IT-Security Tutorübung 09

IDKYAI2H6OADQ

Dorian Zedler

18. Dezember 2023

Technische Universität München

Inhalt der Tutorübung

- Kerberos
- PKI

Quizizz

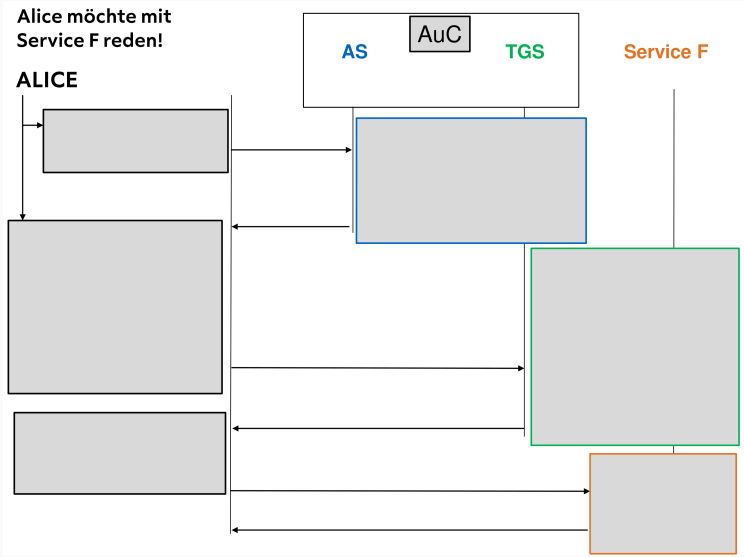
Quizizz

https://quizizz.com/admin/quiz/657ff04f3d2e355d7413e525?searchLocale=

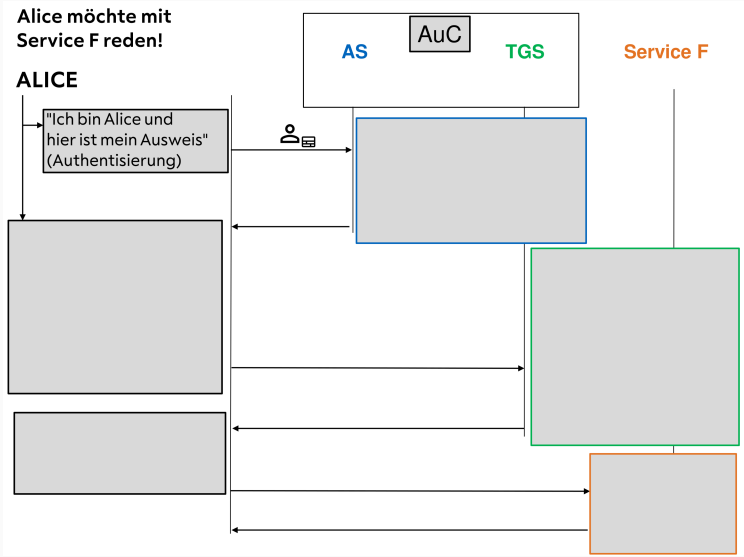
Hausaufgaben Präsentationen

Aufgabe 1

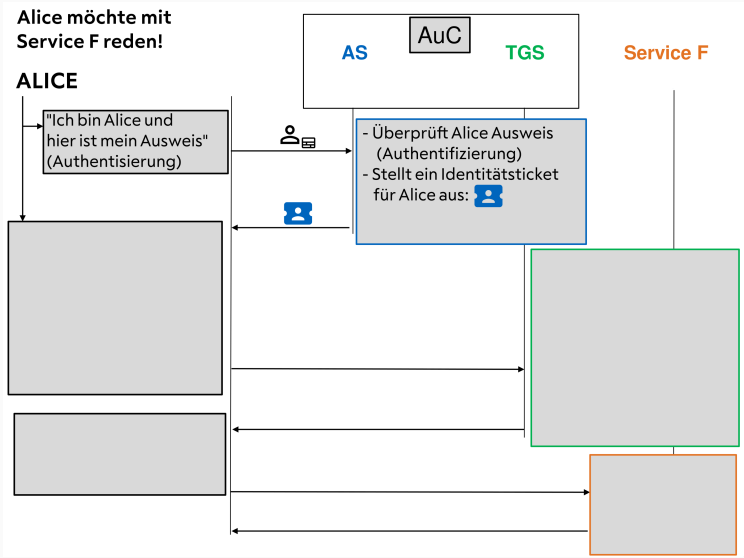
Kerberos - Vereinfacht



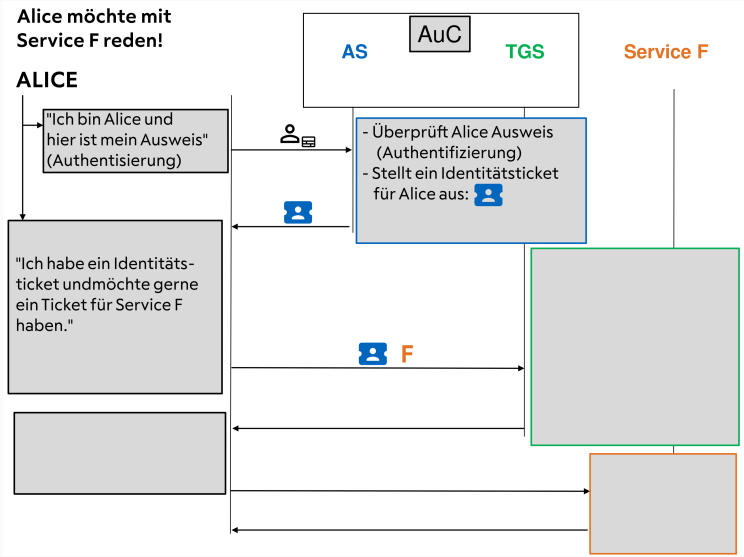
Kerberos - Vereinfacht



