Public-Key-Infrastrukturen

Beim Einsatz asymmetrischer Verfahren ohne zusätzliche Infrastruktur ergeben sich einige Probleme. Diese lassen sich in vier Bereiche aufteilen.

Authentizität der Schlüssel

Wie im vorigen Abschnitt bereits besprochen, haben wir ein Authentizitätsproblem. Wenn Alice Bob eine verschlüsselte Mail schreiben will, benötigt sie Bobs öffentlichen Schlüssel. Wenn Mallory es jedoch schafft, Alice seinen eigenen öffentlichen Schlüssel als den von Bob unterzuschieben kann er selbst die Mail entschlüsseln.

Das kann auf verschiedene Art und Weise geschehen: Wenn Bob Alice seinen öffentlichen Schlüssel übers Netz zuschickt, kann Mallory den Schlüssel abfangen und durch seinen eigenen ersetzen (Man-in-the-Middle-Attacke). Dasselbe kann Mallory machen, wenn Alice Bobs Schlüssel von einem Key-Server herunterlädt. Ein Angreifer kann auch versuchen, seinen eigenen Schlüssel im Netz als den von Bob zu verbreiten. Einem öffentlichen Schlüssel kann man nicht ansehen, wem er gehört.

Sperrung von Schlüsseln

Mallory hat Alices privaten Schlüssel von ihrem Computer gestohlen, jetzt kann er verschlüsselte Nachrichten lesen und digitale Signaturen von Alice fälschen. Nachdem Alice den Diebstahl bemerkt hat, verwendet sie den alten privaten Schlüssel nicht mehr - sie sperrt den Schlüssel. Stattdessen erzeugt sie sich ein ein neues Schlüsselpaar. Aber woher sollen die Kommunikationspartner von Alice wissen, dass Alices alter Schlüssel nicht mehr funktioniert? Das Problem ist, dass man einem öffentlichen Schlüssel nicht ansieht, ob er gesperrt ist.

Ähnliche Probleme ergaben sich während der Corona Pandemie in den Jahren ab 2020 mit fälschlich ausgestellten Impfzertifikaten: Man konnte diesen kryptographischen Signaturen nicht ansehen, ob sie mit Schlüsseln von nicht vertrauenswürdigen Apothekern unterschrieben waren.[1)]

Verbindlichkeit

Der Sinn einer digitalen Signatur ist es unter anderem, für Verbindlichkeit zu sorgen. Das bedeutet, dass Alice im Nachhinein eine angefertigte Signatur nicht abstreiten kann. Ein solches Abstreiten ist aber recht einfach: Alice behauptet, der Schlüssel, mit dem sie eine Signatur angefertigt hat, sei gar nicht ihrer. Das Problem ist wieder, dass man einem öffentlichen Schlüssel nicht ansieht, wem er gehört.

Durchsetzen einer Policy

Wenn die Verwendung von asymmetrischer Kryptographie bestimmten Regeln unterworfen sein soll,

