International Working Group
on Data Protection
in Telecommunications

675.23.14

Arbeitspapier

zu Datenschutzaspekten digitaler Zertifikate und public-key-Infrastrukturen

angenommen auf der 30. Sitzung der Arbeitsgruppe am 28. August 2001 in Berlin

- Übersetzung -

Instanzen, die miteinander kommunizieren – ob mit Hilfe elektronischer oder anderer Mittel – können alle Arten von Anforderungen an die Sicherheit und Verlässlichkeit des Informationsaustausches haben. Wichtige Aspekte beinhalten die Identifikation, Authentifizierung, Autorisierung, Vertraulichkeit, Integrität und Nichtabstreitbarkeit.

Kryptographie ist eine beinahe unverzichtbare Technik, um diese Eigenschaften in einem offenen, elektronischen Umfeld zu garantieren. Eine Technik, deren Popularität rapide zunimmt, ist die *public-key-Kryptographie*. Diese Technik verwendet zwei verschiedene Schlüssel, von denen einer benutzt wird, um Nachrichten zu verschlüsseln, und der andere, um sie zu entschlüsseln. Einer dieser beiden Schlüssel, der private Schlüssel, muss von seinem Inhaber geheim gehalten werden, der andere wird von ihm öffentlich zur Verfügung gestellt. Public-key-Kryptographie kann auf zwei Arten angewendet werden. Wenn der Schlüssel zur Verschlüsselung veröffentlicht wird, kann jedermann diesen Schlüssel benutzen, um eine verschlüsselte Nachricht zu erzeugen, die nur der Besitzer des dazugehörigen privaten Schlüssels entschlüsseln kann. Wenn auf der anderen Seite der Entschlüsselungsschlüssel veröffentlicht wird, kann er benutzt werden, um die Quelle einer verschlüsselten Nachricht zu authentifizieren: Nur der Besitzer des korrespondierenden privaten Schlüssels kann die Nachricht verschlüsselt haben. Diese letztgenannte Anwendung ist als *digitale Signatur* bekannt.

Die Nutzung von public-key-Kryptographie erfordert, dass der Schlüssel in verlässlicher Weise mit der Identität oder anderen Attributen des Schlüsselinhabers verbunden wird. Die Infrastruktur, die benötigt wird, um dies zu ermöglichen, wird als *public-key-Infrastruktur* (PKI) bezeichnet. Ein *vertrauenswürdiger Dritter* (*trusted third party,* TTP) garantiert diese Verbindung in einer PKI[1]. Die TTP erreicht dies, indem sie selbst eine digitale Signatur benutzt. Ein *digitales Zertifikat* ist jegliches digital signierte Dokument. Digitale Zertifikate werden üblicherweise von einer TTP herausgegeben und

[1] Die Europäische Richtlinie 99/93/EG hat die Bezeichnung „Zertifikatsdiensteanbieter“ für TTPs eingeführt, die alle oder einige der Dienste anbieten, die notwendig sind, um diese Garantie herzustellen.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Pallasstr 25/26
D-10781 Berlin
Phone +49 / 30 / 7560 7809
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

von ihr digital signiert; sie verbinden dann einen öffentlichen Schlüssel mit Attributen des Schlüsselinhabers.

Wenigstens drei wesentliche Datenschutzaspekte sind mit der Nutzung von öffentlichen public-key-Infrastrukturen verbunden:

A. Bezeichnung und Identität, Pseudonymität, Anonymität;
B. Verbreitung von PKI-Information;
C. rechtmäßiger Zugang.

A Bezeichnung und Identität, Pseudonymität, Anonymität

Normalerweise ist wünschenswert, dass die Identität eines digital Unterzeichnenden bekannt ist. Dies bedeutet allerdings nicht, dass diese Identität auch in dem Zertifikat enthalten sein muss. Es ist oftmals ausreichend, dass sie, wenn notwendig, festgestellt werden kann, z. B. im Fall von Betrug. Da der Nutzer eines pseudonymen Zertifikats eine offensichtliche Absicht hat, seine Identität zu verbergen, muss genau festgelegt werden, welche Umstände hinreichende Gründe darstellen, diese Daten trotzdem an Dritte weiterzugeben.

Modelle für „PET“[2]-Zertifikate, die durch Nutzung von Pseudonymen unter anderem die Privatsphäre schützen, verdienen mehr Aufmerksamkeit, als sie bisher erhalten haben. Dies würde dazu beitragen, das Potential der public-key-Kryptographie als eine wichtige datenschutzfreundliche Technologie zu verwirklichen.

Traditionelle identifizierende Daten wie Namen, Adresse und Wohnort sind eine nicht hinreichende Basis, personenbezogene Daten verlässlich zu verbinden. Solche Verbindungen können der Qualität der Daten dienen, sie können allerdings auch große Risiken für den Datenschutz mit sich bringen. Aus diesem Grunde ist die Einführung von national oder sogar global eindeutiger Identifikatoren nicht wünschenswert. Sektorale oder ketten-basierte Identifikatoren können eine alternative Lösung darstellen. Öffentliche Schlüssel oder – noch gefährlicher – biometrische Merkmale dürfen nicht zu alternativen, eindeutigen Identifikatoren werden.

B Verbreitung von PKI-Informationen

Innerhalb einer PKI ist es notwendig, verschiedene Arten von Information zu verbreiten. Die bedeutendsten sind Zertifikat-Informationen und Widerrufs-Informationen.