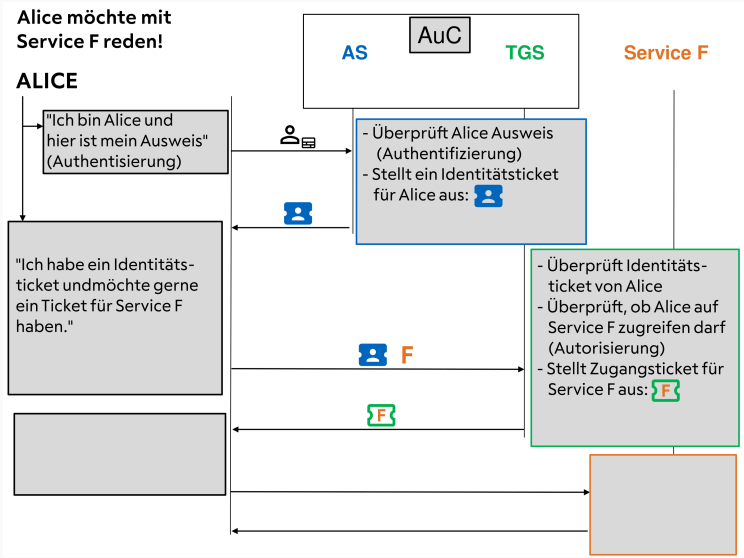
Kerberos - Vereinfacht



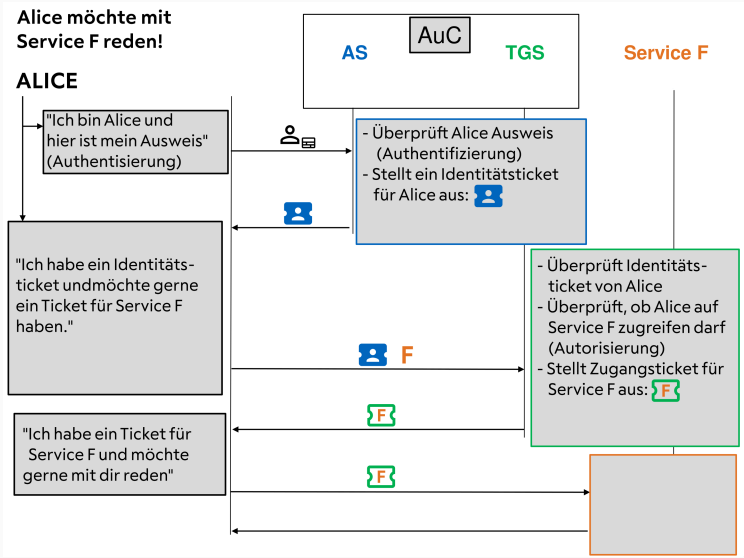
Kerberos - Vereinfacht



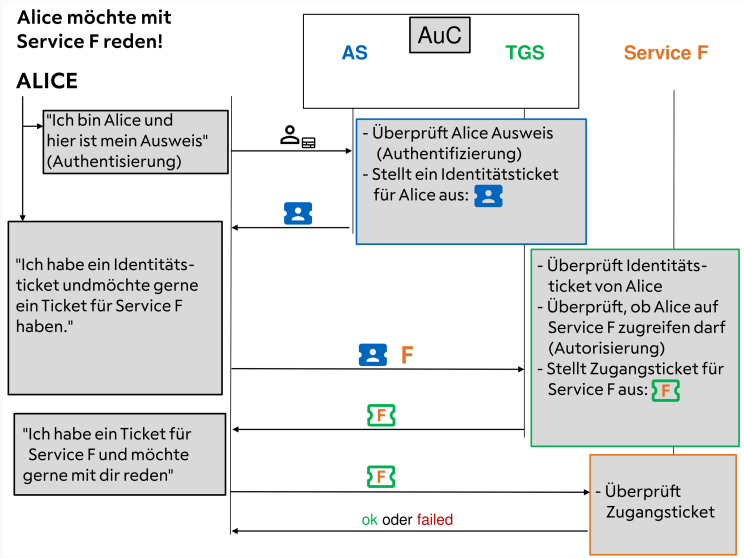
Kerberos - Vereinfacht



Kerberos - Vereinfacht



Kerberos - Vereinfacht



Aufgabe 1a - Kerberos - Was soll das?

a) Welche Aufgaben erfüllt das Kerberos-Protokoll?

Aufgabe 1a - Kerberos - Was soll das?

a) Welche Aufgaben erfüllt das Kerberos-Protokoll?

- Authentifizierung
- Autorisierung
- Verschlüsselung / Schlüsselverteilung
