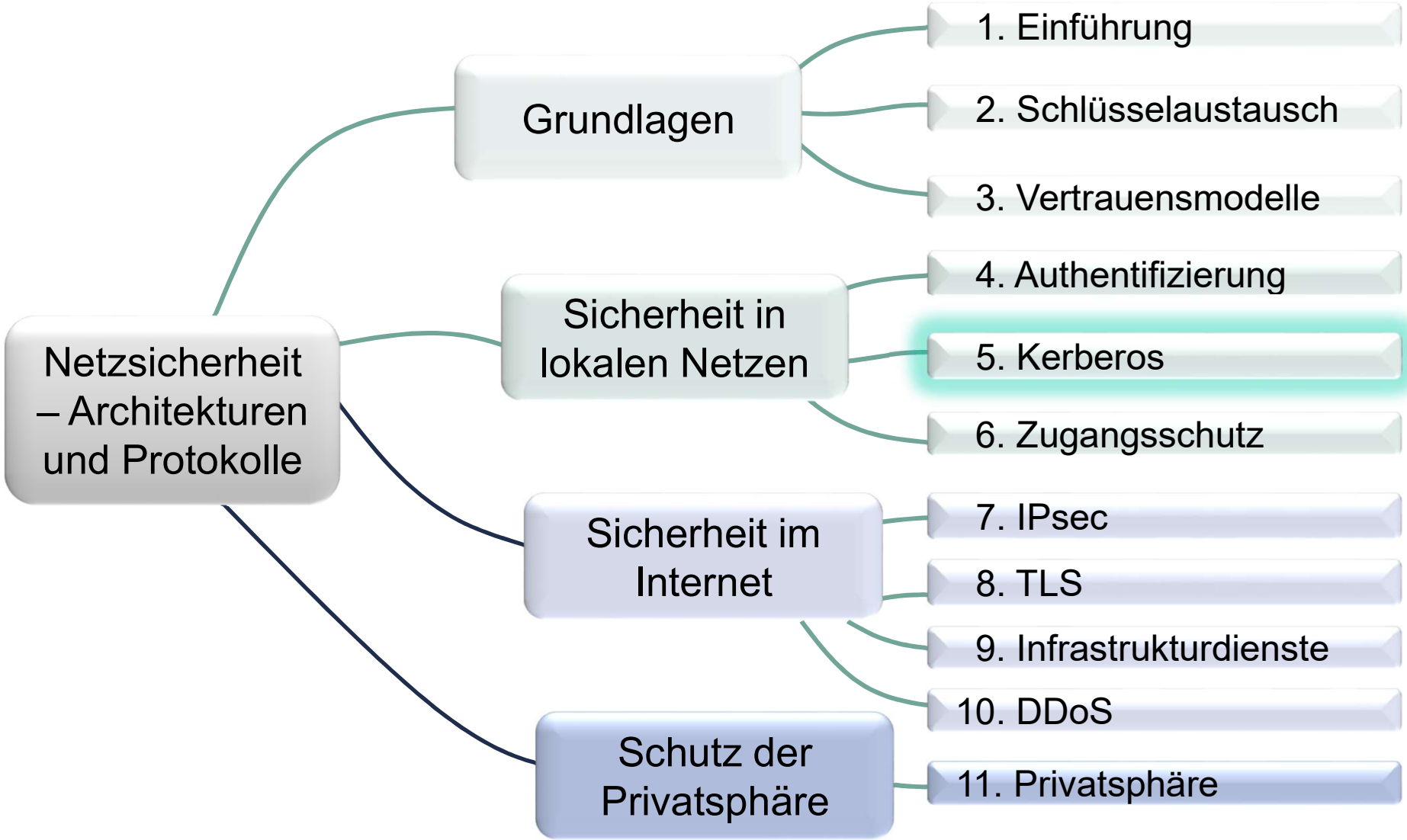
Karlsruher Institut für Technologie

Vorlesung Netzsicherheit
Kapitel 5 – Kerberos

PD Dr. Ingmar Baumgart, PD Dr. Roland Bless, Matthias Flittner, Prof. Dr. Martina Zitterbart
baumgart@fzi.de, [bless, flittner, zitterbart]@kit.edu

Institut für Telematik, Prof. Zitterbart

Inhalte der Vorlesung



Karlsruher Institut für Technologie

Kapitel 5.1 Überblick über Kerberos

Ziel von Kerberos

- Kerberos ist ein verteilter Authentifizierungsdienst
  - Bietet Authentifizierung von Entitäten (Nutzer oder Server) an
  - Netzwerk muss nicht geschützt sein (Dolev-Yao-Angreifer)
  - Single Sign-On für verteilte Dienste in einer Netzdomäne
    - Benutzer muss sich nur einmal anmelden

- Zusätzlich kann Kerberos als Basis verwendet werden für
  - Schlüsselaustausch
  - Autorisierung
  - Schutz von Integrität und Vertraulichkeit

- Einsatz einer vertrauenswürdigen dritten Partei (*Trusted Third Party*)

Kerberos – Überblick

Key Distribution Center (KDC)
(Authentication Server +
Ticket-Granting Server)

Benutzer-
Datenbank

Dem KDC
muss vertraut
werden.

KDC ist
single point
of failure.

Alice

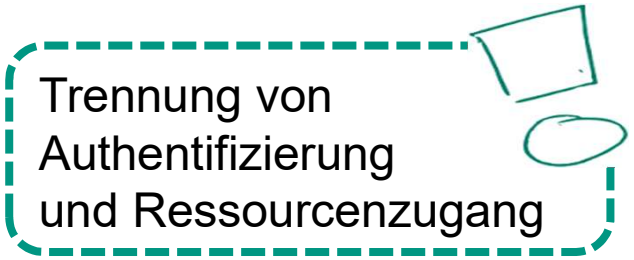
Workstation

Netz-Ressourcen

Single Sign On
von Alice an der
Workstation

Kerberos Komponenten

- *Authentication Server* (AS)
  - Authentifizierung der Benutzer
  - Ausstellen eines Authentifizierungs-Tokens
    - *Ticket-Granting-Ticket* (TGT)



- *Ticket-Granting Server* (TGS)
  - Ressourcen-Zugangs-Server
  - Autorisierung des Ressourcen-Zugriffs bei Vorlage eines gültigen TGT
  - Ausstellen von Zugangsberechtigungen (*Ressourcen-Tickets*)

- Benutzer-Datenbank
  - Speichert *Master-Secrets* aller Benutzer und Ressourcen

Kerberos allgemein

- Kerberos Versionen
  - Version 1 bis 3 heute nicht mehr im Einsatz
  - Version 4 und Version 5 konzeptionell ähnlich
    - Version 4 ist einfacher und leistungsfähiger
    - Version 5 ist sicherer und mächtiger
  - In dieser Vorlesung wird Kerberos v5 betrachtet

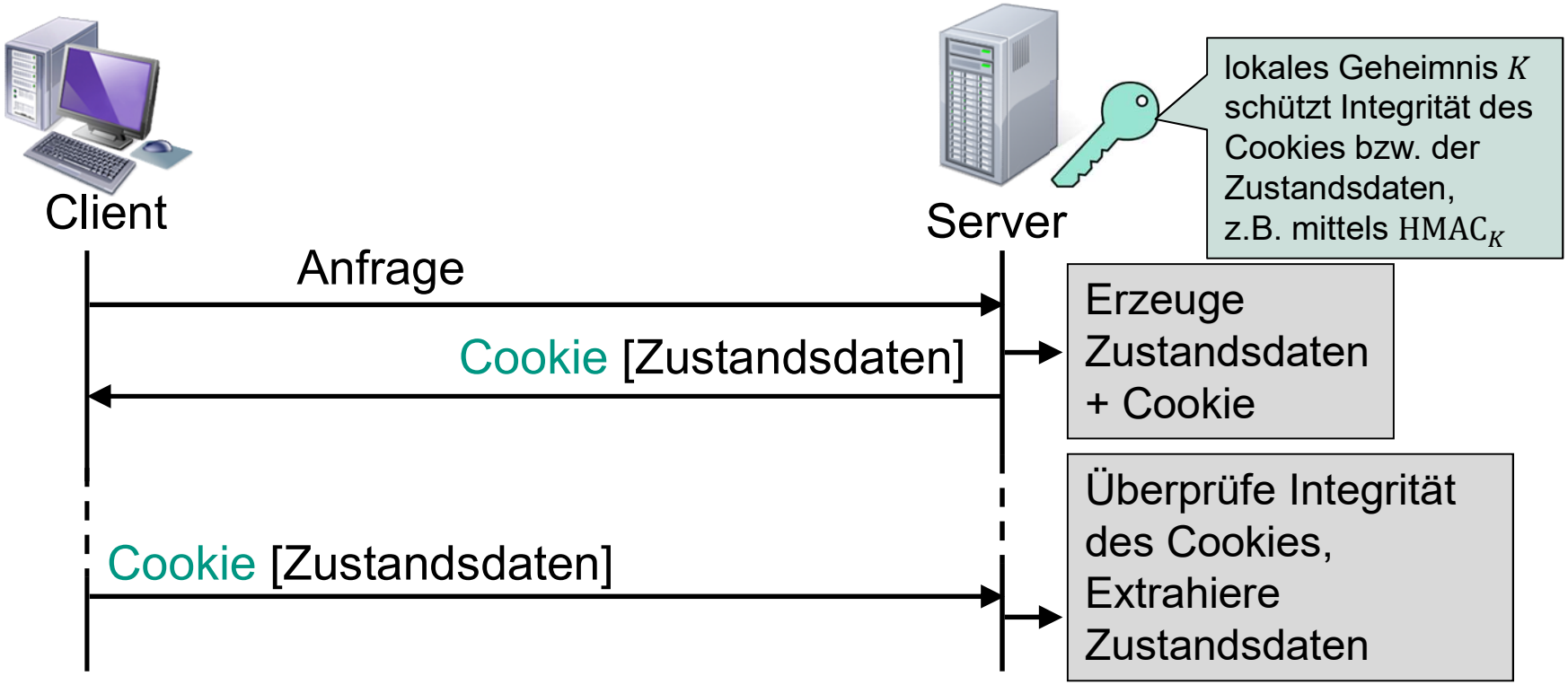
- Anwendungen, die Kerberos unterstützen
  - Telnet
  - BSD rtools
  - NFS
  - SSL, SSH
  - Windows 2000, 2003, XP, Vista, ...

