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 Wiese 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 von Alice Signaturen fälschen. Nachdem Alice den Diebstahl bemerkt hat, verwendet 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.

[1)]

Eine vollständige PKI für die Impfzertifikate hätte dieses Problem gelöst