- Integritätsschutz
- Alles **ohne** asymmetrische Kryptografie!

Aufgabe 1b - Kerberos - Ticket

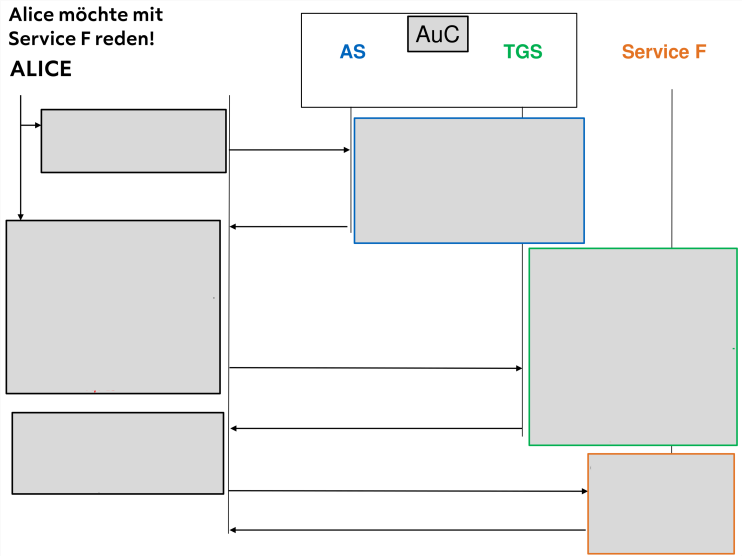
b) Beschreiben Sie die Funktion eines *Tickets* im Kontext von Kerberos! Woher stammt es und aus welchen Bestandteilen besteht es?

Aufgabe 1b - Kerberos - Ticket

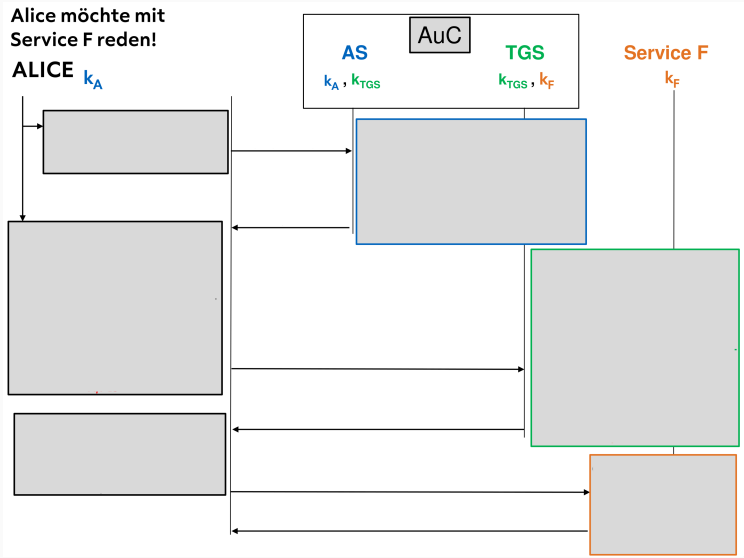
b) Beschreiben Sie die Funktion eines *Tickets* im Kontext von Kerberos! Woher stammt es und aus welchen Bestandteilen besteht es?

