Kryptologie

📜🛡️ Digitale Zertifikate & PKI

Cyril Blum

Fachschaft Informatik
Kantonsschule Im Lee

Das Vertrauensproblem in der Praxis

Eine mathematisch korrekte RSA-Signatur beweist **Integrität** und den Besitz des privaten Schlüssels.

Die fundamentale Vertrauensfrage

Woher weiss der Empfänger (Bob), dass ein bestimmter öffentlicher Schlüssel tatsächlich Alice (oder der Bank) gehört?

- **Man-in-the-Middle-Angriff**: Eve generiert ein eigenes Schlüsselpaar (e_E, d_E) und gibt vor, Alice zu sein.

Das Vertrauensproblem in der Praxis

Eine mathematisch korrekte RSA-Signatur beweist **Integrität** und den Besitz des privaten Schlüssels.

Die fundamentale Vertrauensfrage

Woher weiss der Empfänger (Bob), dass ein bestimmter öffentlicher Schlüssel tatsächlich Alice (oder der Bank) gehört?

- **Man-in-the-Middle-Angriff**: Eve generiert ein eigenes Schlüsselpaar (e_E, d_E) und gibt vor, Alice zu sein.
- Signiert Eve eine gefälschte Nachricht mit d_E, so bestätigt Bobs Prüfung mit e_E formal die Gültigkeit der Signatur.

Das Vertrauensproblem in der Praxis

Eine mathematisch korrekte RSA-Signatur beweist **Integrität** und den Besitz des privaten Schlüssels.

Die fundamentale Vertrauensfrage

Woher weiss der Empfänger (Bob), dass ein bestimmter öffentlicher Schlüssel tatsächlich Alice (oder der Bank) gehört?

- **Man-in-the-Middle-Angriff**: Eve generiert ein eigenes Schlüsselpaar (e_E, d_E) und gibt vor, Alice zu sein.
- Signiert Eve eine gefälschte Nachricht mit d_E, so bestätigt Bobs Prüfung mit e_E formal die Gültigkeit der Signatur.
- **Ergebnis**: Bob wiegt sich in falscher Sicherheit, da er den Schlüssel nicht der realen Identität zuordnen kann!

Lösung: Digitale Zertifikate & PKI

Um die Identität von Schlüsselinhabern zweifelsfrei zu bestätigen, nutzen wir eine **Public-Key-Infrastruktur** (PKI):

Definition (Komponenten einer PKI)

- **Zertifizierungsstelle (*Certificate Authority*, CA)**: Eine vertrauenswürdige Institution, die vor der Schlüsselausgabe die reale Identität prüft.

Lösung: Digitale Zertifikate & PKI

Um die Identität von Schlüsselinhabern zweifelsfrei zu bestätigen, nutzen wir eine **Public-Key-Infrastruktur** (PKI):

Definition (Komponenten einer PKI)

- **Zertifizierungsstelle (*Certificate Authority*, CA)**: Eine vertrauenswürdige Institution, die vor der Schlüsselausgabe die reale Identität prüft.
- **Digitales Zertifikat**: Ein elektronisches Dokument, das die Identität an den öffentlichen Schlüssel bindet und von der CA digital signiert ist:

$$\text{Cert}_A := z^{d_{\text{CA}}} \bmod n_{\text{CA}} \qquad \text{mit } z = (\text{„Alice“}, e_A, n_A)$$

Lösung: Digitale Zertifikate & PKI

Um die Identität von Schlüsselinhabern zweifelsfrei zu bestätigen, nutzen wir eine **Public-Key-Infrastruktur** (PKI):

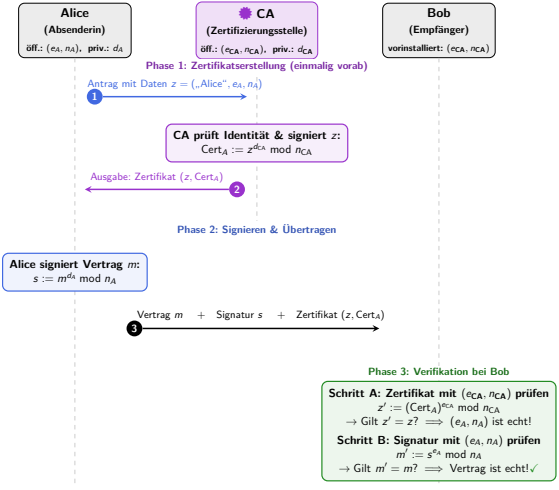
Definition (Komponenten einer PKI)

