SocietyByte Wissenschaftsmagazin der Berner Fachhochschule

Was ein zeitgemässes Identitätsmanagement-System erfüllen soll

Von Gerhard Hassenstein (BFH Technik & Informatik) , Annett Laube (BFH Technik & Informatik) | 1 Kommentar

Mit zunehmenden Datenschutzforderungen wird es immer wichtiger, die Datensouveränität der Benutzer stärker zu berücksichtigen. Daher werden beim Identitätsmanagement benutzerzentrierte Ansätze diskutiert, die neben der Sicherheit des Gesamtsystems auch den Schutz der Privatsphäre der Benutzer gewährleisten. Ein Identitätsinhaber soll einem prüfenden Dienst so wenig Informationen wie möglich preisgeben und zudem soll kein weiterer Dienst Daten über die Aktivitäten eines Inhabers sammeln können. Aber was bedeutet dies für den Inhaber? Was muss ein Herausgeber von Berechtigungsnachweisen berücksichtigen, wenn er diese ausstellt? Was sind umgekehrt die Anforderungen eines prüfenden Dienstes? In diesem Artikel werden die Ansprüche von Aussteller, Inhaber und prüfendem Dienst gegenübergestellt.

Unabhängig davon was für ein Identitätsmanagement-System betrachtet wird, lassen sich folgende Akteure definieren. Zum einen ist die zentrale Figur der Identitätsinhaber *(Holder)*, welcher eine beliebige Anzahl Attribute *(Claims)* über sich von einer jeweils dafür zuständigen Stelle ausstellen lässt. Der Herausgeber *(Issuer)* dieser Attribute attestiert einem Inhaber bestimmte Eigenschaften, indem er diese kryptographisch behandelt und der anfordernden Instanz übergibt. Diese Instanz ist ein prüfender Dienst *(Verifier)*, welchem eine Aussage über den Inhaber vorgelegt wird, damit er entscheiden kann, ob und wie er den Inhaber auf eine von ihm kontrollierte Ressource zugreifen lassen will. Über das Verhältnis und die Ausprägungen des Dreiecks Herausgeber, Inhaber und prüfender Dienst wurde bereits berichtet (vgl. dazu Societybyte-Artikel über Crendentials [https://www.societybyte.swiss/2021/12/16/ersetzen-kuenftig-verifiable-credentials-x-509-zertifikate/]).

Ein sehr wichtiges Kriterium betrifft die Präsentation eines Nachweises bei einem prüfenden Dienst. Es stellt sich dabei die Frage, ob der Herausgeber nur eine Aussage über den Inhaber erstellt, oder ob er am Präsentationsprozess zusätzlich beteiligt ist.

Wenn ein Herausgeber eines Nachweises nicht in den Prozess des Präsentierens gegenüber einem prüfenden Dienst involviert ist, spricht man von benutzerzentrierten *(der Inhaber steht im Zentrum)* Lösungsansätzen. Diese Art der Präsentation, in welcher eine direkte Kommunikation zwischen Inhaber und prüfendem Dienst erfolgt, wird in der Folge genauer betrachtet, indem eine Auswahl von Hauptanforderungen aus verschiedenen Sichten dargestellt wird.

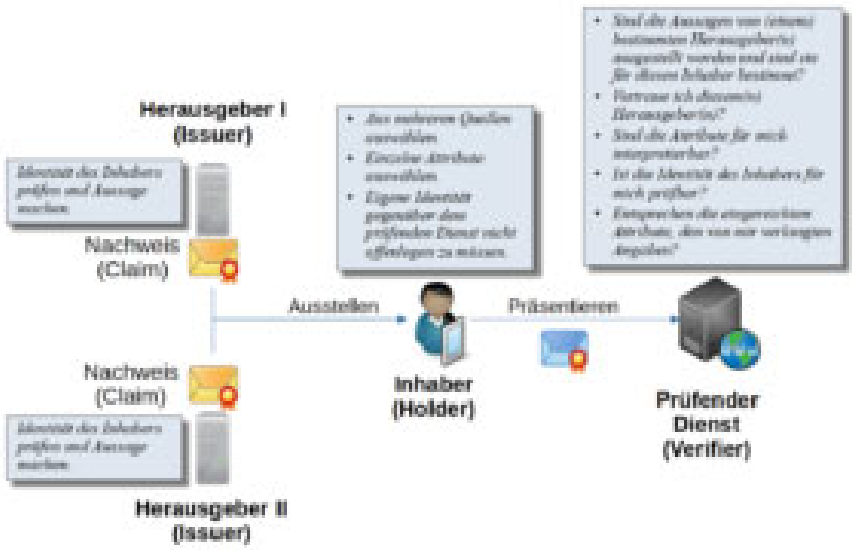

Abbildung 1: Hauptanforderungen der einzelnen Akteure

AUS SICHT DES HERAUSGEBERS:

- *Authentizität des Inhabers:* Bevor ein Herausgeber (Issuer) eine verbindliche Aussage über einen Inhaber machen kann, muss dieser sich zuerst authentisieren. Die erforderliche Stärke der Authentisierung ist abhängig von der Aussage, welche ein Herausgeber macht. Erst wenn ein Herausgeber sich davon überzeugen konnte, dass sich ein Inhaber nach seinen Regeln authentisiert hat, wird er bereit sein, eine allgemein überprüfbare Aussage über diesen Inhaber auszustellen. Diese Aussage wird vielfach als Nachweis oder als Claim bezeichnet.
- Revozierung: Der Widerruf eines Nachweises muss möglich sein, ohne dass die Identität des Inhabers dadurch offengelegt wird. Der Widerruf kann vom Herausgeber oder dem Inhaber ausgelöst werden.

