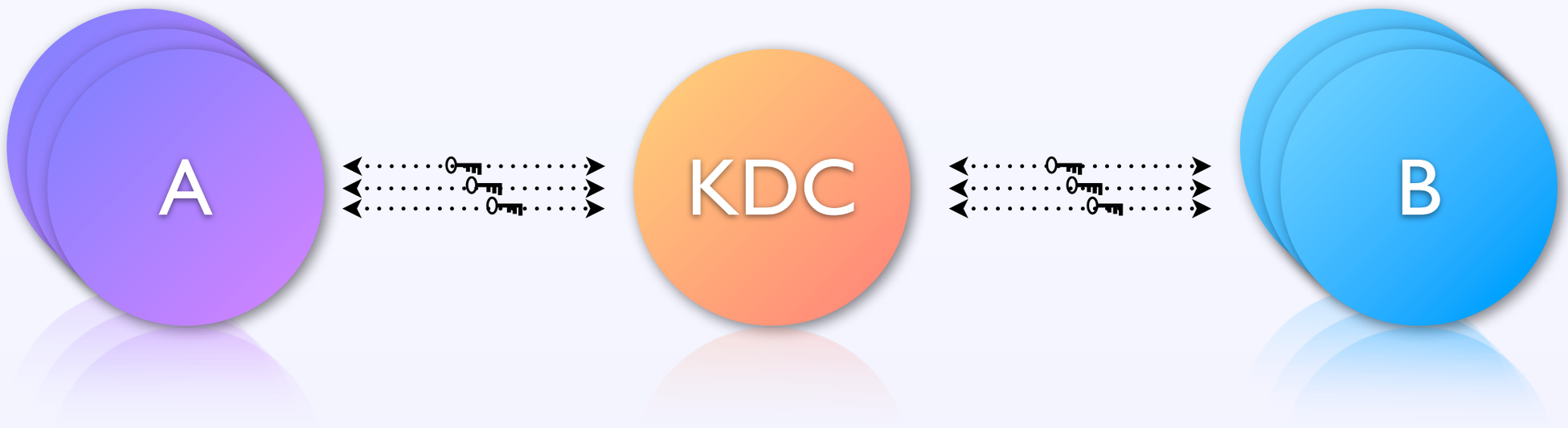
Lösung: Verwendung eines Authentifizierungsprotokolls mit

- Authentifizierung von A und B
- Einrichtung eines gemeinsamen (symmetrischen) Sitzungsschlüssels
- Benutzung dieses Schlüssels für eigentliche Kommunikation