[Proe11]

Kurze Wiederholung: Tokens/Cookies

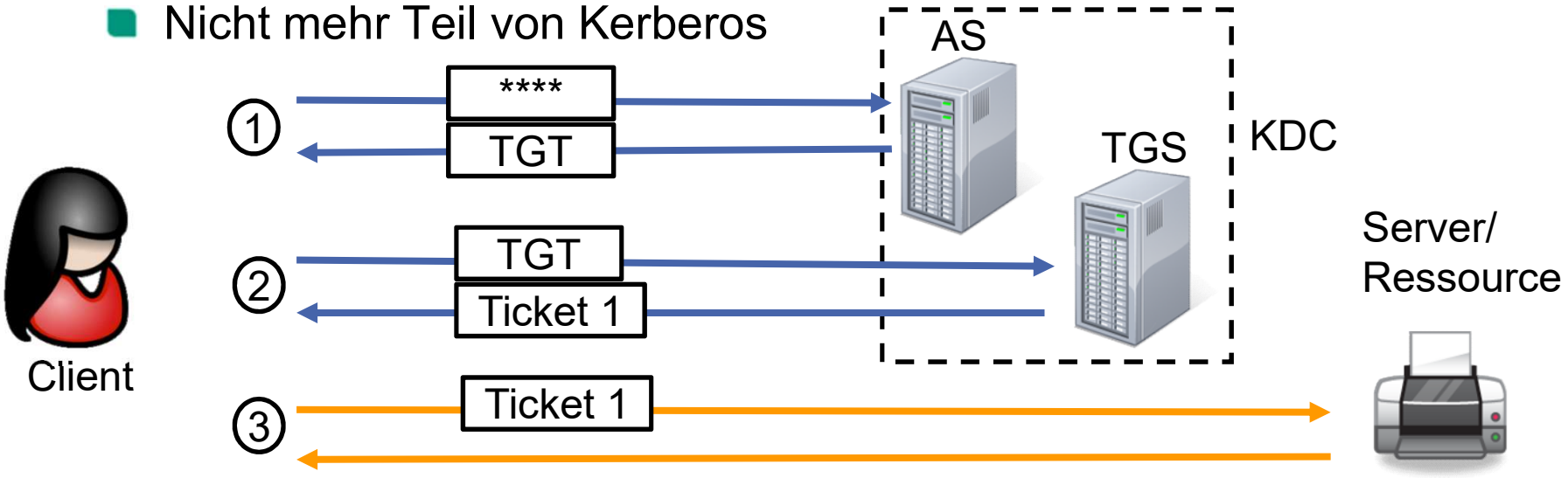
- Zustand vom Server durch Cookie auf Client auslagern

  → Server muss keinen Zustand pro Anfrage speichern

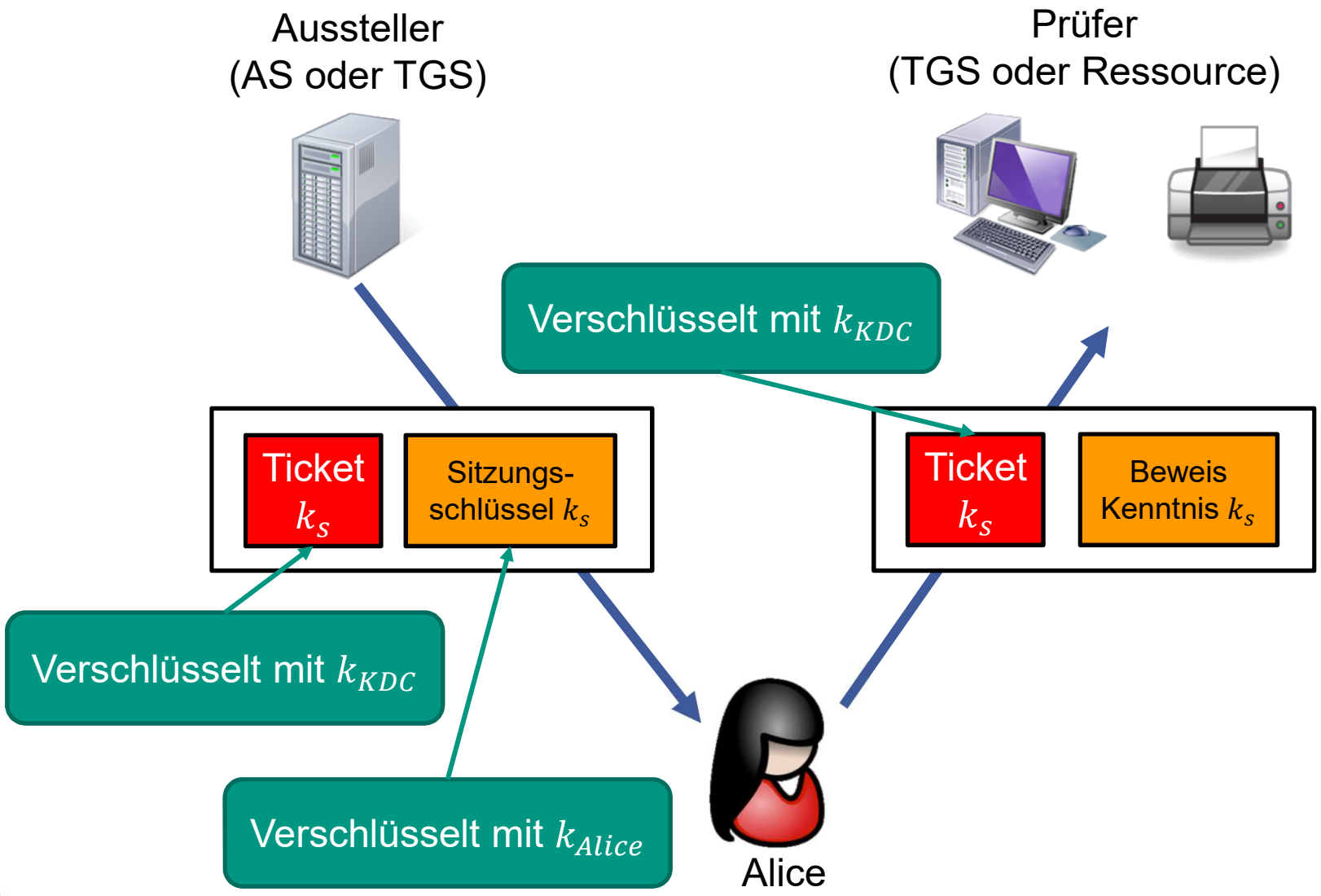


Kerberos-Nutzung: Überblick

1. Anmeldung
   - Client erhält Ticket-Granting-Ticket (= Cookie) vom Authentication-Server
2. Ressourcenanforderung
   - Vorlage des Ticket-Granting-Tickets beim Ticket-Granting-Server
   - Client erhält Ticket für die Ressource
3. Kommunikation mit der Ressource
   - Nicht mehr Teil von Kerberos



Grundprinzip Kerberos-Authentifizierung

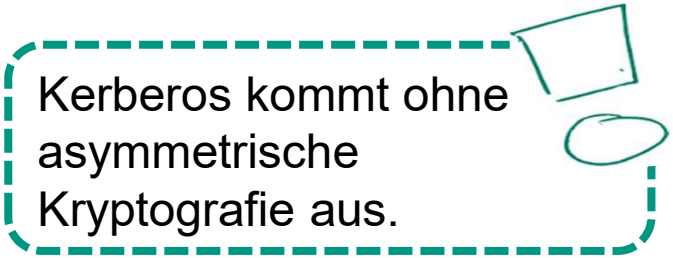


Grundprinzip Kerberos-Authentifizierung

- Aussteller erzeugt Sitzungsschlüssel k_S, den Nutzer und Prüfer erhalten

- k_S ist Bestandteil des Tickets (verschlüsselt mit k_{KDC})
- Zusätzlich k_S verschlüsselt mit k_{Alice} übertragen

- Nutzer legt Ticket Prüfer vor und beweist die Kenntnis vom Sitzungsschlüssel k_S



Überblick verwendeter Schlüssel

- Master-Secret des Client: k_{Alice}

  - Alice und dem KDC bekannt
  - Wird zum Verschlüsseln des Sitzungsschlüssels verwendet

- Master-Secret des KDC: k_{KDC}

  - Nur dem KDC bekannt
  - Wird zum Verschlüsseln des TGT verwendet

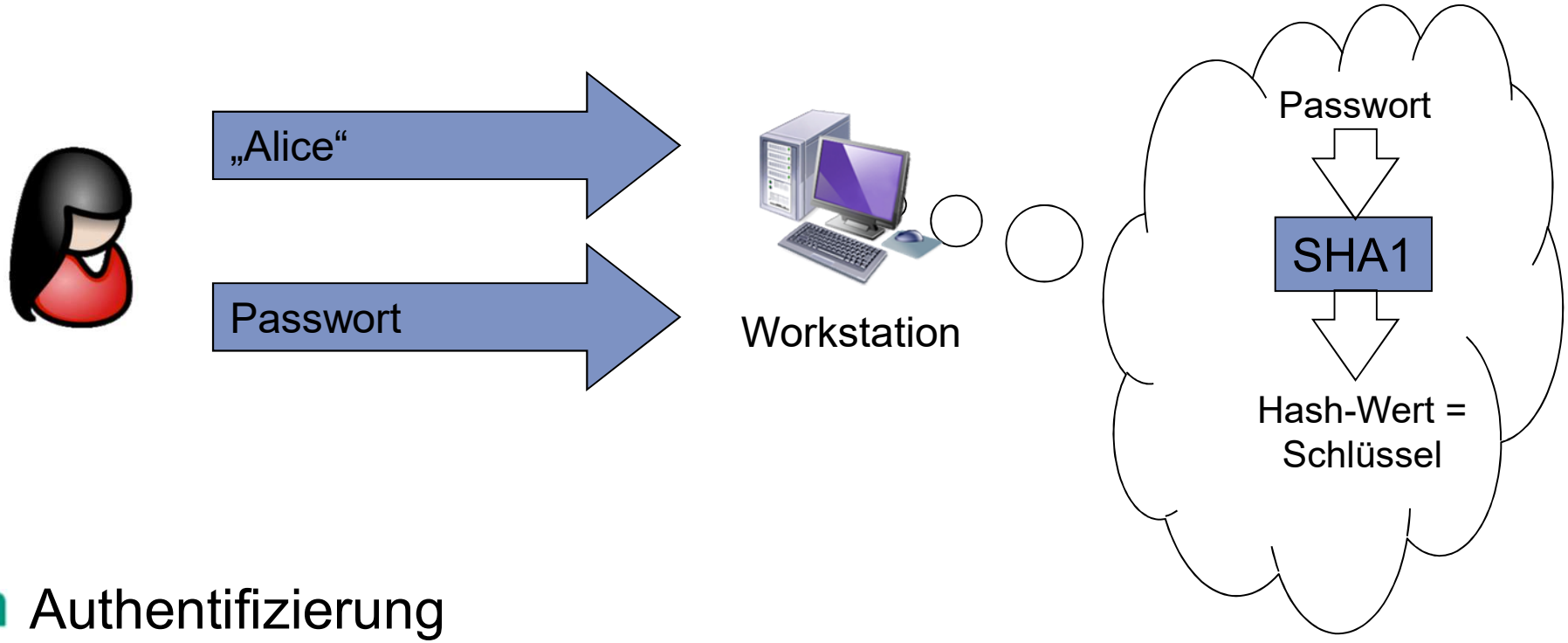
- Sitzungsschlüssel: k_S

  - Temporäre Sitzungsschlüssel zwischen zwei Entitäten
  - Werden vom KDC zufällig pro Sitzung gewählt und mit TGT verteilt