- Wird vom Authentifizierungsservice (AS) oder Ticket granting service (TGS) ausgestellt
- Berechtigt zur Nutzung eines Dienstes
- Transportiert den gemeinsamen Sitzungsschlüssel
- Ticket = $(\text{Service}_{ID}, \text{Principal}_{ID}, \text{Principal}_{(IP-)Addresse}, \text{Timestamp}, \text{Lifetime}, K_{PS})$

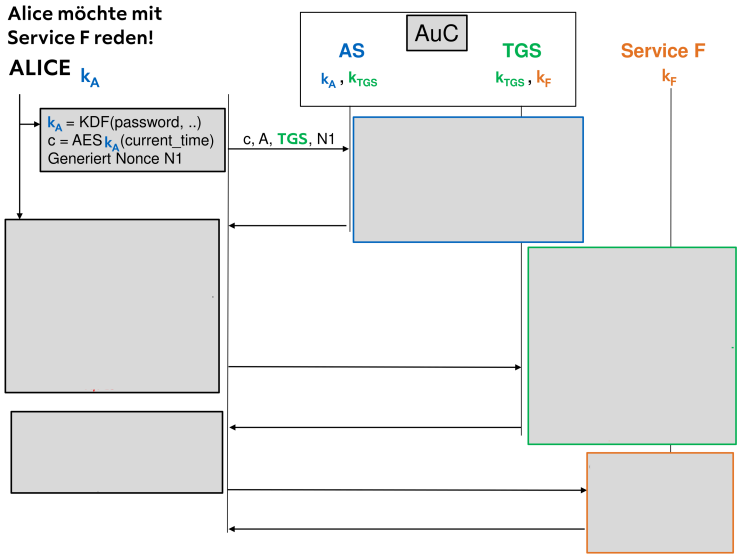
Kerberos - Komplett



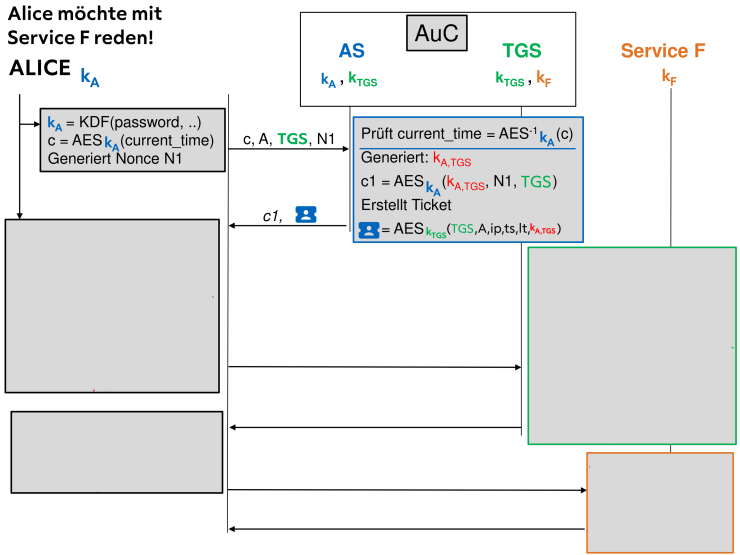