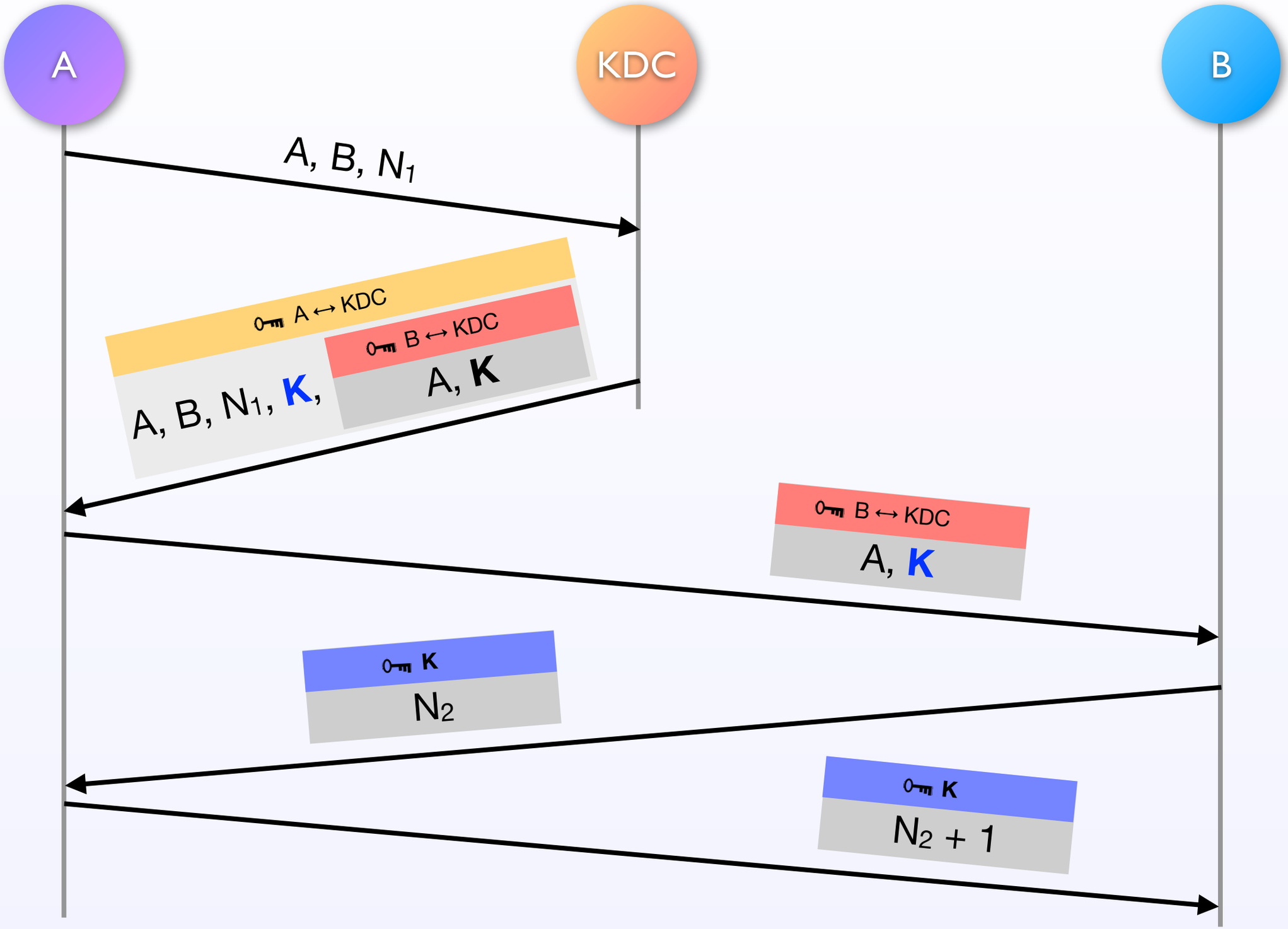
➡ **Needham-Schroeder-Protokoll**

Key Distribution Center

- Vertrauenswürdige Einheit
- hat mit jeder anderen Einheit einen geheimen Schlüssel
- nur noch N-1 statt N(N-1)/2 Schlüssel zu verteilen bei N Einheiten