Karlsruher Institut für Technologie

Kapitel 5.2 Kerberos: Schritt für Schritt

Anmeldung an der Workstation

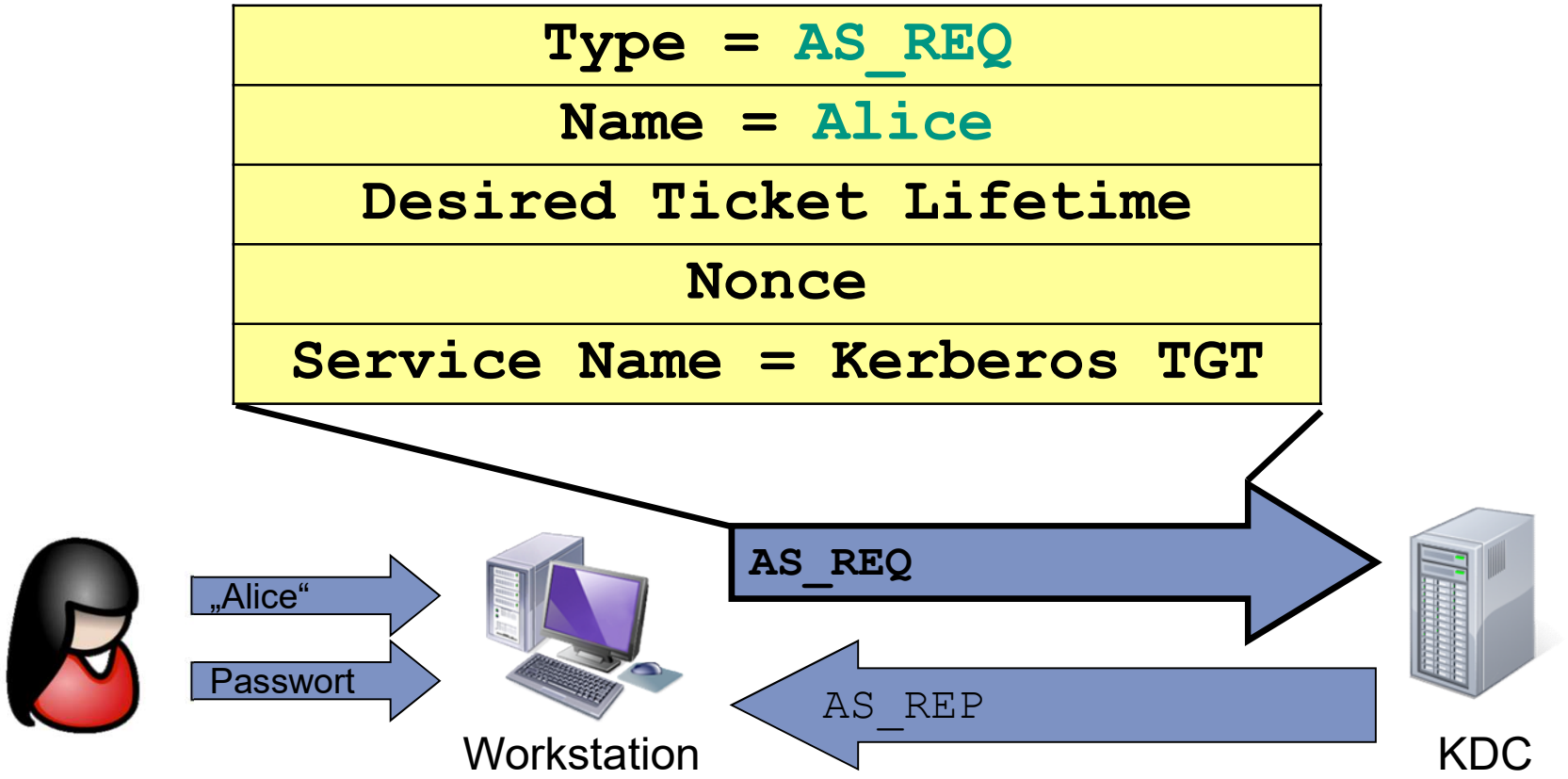


- Authentifizierung
  - Benutzername und Passwort
  - Umwandeln des Passworts in geheimen Schlüssel k_{Alice}
    - Master-Secret des Clients k_{Alice}
    - Umwandlung durch Hash-Funktion (z.B. SHA1)

[RFC4120]

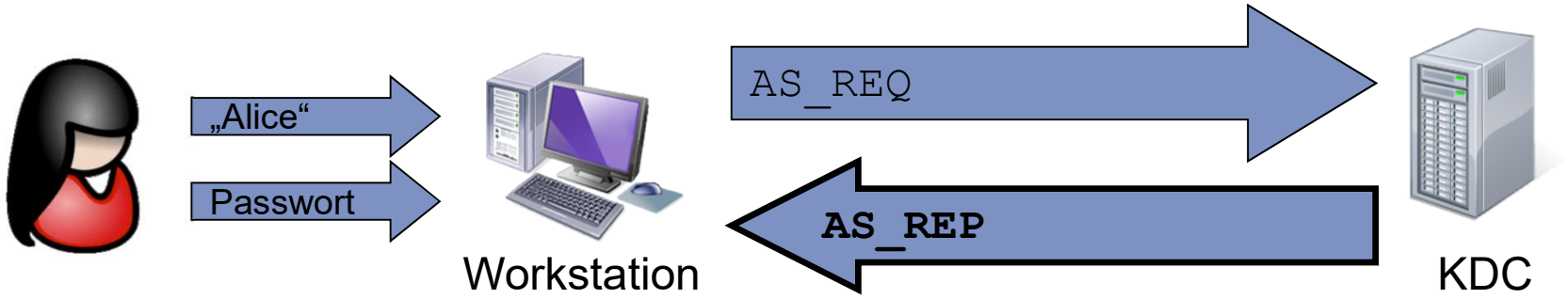
Anmelden am Netz

- Authentication Server Request (AS_REQ)
  - Übertragen des Benutzernamens im Klartext zum KDC
    - Angreifer kann Identität von Alice abhören



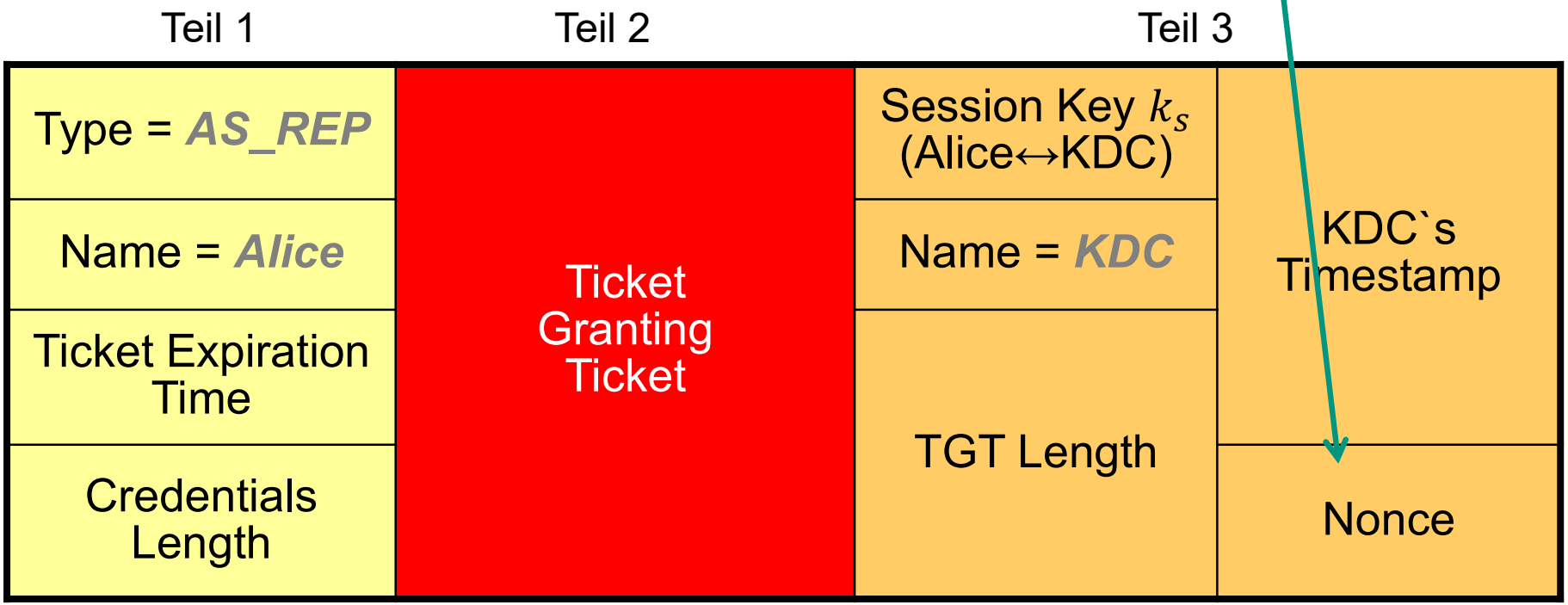
Anmelden am Netz

- Authentication Server Reply (AS_REP)
  - Teil 1: Allgemeines (Typ …)
  - Teil 2: Ticket-Granting Ticket (TGT)
    - Verschlüsselt mit dem Master-Secret des KDC k_{KDC}
  - Teil 3: Transport des Sitzungsschlüssels
    - Verschlüsselt mit Master-Secret von Alice k_{Alice}
      - Verschiedene Verfahren unterstützt, u.a. AES
    - Enthält geheimen Sitzungsschlüssel (Session Key) k_s



