Zeitschrift für Datenrecht und Informationssicherheit

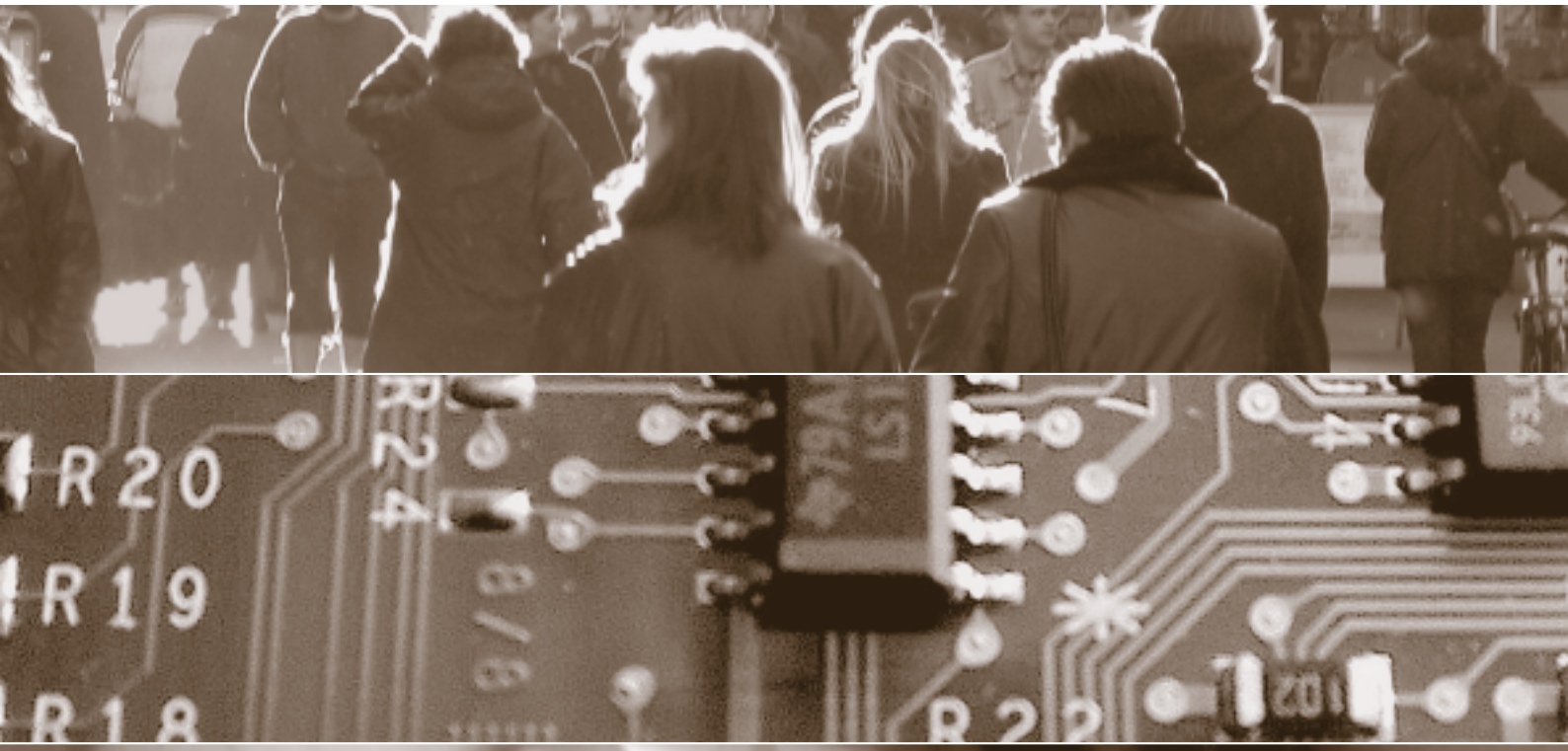
digma

www.digma.info 8. Jahrgang, Heft 1, März 2008

Schwerpunkt:

Anonymisierung

fokus: Das Recht auf Anonymität
fokus: Sind anonymisierte Daten anonym genug?
report: Drahtlose Sensornetze – eine Herausforderung



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

inhalt

fokus

Schwerpunkt:
Anonymisierung

auftakt
Das Recht, in Ruhe gelassen zu werden
von Hans-Rudolf Merz **Seite 1**

Der Schatten über der Anonymität
von Bruno Baeriswyl **Seite 4**

Das Recht auf Anonymität
von Beat Rudin **Seite 6**

zwischentakt
Der kleine Trick mit der Angst
von Urs Buess **Seite 13**

Anonymisierung von genetischen Daten?
von Bruno Baeriswyl **Seite 14**

Sind anonymisierte Daten anonym genug?
von Günter Karjoth **Seite 18**

Anonymes E-Voting – eine Illusion?
von Rolf Oppliger **Seite 24**

Folgerungskontrolle zum Schutz von Information
von Joachim Biskup **Seite 28**

Das Recht auf Anonymität

Das Recht auf Anonymität ist ein Teil des Grundrechts auf informationelle Selbstbestimmung. In der Gesetzgebung finden wir etliche Gewährleistungen. Doch auch ausserhalb dieser Bereiche könnten mit Anonymisierungs- oder Pseudonymisierungslösungen in vielen Fällen die verfolgten Zwecke erreicht werden.