Needham-Schroeder

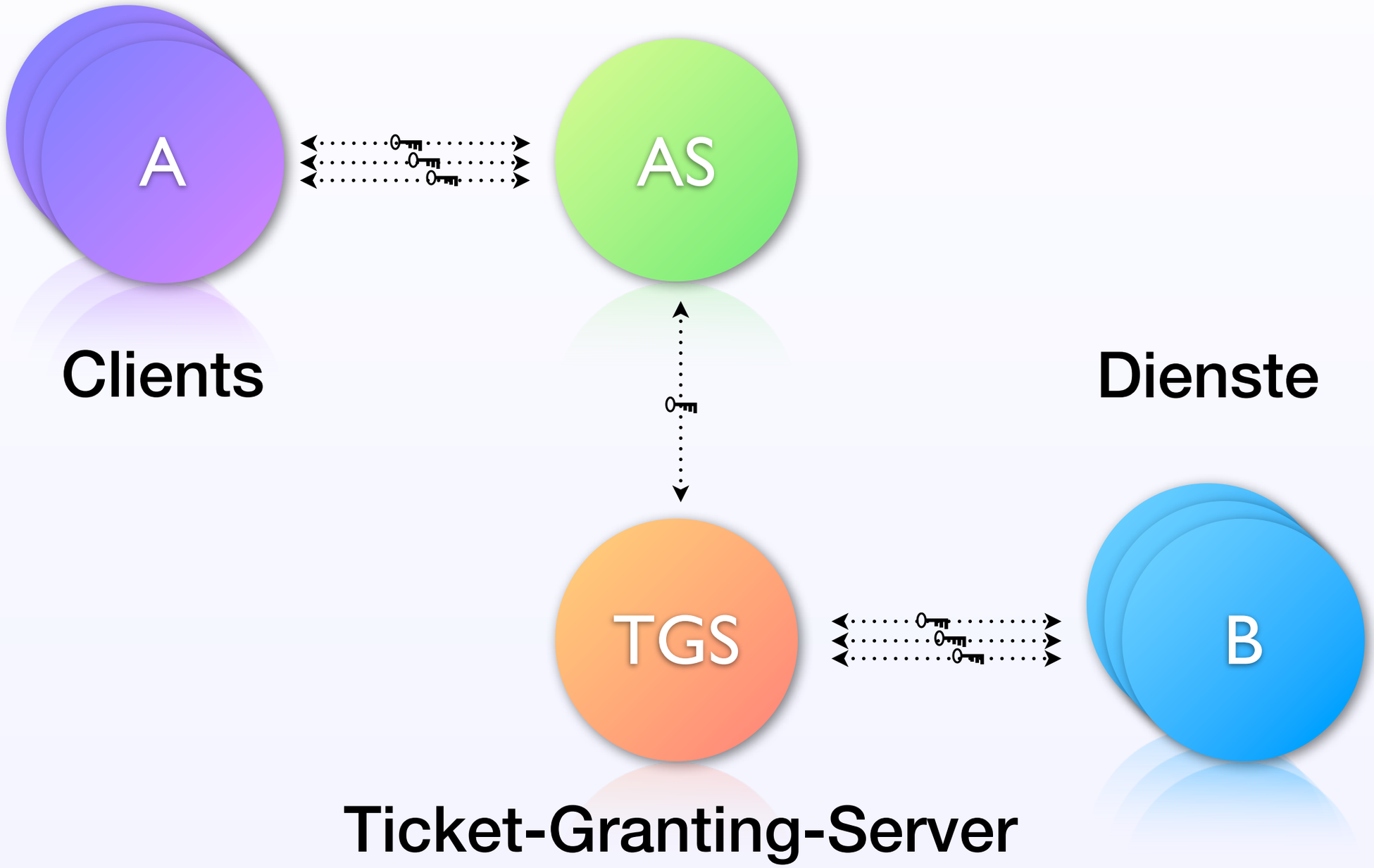


Inhalt

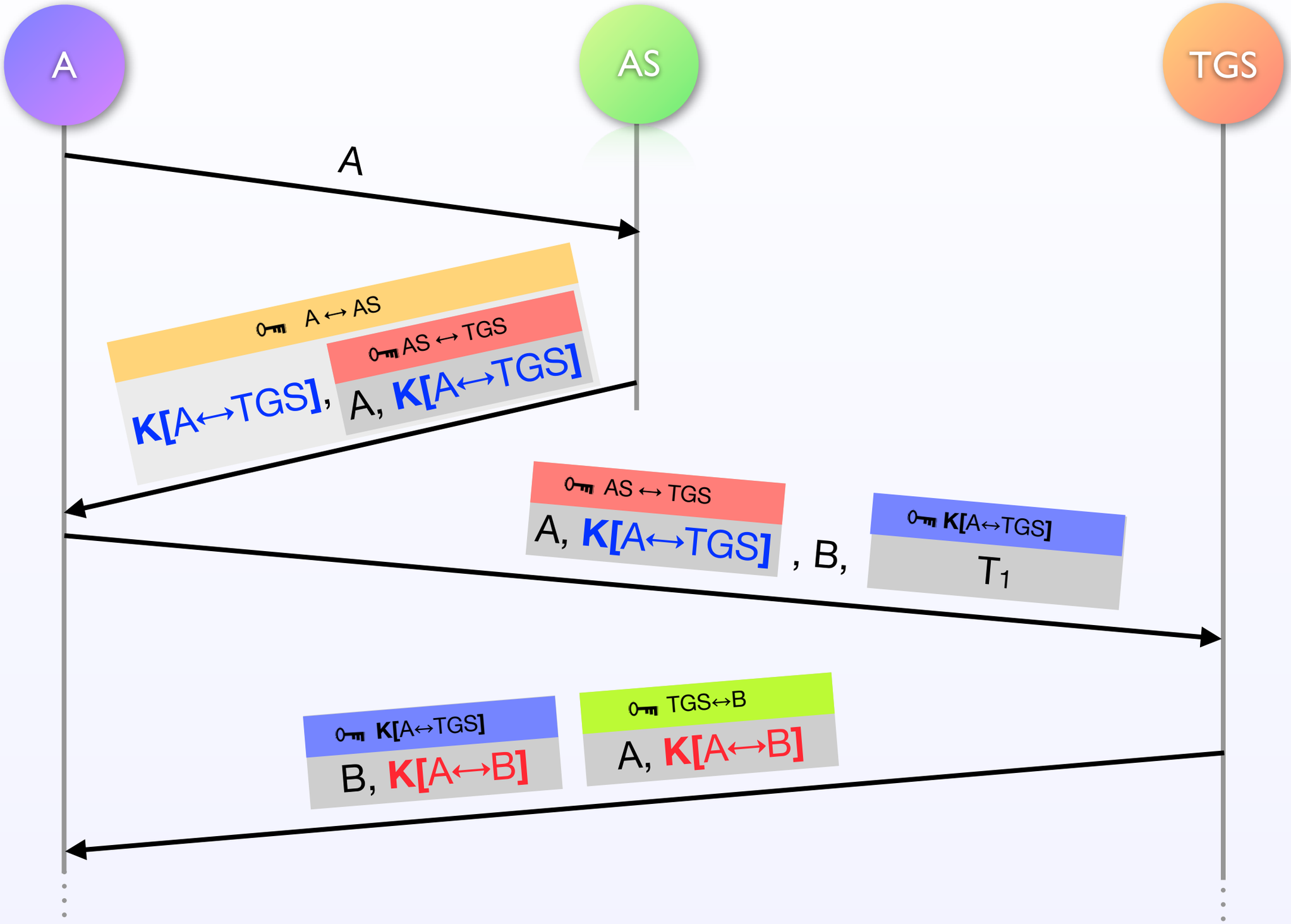
Kerberos

- Authentifizierungssystem auf Basis des Needham-Schroeder-Protokolls
  (nicht zuständig für Autorisierung!)
- Entwickelt am MIT
- Inzwischen IETF-Standard
- Als Open Source und kommerziell verfügbar
- Aktuell Version 5

