Sicherheit in der Informationstechnologie

Universitatea “Transilvania” din Brasov

5. Authentifizierung - Teil: Kerberos

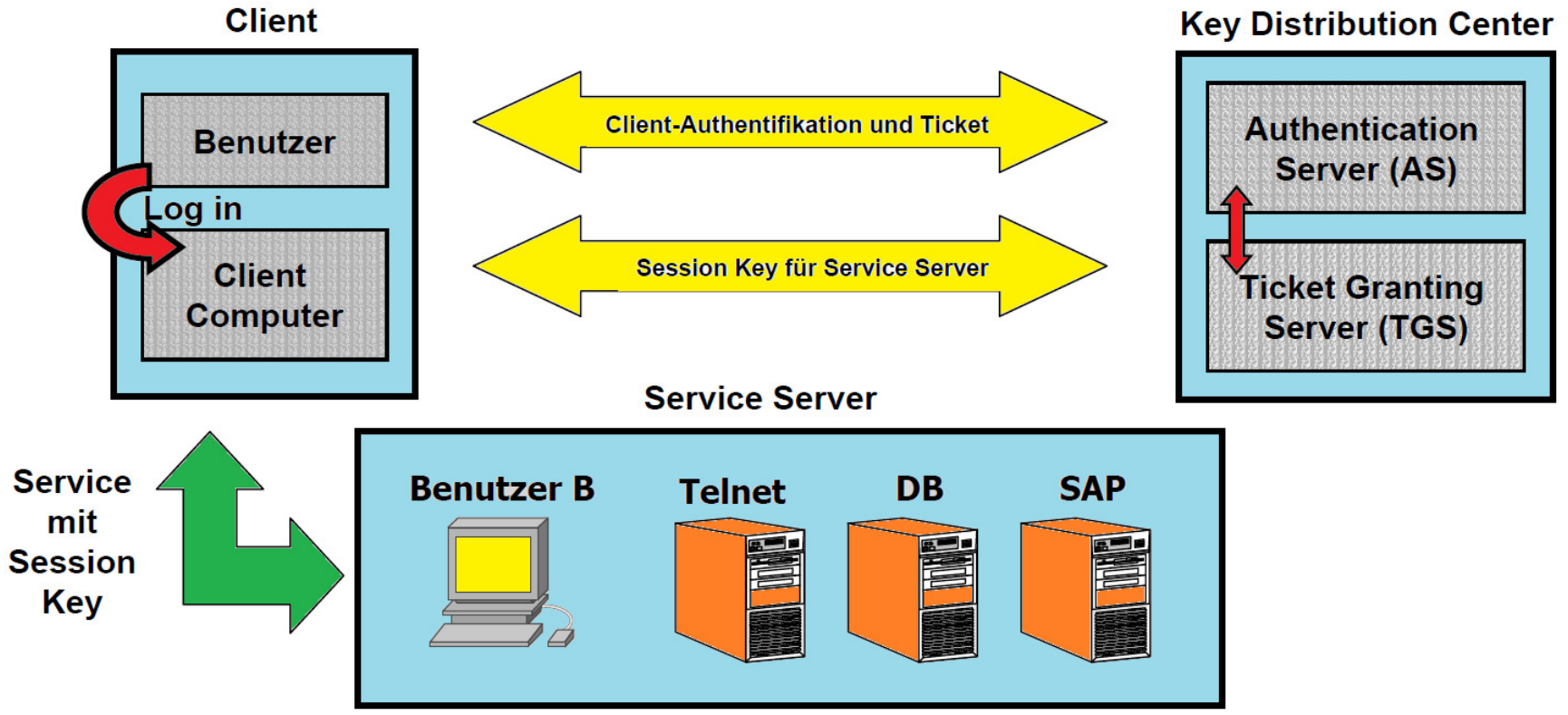
1. Wissen und Besitz
2. Challenge Response Verfahren
3. Kerberos
4. Chipkarte und Biometrie
5. Single Sign On