Vereinfachtes Paketformat *AS_REP*

Nonce aus AS_REQ:
Schutz vor Replay-Angriffen



Verschlüsselt mit Master-Secret des KDC k_{KDC}

Verschlüsselt mit Master-Secret von Alice k_{Alice}

Ticket Granting Ticket (vereinfacht)

Client Name	`Alice`
Network Layer Address	`192.168.178.55`
Session Key	`(Alice` ↔ `KDC)`
Ticket Lifetime	`60`
KDC`s Timestamp	`9:20am`
Server Name	`KDC`

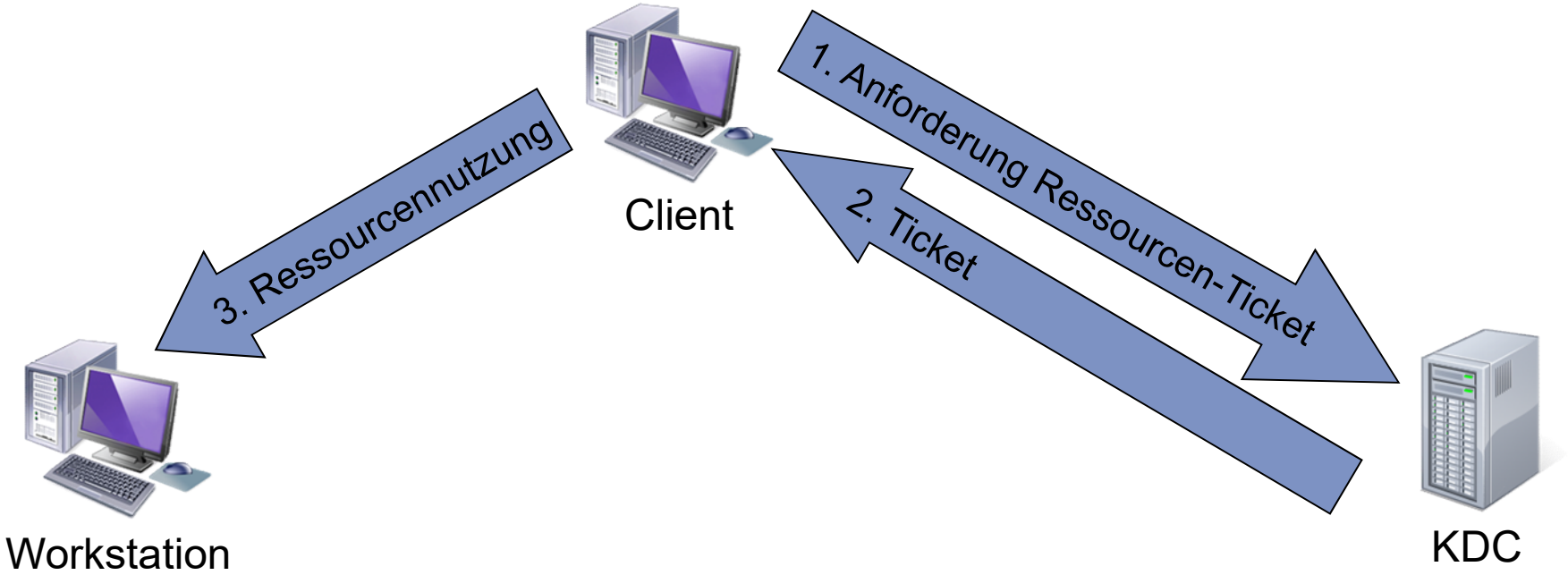
Verschlüsselt mit dem Master-Secret des KDC k_{KDC}

Zusammenfassung Anmeldevorgang

- KDC authentifiziert Alice anhand
  - Kenntnis des Master-Secrets von Alice k_{Alice}
    - Aus Passwort abgeleitet
    - In Benutzer-Datenbank des KDC
- Ticket-Granting-Ticket
  - KDC kann damit vorherige Authentifizierung überprüfen
  - Auslagerung des Server-Zustands
- Alice und KDC verfügen nach Anmeldevorgang über einen Sitzungsschlüssel $k_{S(Alice,KDC)}$
  - Master-Secret von Alice k_{Alice} muss nicht mehr verwendet werden
  - Langlebiges Geheimnis geschützt
  - Sitzungsschlüssel in TGT

Ressourcenanforderung

- Ressourcen-Nutzung nach Vorlage des TGT beim TGS
  - Ticket-Granting-Server (TGS) gibt Ressourcen-Tickets aus
  - Zugangskontrolle durch jede Ressource
  - Erweiterung: Zugriffsbeschränkung durch KDC
    - Ausstellung eines Tickets anhand zusätzlicher Informationen



Anfordern eines Ressourcen-Tickets

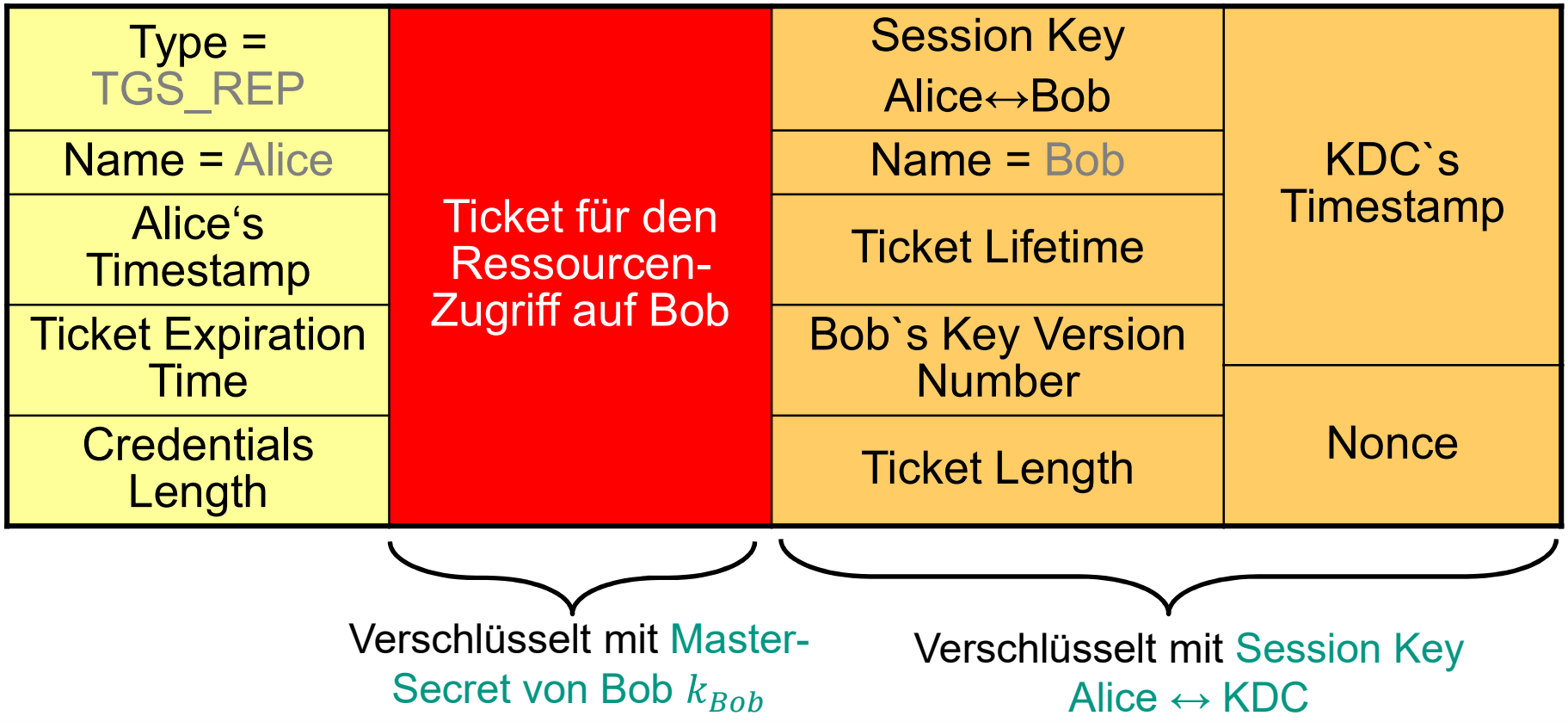
→ Alice möchte ein Ticket für Bob

- Ticket-Granting Server Request (TGS_REQ)
  - Enthält TGT
  - Ressourcen-Name
  - Authenticator
    - verschlüsselt mit Sitzungsschlüssel
- Überprüfung durch Ticket-Granting-Server
  - Absenderadresse
  - Name
  - Zeitstempel

Type = **TGS_REQ**
KDC`s Key Version Number
TGT
Authenticator
Alice`s Timestamp
Desired Ticket Lifetime
Nonce
Server Name = Bob

Anfordern eines Ressouren-Tickets

- Ticket-Granting Server Reply (TGS_REP)
  - Session Key Alice ↔ Bob
  - Ticket verschlüsselt mit Master-Secret der Ressource



Diskussion

- Warum tauscht Kerberos einen Sitzungsschlüssel aus und verwendet nicht das Master-Secret der Ressource für die Kommunikation?
- Warum erfolgt der Zugriff auf Ressourcen über den Umweg über das TGT?