Anonymisierung von genetischen Daten?

Anonymisierung verhindert die Verletzung von Persönlichkeitsrechten. Ist das eine Lösung im Zusammenhang mit Biobanken? Jegliche Verwendung von Daten in einer Biobank setzt eine angemessene Aufklärung voraus.

Sind anonymisierte Daten anonym genug?

Wann reicht eine Anonymisierung aus, damit aus den anonymisierten Daten nicht doch wieder auf die betroffenen Personen zurückgeschlossen werden kann – und die Daten für den Forschungszweck trotzdem noch aussagekräftig genug sind?

Anonymes E-Voting – eine Illusion?

In der Theorie kann anonymes E-Voting mit Hilfe von blinden Signaturen relativ einfach realisiert werden. In der Praxis muss bei einer konkreten Realisierung eines E-Voting-Systems insbesondere darauf geachtet werden, dass nicht über verdeckte Kanäle Informationen über stimmberechtigte Personen z. B. in Tokens hineincodiert werden können.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktor: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 112.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publimag AG, Europastrasse 30, Postfach, CH-8152 Glattbrugg
Tel. +41 (0)44 809 31 11, Fax +41 (0)44 809 32 22, www.publimag.ch, info@publimag.ch

Herstellung: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Die Crux der Auskunft über Verstorbene

Die Verordnungsregelung zur Herausgabe von Daten an die Angehörigen von Verstorbenen ist anspruchsvoll, weil sie eine Interessenabwägung voraussetzt. Unter welchen Voraussetzungen ist ein Privatversicherer zur Auskunft an die Angehörigen berechtigt? Wann besteht eine Pflicht dazu?

Datenschutz und wirtschaftliche Realität

Unter welchen Voraussetzungen kann die Wirtschaft Datenschutz realistischerweise umsetzen? Der Diskussionsbeitrag aus dem Kreis des Vereins Unternehmens-Datenschutz fordert mehr Anreize (z. B. Steuererleichterungen) für erwiesenermassen datenschutzkonform handelnde Unternehmen. Steuererleichterung für die Einhaltung von Gesetzen – eine aus Sicht der Redaktion etwas realitätsfremde Forderung.

Drahtlose Sensornetze – eine Herausforderung

Drahtlose Sensornetze werden als die nächste Technologiewelle nach RFID gehandelt. Dabei offenbaren die im Beitrag erörterten Anwendungsfelder, dass es ratsam ist, datenschutzrechtliche, aber auch ethische Fragestellungen frühzeitig zu erörtern.

Europarechtliche Herausforderungen

Bund und Kantone stehen zurzeit im Evaluationsverfahren der EU im Hinblick auf die Assoziation der Schweiz an Schengen/Dublin. Passend dazu ist ein Buch erschienen, das umfassend die europarechtlichen Vorgaben darstellt, nach denen sich das schweizerische Datenschutzrecht künftig zu richten hat.

report

RECHT IN DER PRAXIS
Die Crux der Auskunft über Verstorbene
von Martin Hofer **Seite 34**

BETRUGSPRÄVENTION
Fraud Management: Kampf dem IT-Betrug
von Stefan Näpflin **Seite 40**

RECHT UND PRAXIS
Datenschutz und wirtschaftliche Realität
von Esther Hefti
und Susanne Amrein-Fischer **Seite 42**

IT-SICHERHEIT
Unterwegs im World Wild Web
von Thomas Dübendorfer **Seite 46**

FORSCHUNG
Drahtlose Sensornetze – eine Herausforderung
von Dirk Westhoff
und Heinrich Stüttgen **Seite 48**

RECHTSPRECHUNG
Vertrauensarzt bis-repetitas
von Amédéo Wermelinger **Seite 50**

TRANSFER
Wie ist die Lage in der Informationssicherheit?
von Roland Portmann **Seite 52**

forum

BUCHBESPRECHUNG
Europarechtliche Herausforderungen
von Beat Rudin **Seite 54**

agenda **Seite 55**

schlusstakt
Wo sind die Liberalen in der Schweiz?
von Beat Rudin **Seite 56**

Cartoon
von Hanspeter Wyss

Anonymes E-Voting – eine Illusion?

