Netzwerktechnik und Verteile Systeme

Sebastian Simon

Teil 6: Authentifikation

Kryptographie

Ist ursprünglich die Wissenschaft der Verschlüsselung von Informationen

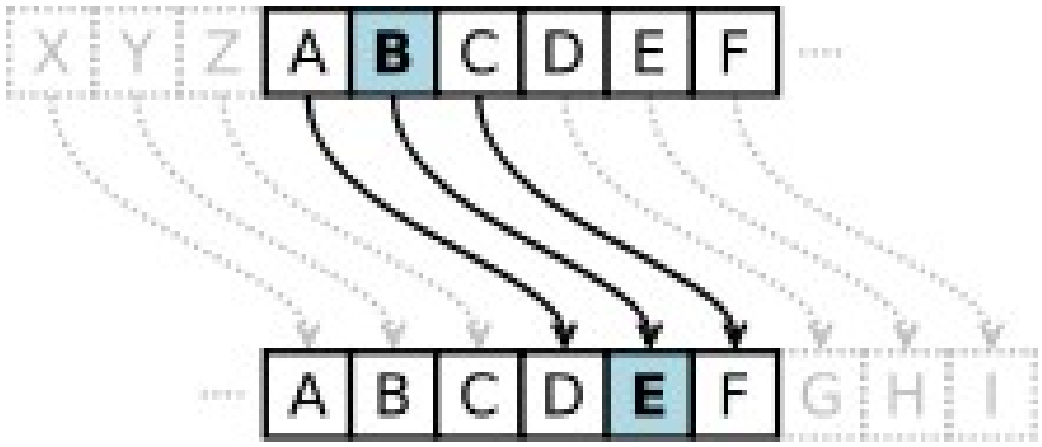
Geschichte der Kryptographie

Kryptographie im Altertum

- Bereits im Altertum gab es Geheimschriften
- Älteste Funde in Mesopotamien und in Ägypten
- Julius Cäsar verwendete die nach ihm benannte Cäsar-Verschlüsselung
  - Schutz militärischer Geheiminformationen
  - Buchstaben werden um definierten Wert rotiert

Cäsar-Verschlüsselung

- Verschlüsselt werden lateinische Nachrichten
- Buchstaben werden um fixen Wert verschoben
- Bekannte Variante ist “ROT13”
  - Buchstaben werden um 13 Stellen verschoben



Knacken der Cäsar-Verschlüsselung

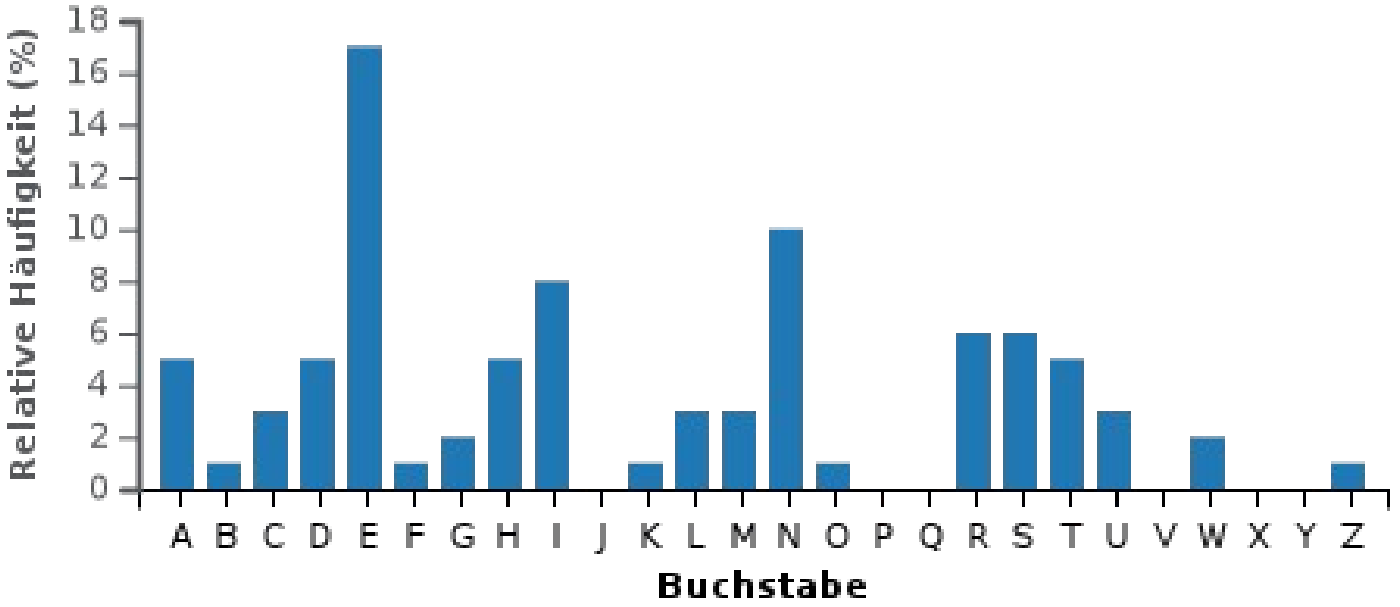
- Für die Verschlüsselung existieren nur 25 mögliche Schlüssel
- Einfaches durchprobieren bringt spätestens nach dem 25. Versuch den Klartext
- Cäsar-Verschlüsselung funktioniert daher nur, wenn auch das Verfahren unbekannt ist
- Moderne Verschlüsselungsverfahren funktionieren, weil der Schlüssel geheim ist, nicht das Verfahren!