Zusammenfassung Ressourcen-Anforderung

- Vorlage TGT
  - Ticket Granting Ticket beim Ticket Granting Server
  - Ticket Granting Server muss keinen Zustand halten
  - Wiedergewinnung des Sitzungsschlüssels Alice ↔ KDC
- Ticket zum Zugriff auf Ressource
  - Ausgestellt durch Ticket Granting Server
  - Enthält vom TGS erzeugten Sitzungsschlüssel Alice↔Bob

Kommunikation mit der Ressource

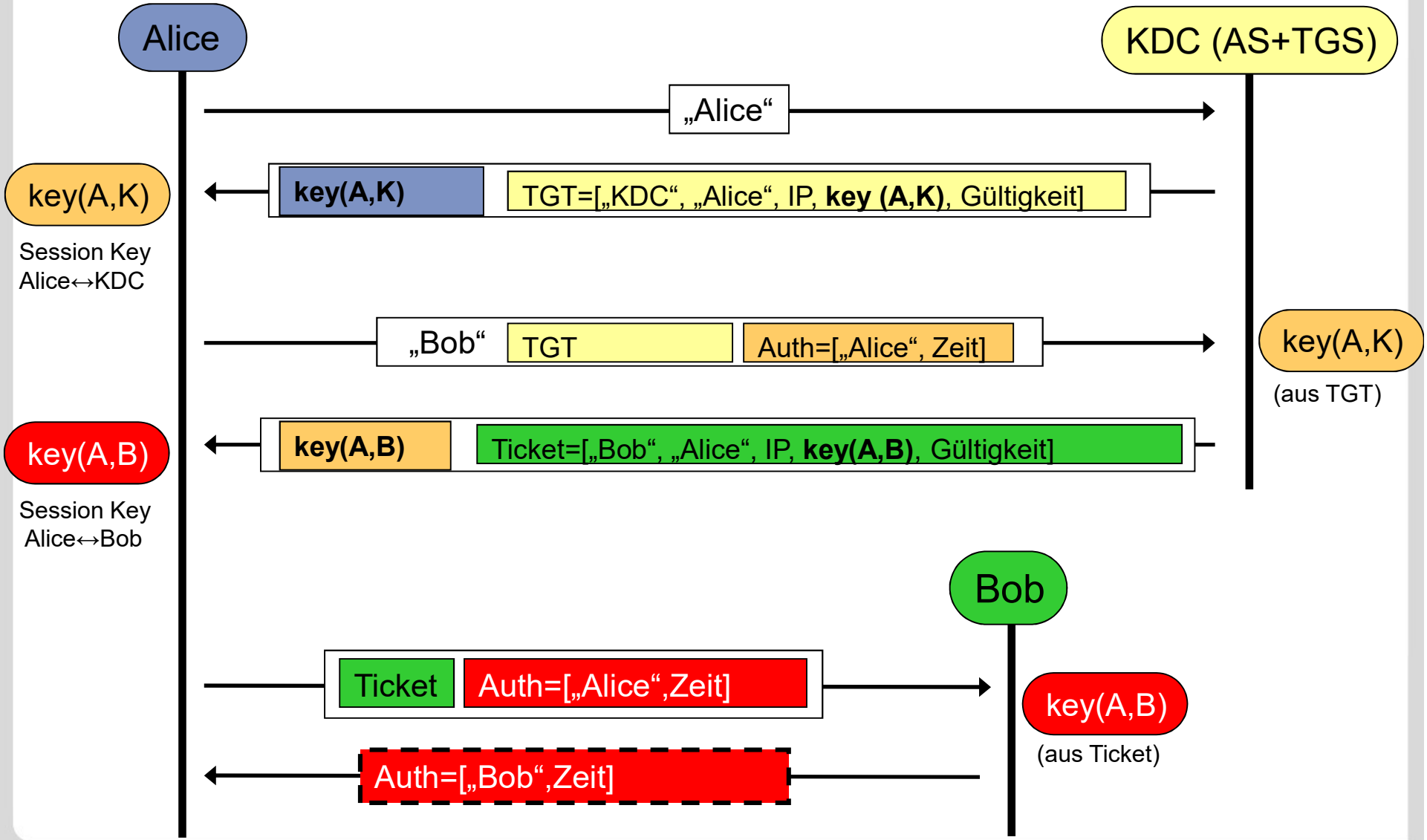
- Application Request (AP_REQ) enthält
  - Ticket und Authenticator
  - Überprüfung durch Ressource analog zu Überprüfung eines TGT durch TGS

Kommunikation mit der Ressource

- Application Reply (AP_REP)
  - Enthält Authenticator
  - Danach Austausch der Anwendungsdaten (ungeschützt!)
    - Integritätsschutz oder Verschlüsselung mit Integritätsschutz, …
      → Aufgabe der Anwendungsprotokolle

- AP_REP eigentlich in Dokumentation nicht erwähnt, aber von vielen Anwendungen so verwendet

Zusammenfassung Protokollablauf (vereinfacht)



Kapitel 5.3 Diskussion Angriffe, Entwurfsentscheidungen etc.

Offline-Password-Guessing Angriff

- Ziel: Erlangen des Benutzer-Passworts

- AS_REQ und AS_REP abhören und speichern
  - Eindeutig einem Benutzer zuzuordnen
  - Client Name im Klartext enthalten

- Wörterbuch-Angriff
  - Pro Wort aus dem Wörterbuch
    - Wort mittels Hashfunktion in Schlüssel umwandeln
    - AS_REP entschlüsseln
    - Testen der entschlüsselten Nachricht auf Plausibilität
      - z.B. über Zeitstempel
    - Schlüsselkandidaten an weiteren Nachrichten testen
  - Ist Sitzungsschlüssel bekannt, können alle weiteren Nachrichten entschlüsselt werden

Aktive Password-Guessing-Angriffe verhindern

- In Kerberos v4: Aktiver Angriff durch Generierung von AS_REQ für beliebigen Nutzer möglich!
- Neu in Kerberos v5: *Optionaler* Schutz vor aktiven Password-Guessing-Angriffen
  - Passiver Angriff durch Mithören ist auch bei Kerberos v5 weiterhin möglich!
- Preauthentication-Data
  - In AS_REQ enthalten
  - Aktueller Zeitstempel mit Master-Secret des Clients verschlüsselt
  - Authentication Server antwortet nur mit AS_REP, falls Zeitstempel korrekt entschlüsselt wird

Diskussion: Password-Guessing-Angriffe verhindern?

Welche Angriffe werden mit
Preauthentication-Data verhindert?

Welche Angriffe sind weiterhin möglich?

Aktive Password-Guessing-Angriffe verhindern

- Weiterhin möglicher Angriff
  - Ticket für Zugriff auf einen Benutzer beantragen
  - Offline Password-Guessing-Angriff auf dieses Ticket
- Markieren von Benutzereinträgen
  - TGTs nur für menschliche Nutzer
  - KDC stellt keine Tickets zu Clients aus, deren Master-Key aus einem Passwort abgeleitet wird (=meist Benutzer)
- Verbleibende Risiken
  - Brute-Force-Angriffe: Passwort raten, daraus Preauthentication-Data
    - Dauert lange und Logging von fehlgeschlagenen Authentifizierungsversuchen am KDC
  - Passiver Angriff (Abhören + Password-Guessing) weiterhin möglich

Kerberos Credentials

- Ticket-Granting-Ticket
  - Ausgestellt vom Authentication-Server
  - Ermöglicht Nutzung des Ticket-Granting-Servers
- Ressourcen-Ticket
  - Ausgestellt von Ticket-Granting-Server
  - Ermöglichen Nutzung von Ressourcen
- Authenticator
  - Einschränkung von Replay-Angriffen

Aufbau eines Tickets

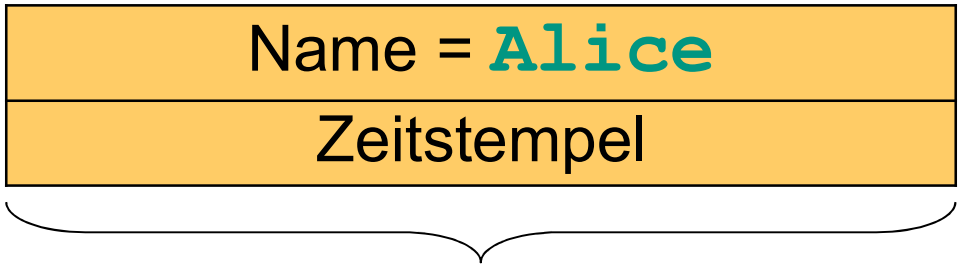
- Ticket für
  - Kommunikation von Alice mit Bob
  - Angefordert von Alice

Client Name	**Alice**
Network Layer Address	**192.168.178.55**
Session Key	**(Alice ↔ Bob)**
Ticket Lifetime	**60**
KDC‘s Timestamp	**9:20am**
Server Name	**Bob**

Verschlüsselt mit Master-Secret von Bob k_{Bob}

Kerberos Credentials

- Authenticator
  - Erzeugt von Alice (=Client)
  - Nur *einmal* einsetzbar
  - Verhinderung von Replay-Angriffen
  - Bedingung: Synchronisation der Systemuhren
    - Nur in Zeitfenster gültig



Verschlüsselt mit dem jeweils verwendeten Schlüssel
(z.B. Session Key Alice↔KDC oder Session Key Alice↔Bob)

Adressen in Tickets

- Optional Netzwerk-Adresse(n) des Clients in jedem Ticket
  - Vergleich der Absender-Adresse mit der enthaltenen Adresse bei Empfang eines Tickets
    - Keine Weitergabe von Tickets möglich
    - Schutz vor *Ticket-Diebstahl*
    - Verhinderung der Nutzung eines abgefangenen Tickets

- Problem
  - Fälschung der Absender-Adresse („IP Spoofing“) einfach
    - Kein wirksamer Sicherheitsmechanismus
  - Funktioniert nicht in Kombination mit Network Address Translation
  - Rechteübertragung ist nicht möglich
    - Gewünscht, z.B. Batch-Prozess, der auf eigene Daten zugreift

Authentifizierung und Autorisierung in zwei Schritten

- Immer zwei Schritte
  - Beantragung TGT beim AS
  - Beantragung Ressourcen-Ticket beim TGS
- Vorteil
  - Master-Secret Client wird nur einmal benötigt
    - Weder Passwort noch abgeleitetes Master-Secret muss im PC gespeichert werden
    - Reduzierte Wahrscheinlichkeit, dass Angreifer bei Kompromittierung des PC langlebiges Geheimnis erlangt
  - Nutzer muss Passwort nur einmal eingeben

Keine Zustandshaltung beim KDC

- Vermeidung der Überlastung zentraler Komponenten
  - KDC muss nicht wissen, wer sich authentifiziert hat
- Vorteil
  - Skalierbarkeit im normalen Betrieb (Speicher)
    - … aber mehr Computing-Power erforderlich
  - Schutz vor Denial-of-Service-Angriffen

