Institut für Informatik und Gesellschaft, Abteilung Telematik
Albert-Ludwigs-Universität Freiburg

Privatsphäre und Datenschutz mittels Private Credential Systems

Ausarbeitung im Seminar
Technologien der Informationsgesellschaft

Bearbeiter:	Matthias Bernauer
Matrikelnummer:	150 xx xx
Aufgabensteller:	Prof. Dr. Günter Müller
Betreuer:	-
Abgabedatum:	20. Januar 2005

Zusammenfassung

Zertifikate ermöglichen es in der digitalen Welt, rechtsverbindliche Geschäfte abzuschließen, indem sie die Identität des Vertragspartner bescheinigen und evtl. vorhandene Handlungsvollmachten beglaubigen. Zugleich entstehen durch den möglichen Austausch von Informationen verschiedener Datennetze erhebliche datenschutzrechtliche Probleme und Bedenken. Diese Arbeit gibt einen kurzen Einblick in die Funktionsweise und den Einsatz digitaler Zertifikate. Mit der Vorstellung von Private Credential Systems wird komfortabler Einsatz unter Umgehung datenschutzrechtlicher Bedenken erläutert.

Inhaltsverzeichnis

1 Einleitung

Die Informationstechnik trug in den vergangenen Jahren wesentlich dazu bei, alltägliche Anwendungen, Prozesse und Tätigkeiten sowohl für die einzelnen Benutzer als auch den Anbietern dieser Technik erheblich zu beschleunigen und zu vereinfachen. Durch den Einsatz digitaler Medien können Informationen und Dienstleistung unter Einsparen von Zeit und Kosten angeboten werden und erhöhen somit die Effektivität regulärer Abläufe. Die Nutzung elektronischer Datenverarbeitungssysteme ermöglicht es jedoch zugleich, personenbezogene Informationen kostengünstig zu archivieren und auszuwerten, wodurch ungeahnte Einblicke in die Privatsphäre ermöglicht werden. Mit der Abkehr vom gewohnten Briefverkehr durch die zunehmende Verwendung von schnelleren und kostengünstigeren, digitalen Medien und elektronischen Systemen in vertraulichen Bereichen, wie der elektronischen Gesundheitskarte, dem biometrischen Reisepass, registrierungspflichtigen Kommunikationsmitteln, electronic Banking, Lokalisierungsmöglichkeiten, eVoting, u.v.a., entstehen daher erhebliche Datenschutzprobleme. Die von Anbietern personalisierter Dienste erhobenen, vertraulichen Daten dienen nicht nur zur Begründung und Berechnung kostenpflichtiger Dienstleistungen, sondern werden auch auf Grund gesetzlicher Anforderungen und Überwachungsverordnungen erhoben. So ist es heutzutage gebräuchlich, möglichst viele Daten zu erheben und für die Weiterverarbeitung zu Marketingzwecken und künftiger Eventualitäten zu sichern.

2 Identity-Management

Um die Privatsphäre der Benutzer zu schützen und das Risiko des „gläsernen Bürgers“einzuschränken, kommen Privacy and Identity Management Systeme zum Einsatz. In der analogen Welt sind wir in der Lage, unterschiedliche Rollen in der jeweiligen Situation anzunehmen und die Weitergabe von Informationen dem jeweiligen Umfeld anzupassen, wie bspw. der Trennung von Privat- und Berufsbereich. Durch die Verwendung unterschiedlicher Identitäten kann der Benutzer personenbezogener Dienste auch im virtuellen Bereich die Zurückhaltung persönlicher Daten erreichen und unterschiedliche Profile annehmen.

2.1 Zertifizierung

Zur Wahrung notwendiger Kontrollmöglichkeiten, die u.a. für die Strafverfolgung oder das Versicherungswesen erforderlich sind, können die zur Annahme unterschiedlicher Identitäten verwendeten Pseudonyme jedoch nicht willkürlich gewählt werden, sondern werden aus bestehenden Zertifikaten glaubwürdiger Instanzen abgeleitet. So ist es einer als zuverlässig eingestuften Verwaltungsbehörde möglich, ein vom Bürger selbst generiertes, kryptografisches Zertifikat - seinem digitalen Ausweis in Form eines asymmetrischen Schlüsselpaares - zu signieren und seine Identität damit amtlich zu beglaubigen. Der Inhaber des Zertifikates verfügt somit über ein vertauenswürdiges Dokument, mit dem er sich gegenüber anderen Institutionen anonym und ohne Nennung persönlicher Daten ausweisen kann. Sich anonym auszuweisen ist dabei weder ein Widerspruch in sich selbst noch ein Novum der digitalen Welt. Ein An-

wendungsbeispiel fände sich in der Ausstellung eines Führerscheines, auf dem nur ein Bild des Absolventen versehen mit dem Beglaubigungsstempel einer vertrauenswürdigen Ausgabestelle vorzufinden ist. Eine Verkehrskontrolle könnte zweifelsfrei die Fahrerlaubnis anhand des Bildes des Inhabers feststellen ohne weitere personenbezogene Daten zu erlangen.