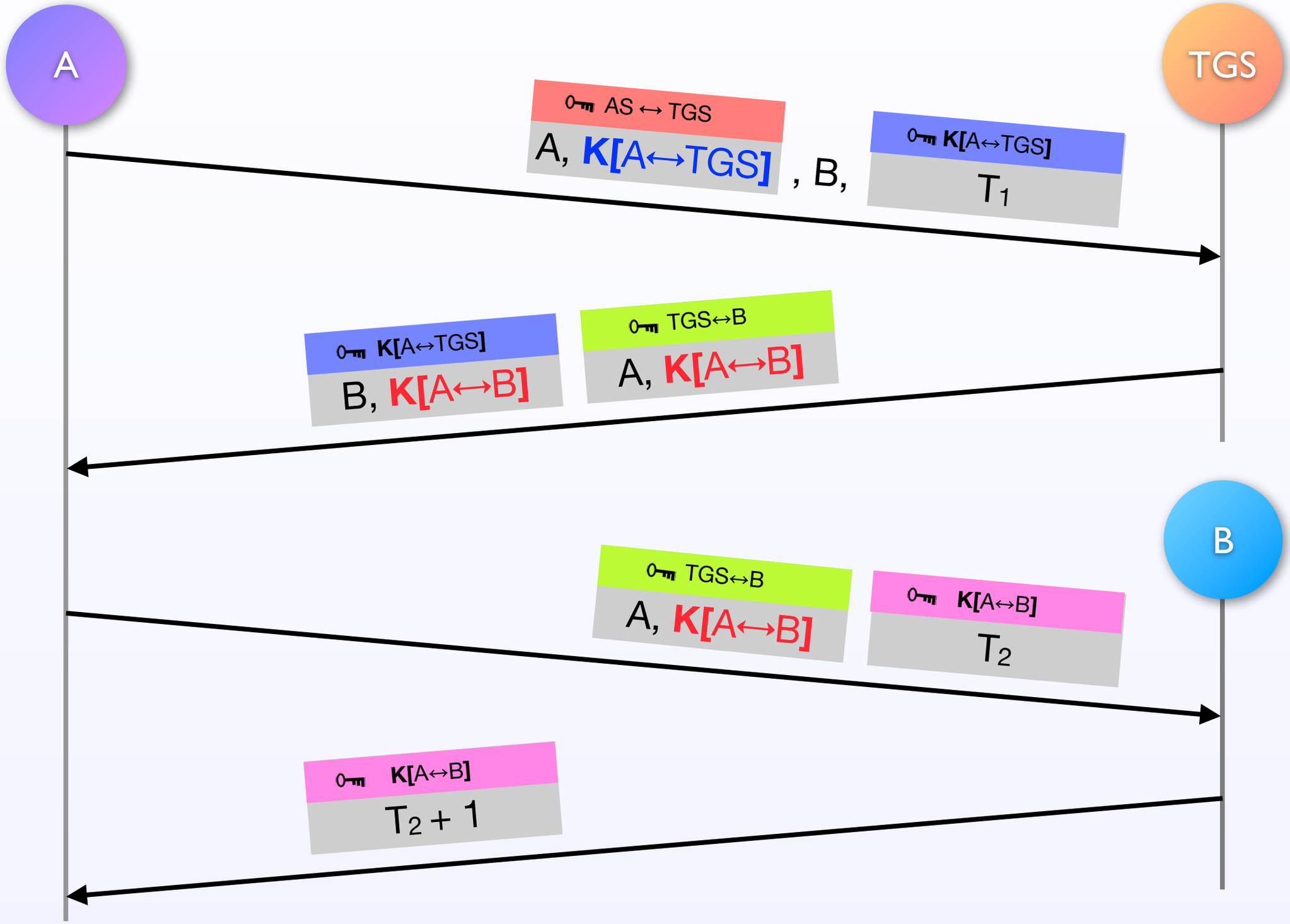
Komponenten



Protokollablauf (1)



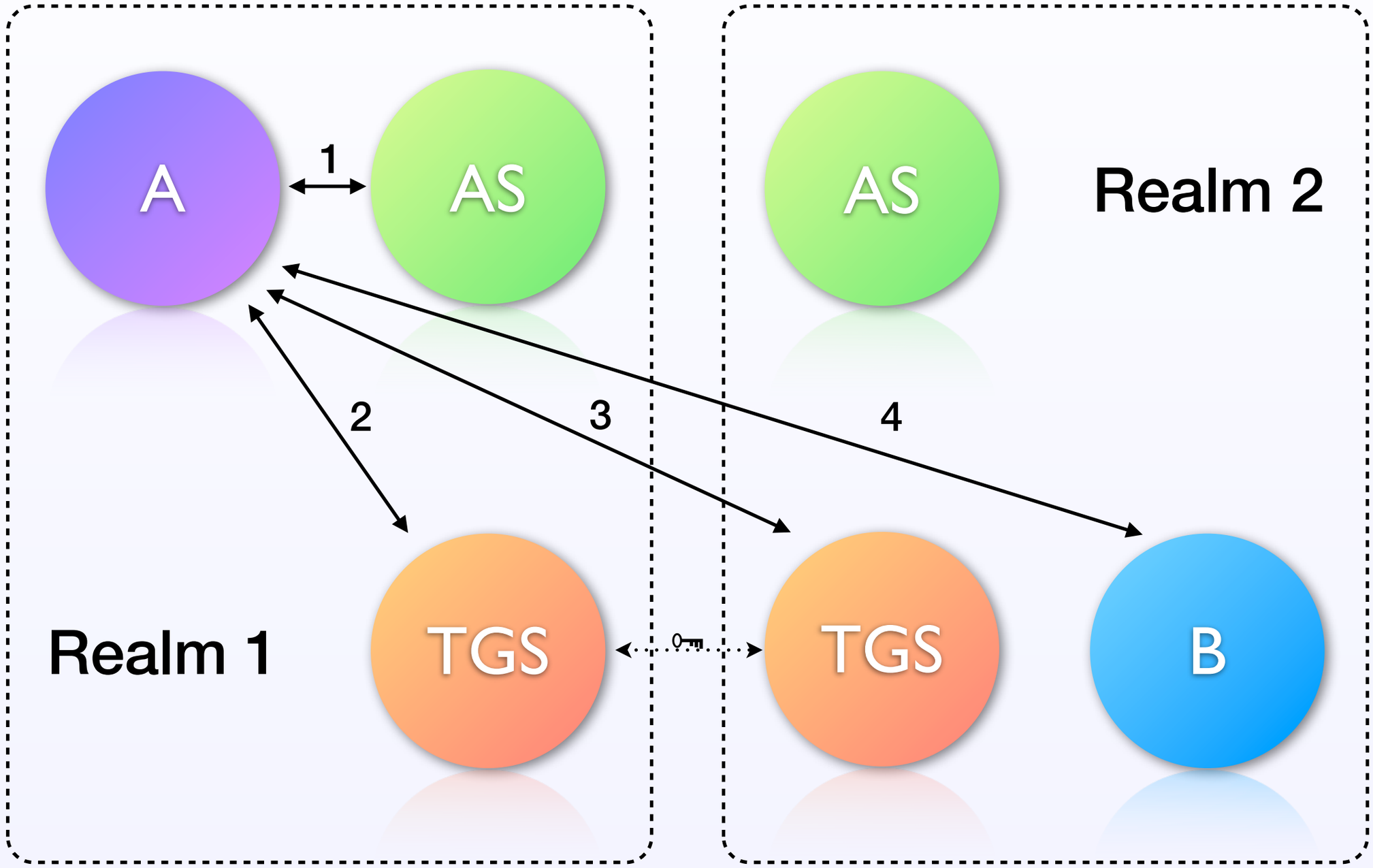
Protokollablauf (2)