Verzicht auf asymmetrische Kryptographie

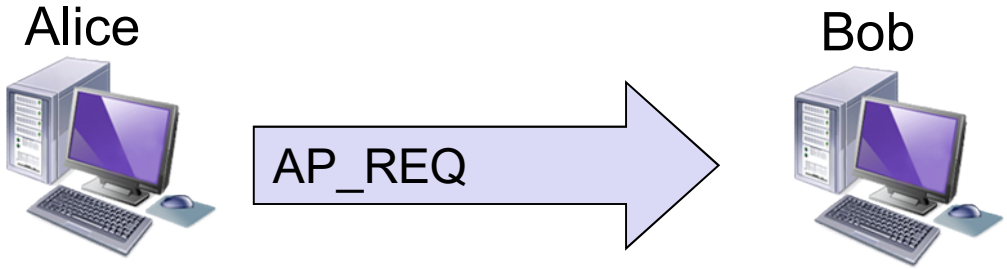
- Keine digitalen Signaturen, keine asymmetrische Verschlüsselung
- … zum Entwurfszeitpunkt (1993) hätte Rechenleistung nicht ausgereicht
- Alternativen
  - Nutzung von Zertifikaten (mit ID Nutzer, Zugriffsberechtigungen)
  - Aber
    - Zentrale Instanz zur Ausstellung der Zertifikate benötigt
    - Widerruf muss während Authentifizierung geprüft werden
    - Privater Schlüssel muss im Hauptspeicher liegen
  - … wird also nicht unbedingt viel einfacher

Karlsruher Institut für Technologie

Kapitel 5.4 Spezielle Eigenschaften von Kerberos

Passwort-Änderung

- Passwort-Änderung
  - Benutzer eines OS kann jederzeit Passwort ändern
    → Änderung beeinflusst nur ihn
  - Änderung des Master-Secrets eines Clients genauso einfach?
  - Problem: Ausgestellte Tickets sind mit Master-Secret des Clients verschlüsselt, das aus dem alten Passwort generiert wurde!



Ticket für Bob ist mit dessen Master-Secret verschlüsselt

Änderung des Passworts
→ neues Master-Secret für Client

- Frage: Werden alle bereits ausgestellten Tickets ungültig?

Passwort-Änderung

- Lösung: Versionsnummer der Schlüssel
  - Speicherung mehrerer Schlüsselversionen
  - Jedes Ticket, jede Nachricht enthält Versionsnummer
    - ID des verwendeten Schlüssels
- Problem: Replizierung des KDCs
  - Verteilung des neuen Master-Secrets auf Slave-KDCs
  - Einloggen mit neuem Passwort unter Umständen nicht sofort möglich
  - Altes Passwort weiterhin gültig
  - → Verwirrung des Benutzers


[RFC3244]

Rechteübertragung

- Kerberos v4: Rechte aus Sicherheitsgründen nicht übertragbar
- In Kerberos v5: Übertragung von Rechten unterstützt

→ Welche Anforderungen würden Sie an ein übertragbares Ticket stellen?

→ Welche Tickets würden Sie in Kerberos übertragbar machen?

→ Wen würden Sie über die Übertragbarkeit von Tickets entscheiden lassen?

Rechteübertragung

- Anforderungen an übertragbares Ticket
  - Zeitliche Beschränkung der Rechteübertragung
  - Beschränkung der übertragenen Rechte durch Besitzer
- Mögliche übertragbare Tickets
  - Ticket Granting Ticket
  - Tickets
- Wer darf über Übertragbarkeit entscheiden?
  - Nutzer (beim Beantragen)
  - KDC (über Richtlinie beim Ausstellen)
  - Ressource (über Akzeptanz bei der Annahme)
  - → Transparenz erforderlich

Vorteile/Nachteile Rechteübertragung

- Vorteile
  - Protokollierung aller Rechteübertragungen durch KDC
  - Beschränkung der Rechteübertragungen durch KDC und Anwendung
- Nachteile
  - Verringerung der Performanz durch Kontaktierung des KDC
  - Komplizierte Zugriffsbeschränkungsregeln im KDC und in den Anwendungen

Übertragbare Tickets in Kerberos v5

- Übertragbare Tickets
  - Forwardable TGT: übertragbares Ticket-Granting Ticket
  - Proxy Ticket: übertragbares Ticket für genau eine Ressource
  - Erkennung übertragbarer Tickets durch Flag
  - Übergabe des dazugehörigen Sitzungsschlüssels mit dem übertragbaren Ticket

- Gültigkeit von Tickets
  - Angabe der IP-Adresse(n), von wo Ticket verwendet werden kann
  - Überall gültig wenn keine IP-Adresse angegeben, mehrere IP-Adressen möglich
  - Restriktion durch IP-Spoofing umgehbar
    - *“Including the network addresses only makes it more difficult, not impossible, for an attacker to walk off with stolen credentials and then use them from a "safe" location.”* (RFC1510)

Einschränkungen übertragbarer Tickets

- Sicherheitsrichtlinien des KDC regelt Vergabe von übertragbaren Tickets
  - z.B. Einschränkung der Ausgabe von Tickets ohne IP-Adresse
- Jede Ressource (Anwendung) regelt Akzeptanz von übertragbaren Tickets für sich
  - Erkennt übertragenes Ticket durch entsprechendes Flag
  - Sicherheitsrichtlinien für jede Ressource (Anwendung)
  - Akzeptanz bzw. Ablehnung von Tickets ohne IP-Adresse

Lebenszeit von Tickets

- Problem der Lebenszeit von Tickets
  - Feste und begrenzte Lebenszeit in Kerberos v4
  - In Kerberos v5 Beschreibung wegen ASN.1 kein Problem
  - Gefahr durch langlebige Tickets
    - Widerrufen schwierig
    - Keine Auswirkung von geänderten Zugriffsrechten auf bereits ausgestellte Tickets

- Zwei neue Arten von Tickets in Kerberos v5
  - *Erneuerbare Tickets* (langfristig gültige Tickets)
  - *Zukünftige Tickets* (Gültigkeitsbeginn in der Zukunft)

Karlsruher Institut für Technologie

Kapitel 5.5 Kerberos in großen Netzen

Diskussion: Kerberos in großen Netzen

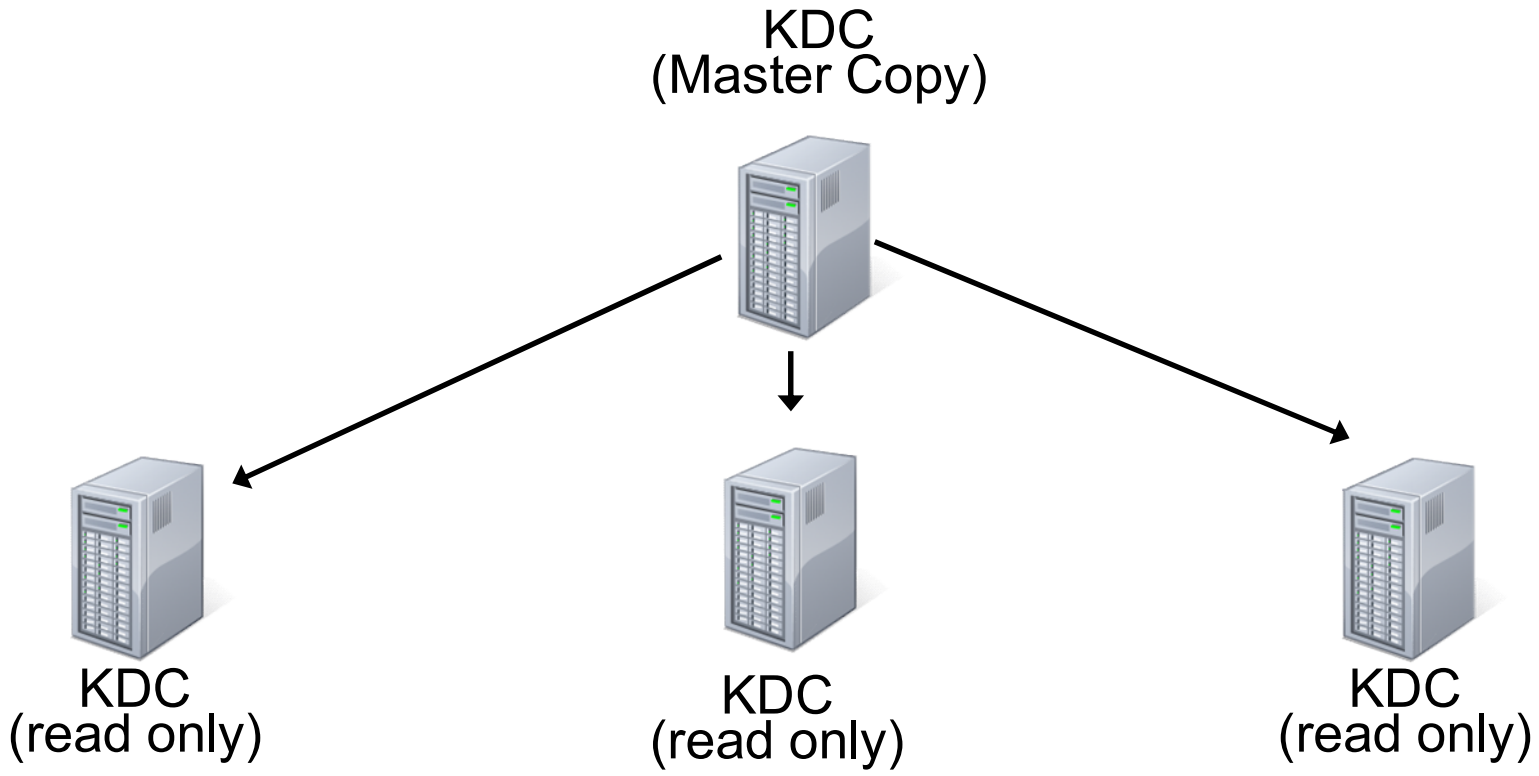
Welche Probleme können Sie sich vorstellen, wenn Kerberos in einem großen Netz eingesetzt wird?