2.2 Datenschutz

Durch die Verwendung jeweils unterschiedlicher Zertifikate, kann der Benutzer die Herausgabe persönlicher Daten beschränken und kontrollieren. Idententity Management Systeme helfen hierbei, die Vielzahl von Zertifikaten zu verwalten und sinngemäßeinzusetzen. Um ein hohes Maßan Anonymität zu erreichen ist es wichtig, dass herausgegebene Daten nicht miteinander verknüpft und in Bezug gesetzt werden können. Daher benutzt der Anwender von 'Private Credential Systems' bei jeder Transaktion möglichst ein neues Pseudonym. Dem Inhaber eines Online Shops oder einer anderen Institution steht somit jedesmal ein neuer virtueller Kunde gegenüber, der nicht mit der tatsächlichen Person oder bereits registrierten Kunden in Verbindung gebracht werden kann. Bei Abschluss der Transaktion erhält der Benutzer ein sogenanntes Credential – ein digital signiertes Zertifikat, das die Durchführung der Aktion wie im oben beschriebenen (analogen) Fall der Verkehrskontrolle bescheinigt. Damit bei jeder Transaktion nur die jeweils erforderlichen Daten übermittelt werden, kontrolliert das Crendential System die Verwendung der Zertifikate und verhindert aus externer Sicht die Bildung von Zusammenhängen durch Verknüpfung der der gesammelten Informationen.

Trotz der sorgfältigen Verwendung und Übermittlung persönlicher Daten, ist die Zusicherung absoluter Anonymität nicht möglich. So begründen übergeordnete Interessen und spezielle Situationen die Herausgabe weiterer Informationen. Das eingesetzte System wird damit jedoch nicht überflüssig, sondern schützt auch hier für die jeweilige Ermittlung irrelevante persönliche Daten. So kann der Strafverfolgungsbehörde bspw. die Identität des Beschuldigten bekannt gegeben werden ohne für den Tatbestand unbedeutende Daten preiszugeben, indem diese unter einem weiteren Pseudonym bei einer anderen Institution erhoben werden. Die Ausstattung mit Befugnissen kann dabei streng an gerichtliche Bestimmungen und Überprüfungen geknüpft werden.

3 Authenzitaet von Credentials

Ein bedeutender Aspekt in der Verwendung digitaler Zertifikate ist die Authenzität der Credentials. Es muss gewährleistet werden können, dass der Besitzer eines Crendentials zur Benutzung befugt und die Beglaubigung des Zertifikates korrekt ist. Mit dem Einsatz von Crendential Systems reduziert sich die Authentifizierung für die Inanspruchnahme von Dienstleistungen auf die eingesetzten digitalen Zertifikate. Sind diese manipulierbar, ließen sich Dienste unbefugt nutzen und fremde Identitäten übernehmen.

3.1 Sicherheit

Durch die Verwendung asymmetrischer Verschlüsselung zur Erstellung neuer Credentials, kann diese Problematik auf die Sicherheit des RSA-Verfahrens zurückgeführt werden. Durch die Verwendung großer Primzahlen zur Ver- und Entschlüsselung sowie Erstellung von Zertifikaten, garantiert der RSA-Algorithmus keinen hundertprozentigen Schutz, verhindert jedoch das Erraten der als Verschlüsselungscode eingesetzten Primzahl in angemessener Zeit. Damit wird ein auf Wahrscheinlichkeit beruhender Sicherheitsgrad erreicht, der den hohen Anforderungen heutiger und auch zukünftiger Anwendungsbereiche genügt.