- **Zertifizierungsstelle (*Certificate Authority*, CA)**: Eine vertrauenswürdige Institution, die vor der Schlüsselausgabe die reale Identität prüft.
- **Digitales Zertifikat**: Ein elektronisches Dokument, das die Identität an den öffentlichen Schlüssel bindet und von der CA digital signiert ist:

$$\text{Cert}_A := z^{d_{\text{CA}}} \bmod n_{\text{CA}} \qquad \text{mit } z = (\text{„Alice“}, e_A, n_A)$$

- **Vertrauensanker (Root-CA)**: Betriebssysteme und Browser besitzen einen vorinstallierten Speicher vertrauenswürdiger Stammzertifikate (*Trust Store*).

Zweistufige Verifikation mit PKI

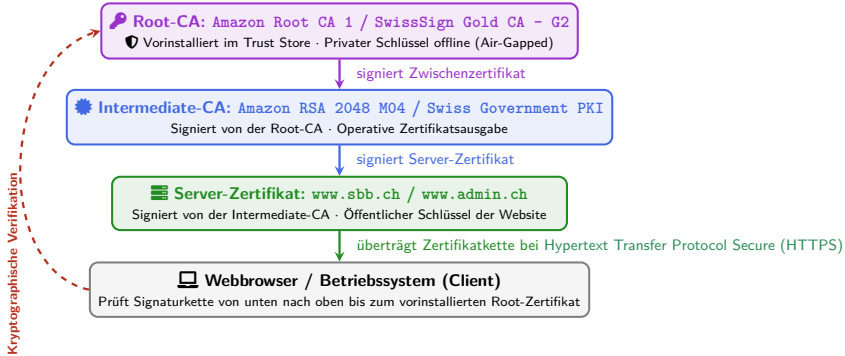


Auftrag: Zertifizierte digitale Signaturen

Lösen Sie Aufgabe 5.1 im Skript (Zertifikat)

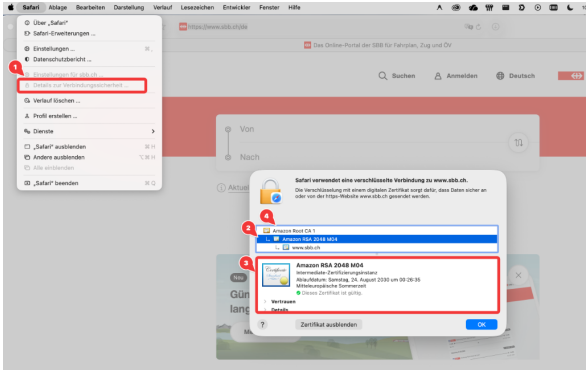
Die Vertrauenskaskade: Zertifikatskette

In der Praxis signiert eine Root-CA fast nie direkt einzelne Server-Zertifikate, sondern nutzt Zwischenzertifikate:



- **Sicherheitsvorteil**: Der private Root-Schlüssel bleibt streng isoliert *offline* (Air-Gapped). Bei einem Zwischenfall muss nur das Intermediate-Zertifikat widerrufen werden.

Zertifikatsinspektion im Webbrowser (SBB)



Zertifikatsaufbau bei `https://www.sbb.ch`:

1. **Root-CA**: `Amazon Root CA 1` (im Betriebssystem vorinstalliert).
2. **Intermediate-CA**: `Amazon RSA 2048 M04`.
3. **Blatt-Zertifikat**: `www.sbb.ch` (Inhaberin: Schweizerische Bundesbahnen).

Verschlüsselung: TLS mit AES / RSA / ECC.