Ist anonymes E-Voting in der Praxis realisierbar oder handelt es sich um eine mathematische Illusion?

Prof. Dr. Rolf Oppliger, Informatikstrategieorgan Bund ISB, Bern, eSECURITY Technologies, Gümligen, und Universität Zürich rolf.oppliger@esecurity.ch

In der Theorie ist anonymes E-Voting technisch möglich. In der Praxis müssen dazu aber verdeckte Kanäle aufgedeckt bzw. verhindert werden.

Im Artikel «E-Voting sicherheitstechnisch betrachtet» (digma 2002, 184 ff.) hat der Autor verschiedene Formen des E-Voting unterschieden und begründet, weshalb in der Schweiz primär das «Remote Internet Voting» im Vordergrund steht bzw. stehen muss. Bei dieser Form des E-Voting erfolgt die Stimmabgabe auf dem Client-System des Benutzers (typischerweise einem handelsüblichen PC) und für die Übertragung der abgegebenen Stimme zum Abstimmungsserver wird das Internet genutzt. Aus sicherheitstechnischer Sicht stellt Remote Internet Voting die anspruchsvollste Form des E-Voting dar.

Eine Frage, die sich im Zusammenhang mit E-Voting – und speziell Remote Internet Voting – immer stellt, ist, ob aus der Sicht der Wahl- oder Abstimmungsteilnehmer(innen) die Anonymität gewährleistet ist bzw. ob die die Wahl oder Abstimmung durchführende Organisation (in der Regel der Staat) feststellen kann, wie eine bestimmte Person gewählt oder abgestimmt hat. Anders ausgedrückt: Ist anonymes E-Voting technisch möglich oder handelt es sich dabei nur um eine zugegebenermassen schöne mathematische Illusion? Um diese Frage beantworten zu können, ist es nützlich, zunächst einmal die Situation in der realen Welt zu betrachten und mit der digitalen Welt zu vergleichen.

Reale Welt

In der realen Welt wird bei Wahlen und Abstimmungen Anonymität typischerweise dadurch erzeugt, dass man die Authentifizierung und Autorisierung der stimmberechtigen Person – d.h. die Berechtigungs(über)prüfung – von der eigentlichen Stimmabgabe entkoppelt und logisch trennt. Dies gilt sowohl für die Stimmabgabe an der Urne als auch für die in der Schweiz verbreitet genutzte briefliche Stimmabgabe.

- Wenn eine stimmberechtigte Person ihre Stimme an der Urne abgeben will, muss sie sich zunächst an einen bestimmten Ort begeben (typischerweise ein Gemeinde- oder Schulhaus) und dort folgende Schritte durchlaufen: (1) Sie muss sich ihren Stimmausweis abstempeln lassen, (2) den abgestempelten Stimmausweis in eine erste Urne und (3) den Zettel mit der abgegeben Stimme – d.h. den Stimmzettel – in eine zweite Urne werfen. Durch den Einsatz von zwei Urnen wird eine einfache Entkoppelung und logische Trennung von Stimmausweis und Stimmzettel erreicht. Wenn nach der Wahl oder Abstimmung zufällig ein Stimmzettel herausgegriffen wird, wird es in der Regel nicht mehr möglich sein, zu entscheiden, wer diesen Zettel ursprünglich in die Urne geworfen hat (wenigstens solange die Urne mehr als einen Zettel enthält). Dazu müsste man schon die Stimmzettel auf eine nicht leicht erkennbare Art und Weise markieren bzw. mit ihren unterschiedlichen physikalischen (Struktur-)Eigenschaften registrieren. Wir vertrauen darauf, dass das nicht geschieht, und gehen entsprechend davon aus, dass wir unsere Stimmen an der Urne anonym abgeben können.
- Wenn eine stimmberechtigte Person brieflich abstimmen will, kann sie das grundsätzlich von irgendwo aus tun (typischerweise von zuhause). Wiederum muss sie eine definierte Folge von Schritten durchlaufen: (1) Sie muss ihren Stimmzettel ausfüllen und in einen neutralen Briefumschlag stecken. (2) Diesen Brief muss sie – zusammen mit dem handschriftlich unterschriebenen Stimmausweis – in einen zweiten Briefumschlag stecken und (3) diesen Brief postalisch der die Wahl oder Abstimmung durchführenden Organisation zustellen. In der Regel ist das die Gemeindeverwaltung, die die Stimmen auch für kantonale und eidgenössische Wahlen und Abstimmungen sammelt und auszählt. Diese Organisation (bzw. deren Vertreter[innen]) kann (können) den Brief öffnen und den beiliegenden Stimmausweis kontrollieren. Im positiven Fall wird der innere Briefumschlag mit dem Stimm-

zettel zu den noch auszuzählenden Stimmen gelegt. Am Stichtag (d.h. wenn die Stimmen ausgezählt werden müssen) wird dieser Umschlag geöffnet und der darin enthaltene Stimmzettel kommt zur Auszählung. Wiederum ist es im Nachgang zu einer Wahl oder Abstimmung nicht mehr möglich zu bestimmen, wie eine bestimmte Person gewählt oder abgestimmt hat, und wiederum müsste dazu ein Stimmzettel markiert und/oder mit seinen physikalischen (Struktur-) Eigenschaften registriert werden.