Kerberos - Komplett



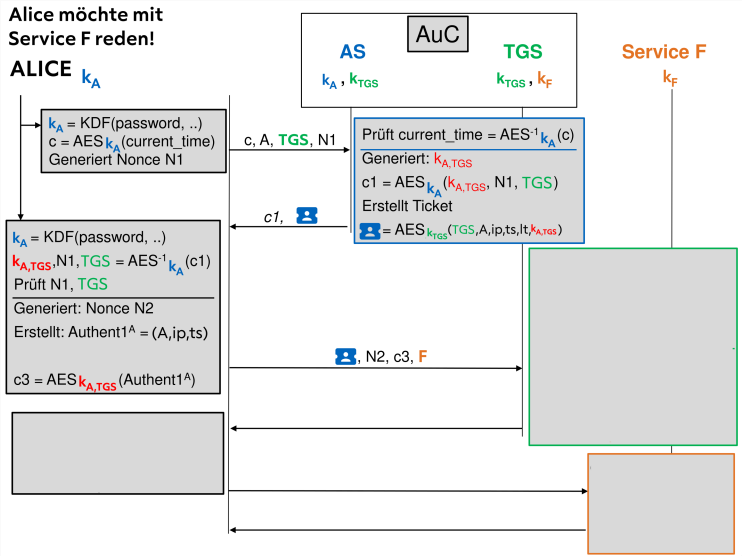
Kerberos - Komplett



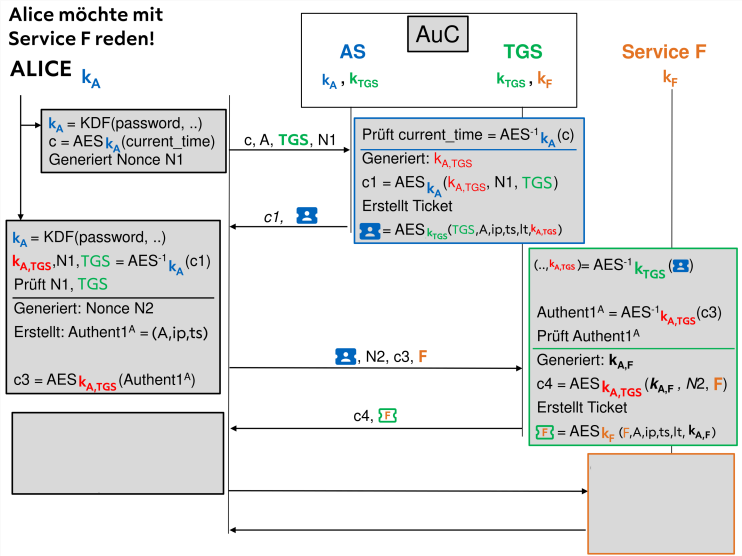
Kerberos - Komplett



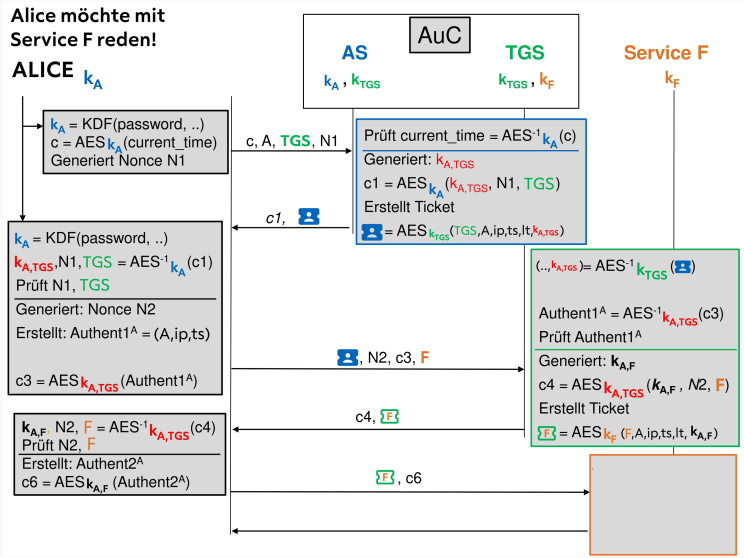
Kerberos - Komplett



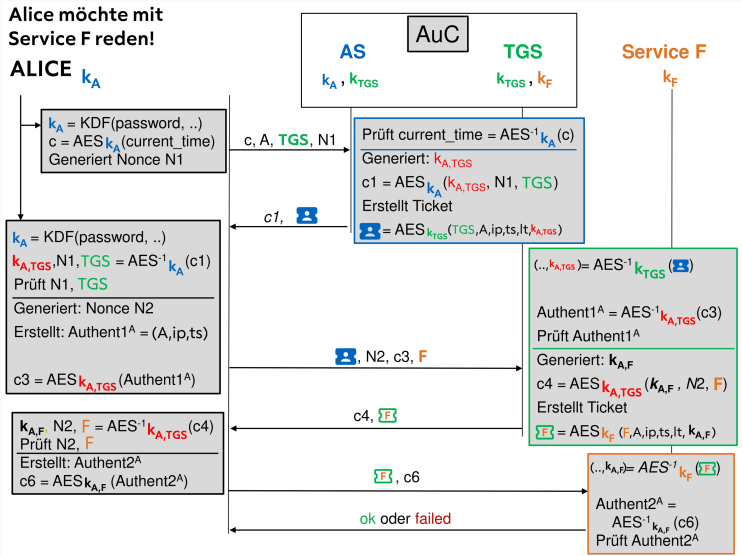
Kerberos - Komplett



Kerberos - Komplett



Kerberos - Komplett



Aufgabe 1c - Kerberos - Authent

c) Wozu dient der *Authenticator* (z.B. `Authent1`) im Kontext von Kerberos?

