Datenschutz und Datensicherung DuD 21/2 (1997), 98-99

DuD Forum: Schlüsselgenerierung

Position 1: Einseitig sicher ist nicht sicher genug

Hannes Federrath

Die digitale Signatur im elektronischen Rechtsverkehr basiert auf kryptographischen Verfahren mit öffentlichen und geheimen Schlüsseln. Es ist im Interesse aller Beteiligten, diese Schlüssel so sicher wie möglich zu generieren.

Das Ziel der mehrseitig sicheren Schlüsselgenerierung ist es, daß alle Beteiligten der sicheren Generierung vertrauen können, da ohne dieses Vertrauen keine rechtsverbindliche Kommunikation möglich ist. der Autor vertritt die Auffassung, daß dies mit einer alleinigen Schlüsselgenerierung in einem Trust Center nicht vereinbar ist.

Dipl.-Inform. Hannes Federrath, seit 1994 wissenschaftlicher Mitarbeiter an der TU Dresden, Institut für Theoretische Informatik. Arbeitsgebiete: Sicherheit in verteilten Systemen, Technischer Datenschutz in Mobilkommunikationssystemen.

Aspekt 1: Mächtigkeit eines Trust Centers

Der Zusammenhang zwischen der Identität des Teilnehmers und seinen öffentlichen Schlüsseln wird mittels Zertifikaten (siehe Rubrik „Gateway„ in diesem Heft) hergestellt. Zur Erstellung eines solchen Zertifikates benötigt das Trust Center den öffentlichen Schlüssel des Teilnehmers sowie einen Identitätsnachweis des Inhabers. Als Quittung der Zertifizierung erhält der Teilnehmer das digitale Zertifikat und unterschreibt dem Trust Center eigenhändig (auf Papier) seinen öffentlichen Schlüssel als Garantie dafür, daß er die mit dem geheimen Schlüssel geleisteten Signaturen anerkennt. Der geheime Schlüssel des Teilnehmers wird zu keinem Zeitpunkt bei der Zertifizierung benötigt.

Worin besteht das Vertrauen in ein Trust Center, und wofür ist es haftbar? Alle Teilnehmer müssen darauf vertrauen, daß es nur korrekte Zertifikate ausstellt, d.h. sich gründlich von der Identität des Teilnehmers überzeugt hat und nicht wissentlich falsch handelt.

> *Fall 1: Das Trust Center erfüllt ausschließlich Zertifizierungsaufgaben:*
> Die technische Mächtigkeit eines korrupten Trust Centers beschränkt sich darauf, falsche Zertifikate auszustellen. Es ist nicht in der Lage, einem Teilnehmer einen gefälschten, d.h. selbst generierten Schlüssel unterzuschieben, da es hierzu ebenfalls dessen eigenhändige Unterschrift unter dem falschen öffentlichen Schlüssel fälschen müßte.

Wo und wie werden die öffentlichen und geheimen Schlüssel erzeugt? Dies ist zunächst ein kryptographisches Problem. In die Generierung fließen Zufallszahlen ein, die sozusagen der Anker der Sicherheit der Schlüssel sind. Wer die Zufallszahlen kennt, kennt auch die generierten Schlüssel. Es liegt im eigenen Interesse des Teilnehmers, daß die Schlüsselgenerierung in einer für ihn vertrauenswürdigen Umgebung geschieht. Vertrauenswürdig heißt hier:

- Die Zufallszahlen werden nach ihrer Verwendung unwiederbringlich gelöscht.
- Der geheime Schlüssel wird derart zu einem Gerät transferiert und dort abgespeichert, daß ihn niemand außer dem Besitzer benutzen kann.