Kryptographie im Mittelalter

- Europa hat sich in den Jahren 500 bis 1400 keine Neuerung auf diesem Gebiet entwickelt
- Im arabischen Raum hat der irakische Theologe und Philosoph “al-Kindi” auf diesem Gebiet geforscht
  - Pionier auf dem Gebiet der Kryptoanalyse
  - Knacken von Verschlüsselungen mit Hilfe statistischer Häufigkeitsanalyse
  - Seine Abhandlungen wurden erst 1987 entdeckt

Kryptoanalyse

- Kryptoanalyse ist die Kunst ohne Kenntnis des Schlüssels den Klartext wiederherzustellen
  - zB durch Häufigkeit der Buchstaben in der natürlichen Sprache



Kryptographie in der Neuzeit

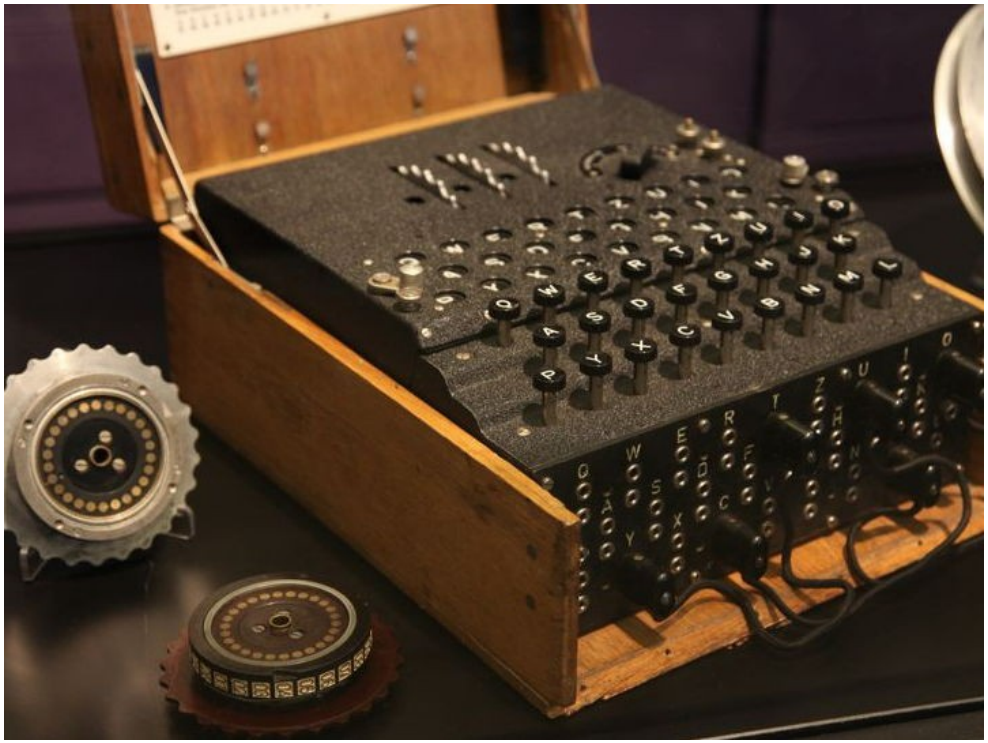
- In der Renaissance erlebt die Wissenschaft der Kryptographie wieder einen Aufschwung
- Ab Ende des 14. Jh. werden seit dem Altertum unveränderte Verfahren weiterentwickelt
- Beispielsweise die nach Blaise de Vigenère (1523–1596) benannte Vigenère-Chiffre
  - Klartext wird durch Schlüsselwort verschoben
  - Mit Schlüssellänge = 1 erhält man Cäsar-Verschl.
  - https://gc.de/gc/

1. Weltkrieg

- Einsatz vergleichsweise simpler Verfahren
  - per Hand mit Papier und Bleistift erreichnet
- Deutsche Code “ADFGX” wurde kurz vor Kriegsende von Franzosen geknackt
- Deutsche Frühjahrsoffensive scheiterte
- Entschlüsselung des deutschen Nachrichten-verkehrs war ein maßgeblicher Grund
  - Paris konnte nicht erobert werden

Enigma

- Bisherige manuelle Verschlüsselungsverfahren waren veraltet, umständlich und unsicher
- 1918 wurde in Deutschland die Enigma erfunden



Enigma (2)

- Ab 1923 auf Messen zum Verkauf angeboten
- Deutsche Militärs wurden rasch darauf aufmerksam
- Eine erneute kryptographische Katastrophe wie im 1. Weltkrieg sollte vermieden werden

Einigma (3)

- Bestandteil der Enigma:
  - Tastatur zur Eingabe
  - Leuchten die den verschlüsselten Buchstaben anzeigen
  - Walzen, Rotoren und Verkabelung sorgen für maschinelle Verschlüsslung
  - https://www.youtube.com/watch?v=-_j_HweXlHI

Enigma (4)

- Im 2. Weltkrieg von der deutschen Wehrmacht tausendfach im Einsatz
- Enigma von 1918 wurde weiterentwickelt und verbessert (zB Walze IV und V zum Tauschen)
- Tagesschlüssel wurde täglich um Mitternacht gewechselt
- Theoretisch 200 Trilliarden Verschlüsselungs-möglichkeiten
- Manuelles knacken unmöglich

Turing-Bombe

- Polen arbeiten bereits vor dem Start des 2. Weltkrieges an der Analyse der Enigma
- Vor der Einnahme Polens durch die Deutschen geben sie ihr Wissen an die Briten weiter
- Codeknackerteam rund um Alan Turing gelingt es während des Kriegs den Code zu knacken
- Turing-Bombe verringert durch Diagonalbrett den Suchraum des Schlüssels dramatisch
- 2014 verfilmt in “The Imagination Game”

Kryptographie und Gesellschaft

- Kryptographie lange Zeit nur Regierungen und Großunternehmen zugänglich
  - Berechnung nur auf teuren, leistungsstarken Großcomputern möglich
- 1991 entwickelt amerikanische Physiker Phil Zimmermann RSA-Verschlüsselung für die breite Öffentlichkeit
- Er nennt sie Pretty Good Privacy (PGP) und veröffentlicht sie

Kryptographie und Gesellschaft (2)

- In den USA gibt es jedoch Exportbeschränk-ungen für Kryptographietechnologie
- Ein Verfahren wegen illegalen Waffenexports wird gegen Phil Zimmermanns eingeleitet
- Nur Aufgrund öffentlicher Proteste wird dieses eingestellt

Kryptographie und Gesellschaft (3)