Aufgabe 1c - Kerberos - Authent

c) Wozu dient der *Authenticator* (z.B. `Authent1`) im Kontext von Kerberos?

- Nachweis, dass Principal (z.B. Alice) berechtigt ist, das Ticket zu nutzen
- Beweist, dass Principal den gemeinsamen Sitzungsschlüssel (z.B. $k_{A,F}$) kennt
- Schützt durch enthaltenen Timestamp vor Replay-Angriffen

Aufgabe 1d - Kerberos - Probleme

d) Nennen und erklären Sie **zwei** Probleme, die beim Einsatz eines KDC entstehen!

Aufgabe 1d - Kerberos - Probleme

d) Nennen und erklären Sie **zwei** Probleme, die beim Einsatz eines KDC entstehen!

1) **Kein Perfect Forward Secrecy**: Kompromittierung des Schlüssels eines Prinzipals (z.B. k_A), kann alle seine Kommunikation entschlüsselt werden
2) **Single Point of Failure**: KDC kennt alle Schlüssel und muss jede Kommunikation initiieren

Aufgabe 1e - Kerberos - AS und TGS

e) Könnten AS und TGS in einen Server zusammengefasst werden?

Aufgabe 1e - Kerberos - AS und TGS

e) Könnten AS und TGS in einen Server zusammengefasst werden?

- **JA**, sie könnten beide auf demselben Server laufen
- Erfüllen aber unterschiedliche Aufgaben und werden deshalb im Protokoll getrennt

Aufgabe 1f - Kerberos - Preauthentication

f) Wozu wird Alice im ersten Schritt mittels der Nachricht c authentifiziert?

Aufgabe 1f - Kerberos - Preauthentication

f) Wozu wird Alice im ersten Schritt mittels der Nachricht c authentifiziert?

- Alice authentifiziert sich gegenüber dem AS und beweist, dass sie das Passwort kennt

Aufgabe 1f - Kerberos - Preauthentication

f) Wozu wird Alice im ersten Schritt mittels der Nachricht c authentifiziert?

- Alice authentifiziert sich gegenüber dem AS und beweist, dass sie das Passwort kennt
- Ohne PreAuth könnte ein Angreifer ein C_1 für Alice anfordern und das Passwort lokal bruteforcen

Aufgabe 1f - Kerberos - Preauthentication

f) Wozu wird Alice im ersten Schritt mittels der Nachricht c authentifiziert?

- Alice authentifiziert sich gegenüber dem AS und beweist, dass sie das Passwort kennt
- Ohne PreAuth könnte ein Angreifer ein C_1 für Alice anfordern und das Passwort lokal bruteforcen
- Mit PreAuth müsste der Angreifer zunächst eine Man-in-the-Middle-Position erreichen
- PreAuth ist in Kerberos trotzdem optional

Aufgabe 1g - Kerberos - Integrität

g) Wie wird die Integrität der Nachrichten in Kerberos sichergestellt?

Aufgabe 1g - Kerberos - Integrität

g) Wie wird die Integrität der Nachrichten in Kerberos sichergestellt?

- Verschlüsselte Nachrichten haben eine HMAC Checksumme über den Klartext (MAC-then-encrypt)
- Früher auch Checksummen ohne Schlüssel (z.B. CRC32) erlaubt, aber inzwischen deprecated

Aufgabe 1h - Kerberos - Replay

h) Die an Kerberos angeschlossenen Services müssen einen Replay Cache führen. Wozu ist das notwendig?

Aufgabe 1h - Kerberos - Replay

h) Die an Kerberos angeschlossenen Services müssen einen Replay Cache führen. Wozu ist das notwendig?

- Szenario:
  - Alice sendet Authent (c6) und Ticket an den Service
  - Alice sendet einen Befehl für eine Zahlung an den Service
  - Diese beiden Nachrichten werden von einem Angreifer aufgezeichnet

Aufgabe 1h - Kerberos - Replay

h) Die an Kerberos angeschlossenen Services müssen einen Replay Cache führen. Wozu ist das notwendig?