Trust Center haben, wie oben erläutert, mit öffentlichen Schlüsseln des Teilnehmers zu tun. Es bietet sich deswegen aus Effizienzgründen an, auch die Generierung der öffentlichen und geheimen Schlüssel gleich dort zu erledigen. Der Nutzer kann mit seinen Schlüsseln sowieso nichts im elektronischen Rechtsverkehr anfangen, bevor er nicht sein Zertifikat besitzt. Dann gilt jedoch:

> *Fall 2: Die Trust Center generieren ebenfalls die Schlüssel eines Nutzers:*
> Die technische Mächtigkeit eines Trust Centers wird erweitert um die Möglichkeit, digitale Signaturen eines Teilnehmers zu fälschen. Hierzu muß es lediglich den geheimen Schlüssel bzw. die bei der Generierung verwendeten Zufallszahlen abspeichern.

Sollte es zu einem Vertrauensverlust kommen, haben die Teilnehmer schlechte Karten. Das gilt nicht nur für den Eigentümer des geheimen Schlüssels, sondern evtl. auch für desssen Geschäftspartner, da der Eigentümer natürlich jetzt auch alle unliebsamen, aber korrekten Signaturen als gefälscht zurückweisen kann.

> *Die Unabstreitbarkeit digitaler Signaturen wird diskreditiert:*
> Bei der Generierung der Schlüssel durch das Trust Center kann ein Teilnehmer in Streitfällen unwiderlegbar behaupten, das Trust Center hätte seinen geheimen Schlüssel kopiert und mißbraucht. Damit verliert eine digitale Signatur weitgehend ihren Beweiswert.

Folglich ist, solange man nicht von vornherein jede Haftung eines Trust Centers bzgl. der korrekten Schlüsselgenerierung ausschließt (was gleichbedeutend mit einem Freifahrtschein für den Mißbrauch ist, falls Teilnehmer ihre Chipkarten ausforschen können), keine vernünftige Kommunikation im elektronischen Rechtsverkehr mehr möglich.

Die korrekte und sichere Schlüsselgenerierung ist eigentlich nicht das Problem eines korrekt arbeitenden Trust Centers: Es hat überhaupt kein Interesse daran, die geheimen Schlüssel der Teilnehmer zu erfahren. Auch der Staat dürfte kein solches Interesse haben. Schließlich handelt es sich hierbei nicht um ein Krypto-Regulierungsproblem, das die Strafverfolgung behindert, denn der geheime Schlüssel des Teilnehmers dient nicht zur Datenver- bzw. -entschlüsselung, obwohl er auch hierfür begrenzt geeignet ist. Eine etwaige Verschlüsselung der signierten Daten hat damit aber nichts zu tun. Die Vertrauenswürdigkeit eines Trust Centers ist viel leichter (bzw. nur) zu erreichen, wenn es keine geheimen Teilnehmerschlüssel kennt. Selbst wenn die Schlüssel nach der Erzeugung wirklich sofort gelöscht werden, läßt sich dies nicht beweisen. Es bleibt stets Raum für Gerüchte und Unterstellungen. Es sollte also im eigenen Interesse eines Trust Centers sein, keine geheimen Schlüssel zu erzeugen.

Wer eine Sicherungsinfrastruktur aufbaut, muß dem Teilnehmer Optionen geben, seine Schlüssel sicher zu generieren. Wie die obigen Bemerkungen gezeigt haben, ist aber die alleinige Generierung in einem Trust Center ungeeignet.

Aspekt 2: Physisch sichere Geräte

Wie sieht es mit der alleinigen Generierung beim Teilnehmer aus? In jedem Fall benötigt er sichere Rechentechnik, genügend Zufallszahlen und ein sicheres Gerät, auf dem er den geheimen Schlüssel dauerhaft speichert. Die Generierung der Schlüssel braucht nicht sicherer zu sein, als das sichere Gerät die folgende sichere Aufbewahrung des geheimen Schlüssels gewährleistet. Eine abstrahlungssichere Umgebung bei der Generierung dürfte deshalb nicht zwingend erforderlich sein, sie schadet jedoch auch nichts. Da der Signieralgorithmus den geheimen Schlüssel zum Signieren benötigt, muß er ebenfalls in dem Vertrauensbereich des Teilnehmers stattfinden, in dem der geheime Schlüssel gespeichert ist. Technisch gesehen wird dies meistens dasselbe Gerät sein. Da dieses Gerät also Rechenkapazität besitzt, bietet es sich an, die Schlüsselgenerierung gleich dort ablaufen zu lassen. Auf diese Weise verläßt der geheime Schlüssel nie das sichere Gerät.

