SocietyByte Wissenschaftsmagazin der Berner Fachhochschule

Ersetzen künftig «Verifiable Credentials» X.509-Zertifikate?

Von Gerhard Hassenstein (BFH Technik & Informatik) , Annett Laube (BFH Technik & Informatik) | 0 Kommentare

X.509-Zertifikate gibt es schon seit über 40 Jahren. Sie werden für die Identifikation von Subjekten (Web-Servern, Personen, usw.) verwendet. Sie gelten als vertrauenswürdige und erprobte Berechtigungsnachweise und wir verlassen uns tagtäglich auf sie. Warum also mit Verifiable Credentials (VC) eine neue, in der breiten Öffentlichkeit unbekannte Technologie einführen? Um eine Public Key Infrastruktur (PKI) Lösung (welche auf X.509-Zertifikaten beruht) mit einer Self-Sovereign Identity (SSI) Lösung vergleichen zu können, muss zuerst der Unterschied und die Eigenschaften ihrer Berechtigungsnachweise beleuchtet werden.

Bei einem benutzerzentrierten Ansatz [https://www.societybyte.swiss/2021/10/01/zentrale-oder-dezentrale-identitaeten/] werden Informationen zu einer Identität in Form eines standardisierten Container dem Inhaber übergeben, denn er verfolgt den Prozess «Ausstellen-Erhalten-Besitzen und Vorzeigen-Verifizieren».

Abbildung 1: Benutzerzentriertes Dreieck

Wie sieht dieser Prozess aus?

Nachweise werden von einem Herausgeber (Issuer) erstellt. Der Nachweis wird dann dem Inhaber (Holder) ausgehändigt, der ihn zur späteren Verwendung speichert. Ohne dass der Herausgeber dies mitkriegt, kann der Inhaber etwas über sich selbst nachweisen, indem er seine Nachweise einem Überprüfer (Verifier) vorlegt. Dieser kann dann entscheiden, ob die präsentierten Nachweise für den Zugriff auf eine Ressource ausreichen und ob er dem Herausgeber vertraut.

In diesem Artikel wird keine Untersuchung darüber gemacht, ob es in VCs gegenüber X.509 Zertifikaten Sicherheitslücken gibt. Das Ziel ist viel eher eine Gegenüberstellung der beiden Gefässe zu machen, denn sowohl VCs wie auch X.509-Zertifikate repräsentieren eine Identität, welche von einem prüfenden Dienst verifiziert werden kann.

Digitale Signaturen

Eine digitale Signatur ist ein grundlegendes kryptografisches Verfahren, bei welcher ein Besitzer eines privaten Schlüssels mit diesem eine Nachricht signieren kann, und jeder der im Besitz des entsprechenden öffentlichen Schlüssels ist, diese Signatur überprüfen kann. Mit einer digitalen Signatur wird die Herkunft (Authentizität) und Unversehrtheit (Integrität) der Daten nachweisbar gemacht.

X.509 Zertifikat

Damit ein öffentlicher Schlüssel eines Teilnehmers vertrauenswürdig von jemand anderem angewendet werden kann, wird dieser zusammen mit Informationen (z.B. dem Namen) des Inhabers in ein Zertifikat gepackt und vom Herausgeber digital signiert. Damit macht der Herausgeber das Zertifikat fälschungssicher und beglaubigt, dass die Information von ihm stammt.
Grundsätzlich kann ein X.509 Zertifikat folgende Informationen beinhalten:

- Name (optional einige Attribute) des zu schützenden Subjekts
- Öffentlicher Schlüssel des Subjekts
- Zusatzinformationen des Ausstellers, Verwendungszweck des Schlüssels und des Zertifikats
- Revokationsinformationen
- Signatur eines Ausstellers, die den gesamten Zertifikatsinhalt abdeckt

Dieses Format eines X.509 Zertifikats ist bereits seit langem standardisiert und wird seit Jahrzehnten vielseitig eingesetzt.

Verifiable Credential (VC)

VCs sind digitale Nachweise, welche es einem Herausgeber erlaubt, eine Behauptung über einen Inhaber zu erstellen. Sie werden vom Herausgeber digital signiert, damit ein Prüfer die Behauptung des Ausstellers verifizieren kann.

*Abbildung 2 Beispiel eines Verifiable Credentials*X.509

Zertifikate und VCs haben denselben Zweck und gleichen sich bezüglich Inhalt.

Worin besteht also der Unterschied zwischen diesen beiden Nachweisen?