Kerberos

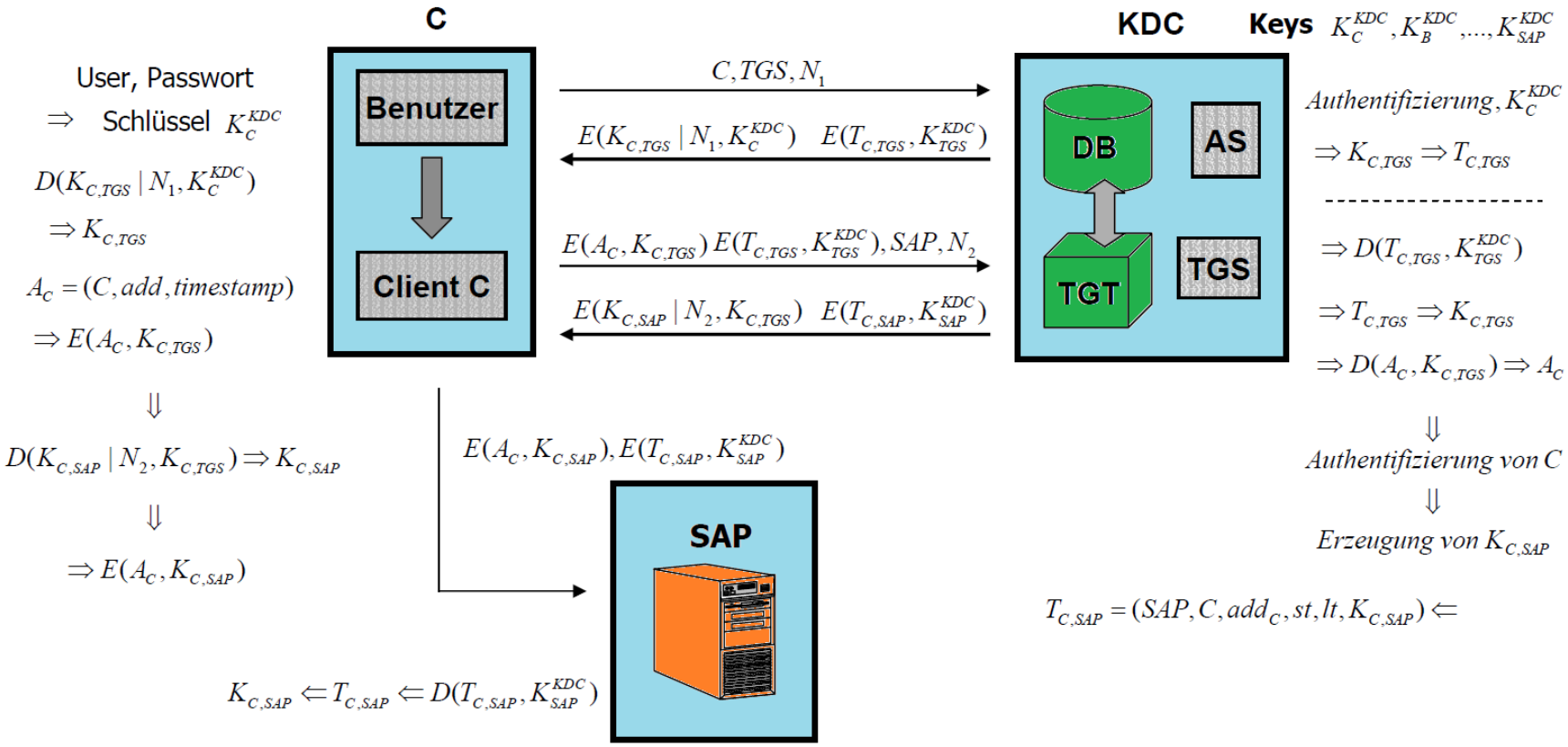
- **Authentifizierungsmechanismus** für verteilte Client/Server-Systeme.
- 1986 vom MIT (Massachusetts Institute of Technology) in Zusammenarbeit mit IBM und DEC entwickelt.
- **Ziel:** authentifizierter Zugriff auf Netzwerkdienste.
- **Funktionalität:**(A) Authentifizierung der Principals
  (B) Erzeugung und Verteilung einmaliger Sitzungsschlüssel
- **Idee:** Ticket-Granting Ticket to get a service ticket after authentication
- Basiert auf dem Needham-Schroeder Protokoll erweitert durch Zeitstempel
- Verschlüsselung durch **symmetrische Verschlüsselungsverfahren**, die ab Version 5 zwischen Client und Server ausgehandelt werden können
- Durch eine Hierarchie von **Authentifikationsservern,** die jeweils autonom in ihrem Bereich (engl. Realm) Tickets für Sitzungsschlüssel vergeben, können auch Services für Clients außerhalb des Zuständigkeitsbereichs ermöglicht werden, ohne dass der Client sich erneut authentifizieren muss; man spricht von kerberosierten Clients und Servern in vernetzten Systemen (Single Sign On).