- In Frankreich ist es noch bis 1996 verboten kryptographische mit einer Schlüssellänge über 40 Bit einzusetzen
  - >40Bit: Schlüssel muss beim Staat hinterlegt sein
  - Heute noch sind bestimmte Kryptographievarianten genehmigungspflichtig

Kryptographie und Gesellschaft (4)

- Den Regierungen ist es ein Dorn im Auge, dass sich ihre Bürger geheim austauschen können
- Diskussionen um Beschränkungen von kryptopgraphischen kochen immer wieder hoch
  - In Österreich zB will die Regierung verschlüsselte Nachrichten von Skype/Whatsapp entschlüsseln

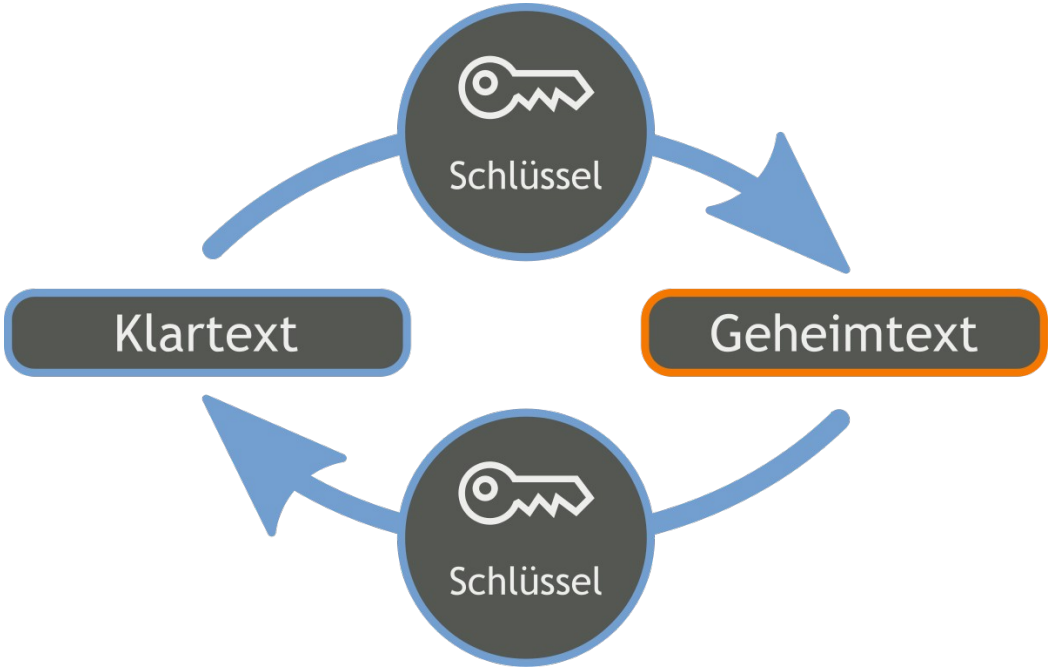
Kerckhoffs' Prinzip

- Kerckhoffs' Prinzip ist Grundsatz moderner Kryptographie
- Sicherheit beruht auf Geheimhaltung des Schlüssels und nicht des Verfahrens
- Alles andere ist "Security by Obscurity"
  - auf Deutsch etwa "Sicherheit bei Unklarheit"
  - Sobald man zB weiß, dass es sich um eine Cäsar-Verschlüsslung handelt, ist der Text schnell geknackt

Gegenwart der Kryptographie

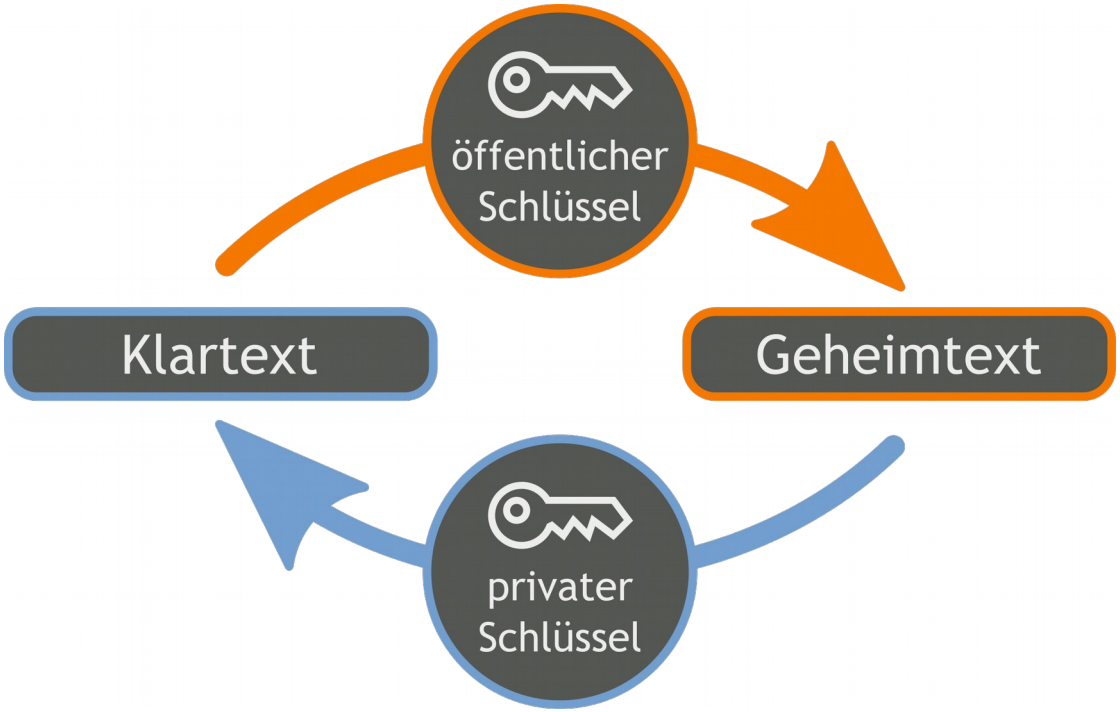
Aktuelle Kryptostandards

- 1976 wurde symmetrische Verschlüsselung “DES” erfunden
  - 64 Bit Schlüssel zum Ver- und Entschlüsseln
  - Heutige Weiterentwicklungen 3DES und AES