Ein X.509-Zertifikat ist gegenüber einem Verifiable Credential ein starres Gebilde. X.509-Zertifikate haben ein ganz bestimmtes Format und man hat sich im Laufe der Zeit auf einen Inhalt geeinigt. So hat das Zertifikat eines Servers oder eines Benutzers je nach Güteklasse einen vorgegebenen Inhalt. Es gibt zwar einige Vorstösse und Bestrebungen X.509-Zertifikate und das zugrundeliegende PKI-System zu erweitern, wie z.B. Attribut-Zertifikate. Aber bringt es das? Umgekehrt kann man sagen, dass Verifiable Credentials vom Prinzip her viel flexibler sind. Ein VC kann von einem einfachen Statement («true/false») bis hin zu einer komplexen Struktur alles beinhalten (z.B. IMS Comprehensive Learner Record [] [1]), sofern diese Aussage bestimmten Formaten entspricht (z.B. JSON-LD oder JSON-JWT). Das Einzige, was bestehen bleibt, ist die Bedingung, dass ein Prüfer den Inhalt eines Nachweises interpretieren können muss. Dazu wird in obigem Beispiel eines VCs die *Schemadefinition* angegeben. Dies macht ein VC gegenüber einem X.509-Zertifikat vielseitig einsetzbar.

Der wichtigste Unterschied zwischen X.509-Zertifikaten und Verifiable Credentials besteht aber in der **Privacy**. Als X.509-Zertifikate entwickelt wurden (die Erstveröffentlichung war 1988), gab es noch keine Privacy-Anforderungen. Diese kamen erst später hinzu. Früher lag die «Nichtfälschbarkeit» als einzige Anforderung im Zentrum. Heute sind Nichtfälschbarkeit des Nachweises **und** der Schutz der Privatsphäre gefragt.

In der heutigen Zeit sind die Hauptanforderungen an die Privacy folgende:

- *Selektive Offenlegung:* Ein Benutzer muss auswählen können, welche persönlichen Daten mit einem prüfenden Dienst teilen will.
- *Missbrauch:* Ein Benutzer muss sichergehen können, dass ein prüfender Dienst keinen benutzeridentifizierenden Identifikator von ihm erhält, ausser der Benutzer übergibt diesen willentlich.
- *Anonymität:* Der Benutzer muss die Möglichkeit haben, seine Identität gegenüber dem prüfenden Dienst verstecken zu können.

Mit X.509-Zertifikaten beispielsweise ist die erste Anforderung nur sehr schwer umsetzbar, da klassische Applikationen nur eine «en-bloc» (alles oder nichts) Verifizierung zulassen. Hingegen mit VCs – sofern sie einem bestimmten Protokoll (bei Ausstellung und Präsentation) folgen – ist dies einfacher realisierbar.

Auf der anderen Seite muss ein prüfender Dienst die Möglichkeit haben, die Behauptungen, die ihm präsentiert werden, zu verifizieren und sicherzustellen, dass diese noch gültig sind und genau für diesen Benutzer von einem vertrauenswürdigen Herausgeber ausgestellt wurden.

Diese einfache Art der Überprüfung erfüllen X.509 Zertifikate längst, bedingt durch ihre fest vorgegebene Struktur. Sobald hingegen ein Mindestmass an Privacy eingehalten werden soll, werden Gefässe und ihre Anwendungen vor ganz andere Herausforderungen gestellt.

Ein Vergleich in tabellarischer Form der oben aufgeführten Hauptanforderungen:

Fazit

Verifiable Credentials haben X.509-Zertifikaten einiges voraus. Erstens sind sie viel flexibler, was ihren Inhalt anbelangt und zweitens adressieren sie den Schutz der Privatsphäre besser. Zudem sind sie die Basis von «Self-Sovereign Identity», welches ein ernstzunehmender Technologieansatz im Bereich Identitäten werden könnte.

VCs ersetzen aber nicht einfach X.509-Zertifikate. Beide Gefässe werden in Zukunft gleichzeitig auftreten. Dort wo der Schutz der Privatsphäre eines Inhabers wichtig ist, werden voraussichtlich VCs vermehrt eingesetzt werden. Für die Absicherung von Kommunikationskanälen (Secure Channels) hingegen werden auch künftig X.509 Zertifikate eingesetzt werden. Zurzeit unterstützen klassische Protokolle, wie S/MIME oder TLS, VCs nicht. Dies kann sich aber bald ändern.

Es macht deshalb Sinn, existierende Umgebungen so anzupassen, dass sie neben X.509-Zertifikaten auch VCs unterstützen um damit ein Nebeneinander der beiden Technologien zu ermöglichen.

Referenzen

[1] https://www.imsglobal.org/activity/comprehensive-learner-record [https://www.imsglobal.org/activity/comprehensive-learner-record]

[2] Mit einzelnen Attributzertifikaten (eine Erweiterung von X.509 Identitätszertifikaten) wäre dies möglich.

[3] Mit BBS+ Signaturen (BbsBlsBoundSignature2020).

[4] Mit einer angepassten Präsentation (BbsBlsBoundSignatureProof2020)

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 leitet das Institute for Data Applications and Security (IDAS) an der BFH Technik & Informatik und ist verantwortlich für den Schwerpunkt Identität und Privatsphäre am BFH-Zentrum Digital Society.

Posts von Annett Laube | Website

PDF erstellen

Ähnliche Beiträge

Es wurden leider keine ähnlichen Beiträge gefunden.

0

KOMMENTARE