LU07a - Authentifizierung

Grundlagen

Begriffe

Bei der Anmeldung an einer Applikation muss ein Benutzer seine Identität beweisen.

1. Der Benutzer gibt an, eine bestimmte Person (z.B. Marcel Suter) zu sein.
2. Die Applikation prüft, ob der Benutzer wirklich die angegebene Person zu sein.

Authentisierung

Bei der **Authentisierung** behauptet ein Benutzer eine bestimmte Person zu sein. Dies geschieht in den meisten Fällen indem er einen Benutzernamen und ein Passwort eingibt.

Ich will meine Steuererklärung auf der E-Government-Plattform „ZHservices“ bearbeiten. Durch die Eingabe meines Benutzernamens und Passwortes *behaupte* ich, Marcel Suter zu sein.

Authentifizierung

Bei der **Authentifizierung** prüft die Applikation die Identität des Benutzers. Zum Beispiel sucht die Applikation in einer User-Tabelle nach einem Datensatz mit dem angegebenen Benutzernamen und Passwort.

ZHservices prüft meinen Benutzernamen und Passwort. Sollten meine Angaben nicht zu einem bekannten User passen, so erhalte ich eine Fehlermeldung.

Autorisierung

Die **Autorisierung** ist die Einräumung von Rechten. Nachdem die Identifizierung einer Person erfolgreich war, bedeutet das noch nicht automatisch, dass diese Person bereitgestellte Daten, Dienste und Leistungen sehen oder nutzen darf. Die Autorisierung entscheidet darüber, welche Berechtigungen und Zugriffsrechte einer Person gewährt werden. Kurz gesagt: Während die Authentifizierung die Identität bestätigt, legt die Autorisierung fest, welche Aktionen oder Ressourcen

eine identifizierte Person verwenden darf.

Hat ZHservices meine Identität erfolgreich geprüft, werden mir die entsprechenden Rechte und Funktionen zugeteilt.

Möglichkeiten der Authentifizierung

Es gibt 3 grundlegende Möglichkeiten die Identität eines Benutzers zu prüfen.

Etwas, was ich weiss

Der Benutzer kennt eine bestimmte Information die nicht allgemein bekannt ist.

- Passwort
- Eindeutiger Code wie bei Doodle

Etwas, das ich besitze

Der Benutzer besitzt einen Gegenstand oder eine Schlüssel-Datei.

- SMS mit Code an mein Smartphone
- Smartcard für eBanking
- Datei mit meinem private Key
- App mit Einmalpasswort

Nachdem ZHservices meinen Benutzernamen und Passwort geprüft hat, erhalte ich per SMS einen Code auf mein Smartphone. Erst nach Eingabe des korrekten Codes kann ich meine Steuererklärung bearbeiten.

Etwas, das ich bin

Der Benutzer beweist seine Gegenwart durch ein biometrisches Merkmal.

- Fingerabdruck
- Stimmerkennung
- Retinamerkmale (Augenhintergrund)

Beim Speichern und Verarbeiten von biometrischen Merkmalen muss der Datenschutz besonders beachtet werden. Viele dieser Merkmale lassen Rückschlüsse auf Gesundheitszustand und/oder Rassenzugehörigkeit einer Person zu. Sie gelten daher als besonders schützenswerte Daten (DSG Artikel 3 Buchstabe c). Solche Daten dürfen nur mit ausdrücklicher Einwilligung der betroffenen Person erfolgen (DSG Artikel 4 Ziffer 5).

2-Faktoren-Authentifikation

Heutzutage gilt die typische Authentifikation mittels Benutzernamen und Passwort als wenig sicher. Der Benutzername ist in der Regel entweder eine Kombination aus Vor- und Nachnamen oder eine EMail-Adresse. Beides sind Informationen, die problemlos zugänglich sind. Ausserdem verwenden die meisten Benutzer überall die gleichen, einfach zu erratenden Passwörter.

Viele Betreiber von Webservices gehen dazu über, die Authentifikation durch ein weiteres Merkmal zu sichern. Die oben beschriebenen „zhServices“ verwenden eine 2-Faktoren-Authentifizierung indem ein SMS an mein Smartphone geschickt wird. Erst nach Eingabe dieses Codes kann ich die Webservices benutzen.

Authenticator-App

Für das Login am BZZ setze ich einen Authenticator als zweiten Faktor ein. Dieser besteht aus einer App für das Smartphone, welche in regelmässigen Abständen einen einmal gültigen Code generiert. Bei der Anmeldung muss ich zusätzlich den aktuellen Code eingeben. Auch andere Firmen nutzen eine Smartphone-App als zweiten Faktor.

FIDO2

Siehe auch *fido2 und fidoalliance - FIDO2* FIDO2 ist eine Spezifikation für eine starke Authentifizierung mittels eines Hardwaretokens. Dieses Token kann im Gerät integriert sein (Chip im Laptop oder Smartphone) oder als separater Stick vorliegen. Im Gegensatz zu anderen 2-Faktoren-Authentifikationen ermöglicht es FIDO2, eine Authentifikation ohne Passwort zu realisieren. Siehe ct-Artikel vom August 2019.

---

m231-AnG