Aktuelle Kryptostandards (2)

- Im Jahr 1976 wurde auch das asymmetrische Verschlüsselungverfahren RSA entwickelt
  - nach den Mathematiker Rivest, Shamir, Adleman
- Ein Schlüsselpaar zum Ver- und Entschlüsseln



Symmetrisch vs. Asymmetrisch

- Symmetrische Verschlüsselung
  - Gleicher Schlüssel zum Ver- und Entschlüsseln
  - Ermöglicht die Geheimhaltung von Information
- Asymmetrische Verschlüsselung
  - 2 zusammengehörige Schlüssel (=Schlüsselpaar)
  - Den privaten Schlüssel kennt nur der Eigentümer
  - Ermöglich neben Verschlüsselung auch den Nachweis der Urheberschaft
  - Grundlage für die digitale Signatur

Schutzziele

- Vertraulichkeit → Verschlüsselung
  - Daten können nicht von Dritten gelesen werden
  - Möglich mit synchroner + asynchronen Algorithmen
- Integrität → Prüfsumme/Hash
  - Schutz vor unbefugter Datenmanipulation
- Authentizität → Signatur
  - Ermöglicht Empfänger zu prüfen, ob die Nachricht wirklich von Person X gesendet wurde
  - Nur mit asymmetrischer Verschlüsselung möglich

Hashverfahren

- Hash ist eindeutiger Fingerprint einer Datei
  - 2 Dokumente mit unterschiedlichen Inhalten dürfen (in der Theorie) nicht denselben Fingerprint erhalten
- Wird die Datei nur minimal verändert (1 Bit), ändert sich auch der Hashwert
- Damit kann geprüft werden, dass die Datei seit Berechnung des Hashes nicht verändert wurde

Hashverfahren (2)

- Hash-Verfahren sind Einwegfunktionen
- $y = f(x)$ ist mit wenig Aufwand zu berechnen
- Umkehrfunktion $x = f^{-1}(y)$ nicht/schwer anwendbar
- Beispiele für Verfahren
  - MD5, SHA-1 → gelten bereits als unsicher
  - SHA-2 Familie (SHA-256, SHA-512, …)

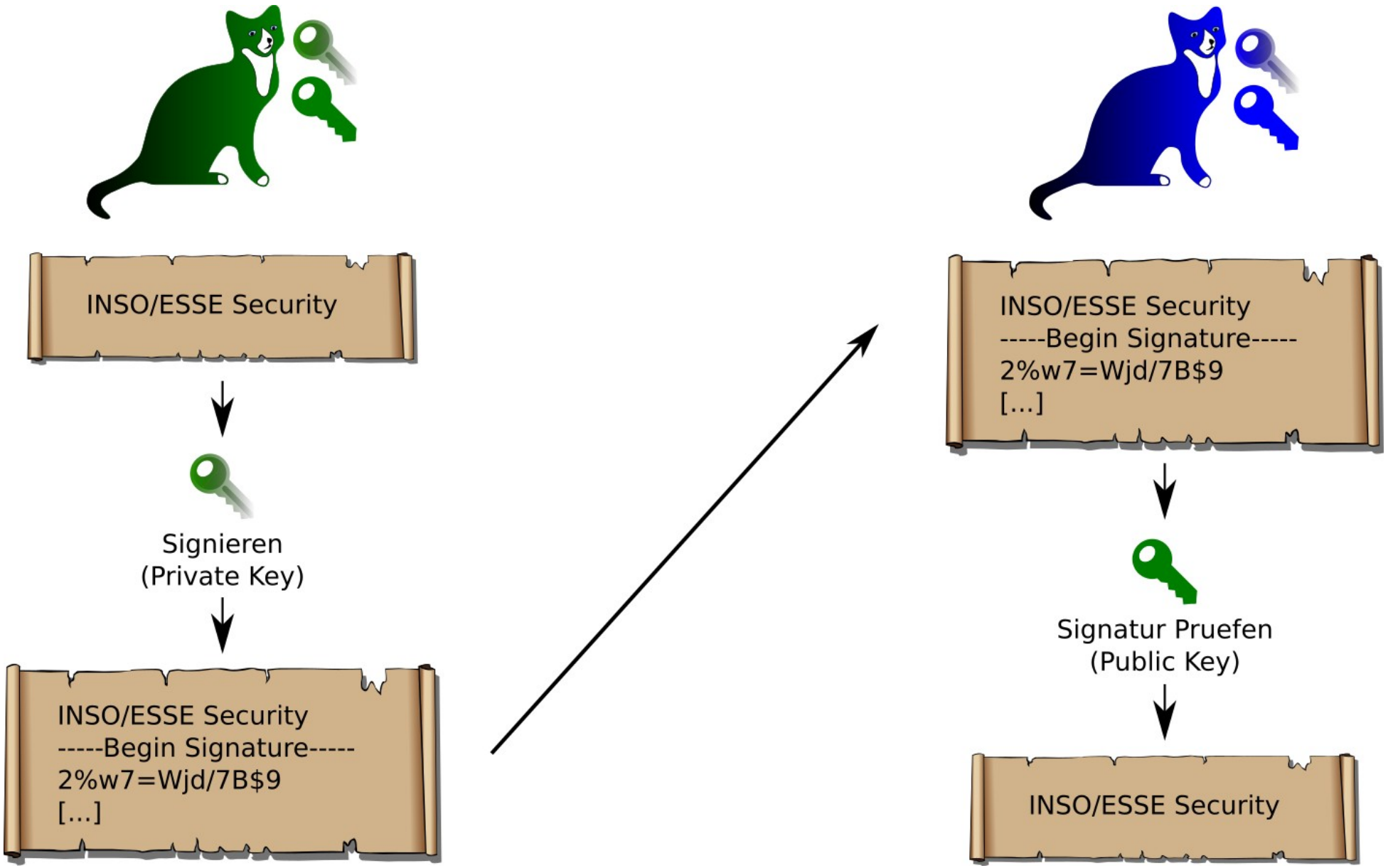
Signatur

- Alice verschlüsselt Daten mit ihrem privaten Schlüssel und sendet sie Bob
  - Privater Schlüssel nur in ihrem Besitz!
- Empfänger Bob kann mit öffentlichem Schlüssel von Alice entschlüsseln
- Empfänger Bob weiß dadurch, dass die Nachricht von Alice stammen muss
  - Niemand sonst kann Nachricht erstellen, die mit ihrem öffentl. Schlüssel enstschlüsselt werden kann

Signatur (2)

- Verschlüsselung großer Dateien sehr rechen-intensiv
- Um Authentizität und Integrität zu garantieren genügt es, den Hashwert einer Datei zu verschlüsseln
  - Empfänger berechnet Hashwert erhaltener Datei
  - Empfänger entschlüsselt Signatur (erhält Hash)
  - Beide Hashes müssen übereinstimmen!