Prinzip: Kerberos-Protokoll

- Ziel: Geheimer symmetrischer Schlüssel für Kommunikation zwischen Client und Service Server



Kerberos-Protokoll-Verlauf



Kerberos-Protokoll

- **Gegenseitige Authentifizierung**: Auch der Service Server sollte sich gegenüber dem Client authentifizieren; dies ist einfach dadurch möglich, dass dieser den im Authentikator des Clients enthaltenen Zeitstempel je nach Vereinbarung verändert und mit geheimen Session Key $K_{C,S}$ verschlüsselt an den Client sendet. Der Server macht gegenüber dem Client dadurch glaubhaft, dass er die geheimen Schlüssel K_S^{KDC}, $K_{C,S}$ kennt und nur er den Zeitstempel z.B. um 1 erhöht haben kann.
- **Datenintegrität und Nichtbestreitbarkeit: Entsprechend dem Design von Kerberos** ist weder die Integrität der Daten noch die Nichtbestreitbarkeit der Nachricht gegeben.

Mängel des Kerberos-Protokolls

- Wesentliche Mängel des Protokolls in der Version 4 wurden mit der Version 5 beseitigt.
- In Version 5 wird zusätzlich ein Challenge-Response Verfahren angeboten.
- Schwachstelle ist die sichere Geheimhaltung und Verwaltung der Sitzungsschlüssel (im Client-Rechner) zur vertraulichen Kommunikation zwischen Client und Server.
- Gelingt einem Angreifer den geheimen Schlüssel für den Authentikator zu kompromittieren, so kann er die darin enthaltene IP-Adresse des Clients maskieren.
- **Hauptschwachpunkt** ist jedoch die Passwortbasierte Authentifizierung, die durch eine digitale Signatur auf der Basis von Smart Cards (Signaturgesetz) ersetzt werden sollte.
- **Zukünftig:** asymmetrische Verfahren mit signaturgesetz-konformer PKI.
- **Zeitsynchronisation:** Da der Ticket-Granting Server die Ausstellung des geheimen Sitzungsschlüssels für die Kommunikation zwischen Client und Server von der Aktualität des Zeitstempels im Client-Authentikator abhängig macht, können durch Zeitmanipulationen eines Angreifers bereits veraltete Authentikatoren wieder eingespielt werden

Ticket Forwarding von Kerberos

- Tickets sind nur in einem Bereich (Realm) um den KDS gültig, der das Ticket für einen Client ausgestellt hat; möchte dieser aber einen Dienst in Anspruch nehmen, der außerhalb des Gültigkeitsbereichs liegt, so benötigt er ein gültiges Ticket des dafür zuständigen KDS.
- KDS tauschen hierfür entsprechende Daten aus (später).