3.2 Verhinderung von Missbrauch

Die Übertragung und unbefugte Weitergabe erfordert weitergehende Überlegungen. So darf es dem rechtmäßigen Inhaber eines Credentials nicht möglich sein, das erworbene Zertifikat an Dritte zur unbefugten Benutzung abzutreten. Eine Lösung ist die Bindung der Credentials an ein Masterzertifikat, ohne das die einzelnen Zertifikate nicht eingesetzt werden können, mit dessen Weitergabe jedoch alle Dienste uneingeschränkt verfügbar wären. Damit erfordert dieses Konzepts die Implementierung weiterer Vorkehrungen, um die ungewollte oder versehentliche Weitergabe eines Credentials und damit der Weitergabe der eigenen Identität zu verhindern. Mit der Vergabe von Kennwörtern für die einzelnen Credentails oder das Masterzertifikat kann Missbrauch verhindert werden. Durch den Rückzug von Credentials kann die unbefugte Verwendung sanktioniert werden. Die Einstellung begrenzter Gültigkeit einzelner Zertifikate unterbindet die Verwendung über einen vorgesehenen Zeitraum hinaus. Mit einem Abgleich des Zertifikates durch die entgegennehmenden Person bei der Ausgabestelle oder einem zentralen Server für zurückgezogene Zertifikate kann weitere Sicherheit über die Befugnis erlangt werden. Der Abgleich mit einem zentralen Server ermöglicht des weiteren die Begrenzung der Nutzung auf eine festgelegte Anzahl. So können Einmalzertifikate für die Stimmabgabe bei Wahlen erstellt oder anstelle heutiger Transaktionsnummern beim 'electronic banking' verwendet werden.

4 Einsatzgebiete

Private Credential Systems schaffen mit dem Einsatz digitaler Zertifikate nicht nur den Schutz persönlicher Daten sondern ermöglichen zugleich die zuverlässige Authentifizierung. Das Risiko unsicherer Passwörter wird reduziert, wobei der Zugriff auf sensible Daten mit geringerem administrativen Aufwand nachvollzogen werden kann. Berechtigungen können differenzierter und effizienter erteilt und kontrolliert werden. Doch nicht nur im Bereich des Zugriffs- und Benutzer-Managements findet diese Technologie Anwendung. Als Trusted Computing Platform TCP dient das Konzept bei der Entwicklug hardwaregestützter Systeme, zur Absicherung von Computern bzw. Daten vor Manipulation, Zerstörung und Ausspähung. Ein spezieller Hardware-Baustein, dem sogenannten Trust-Plattform-Modul (TPM), verleiht dem Computersystem dabei eine eindeutige Identität und isoliert die in ihm gespei-

cherten Daten von anderen Komponenten der Plattform. Der Chip authentifizieren und identifizieren dabei nicht nur die Anwender des Systems, sondern übernimmt auch Aufgaben zur Ver- und Entschlüsselung. Durch Erzeugen eines asymmetrischen Schlüssels können Zertifikate auf deren Gültigkeit überprüft und Manipulationen an der installierten Soft- und Hardware erkannt werden. In einem denkbaren Szenario können entsprechend ausgestattete E-Mail-Programme den Absender von Emails verifizieren und somit vor Spam, Viren und Phising-Mails schützen. Gerät ein privates Dokument in fremde Hände, können Unbefugte die Datei nicht ohne Schlüssel öffnen. Durch die Überprüfung zertifizierter Software können schädliche Programme an ihrer Ausführung gehindert und eine sichere Plattform gewährleistet werden.

Visionen für weitere Anwendungsmöglichkeiten auf digitalen Zertifikaten beruhender Sicherheits-konzepte sind damit kaum Grenzen gesetzt. So lässt sich das beschriebene System mühelos als Digital Rights Management (DRM) integrieren, indem die Berechtigung zur Nutzung von Musik, Filmen und Software anhand digitaler Zertifikate in Form erworbener Lizenzen überprüft wird. Dabei greifen DRM-Systeme auf das Konzept der Zugriffskontrolle zurück, mit dem digitale Inhalte mittels Verschlüsselung an Lizenzen gebunden werden können. Ohne die zugehörige gültige Lizenz kann der Benutzer das Objekt zwar erwerben, nicht jedoch auf den Inhalt zugreifen. Durch Identity Management Systeme kann auch hier der Zugriff anhand erlangter Crendentials auf geistiges Eigentum verifiziert und kontrolliert werden.