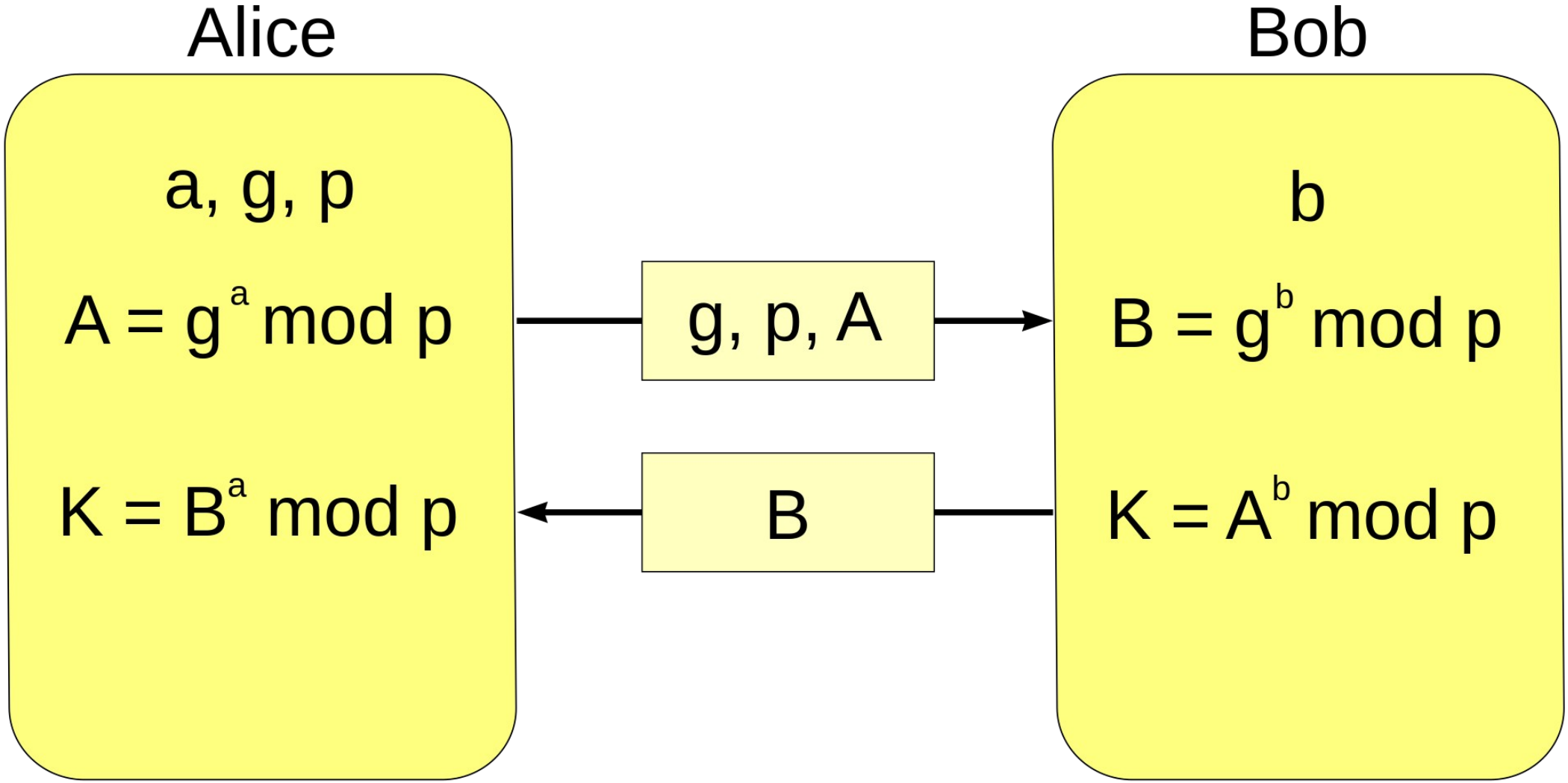
Signatur (3)


INSO/ESSE Security
Signieren
(Private Key)
INSO/ESSE Security
-----Begin Signature-----
2%w7=Wjd/7B$9
[...]
INSO/ESSE Security
-----Begin Signature-----
2%w7=Wjd/7B$9
[...]
Signatur Pruefen
(Public Key)
INSO/ESSE Security

Schlüsseltausch – symmetrisch

- Zwei Personen wollen ihre Kommunikation symmetrisch verschlüsseln
- Problem: Sie müssen sich auf einen gemeinsamen Schlüssel einigen
- Dieser muss geheim bleiben
- Unverschlüsseltes Senden birgt Risiko dass Schlüssel mitgelesen oder manipuliert wird

Diffie-Hellman Schlüsselaustausch



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Schlüsseltausch – asymmetrisch

- Zwei Personen wollen ihre Kommunikation asymmetrisch verschlüsseln
- Jeder sendet dem anderen seinen öffentlichen Schlüssel zu
- Daten werden mit öffentlichem Schlüssel des Empfängers(!) verschlüsselt
- Empfänger kann Daten mit seinem privaten Schlüssel entschlüsseln

Schlüsseltausch – asymmetrisch (2)