Schlüssel-Server für große Netze

- Einzelner KDC ist *Single-Point-of-Failure*
  - Replizierung des Schlüssel-Servers
- Zentraler Punkt: Wissen aller Master-Secrets
  - Gliederung des Netzes in Domänen
    → so genannte *Realms*

Replizierte Schlüssel-Server

- Alle KDCs besitzen gleiches KDC Master-Secret
  - Eine Master Copy der Benutzerdatenbank
  - Ein oder mehrere *read-only*-Slaves

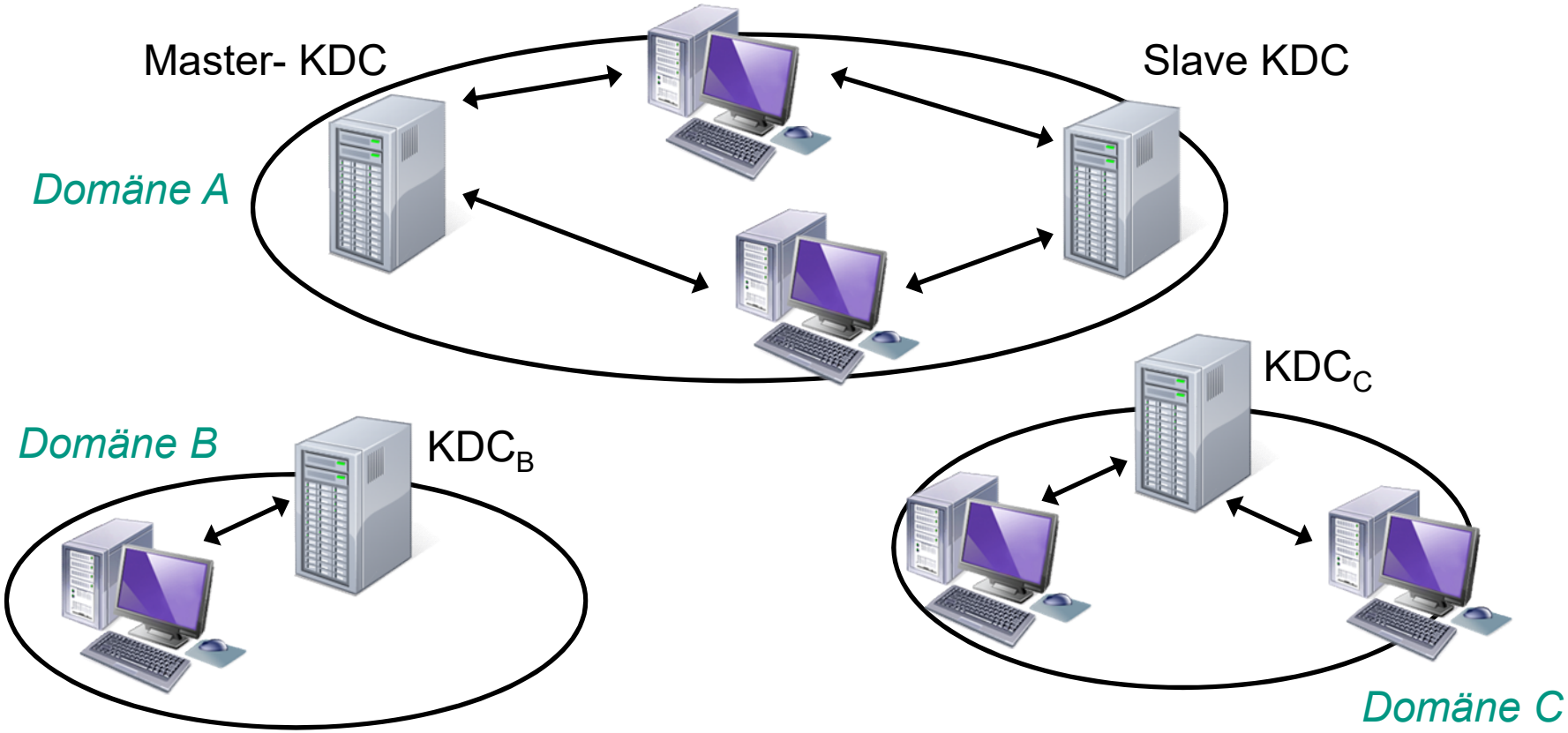


Replizierte Schlüssel-Server

- Master-Copy der Benutzerdatenbank
  - Alle Änderungen auf der Master-Copy
  - Authentifizierung über Master-Copy KDC und read-only KDC
  - Ausfall des Masters
    - Keine Update-Operationen möglich
    - Netz bei Ausfall des Masters aber weiter nutzbar
- Synchronisierung der read-only Slaves
  - Periodisch oder per Administrations-Kommando
  - „Klartext-Übertragung“ mit anschließendem kryptographischen Hash
    - Master-Secrets der Clients verschlüsselt mit KDC Master-Secret
    - Hash zum Schutz vor Manipulation, Vertauschen, Anfügen von Daten

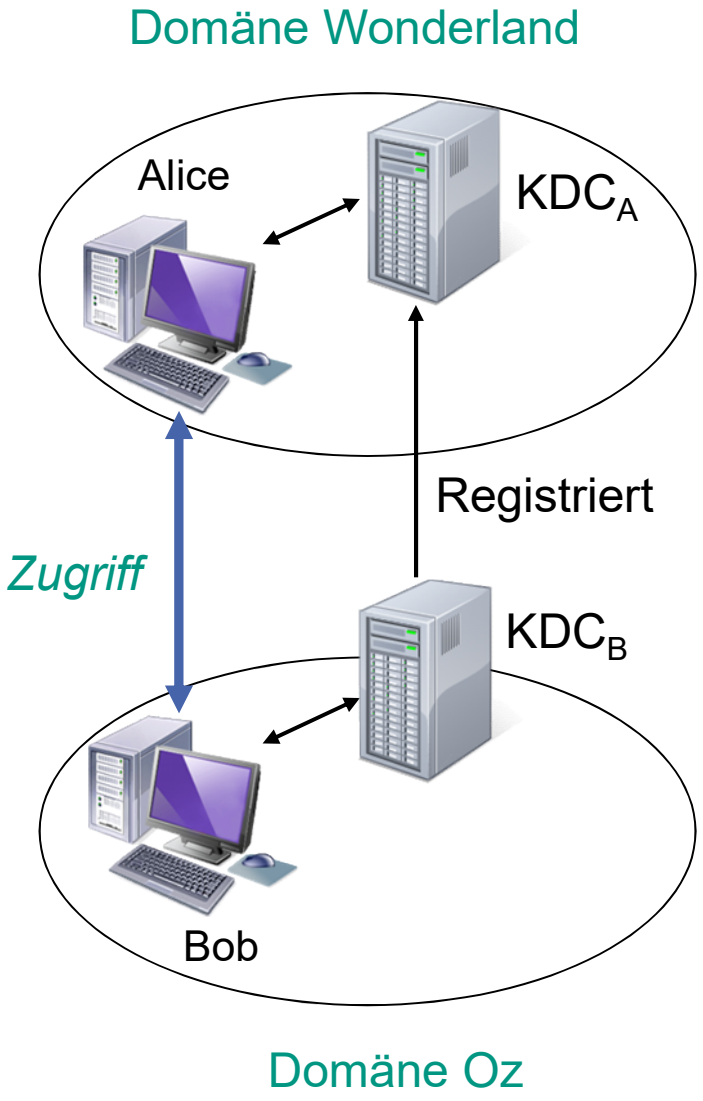
Domänen (Realms)

- Lösung für viele administrative Bereiche: *Domänen*
  - Eigene Benutzer-Datenbank für jede Domäne (Realm)
  - Innerhalb der Domäne Replizierung möglich
  - KDCs einer Domäne besitzen gleiches KDC Master-Secret



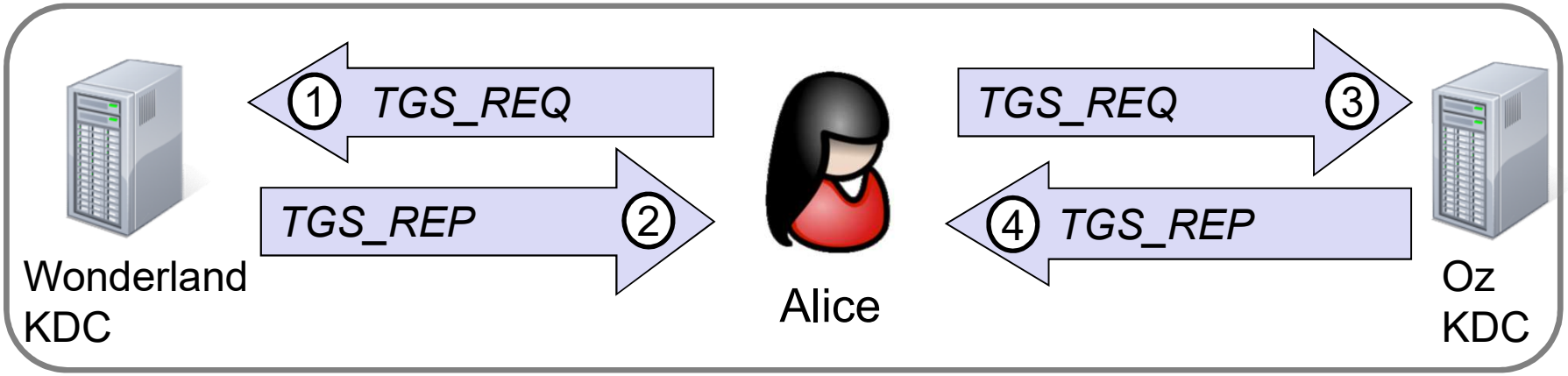
Inter-Domänen-Authentifizierung

- Problem: Authentifizierung über Domänengrenzen hinweg
  - Nutzung von Ressourcen in anderer Domäne
  - Autorisierung durch KDC der anderen Domäne
- Lösung: KDC kann als Client eines anderen KDC registriert sein