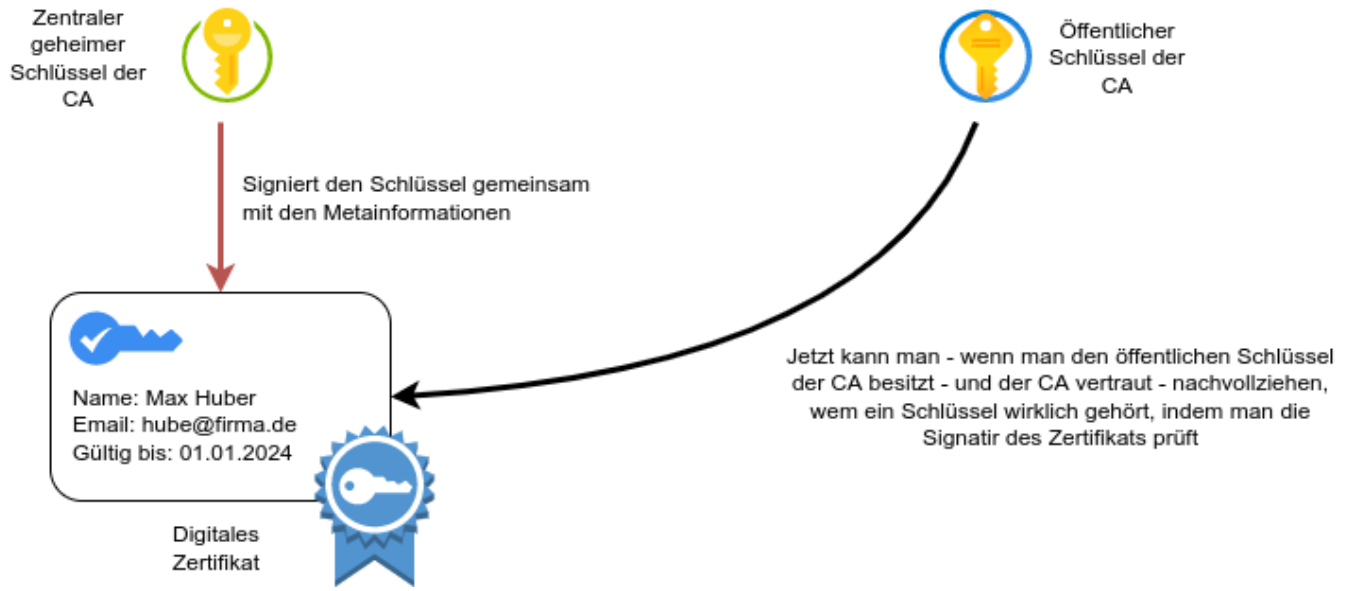
spricht man von einer **Policy**. Das könnte z.B. sein:

- Jeder soll nur ein Schlüsselpaar bekommen.
- Manche Schlüsselpaare sollen nur zum Verschlüsseln eingesetzt werden, nicht aber zur digitalen Signatur.
- Alle öffentlichen Schlüssel sollen zentral registriert sein.
- Wenn jemand das Unternehmen verlässt, dann soll dessen öffentlicher Schlüssel gesperrt werden.

Digitale Zertifikate

Alle Problem rühren daher, dass der öffentliche Schlüssel zunächst nur eine Abfolge von Nullen und Einsen ist - er enhält darüber hinaus keine weiteren Informationen (Name, Mailadresse oder ähnliches) und wenn er diese enthält (z.B. gnuPG) können diese Metainformationen frei gesetzt und geändert werden - sind also nicht vertrauenswürdig.

Ein PKI löst dieses Problem, indem sie einen Datensatz, der aus dem eigentlichen Schlüssel und weiteren Informationen besteht, durch einen "zentralen privaten Schlüssel" signiert und damit eine Verbindlichkeit einführt:

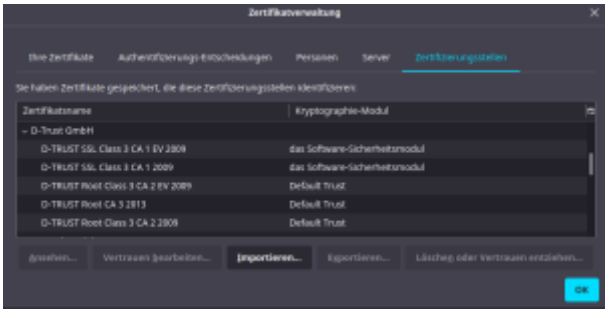


Eine wichtige Frage bei einem solchen digitalen Zertifikat ist, wer es signiert (wer die "Zertifizierung" durchführt). Die naheliegendste Möglichkeit besteht darin, eine unabhängige Instanz einzurichten, die diese Aufgabe übernimmt. Eine solche Instanz wird Zertifizierungsstelle oder **Certification Authority (CA)** genannt. Ein Unternehmen das Public-Key-Verfahren einsetzt kann seine CA durch die IT-Abteilung betreiben, es ist aber auch üblich, dass eine Behörde als CA-Betreiber auftritt oder dass ein Unternehmen die Dienste einer CA am Markt anbietet.