- Zwei Personen wollen ihre Nachrichten auf Authentizität prüfen
  - Daten müssen dazu mit privaten Schlüssel des Senders signiert werden
  - Empfänger prüft Signatur mit öffentlichem Schlüssel
- Problem Schlüsseltausch: Angreifer könnte falschen öffentlichen Schlüssel unterschieben
  - Von ihm gesendete Nachrichten wirken dann authentisch (sind mit privaten Schlüssel des Angreifers signiert)

Schlüsseltausch - asymmetrisch(3)

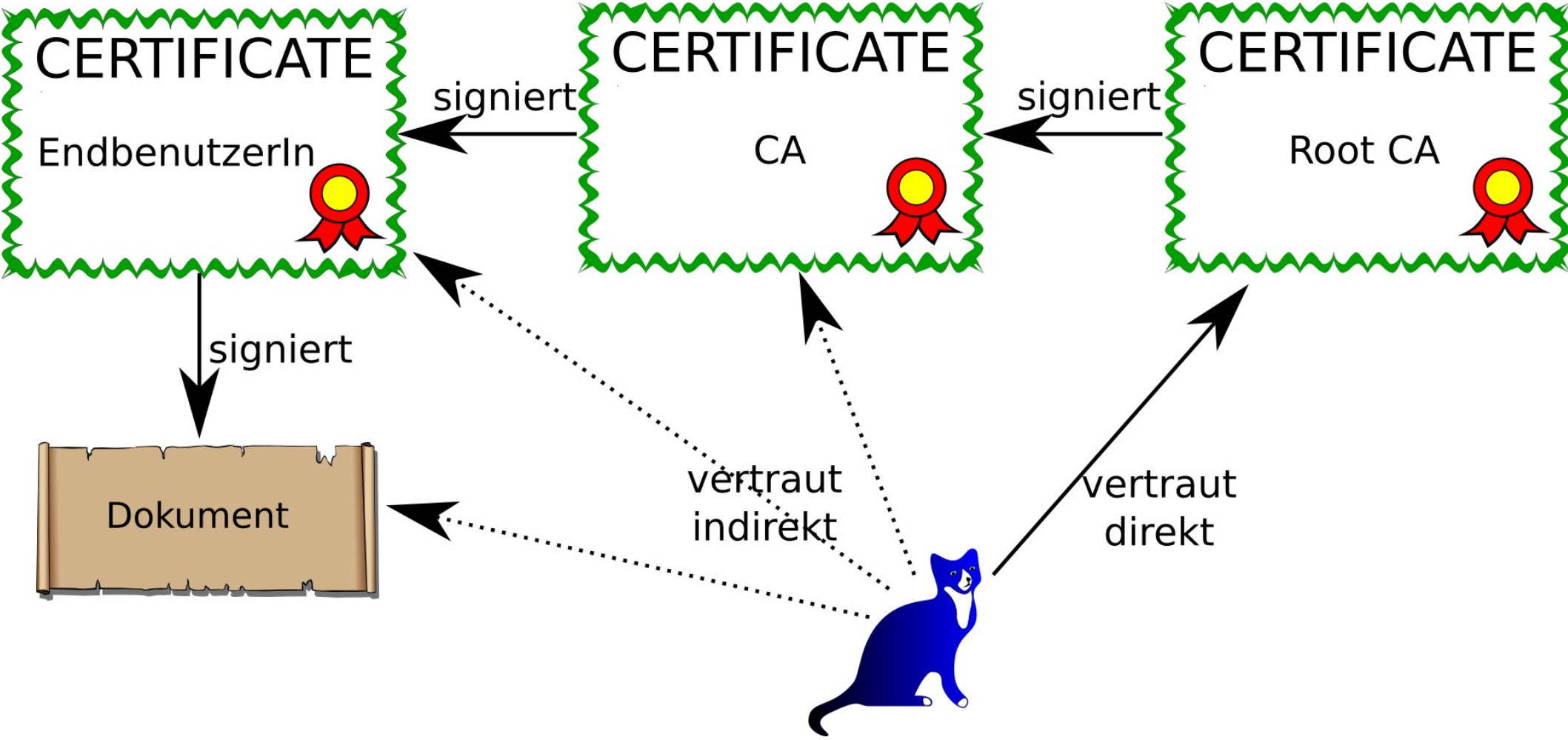
- Austausch der öffentlichen Schlüssel über andere sichere Kanäle möglich (zB USB-Stick)
- Im Internet mit aufgrund der Vielzahl der von Kommunikationsmittel aber unpraktikabel
- Es braucht einen Mechanismus der die Echtheit des jeweiligen öffentlichen Schlüssels garantiert
- Lösung: Public-Key-Infrastruktur (PKI) signiert Schlüssel und bestätitgt damit ihre Echtheit