- Szenario:
  - Alice sendet Authent (c6) und Ticket an den Service
  - Alice sendet einen Befehl für eine Zahlung an den Service
  - Diese beiden Nachrichten werden von einem Angreifer aufgezeichnet
- Der Angreifer kann nun die beiden Nachrichten wiederholen und die Zahlung mehrfach auslösen
- Um das zu verhindern, werden die Nachrichten im Service gecached
- Damit der Cache nicht unendlich groß sein muss, ist in Authent der Timestamp enthalten

Aufgabe 1f - Kerberos - Replay

f) Warum ist Replay bei Principals (z.B. Alice) auch ohne Cache nicht möglich?

Aufgabe 1f - Kerberos - Replay

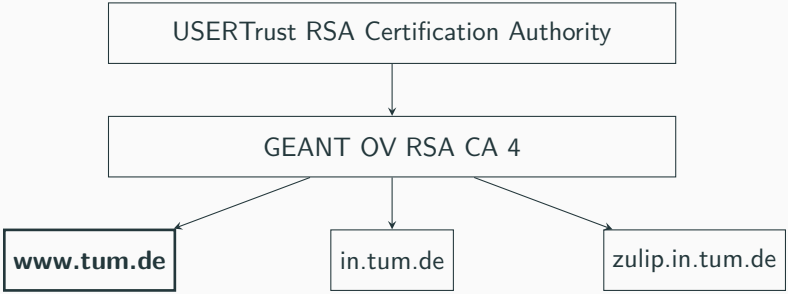
f) Warum ist Replay bei Principals (z.B. Alice) auch ohne Cache nicht möglich?

- Principals bekommen nur auf Anfrage vom AS oder TGS ein Ticket
- Diese Anfragen sind immer durch Noncen geschützt

Aufgabe 2

Aufgabe 2a - PKI

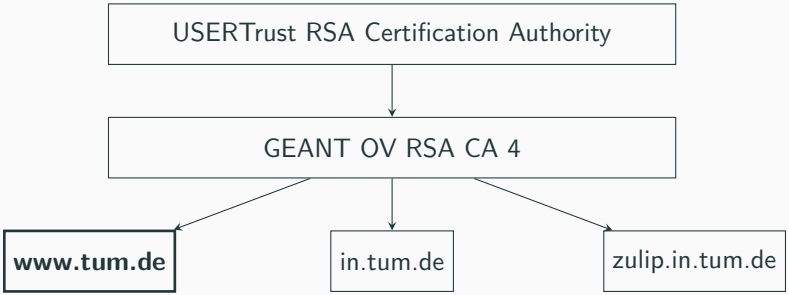
Gegeben sei folgende Zertifikatskette:



a) Welchen Zertifikaten aus der Zertifikatshierarchie muss ihr Browser vertrauen, wenn Sie www.tum.de öffnen?

Aufgabe 2a - PKI

Gegeben sei folgende Zertifikatskette:



a) Welchen Zertifikaten aus der Zertifikatshierarchie muss ihr Browser vertrauen, wenn Sie www.tum.de öffnen?
   - Nur *USERTrust RSA Certification Authority*, da es die Wurzel ist
   - In der Hierarchie wird allen Zertifikaten vertraut, die direkt oder indirekt von diesem **Wurzelzertifikat** signiert wurden

Aufgabe 2b - PKI

b) Geben Sie alle Schritte an die zur Prüfung des Zertifikates erforderlich sind!

Aufgabe 2b - PKI

b) Geben Sie alle Schritte an die zur Prüfung des Zertifikates erforderlich sind!

1) Stimmt das Subject (oder eins der Subject Alternative Names) mit der Webseitendomain überein?

```
39        X509v3 Subject Alternative Name:
40          DNS:wwwv21.tum.de, DNS:develop.www.professoren.tum.de,
41          DNS:live-t3v11.www.tum.de, DNS:release-t3v11.www.tum.d
42          DNS:release.www.tum.de, DNS:tu-muenchen.de, DNS:tum.de
43          DNS:webdb-wwwv21.srv.tum.de, DNS:www.professoren.tum.d
44          DNS:www.tu-muenchen.de, DNS:www.tum.de
```

Aufgabe 2b - PKI

b) Geben Sie alle Schritte an die zur Prüfung des Zertifikates erforderlich sind!
   1) Stimmt das Subject (oder eins der Subject Alternative Names) mit der Webseitendomain überein?
   2) Ist das Zertifikat im Gültigkeitszeitraum?

```
8       Validity
9         Not Before: May  2 00:00:00 2023 GMT
10        Not After : May  1 23:59:59 2024 GMT
```

Aufgabe 2b - PKI

b) Geben Sie alle Schritte an die zur Prüfung des Zertifikates erforderlich sind!
   1) Stimmt das Subject (oder eins der Subject Alternative Names) mit der Webseitendomain überein?
   2) Ist das Zertifikat im Gültigkeitszeitraum?
   3) Sind die verwendeten Krypto-Primitive (wie z.B. das Hashingverfahren zum signieren) stark genug?