Einen Sinn hat eine CA nur dann, wenn man ihre Signaturen verifizieren kann. Dazu muss man den öffentlichen Schlüssel der CA kennen. Woher weiß man jetzt aber, ob man den richtigen CA-Schlüssel hat? Woher weiß man, ob er nicht gesperrt wurde? Ist die Gültigkeitsdauer des CA-Schlüssels schon abgelaufen? Diese Fragen lassen sich nur beantworten, wenn auch der öffentliche Schlüssel der CA in ein digitales Zertifikat gefasst wird. **Aber wer signiert jetzt das Zertifikat der CA?** Das Problem

ist also lediglich eine Stufe "nach oben verschoben".

Praktisch wird das derzeit durch sogenannte Root-Zertifikate umgesetzt, welche Browser und Betriebssysteme mitbringen, hier ein Screenshot aus Firefox:

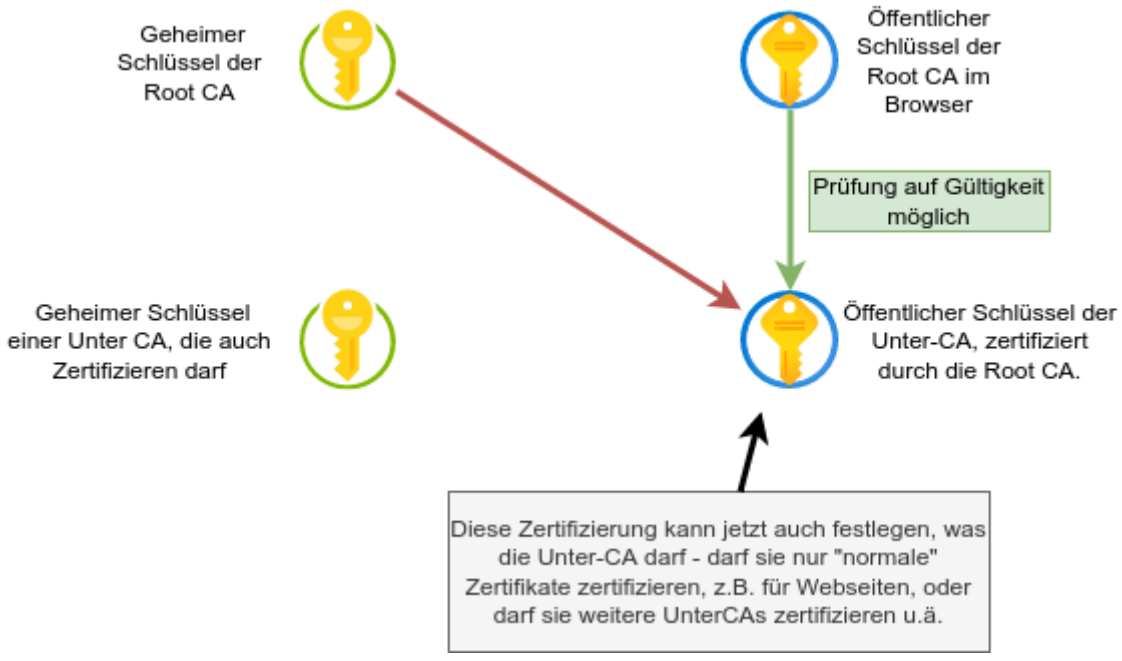


(A1)

Finde heraus, wo du die Zertifikate deines Webbrowsers betrachten kannst und schau dir an, welche Zertifikate dort als vertrauenswürdig hinterlegt sind.

Für andere Anwendungen, beispielsweise bei der CovPass-Check-App, mit der im Zuge der Corona Pandemie 2020 digitale Impfzertifikate auf ihre Gültigkeit geprüft werden konnten, muss das Root-Zertifikat der CA auf andere Weise verteilt werden, z.B bei der Installation der App.

Es ergibt sich eine **Hierarchie** von Zertifikaten, die von Browsern und Systemen als gültig akzeptiert werden.



Man spricht (im Gegensatz zum Web-of-Trust) von **Hierarchical Trust**.

1)

Eine vollständige PKI für die Impfzertifikate hätte dieses Problem gelöst