Authentifizierung in Netzwerken

Public-Key-Zertifikat

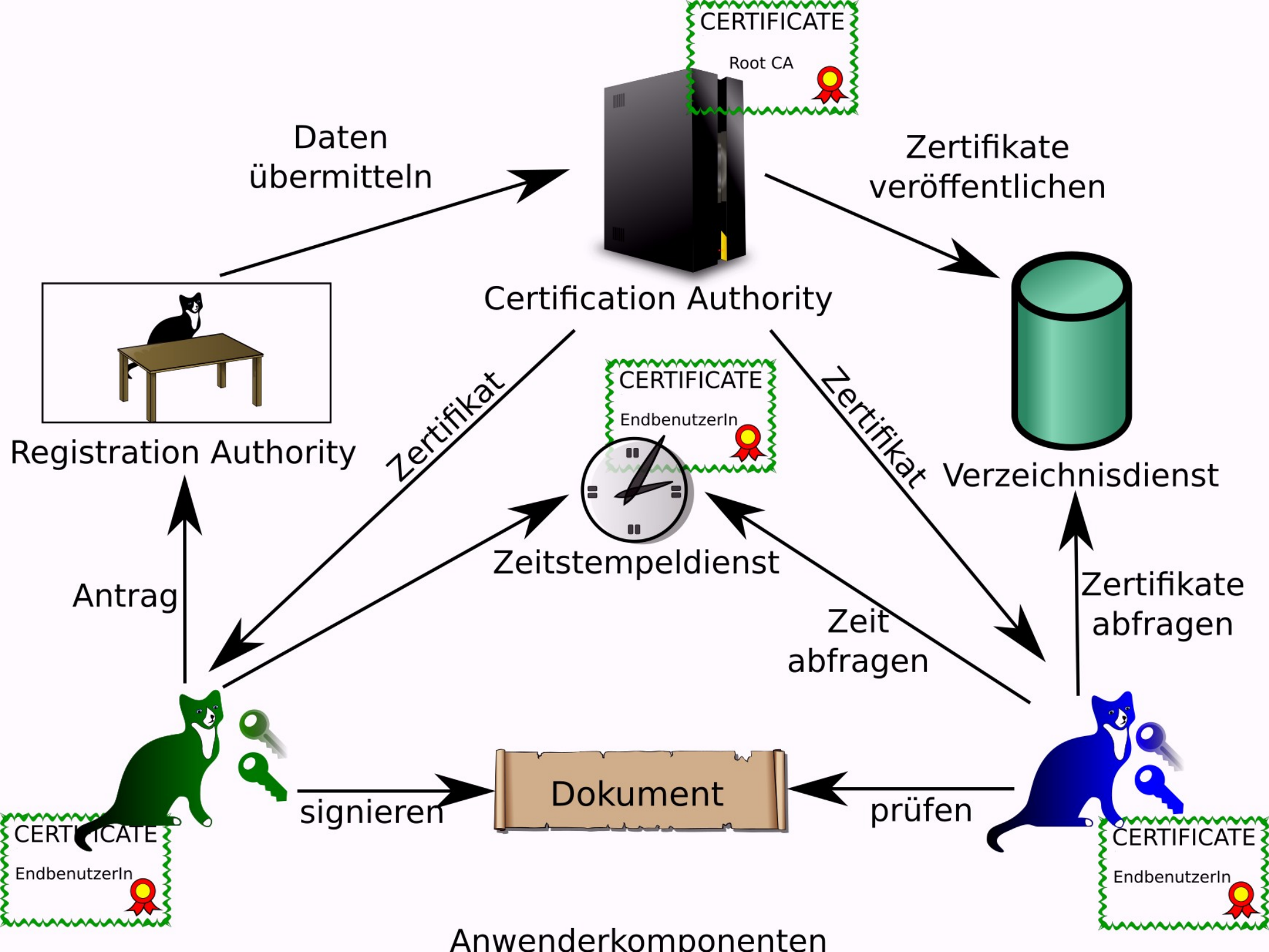
- Bestätigt Eigentümer eines Public-Keys
- Wichtige Bestandteile:
  - Name des Austellers (Issuer)
  - Name des Inhabers (Subject)
  - Der öffentliche Schlüssel
  - Gültigkeitsdauer des Zertifikats
  - Geltungsbereich des Schlüssels
    - zB moodle.htlwrn.ac.at
  - Signatur des Ausstellers über alle Informationen

Zertifikatskette



Zertifikatskette (2)

- Zertifikatskette ist ein Vertrauensmodell
- Am Beginn steht das Vertrauen in die Wurzelzertifizierungsinstanz (Root-CA)
  - zB “Let’s encrypt” von Google
- Durch Vertrauen in die Root-CA kann ich auch den von ihr abgeleiteten Zertifizierungsstellen vertrauen
- Durch vertrauen in die Zertifizierungsstellen kann ich auch den ausgestellten Zertifikaten vertrauen


CERTIFICATE
Root CA
Daten übermitteln
Zertifikate veröffentlichen
Certification Authority
Registration Authority
Zertifikat
CERTIFICATE
EndbenutzerIn
Zertifikat
Verzeichnisdienst
Zeitstempeldienst
Antrag
Zeit abfragen
Zertifikate abfragen
signieren
Dokument
prüfen
CERTIFICATE
EndbenutzerIn
CERTIFICATE
EndbenutzerIn
Anwenderkomponenten

Public-Key-Infrastruktur

- Ermöglicht öffentliche Schlüssel zu zertifizieren
  - Benutzer stellt Zertifizierungsantrag
  - Nach Prüfung stellt Zertifizierungsstelle ein Zertifikat aus
  - Benutzer kann nun Dokumente signieren
- Ermöglich Abfrage von Zertifikaten
  - Benutzer können Zertifikate abfragen
  - Mit öffentlichen Schlüssel aus den Zertifikaten können signierte Dokumente geprüft werden

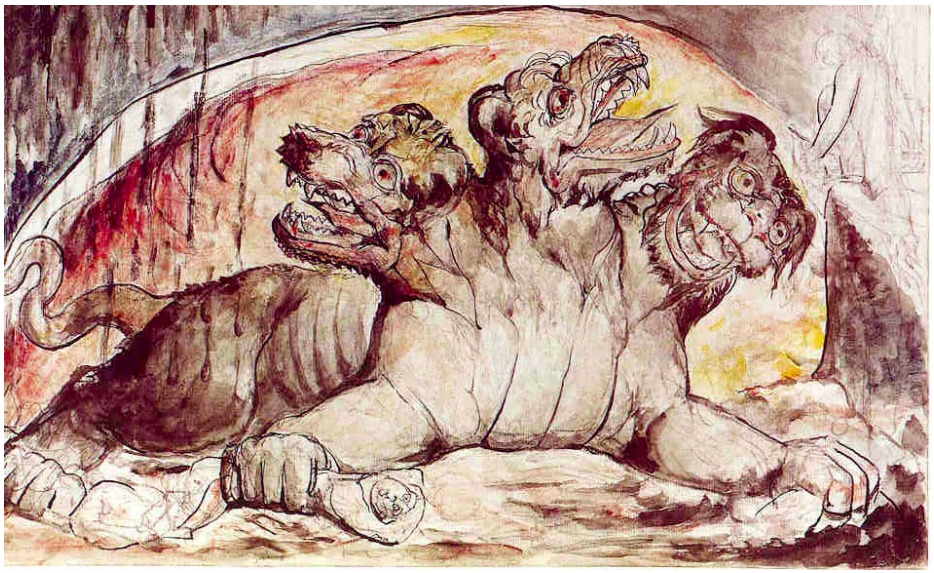
Authentifikation vs. Authorisation

- Authentifizierung
  - Wer sitzt vor dem Bildschirm?
  - Von wem stammt die Nachrichten?
- Autorisierung
  - Darf Bob die Datei “bild.png” lesen?
  - Darf Prozess “Whatsapp” auf Bilder in der Galerie zugreifen?
- Autosierung erfordert zuerst Authentifizierung!