Aufgabe 2b - PKI

b) Geben Sie alle Schritte an die zur Prüfung des Zertifikates erforderlich sind!
   1) Stimmt das Subject (oder eins der Subject Alternative Names) mit der Webseitendomain überein?
   2) Ist das Zertifikat im Gültigkeitszeitraum?
   3) Sind die verwendeten Krypto-Primitive (wie z.B. das Hashingverfahren zum signieren) stark genug?
   4) Wird das Zertifikat für seinen Bestimmungszweck genutzt? (z.B. CA:TRUE oder CA:FALSE)

```
27        X509v3 Basic Constraints: critical
28          CA:FALSE
```

Aufgabe 2b - PKI

b) Geben Sie alle Schritte an die zur Prüfung des Zertifikates erforderlich sind!
   1) Stimmt das Subject (oder eins der Subject Alternative Names) mit der Webseitendomain überein?
   2) Ist das Zertifikat im Gültigkeitszeitraum?
   3) Sind die verwendeten Krypto-Primitive (wie z.B. das Hashingverfahren zum signieren) stark genug?
   4) Wird das Zertifikat für seinen Bestimmungszweck genutzt? (z.B. CA:TRUE oder CA:FALSE)
   5) Ist das Zertifikat zurückgerufen worden? Dies kann mittels CRL oder OCSP geprüft werden.

Aufgabe 2b - PKI

b) Geben Sie alle Schritte an die zur Prüfung des Zertifikates erforderlich sind!
   1) Stimmt das Subject (oder eins der Subject Alternative Names) mit der Webseitendomain überein?
   2) Ist das Zertifikat im Gültigkeitszeitraum?
   3) Sind die verwendeten Krypto-Primitive (wie z.B. das Hashingverfahren zum signieren) stark genug?
   4) Wird das Zertifikat für seinen Bestimmungszweck genutzt? (z.B. CA:TRUE oder CA:FALSE)
   5) Ist das Zertifikat zurückgerufen worden? Dies kann mittels CRL oder OCSP geprüft werden.
   6) $Verify(Cert_{Sig}, C^{pub}_{parent}) \stackrel{?}{=} H(Zertifikat)$

Aufgabe 2b - PKI

b) Geben Sie alle Schritte an die zur Prüfung des Zertifikates erforderlich sind!

1) Stimmt das Subject (oder eins der Subject Alternative Names) mit der Webseitendomain überein?
2) Ist das Zertifikat im Gültigkeitszeitraum?
3) Sind die verwendeten Krypto-Primitive (wie z.B. das Hashingverfahren zum signieren) stark genug?
4) Wird das Zertifikat für seinen Bestimmungszweck genutzt? (z.B. CA:TRUE oder CA:FALSE)
5) Ist das Zertifikat zurückgerufen worden? Dies kann mittels CRL oder OCSP geprüft werden.
6) $Verify(Cert_{Sig}, C^{pub}_{parent}) \stackrel{?}{=} H(Zertifikat)$
7) Wird dem Zertifikat vertraut? (d.h. wird dem Zertifikat direkt vertraut, oder gibt es eine lückenlose Zertifikatskette, die in einem vertrauten Stammzertifikat endet?)

Aufgabe 2c - PKI

c) Sie finden eine Webseite, deren HTTPS-Zertifikat mittels dem von `www.tum.de` signiert wurde. Würde ihr Browser dies akzeptieren?

Aufgabe 2c - PKI

c) Sie finden eine Webseite, deren HTTPS-Zertifikat mittels dem von `www.tum.de` signiert wurde. Würde ihr Browser dies akzeptieren?

- **NEIN**

Aufgabe 2c - PKI

c) Sie finden eine Webseite, deren HTTPS-Zertifikat mittels dem von `www.tum.de` signiert wurde. Würde ihr Browser dies akzeptieren?

- **NEIN**
- Im TUM-Zertifikat ist die Flasg *CA:FALSE* gesetzt

Fragen? Feedback?

Bis zum nächsten Mal!