Cross-Realm-Trust

- Eine eigenständige Kerberos-Installation wird als Realm bezeichnet
- Sich vertrauende Realms können gegenseitig auf Dienste zugreifen ohne neue Authentifizierung beim anderen Realm
- Dazu muss nur ein gemeinsamer Schlüssel zwischen den TGS ausgetauscht werden
- Der entfernte TGS wird dann wie ein normaler Dienst behandelt

Cross-Realm-Trust



Authentifizierung

- Authentifizierung des Benutzers erfolgt nur einmalig beim AS
- Pre-Authentication erfordert das Senden eines mit dem Passwort verschlüsselten Zeitstempels von A zum AS vor dem ersten Ticket vom AS
  (wegen Offline-Passwort-Attacken)
- Neben Passwort auch andere Authentifizierungsmöglichkeiten, z.B. durch eine Smart-Card

Spezielle Tickets

- Erneuerbare Tickets (z.B. lange Prozesse)
- Vordatierte Tickets (z.B. Batch/Cron Jobs)
- Weiterleitbare Tickets (z.B. geschachtelte SSH Verbindungen)

Verwendung

Kerberos ist u. a. verfügbar als Bestandteil von

- Microsoft Active Directory
- Apple Open Directory

Außerdem wird Kerberos benutzt für

- Apple Back to My Mac
- Xbox Live

Nachteile

- Fällt der AS oder TGS aus ist überhaupt keine Nutzung der Dienste mehr möglich
  Lösung: Redundanz
- Zeitsynchronisation erforderlich
  Lösung: NTP
- Wird der AS oder TGS kompromittiert, sind alle Dienste und Benutzer kompromittiert
  Lösung: ?

Zusammenfassung

- **Grundlagen:**
  Authentifizierung (Nachweis der Identität)
  Autorisierung (Prüfung der Berechtigungen)
  Sichere Kommunikation durch symmetrische Schlüssel
- **Needham-Schroeder Protokoll:**
  Protokoll zur Authentifizierung mittels symmetrischer Schlüssel und eines KDC
- **Kerberos:**
  System zur entfernten Authentifizierung

Quellen

- **Computernetze**,
  Larry L. Peterson, Bruce S. Davie,
  dpunkt.verlag, 2007
- **Netzsicherheit**,
  Günter Schäfer,
  dpunkt.verlag, 2003
- **The Kerberos Network Authentication Service (V5)**
  RFC 4120
  http://tools.ietf.org/html/rfc4120

Vielen Dank für die Aufmerksamkeit!

Noch Fragen?