5 Zusammenfassung

Das Konzept von Private Crendential Systems eröffnet damit ein gewaltiges Potiential, dass sich bereits heute vielerorts einsetzen lässt. Neben der Authentifizierung über Pseudonyme, Gewährung weitgehender Anonymität und dem Verwalten einer Vielzahl persönlicher Zertifikate, kontrollieren Identity Management Systeme nicht nur Zugriffe auf Benutzerebene sondern sind ebenso im Soft- und Hardwarebereich einsetzbar. Dabei muss jedoch sichergestellt werden, dass die Vergabe der Zertifikat authentisch ist, d.h. von einer vertrauenswürdigen Instanz erteilt wird. In einem sogenannten Net of Trust übernehmen alle Teilnehmer des public-key-Verfahrens die verantwortungsvolle Aufgabe, die Zertifikate anderer Teilnehmer zu signieren und damit öffentlich zu beglaubigen. Da dieser Vorgang auf einer subjektiven Vergabepraxis beruht, wurden hirarchische Publik-Key-Infrastrukturen (PKI) geschaffen, welche die Authentifizierung digitaler Zertifikate zur Bildung eines sicheren Netzwerks gewährleisten. Bundesbehörden wie das BSI, namenhafte Forschungsinstitute sowie kommerzielle Anbieter sind für die Ausstellung sogenannter Wurzelzertifikate verantwortlich um eine breite Vertrauensbasis bei den Teilnehmern des Systems zu schaffen. Sie bieten die grundlegenden Zertifizierungsdienste an, mit denen die Authentizität, Vertraulichkeit und Verbindlichkeit von Willenserklärungen bei der Teilnahme an elektronischen Diensten garantiert werden kann. Entsprechende Systeme bauen Chiphersteller, Hardware-fabrikanten und Softwareentwickler im Rahmen der Trusted Computing Group auf, wobei bereits heute Zertifikate bei der Installation von Treibern eingesetzt werden.

Private Credential Systems sind damit wesentliche Bestandteile im Aufbau sicherer IT-Netzwerke, in denen Vertrauen und Datenschutz Kernthemen des digitalen Geschäftsverkehrs darstellen. Identity Management Systeme gewährleisten dabei durch die kontrollierte Herausgabe persön-licher Daten nicht nur die Authentizität des Benutzers, sondern werden zugleich hohen Datenschutzaspekten gerecht. Ähnlich wie im alltäglichen Leben stellen diese Systeme jedoch keinen Vertrauensersatz zu Zertifizierungsdiensten dar, sondern erleichtern nur den Umgang mit einer Vielzahl digitaler Ausweise. Die Aufgabe, die Vertrauenswürdigkeit der Spitzenorganisationen festzustellen, die bei der Zertifikatvergabe an oberster Stelle stehen, übersteigt jedoch die technischen Möglichkeiten. Ehe diese leistungsstarke Technik zum Einsatz kommt, sind daher grundlegende Überlegung zum Aufbau einer Publik-Key-Infrastruktur mit der Installation vertrauenswürdiger Zertifizierungsstellen notwendig. Die Bescheinigung eines unbekannten Dritten, dessen Institution nicht auf eine wohlbekannte und anerkannte Ausgabestelle zurückzuführen ist, ist nur schwer in der Lage, Glaubwürdigkeit beim Empfänger zu erlangen. Die Intervention durch die öffentliche Hand oder etablierter Unternehmen ist daher unerlässlich und können durch die zur Entwicklung der Technologie gegründeten Konsortien, wie die Trusted Computing Group oder das European PRIME Projects, erfolgen. Ob dieses Technologie vom Endanwender denn letztlich auch als vertrauenswürdig anerkannt oder als Kontrollsystem skeptisch zurückgewiesen wird, bleibt abzuwarten. Die vertrauensschaffenden Massnahmen liegen hier gleichermaßen im Marketing wie auch der Unternehmensphilosophie beteiligter Unternehmen.

6 Quellen

PRIME White Paper - Privacy and Identity Management for Europe
http://www.prime-project.eu.org/prime/public/press_room/whitepaper/PRIME-Whitepaper-V1.pdf

Technische Universität Dresden - Identity Management
http://drim.inf.tu-dresden.de/

IDEMIX - an anonymous credential system developed by IBM
http://www.zurich.ibm.com/security/idemix/

Dr. Jan Camenisch über Efficient Private Credential Systems
http://www.telematik.uni-freiburg.de/RingvorlesungFolien/rviig_WS0506_camenisch.pdf

Identity Management Day 2005 - Mit Sicherheit Kosten senken (Fallstudie)
http://www.uspmarcom.de/itverlag/idm05/documents/HPTriaton_JuergenBachinger_AntjeHuelli

Digital Rights Management und TCPA
http://www.heise.de/ct/02/22/204/

Web of Trust
http://www.gnupg.org/gph/de/manual/x696.html

Certificate Authority – Zertifizierungsstellen in der Publik-Key-Infrastruktur
http://www.bsi.de/fachthem/verwpki/vpkiallgemeines.htm
http://www.dfn.de/content/dienstleistungen/dfnpki/
http://www.verisign.de/products-services/security-services/pki/index.html

Mitglieder der Trusted Computing Group
https://www.trustedcomputinggroup.org/about/members/

Mitglieder des European PRIME Projects
http://www.prime-project.eu.org/consortium/consortium_overview