Wenn es aus technischen Gründen nicht möglich ist, die Schlüsselgenerierung direkt im sicheren Gerät durchzuführen, wird sichere Rechentechnik benötigt, auf der die Generierung abläuft. Es ist nicht realistisch, daß sich ein Teilnehmer eigens zur Schlüsselgenerierung sichere Rechentechnik anschafft, sie auf trojanische Pferde untersucht, den Generieralgorithmus implementiert bzw. kontrolliert und dann seine Schlüssel generiert. Hier bietet das Trust Center also bessere Voraussetzungen zur sicheren Schlüsselgenerierung.

Aspekt 3: Erzeugung von Zufallszahlen

Sofern die Schlüsselgenerierug im sicheren Gerät durchführbar ist, stellt sich die Frage, wie die nötigen Zufallszahlen in das Gerät kommen, falls das Gerät nicht selbst in der Lage ist, echte Zufallszahlen zu erzeugen oder auch nur eine Instanz (Teilnehmer, Trust Center, Staat etc.) der Erzeugung nicht traut.

Es ist wichtig, daß „genügend Zufall“ in das Gerät eingegeben wird. Das generierte Schlüsselpaar ist dabei mindestens so sicher wie der sicherste Zufallszahlenanteil. Es könnten also sowohl vom Teilnehmer als auch vom Trust Center Zufallszahlen in das Gerät eingegeben werden, wobei der beste Zufallsanteil die minimale Güte der Schlüsselerzeugung bestimmt.

Verallgemeinert heißt das, es könnten der Teilnehmer und mehrere fremde Instanzen ihren Zufallsanteil beisteuern. Wichtig ist: Der Teilnehmer hat die Option, die Dienstleistungen des Trust Centers zur Schlüsselgenerierung zu nutzen; es ist für ihn aber kein Muß.

> *Mehrseitig sichere Schlüsselgenerierung als Chance:*
> Die Beteiligung des Teilnehmers sowie mehrerer unabhängiger dritter Instanzen unterstützt die korrekte und sichere Generierung der Schlüsselpaare des Teilnehmers. Gleichzeitig verletzt sie keinerlei Sicherheitsinteressen anderer Beteiligter einer Sicherungsinfrastruktur (mehrseitige Sicherheit).

Fazit

Die hier aufgezeigten Varianten werden den Sicherheitsinteressen mehrerer Parteien gerecht und unterstützen damit sogar die Schaffung von Vertrauen in die neue Sicherungsinfrastruktur. Die Beteiligten, die die Beweislast im Streitfall haben, sollen und müssen der sicheren Schlüsselgenerierung vertrauen können!

Gerade im Bereich Sicherheit sind Vorsicht und die Respektierung von Mißtrauen und Schutzbedürfnis kritische Erfolgsfaktoren. Um die positiven Merkmale von Sicherungsinfrastrukturen nicht aufs Spiel zu setzen, sollten keine halbsicheren Lösungen eingeführt werden, sonst bleibt Vertrauen in neue Kommunikationstechnik labil. Außerdem sollten technische und organisatorische Regelungen, die unsinnig oder gar gefährlich sind, unterbleiben. Hierzu gehört auch das Vorschreiben der Schlüsselerzeugung im Trust Center, denn sie kann für einige Teilnehmer das Risiko erhöhen, ohne daß dies anderen Teilnehmern nützt.

Dank

Ein herzlicher Dank für Hinweise, Kritik und Verbesserungsvorschläge geht an Dirk Fox, Marit Köhntopp, Andreas Pfitzmann und Kai Rannenberg. Diese Arbeit wurde finanziell unterstützt durch die Gottlieb-Daimler- und Karl-Benz-Stiftung Ladenburg.