Die populärste Art, Zertifikate zu verbreiten, ist ein Verzeichnis. Dies sollte nur mit der Erlaubnis des Inhabers des Zertifikats erfolgen, dem auch eine tatsächliche Alternative zur Verfügung gestellt werden muss. Die Erlaubnis muss freiwillig gegeben werden und auf korrekten, klaren und vollständigen Informationen basieren. Wenn Zertifikate im großen Umfang öffentlich zugänglich sind, eröffnet dies alle Arten von Möglichkeiten zur Erstellung detaillierter Profile. Daher verdient die private Verbreitung als eine Alternative ernsthafte Aufmerksamkeit, bei der der Inhaber des Zertifikats selbst für die Lieferung des Zertifikats an eine verifizierende Instanz verantwortlich ist.

Widerrufs-Information, die verbreitet wird, darf nicht mehr Daten als notwendig enthalten, z. B. nur eine Seriennummer anstatt des gesamten widerrufenen Zertifikats.

[2] PET = privacy-enhancing technology (datenschutzfreundliche Technologie).

PKI-Information wird für einen bestimmten Zweck verbreitet. Die weitere Verarbeitung dieser Information muss mit diesem Zweck vereinbar sein. Dies gilt auch für die Verbreitung durch ein Verzeichnis. Dieses muss entsprechend aufgebaut sein.

C Rechtmäßiger Zugang

Verschiedene Parteien können Zugriff auf die bei den TTPs vorhandenen Daten verlangen. Die gewünschte Information kann die Identität des Inhabers eines pseudonymen Zertifikats sein, der Schlüssel zur Entschlüsselung verschlüsselter Nachrichten oder Dateien oder die Nachrichten oder Dateien selbst. Strafverfolgungsbehörden und Geheimdienste haben üblicherweise verschiedene spezifische gesetzliche Befugnisse in diesem Bereich. Andere Parteien haben normalerweise rechtmäßigen Zugriff auf der Basis eines generelleren Rechts auf bestimmte Informationen. Die Arbeitsgruppe spricht sich für eine Herangehensweise aus, die einen Ausgleich zwischen den Prüfungsbedürfnissen von Regierungen und dem Recht auf Datenschutz ihrer Bürger schafft. Das Vertrauen des Benutzers ist eine *conditio sine qua non* für TTPs. Es ist daher in den Kreisen der TTP üblich, den Prinzipien des Datenschutzes das Wort zu reden. Unglücklicherweise gehen diese Äußerungen selten über generelle Bemerkungen wie „... natürlich halten TTPs die Datenschutzgesetze ein...“ hinaus. Die Garantie eines angemessenen Schutzes personenbezogener Daten verlangt allerdings, dass dieser Aspekt zum frühestmöglichen Zeitpunkt bereits in der Designphase von Technologien und Infrastrukturen in Betracht gezogen wird. Wenn dies getan wird, können TTP-Dienste im Allgemeinen und digitale Zertifikate im Besonderen einen bedeutenden Beitrag zum Datenschutz bei elektronischen Transaktionen und der elektronischen Kommunikation leisten.

Die Arbeitsgruppe gibt daher die folgenden Empfehlungen:

1. Pseudonyme (oder sogar anonyme) Zertifikate sind identifizierenden Zertifikaten in allen Fällen vorzuziehen, in denen die Identifikation des Zertifikatinhabers im Hinblick auf den spezifischen Zweck, für den das Zertifikat benutzt wird, nicht erforderlich ist. TTPs sollten aktiv zur Entwicklung von Technologien und Infrastrukturen beitragen, die die größtmögiche Nutzung solcher Zertifikate, ob im Rahmen des X.509-Standards oder nicht, erlauben. In Situationen, in denen die Nutzung identifizierender Zertifikate nicht verhindert werden kann, sollten solche Zertifikate anonym oder pseudonym genutzt werden, wenn immer dies möglich ist.

2. Die Nutzung von nationalen oder sogar globalen eindeutigen Identifikatoren sollte im Hinblick auf die ernsten Risiken für den Datenschutz vermieden werden. Es gibt andere Möglichkeiten wie den Einsatz von sektoralen oder ketten-basierten Nummern. Ein darauf basierender Informationsaustausch sollte mit hinreichenden Sicherungsmaßnahmen begleitet werden. PKIs sollten so konstruiert sein – z. B. durch das Angebot multipler, kurzlebiger und/oder rollenbasierter Zertifikate -, dass Zertifikatsnummern, öffentliche Schlüssel oder biometrische Merkmale nicht zu alternativen, eindeutigen Indikatoren werden.

3. Verzeichnisse öffentlicher Zertifikate sollten – soweit dies möglich ist – so konstruiert werden, dass sie nur solche Anfragen zulassen, die im Hinblick auf den Zweck des Verzeichnisses erforderlich sind. Die Betroffenen sollten die Möglichkeit erhalten, nicht in einem solchen Verzeichnis aufgeführt zu werden; d. h., die private Verteilung von Zertifikaten muss dem Inhaber des Zertifikats als eine wirkliche Alternative zur Verfügung gestellt werden.

4. TTPs dürfen die zu einem Pseudonym gehörige Identität nur im Falle einer gesetzlichen Verpflichtung, die auf einer dringenden sozialen Notwendigkeit basiert, oder mit der ausdrücklichen Einwilligung des Inhabers des Zertifikats aufdecken.

5. Die Befugnisse von Strafverfolgungseinrichtungen und Geheimdiensten im Hinblick auf den rechtmäßigen Zugang sollten mit dem Schutz der Grundrechte und -freiheiten und insbesondere personenbezogener Daten in Einklang gebracht werden.