Elektronische Signaturen in der Schweiz (ZertES)

Bundesgesetz über die elektronische Signatur (ZertES)

In der Schweiz regelt das **ZertES** die rechtliche Gültigkeit von elektronischen Signaturen:

- **Qualifizierte elektronische Signatur (QES)**: Ist der eigenhändigen handschriftlichen Unterschrift rechtlich vollständig gleichgestellt (Art. 14 Abs. 2^{bis} OR).

Elektronische Signaturen in der Schweiz (ZertES)

Bundesgesetz über die elektronische Signatur (ZertES)

In der Schweiz regelt das **ZertES** die rechtliche Gültigkeit von elektronischen Signaturen:

- **Qualifizierte elektronische Signatur (QES)**: Ist der eigenhändigen handschriftlichen Unterschrift rechtlich vollständig gleichgestellt (Art. 14 Abs. 2^{bis} OR).
- **Anerkannte Vertrauensdienste in der Schweiz**:

Elektronische Signaturen in der Schweiz (ZertES)

Bundesgesetz über die elektronische Signatur (ZertES)

In der Schweiz regelt das **ZertES** die rechtliche Gültigkeit von elektronischen Signaturen:

- **Qualifizierte elektronische Signatur (QES)**: Ist der eigenhändigen handschriftlichen Unterschrift rechtlich vollständig gleichgestellt (Art. 14 Abs. 2^{bis} OR).
- **Anerkannte Vertrauensdienste in der Schweiz**:
  - **SwissSign**: Schweizerische Post / SwissID (z. B. für Verträge und eGovernment).

Elektronische Signaturen in der Schweiz (ZertES)

Bundesgesetz über die elektronische Signatur (ZertES)

In der Schweiz regelt das **ZertES** die rechtliche Gültigkeit von elektronischen Signaturen:

- **Qualifizierte elektronische Signatur (QES)**: Ist der eigenhändigen handschriftlichen Unterschrift rechtlich vollständig gleichgestellt (Art. 14 Abs. 2^{bis} OR).
- **Anerkannte Vertrauensdienste in der Schweiz**:
  - **SwissSign**: Schweizerische Post / SwissID (z. B. für Verträge und eGovernment).
  - **Swisscom Trust Services**: Signaturdienste für Banken und Unternehmen.

Elektronische Signaturen in der Schweiz (ZertES)

Bundesgesetz über die elektronische Signatur (ZertES)

In der Schweiz regelt das **ZertES** die rechtliche Gültigkeit von elektronischen Signaturen:

- **Qualifizierte elektronische Signatur (QES)**: Ist der eigenhändigen handschriftlichen Unterschrift rechtlich vollständig gleichgestellt (Art. 14 Abs. 2^{bis} OR).
- **Anerkannte Vertrauensdienste in der Schweiz**:
  - **SwissSign**: Schweizerische Post / SwissID (z. B. für Verträge und eGovernment).
  - **Swisscom Trust Services**: Signaturdienste für Banken und Unternehmen.
  - **SWITCHpki**: Zertifikate für Schweizer Universitäten und Schulen.

Elektronische Signaturen in der Schweiz (ZertES)

Bundesgesetz über die elektronische Signatur (ZertES)

In der Schweiz regelt das **ZertES** die rechtliche Gültigkeit von elektronischen Signaturen:

- **Qualifizierte elektronische Signatur (QES)**: Ist der eigenhändigen handschriftlichen Unterschrift rechtlich vollständig gleichgestellt (Art. 14 Abs. 2^{bis} OR).
- **Anerkannte Vertrauensdienste in der Schweiz**:
  - **SwissSign**: Schweizerische Post / SwissID (z. B. für Verträge und eGovernment).
  - **Swisscom Trust Services**: Signaturdienste für Banken und Unternehmen.
  - **SWITCHpki**: Zertifikate für Schweizer Universitäten und Schulen.
  - **Swiss Government PKI**: Interne PKI für die Bundesverwaltung.

Auftrag: Zertifikats-Detektiv im Browser

- Aufgabe 5.2 im Skript (Zertifikats-Detektiv)
- **Challenge**: Öffnen Sie Safari, Chrome, Edge oder Firefox und inspizieren Sie die Zertifikate von `https://www.sbb.ch`, `https://www.admin.ch` oder Ihrer Schule.