Autorisierung - Festlegung der Berechtigungen mit Access Control List (ACL)

Kerberos

- Standard Authenitifizierungsprotokoll in Active Directory Umgebung
- Zentralisiert Authentifizierung
  - Sonst müsste sich jede Ressource die zugreifenden Clients umständlich selbst authentifizieren

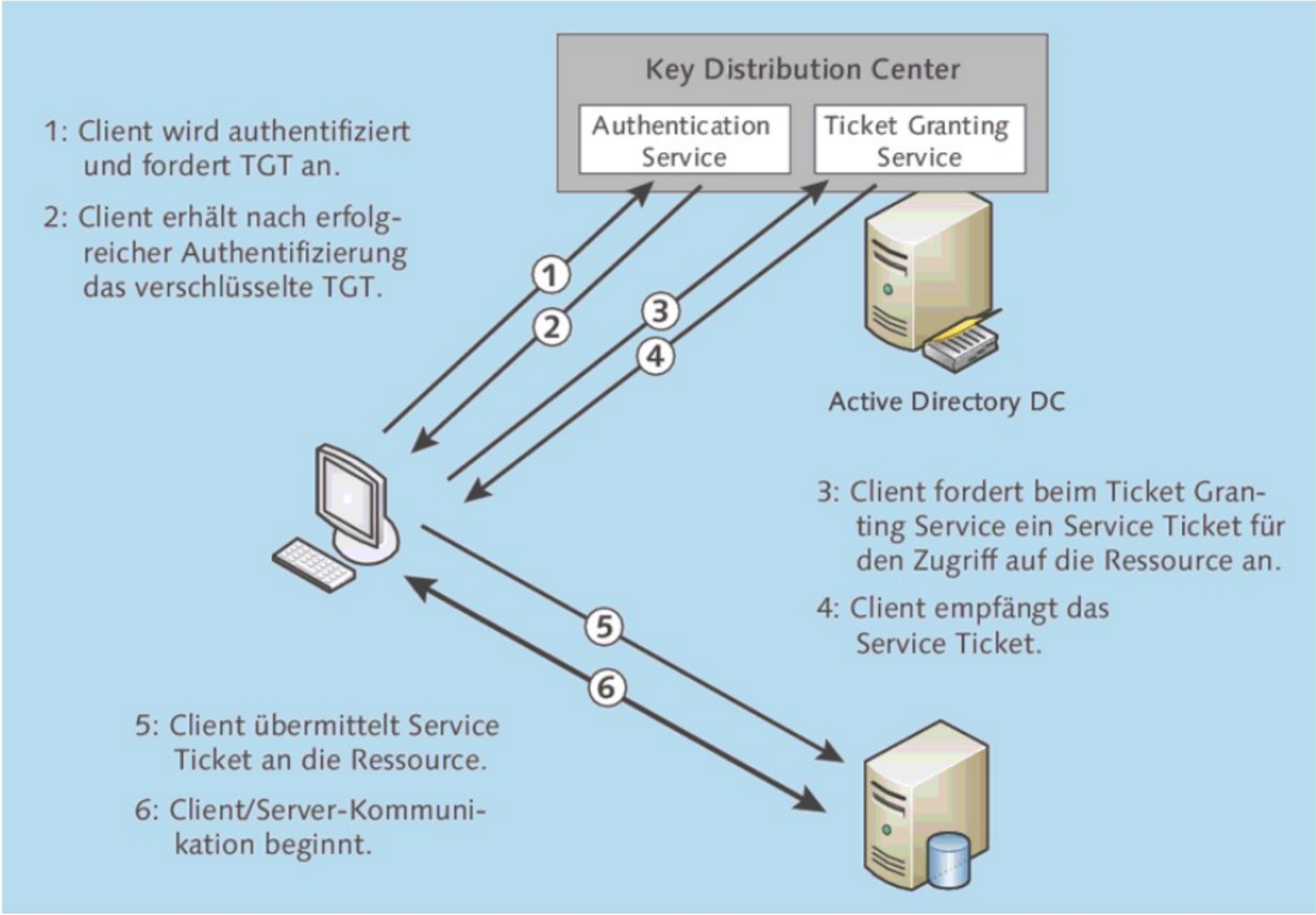


Kerberos - Funktionsweise

- 1. Benutzer nimmt Kontakt mit Authentication Service des Key Distribution Centers (KDC) auf
  - Liegt am Domänencontroller
  - Client weist seine Identität nach (zB User/Passwd)
- 2. Benutzer erhält Ticket Granting Ticket (TGT)
- 3. Für Zugriff auf Resource wird beim Ticket Granting Server (TGS) ein Ticket angefordert
  - Benutzer übermittelt dazu TGT in seiner Anfrage

Kerberos – Funktionsweise (2)

- 4. Wenn das TGT gültigt ist stellt TGS ein Service Ticket aus für die angefragte Resource
  - Ticket enthält einen Session Key
- 5. Benutzer kann sich nun mit Ticket bei der angefragten Resource authentifizieren
  - Service Ticket ist kryptografisch nachweislich vom Ticket Granting Server signiert
- 6. Resource autorisiert Anfrage des Benutzers
  - Ist er autorisiert, dann wird der Zugriff genehmigt


Key Distribution Center
Authentication Service
Ticket Granting Service
1: Client wird authentifiziert und fordert TGT an.
2: Client erhält nach erfolgreicher Authentifizierung das verschlüsselte TGT.
1
2
3
4
Active Directory DC
3: Client fordert beim Ticket Granting Service ein Service Ticket für den Zugriff auf die Ressource an.
4: Client empfängt das Service Ticket.
5
6
5: Client übermittelt Service Ticket an die Ressource.
6: Client/Server-Kommunikation beginnt.