Inter-Domänen-Authentifizierung

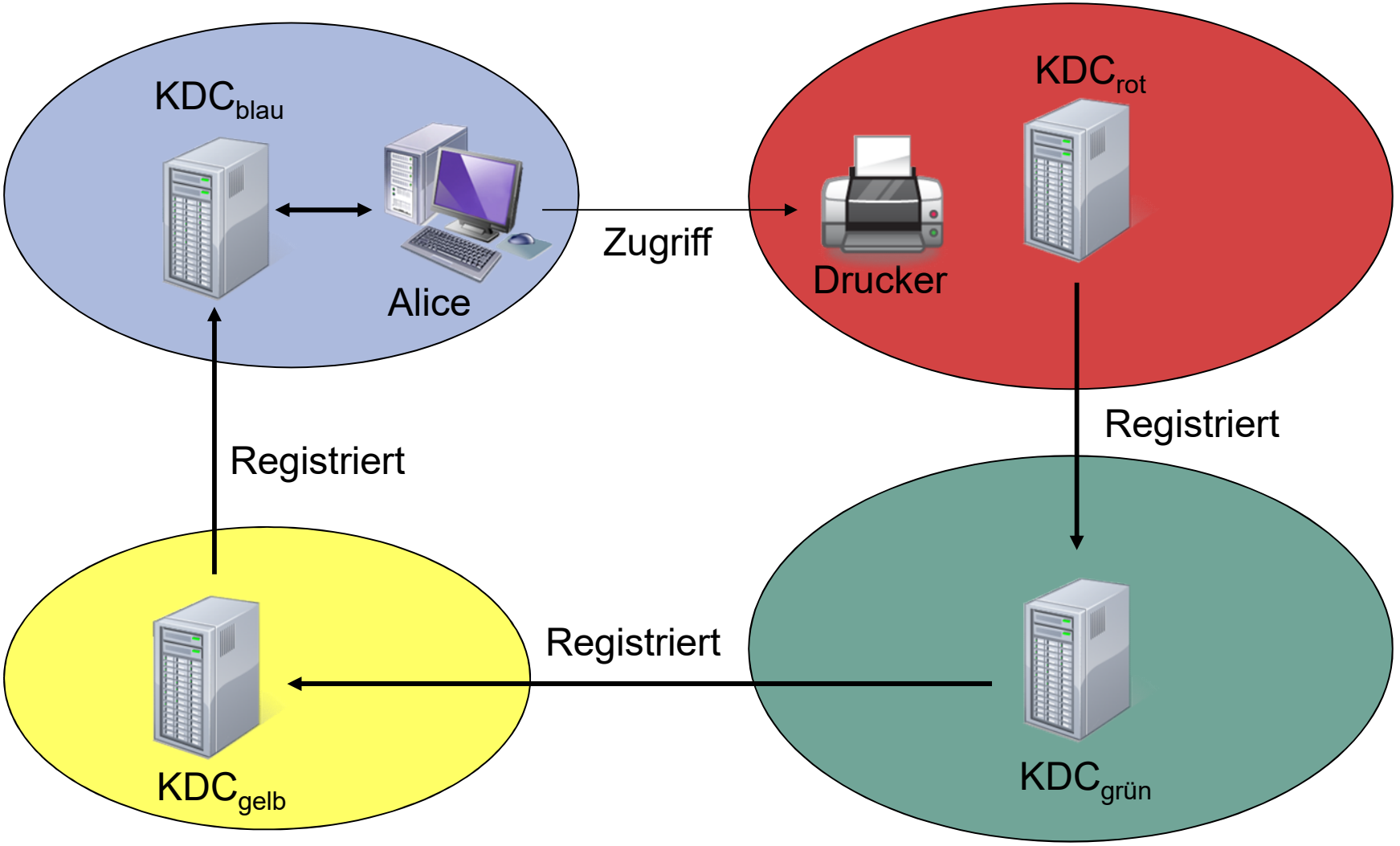
- Alice@Wonderland möchte mit Bob@Oz kommunizieren
  1. Alice fordert Ticket für KDC der Domäne Oz an
  2. Wonderland-KDC erstellt Ticket für Oz-KDC
  3. Alice fordert Ticket für Bob von Oz-KDC an
     - Ticket von Wonderland-KDC als TGT
  4. Oz-KDC erstellt Ticket, mit dem Alice auf Bob zugreift



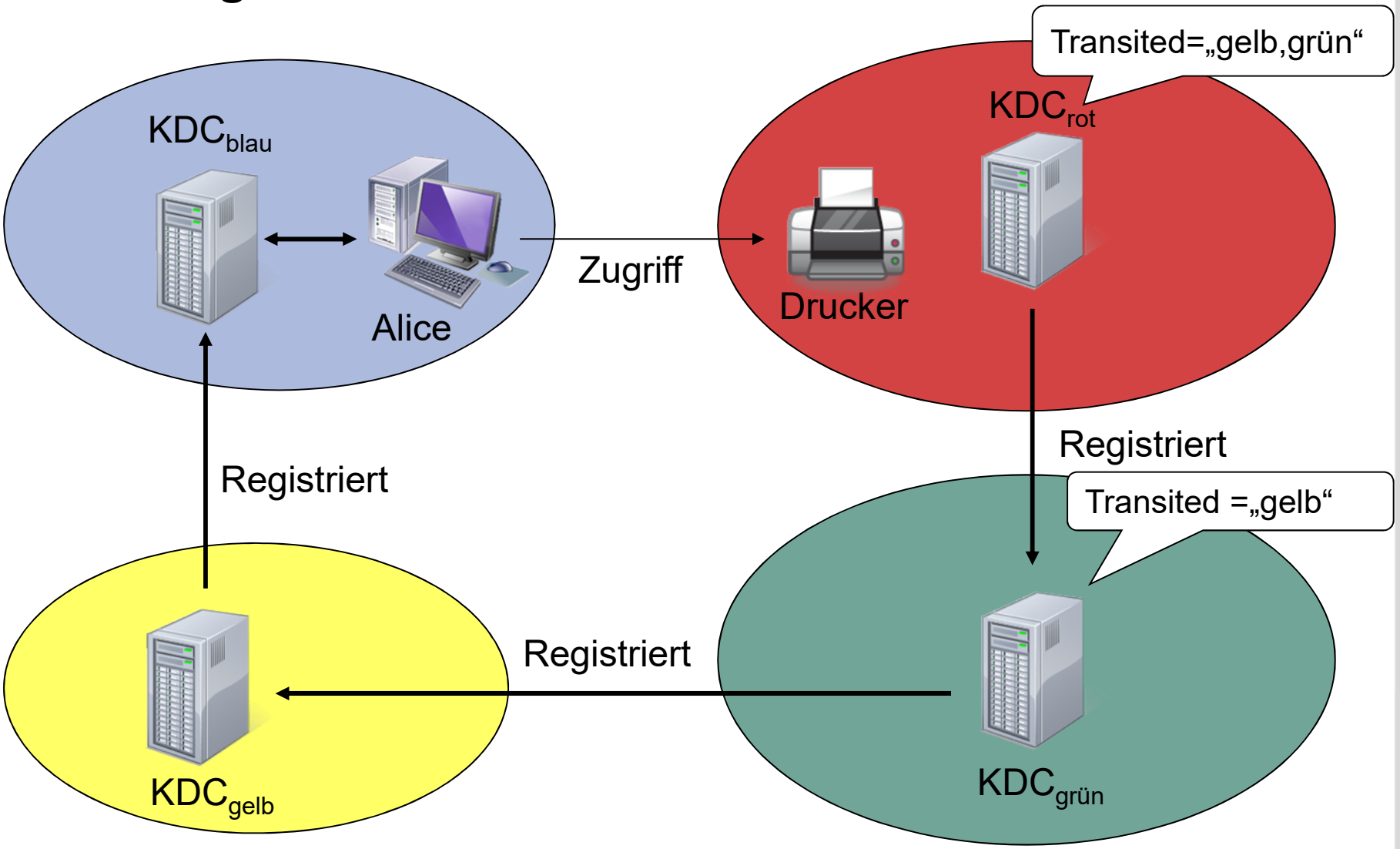
Mehrstufige Domänen

- Verkettung von Inter-Domänen Tickets möglich
  - Neu in Kerberos v5
  - Transited Feld im Ticket
    - Auflistung aller zur Authentifizierung zu durchlaufener Domänen
  - Regelung des Umgangs mit verketteten Inter-Domänen Tickets durch Sicherheitsrichtlinien in Applikation
    - Standard: kürzester Weg durch die Hierarchie bildet Menge vertrauenswürdiger Domänen
- Hierarchische Domänen
  - KDC registriert sich als Client bei KDC der Vaterdomäne
  - Anlehnung an Internet- oder X.500 Name

Mehrstufige Domänen



Mehrstufige Domänen



Karlsruher Institut für Technologie

Kapitel 5.6 Zusammenfassung

Zusammenfassung Kerberos

- Single-Sign-On-Network
  - Authentifizierung mit Benutzernamen und Passwort
  - Anmeldung beim Authentication-Server
  - Anforderung der Ressourcenutzung beim Ticket-Granting-Server
  - „Autorisierung“ durch den Ticket-Granting-Server
  - Schutzmechanismen der Anwendung nicht festgelegt
- Tickets
  - Cookie-Prinzip
  - Übertragung von Rechten möglich
- KDC als Single-Point-of-Failure
  - Replizierung des KDC
  - Mehrstufiges Domänenkonzept

Bewertung Kerberos

- Vorteile
  - Nur ein Passwort zur Anmeldung am Netz (*Single-Sign-On*)
  - Sichere netzwerkweite Authentifizierung
  - Dienst und Nutzer authentifizieren sich gegenseitig
  - Bietet Basis für Erbringung von Vertraulichkeit und Integrität
  - Basiert fast ausschließlich auf symmetrischen Verfahren
- Nachteile
  - KDC Master Secret befindet sich auf dem KDC
    - Kompromittierung legt alle Master-Secrets der Clients offen
  - Alle Ressourcen müssen angepasst werden (Kerberized)
  - Passwort-Überprüfung durch Challenge-Response nur optional
  - Enge Synchronisation der Uhren der Netzkomponenten notwendig

Literatur

[Proe11] Mark Pröhl; Kerberos – Single Sign-on in gemischten Linux/Windows-Umgebungen; dpunkt.verlag, 2011

[RFC3244] M. Swift, J. Trostle, J. Brezak; Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols; RFC 3244, Februar 2002; http://tools.ietf.org/rfc/rfc3244.txt

[RFC4120] C. Neumann, T.Yu, S. Hartman, K. Raeburn; The Kerberos Network Authentication Service (V5); RFC 4120, July 2005; http://tools.ietf.org/rfc/rfc4120.txt

[Sorg13] Sorge, Gruschka, Lo Iacono, Sicherheit in Kommunikationsnetzen, Oldenbourg-Verlag, 2013, ISBN-13: 978-3-486-72016-7