SocietyByte
Wissenschaftsmagazin des BFH-Zentrums Digital Society
https://www.societybyte.swiss

Qualität der Authentifizierung

Autor : Annett Laube

Datum : 1. Januar 2017

Identitätsmissbrauch im Internet kann sehr unangenehm sein. Viele Betroffene erfahren erst davon, wenn eine Rechnung für etwas, was sie nie bestellt oder benutzt haben, per Brief zu Hause eintrifft. Aber wie kann ein Anbieter von Webanwendungen sicherstellen, dass der aktuelle Benutzer wirklich der ist, den er vorgibt zu sein?

In der realen Welt räumen wir Personen, die wir kennen, einen Vertrauensvorschuss ein. Handschlag genügt. Erst wenn es um kritische Vertragsabschlüsse geht, lassen wir uns Beweise in Form von Ausweisdokumenten zeigen oder holen Referenzen ein.

In der digitalen Welt ist das weniger offensichtlich. Eine Webanwendung kann das Vertrauen in die nutzende Person über die Qualität der Authentifizierung abschätzen. Daher legt der Betreiber entsprechend dem Schadenspotential fest, welche Qualität der Authentifizierung notwendig ist. Die Herausforderung wird grösser, wenn die Webanwendung die Registrierung und Authentifizierung nicht selbst durchführt, sondern an einen vertrauenswürdigen Dritten auslagert. Hier braucht es ein Modell, das es ermöglicht, die angebotenen Qualitäten einzustufen.

Die Vielzahl der vorhandenen Qualitätsmodelle1,2,3 und ihre unterschiedlichen Anwendungsbereiche erzeugen allerdings eher Unsicherheit. Daher erarbeitet die BFH im Auftrag des SECO und des ISB und zusammen mit dem Verein eCH ein Qualitätsmodell für das Schweizer E-Government, anwendbar auf die ganze Schweizer eSociety.

Die neue Version des Qualitätsmodells (eCH-0170 Version 2.0) berücksichtigt zudem die in der Schweiz existierenden Authentifizierungslösungen und die Anforderungen aus dem E-Government. Das resultierende Qualitätsmodell besteht aus vier Teilmodellen, die jeweils einem Prozess zugeordnet sind (siehe Abbildung).

Authentifizierung eines Subjekts.

Für jeden Prozess werden Qualitätskriterien definiert, die in der Kombination ihrer Ausprägungen die verschiedenen Stufen für die Modelle definieren. Zuletzt werden die Stufen der Teilmodelle zu einer Vertrauensstufe des Gesamtsystems kombiniert und erlauben damit eine solide Einschätzung der Qualität einer Authentifizierung.

Der Laufzeit-Prozess Subjekt authentifizieren ermöglicht – nebst der Authentifizierung des Subjekts (Benutzer) – die Steuerung des Zugriffs des Subjekts auf eine Ressource.

Erfolgt die Authentifizierung des Subjekts bei einem vertrauenswürdigen Dritten (und nicht direkt in einer Webanwendung), wird anschliessend das Ergebnis der Authentifizierung in Form einer Authentifizierungsbestätigung vom Identitätsprovider an die Relying Party (RP) übertragen (Prozess Identität föderieren).

Bevor sich ein Subjekt zur Laufzeit authentisieren kann, muss es bei einer Registrierungsstelle (RA) registriert werden. Die RA überprüft die Identität des Subjekts und erstellt eine E-Identity für das Subjekt. Der Credential Service Provider (CSP) stellt für diese E-Identity ein neues Authentifizierungsmittel aus oder bindet ein vorhandenes an. Im Credential wird die Verbindung zwischen der E-Identity und dem Authentifizierungsmittel abgelegt.

Alle Beteiligten müssen im Voraus gemeinsam die Rahmenbedingungen für den Betrieb des IAM-Systems abgestimmt haben (Prozess Registrierung und Authentifizierung steuern).

[Originalbeitrag in Spirit biel/bienne 03/16]