Authentifizierung in Netzwerken – Faktoren, Token und 2FA



Authentifizierung: Identität nachweisen

- Netzwerke und Computersysteme müssen vor **unbefugtem Zugriff** geschützt werden.
- Deshalb überprüft ein System bei der **Authentifizierung**, ob ein Benutzer tatsächlich die Person ist, für die er sich ausgibt.
- Dazu muss der Benutzer einen geeigneten **Nachweis** erbringen.
- Die Art des Nachweises wird als **Authentifizierungsfaktor** (kurz: **Faktor**) bezeichnet.
- Ein konkretes Authentifizierungsmittel kann dabei als **Token** bezeichnet werden.
- Bei der **Zwei-Faktor-Authentifizierung (2FA)** werden zwei unterschiedliche Faktoren miteinander kombiniert.

Was ist ein Faktor?

- Ein **Authentifizierungsfaktor** bezeichnet eine **Art von Nachweis**, mit dem eine Person ihre Identität gegenüber einem System nachweist.
- Man unterscheidet drei grundlegende Faktoren:
  - **Wissen: „etwas, das du weißt“**
    z. B. Passwort, PIN, Geheimzahl
  - **Besitz: „etwas, das du hast“**
    z. B. Chipkarte, Sicherheitsschlüssel, Smartphone mit registrierter Authenticator-App
  - **Biometrie: „etwas, das du bist“**
    z. B. Fingerabdruck, Gesicht, Iris
- **Beispiel:** Ein Passwort ist ein Nachweis des Faktors **Wissen**.

Was ist ein Token?

- Ein **Token** ist im Zusammenhang mit der Authentifizierung ein **konkretes Authentifizierungsmittel**, das ein Benutzer besitzt bzw. kontrolliert und zur Authentifizierung verwendet.
- Typische Token lassen sich unterscheiden in:
  - **Hardware-Token**, also physische Authentifizierungsmittel, z. B. Chipkarten, Sicherheitsschlüssel oder TAN-Generatoren.
  - **Software-Token**, also digitale Authentifizierungsmittel, die bspw. von einer Authenticator-App verwaltet werden.
- Auch ein **Smartphone** kann zur Authentifizierung eingesetzt werden, bspw. wenn darauf eine **Authenticator-App** mit einem Software-Token eingerichtet ist und damit ein **Einmalcode** erzeugt wird.
- Ein gewöhnlicher **USB-Stick** ist nicht automatisch ein Hardware-Token. Ein Hardware-Token ist ein speziell für Authentifizierungs- oder Sicherheitsfunktionen entwickeltes Gerät.

Wie hängen Faktor und Token zusammen?

- Faktor und Token bezeichnen unterschiedliche Ebenen:
  - **Faktor:** Welche Art von Nachweis wird erbracht?
  - **Token:** Welches konkrete Authentifizierungsmittel wird verwendet?
- In einer **vereinfachten Annahme** kann man ein **Token** als **konkretes Authentifizierungsmittel für den Faktor Besitz** betrachten. Es dient dabei dazu, nachzuweisen, dass eine Person ein bestimmtes Authentifizierungsmittel besitzt bzw. kontrolliert.
- **Hinweis:** Der Begriff Token wird in der Informatik je nach Zusammenhang unterschiedlich verwendet. In der modernen Fachterminologie wird für ein Authentifizierungsmittel häufig auch der Begriff **Authenticator** verwendet. In diesem Lernpapier verwenden wir Token im oben beschriebenen Sinn.
- Übersicht:

Nachweis / Authentifizierungsmittel	Welcher Faktor wird nachgewiesen?	Token?
Passwort	Wissen	nein
PIN	Wissen	nein
Fingerabdruck	Biometrie	nein
Chipkarte	Besitz	ja
Sicherheitsschlüssel	Besitz	ja
TAN-Generator	Besitz	ja

- Beispiel: Ein Sicherheitsschlüssel ist ein Token und weist den Faktor Besitz nach.

Zwei-Faktor-Authentifizierung (2FA)

- Bei der **Zwei-Faktor-Authentifizierung** werden **zwei unterschiedliche Authentifizierungsfaktoren** miteinander kombiniert.
- Dabei kann ein **Token** verwendet werden, muss aber nicht.
- Übersicht:

Authentifizierung	Faktoren	Token-anzahl	2FA?
Passwort + Fingerabdruck	Wissen + Biometrie	0	Ja
Passwort + Einmalcode aus einer Authenticator-App auf dem Smartphone	Wissen + Besitz	1	Ja
Chipkarte + PIN	Besitz + Wissen	1	Ja
Fingerabdruck + Iris	Biometrie + Biometrie	0	Nein
Sicherheitsschlüssel + Sicherheitsschlüssel	Besitz + Besitz	2	Nein

- **Entscheidend** ist nicht die Anzahl der Nachweise oder Tokens, sondern die **Anzahl der unterschiedlichen Faktoren.**
  - **Zwei unterschiedliche Faktoren = 2FA**
  - **Zwei Nachweise desselben Faktors = keine 2FA**

Zusammenfassung

- **Faktor** = **Art des Nachweises**, z. B. **Wissen**, **Besitz** oder **Biometrie**
- **Token** = konkretes **Authentifizierungsmittel** für den **Faktor Besitz**, z. B. ein **Sicherheitsschlüssel**
- **2FA** = Kombination aus **zwei unterschiedlichen Faktoren**, z. B. Wissen + Besitz