AUS SICHT DES INHABERS:

- *Verschiedene Quellen:* Der Inhaber soll Aussagen über sich aus mehreren Quellen (von verschiedenen Herausgebern) zusammenstellen und einem prüfenden Dienst präsentieren können.
- *Selektive Offenlegung:* Ein Inhaber soll wählen können, welche Attribute er gegenüber einem prüfenden Dienst offenlegen will. Der Rest der Attribute soll einem prüfenden Dienst verborgen bleiben.
- *Anonymität:* Ein prüfender Dienst darf die Identität eines Inhabers nicht in Erfahrung bringen können (Ausser, wenn ihm der Inhaber bewusst alle notwendigen Informationen liefert).
- *Abgeleitete Attribute:* Die Verwendung von abgeleiteten Attributen muss möglich sein (z.B. Altersgrenze oder Liquidität).
- *Portabilität:* Ein Inhaber muss seine Identitätsinformationen von verschiedenen Endgeräten aus (Desktop, Notebook, Handy, Tablet) verwenden können.
- *Vertrauen:* Ein Inhaber muss zu einem verifizierenden Dienst ein Vertrauen aufbauen können. Er muss sicher sein, dass ein prüfender Dienst seine persönlichen Daten nicht missbrauchen kann. Ein Inhaber muss sicher sein können, dass der prüfende Dienst berechtigt ist, diese Attribute von ihm zu verlangen und in der Funktion auftreten darf.
- *Einfachheit:* Eine Applikation auf einem Endgerät muss für den Inhaber leicht verständlich einsetzbar und transparent sein.

Der Inhaber bereitet die von den Herausgebern ausgestellten Nachweise auf und präsentiert sie in geeigneter Form einem prüfenden Dienst. Dies wird in der oben dargestellten Abbildung mit Briefumschlag-Symbolen dargestellt.

AUS SICHT DES PRÜFENDEN DIENSTES:

- Ein prüfender Dienst muss die Möglichkeit haben, Nachweise, die ihm präsentiert werden, zu verifizieren und auf Aktualität zu prüfen. Er muss prüfen, ob die vorgelegten Nachweise für den Inhaber ausgestellt wurden.
- Um den Schutz der Privatsphäre des Inhabers zu gewährleisten, darf ein prüfender Dienst keinen eindeutigen Identifikator des Inhabers erhalten.
- Wenn ein prüfender Dienst einen Nachweis akzeptiert, vertraut er damit dem Herausgeber.
- Ein prüfender Dienst muss validieren können, dass die eingereichten Nachweise den von ihm verlangten Attributen entsprechen.

Anforderungen müssen nicht vollständig erfüllt werden, um ein System betreiben zu können. Es gibt Anforderungen, welche sich gegenseitig aufheben oder nur mit grossem Aufwand umgesetzt werden können. Viel eher soll dieser Anforderungskatalog eines Identitätsmanagementsystems Fragen aufwerfen und die Diskussion um mögliche Lösungsansätze anzufachen.

Schlussfolgerung

Aus diesen Anforderungen können folgende Eigenschaften eines Identitätsmanagement-Systems abgeleitet werden:

Ein *Herausgeber* muss Informationen eines Inhabers vorgängig prüfen, für welche er zuständig ist. Er erstellt einen Nachweis auf Grund der Authentisierung (die Stärke ist abhängig von der Information). Wenn er dies nicht macht, ist die Aussage nicht seriös und belastbar. Ein Inhaber kann sich daher gegenüber einem Herausgeber nicht anonym verhalten.

Ein *Inhaber* muss davon ausgehen können, dass die Informationen, die er einem prüfenden Dienst übermittelt, nicht missbraucht werden können. Der Inhaber soll die Möglichkeit haben, sich anonym gegenüber einem prüfenden Dienst zu verhalten, auch wenn dies illusorisch ist, denn ein prüfender Dienst erstellt im Normalfall keine Geschäftsbeziehung mit anonymen Benutzern.

Ein *prüfender Dienst* muss sich auf die Validität der vorgelegten Nachweise und auf deren berechtigte Nutzung verlassen können.

AUTOR/AUTORIN: GERHARD HASSENSTEIN

Gerhard Hassenstein ist Dozent an der BFH Technik und Informatik.

Posts von Gerhard Hassenstein | Website

AUTOR/AUTORIN: ANNETT LAUBE

Annett Laube ist Dozentin der Informatik an der BFH Technik & Informatik und leitet das Institute for Data Applications and Security (IDAS). Sie hat die fachliche Verantwortung für das Wissenschaftsmagazine SocietyByte, insbesondere für den Schwerpunkt Digital Identity, Privacy & Cybersecurity.

Posts von Annett Laube | Website

PDF erstellen

Ähnliche Beiträge

Die Rolle der E-ID für das Digital Government
Ersetzen künftig «Verifiable Credentials» X.509-Zertifikate?
Self-Sovereign Identities - Kontrollieren wir in Zukunft unsere Identität selbst?
Self-Sovereign Identities: Von der Vision bis heute
Über die Privacy beim Login

1

ANTWORT

MUHAMMAD SOBARI
23. Juni 2022 um 12:39

Thank you for nice information. Visit us https://uhamka.ac.id

Antworten