Digitale Welt

Wie in der realen Welt kann man auch in der digitalen Welt Anonymität grundsätzlich dadurch erzeugen, dass man die Kontrolle der Stimmberechtigung von der abgegebenen Stimme entkoppelt und logisch trennt. Insofern ist die Situation in der digitalen Welt mit der realen Welt vergleichbar. Allerdings ist die Umsetzung in der digitalen Welt schwieriger. Die eine Wahl oder Abstimmung durchführende Organisation kann natürlich immer behaupten, dass Stimmberechtigung und abgegebene Stimme entkoppelt und logisch getrennt werden. So richtig kontrollieren kann man diese Aussage aber nicht, und entsprechend wird man der Organisation diesbezüglich einfach vertrauen müssen. Das ist nicht ideal, und natürlich wünscht man sich hier technische Unterstützung.

Eine Möglichkeit, in der digitalen Welt einen brieflichen Abstimmungsgang nachzubilden, würde z. B. darin bestehen, dass die stimmberechtigte Person ihren Stimmzettel mit dem öffentlichen Schlüssel eines Abstimmungsservers chiffriert, das Chiffrat digital signiert und die resultierende Signatur mit dem öffentlichen Schlüssel eines Berechtigungsservers chiffriert. Leider bietet dieser Ansatz keine Anonymität, wenn – was sich kaum verhindern lässt – beide Server(betreiber) zusammenarbeiten.

Eine andere und für das vorliegende Problem erfolgversprechendere Möglichkeit ist in den frühen 1980er-Jahren von David Chaum entwickelt und vorgeschlagen worden: die blinde Signatur[1]. Viele der in der Literatur vorgeschlagenen anonymen E-Voting-Protokolle und -Systeme basieren auf dem Einsatz von blinden Signaturen.

Blinde Signaturen

Eine digitale Signatur ist im Prinzip eine kryptografisch abgesicherte Prüfsumme, die mit einem privaten (Signier-)Schlüssel erzeugt und mit einem dazugehörigen öffentlichen (Verifizier-) Schlüssel überprüft (d.h. verifiziert) werden kann. Der private Schlüssel gehört dem Signierer und muss geheim gehalten werden, während der öffentliche Schlüssel jedermann zur Verfügung steht und z. B. auch (im Rahmen eines Verzeichnisdienstes) veröffentlicht werden kann. Gemeinsam bilden der private und der öffentliche Schlüssel ein asymmetrisches Schlüsselpaar.

In der Literatur sind viele digitale Signatursysteme mit unterschiedlichen Eigenschaften vorgeschlagen worden. Das erste und in der Praxis besonders häufig eingesetzte digitale Signatursystem ist RSA – benannt nach seinen Erfindern Rivest, Shamir und Adleman[2]. In diesem System besteht der öffentliche Schlüssel aus zwei Komponenten:

- Eine grosse Zahl n, die das Produkt zweier Primzahlen p und q darstellt und – mathematisch gesprochen – einen Restklassenring modulo n (d.h. Z_n) definiert. Die Primfaktoren p und q müssen dabei geheim bleiben.
- Eine Zahl e zwischen 1 und $\phi(n) = (p-1)(q-1)$, die mit $\phi(n)$ teilerfremd ist (d.h. $ggT(e,\phi(n))=1$).
- Der private Schlüssel d ist dann das multiplikativ inverse Element von e modulo $\phi(n)$, d.h. $de \equiv 1 \pmod{\phi(n)}$.

Jemand, der die Primfaktorenzerlegung von n kennt, kann aus e leicht d berechnen (z. B. mithilfe des erweiterten Euklidschen Algorithmus). Für jemanden, der die Primfaktorenzerlegung von n aber nicht kennt, ist bis heute nicht bekannt, ob und, wenn ja, wie er d bestimmen kann, ohne n zu faktorisieren. Entsprechend basiert die Sicherheit von RSA auf der (angenommenen) Schwierigkeit, grosse Zahlen zu faktorisieren, d.h. in ihre Primfaktoren zu zerlegen.

Eine erfolgversprechendere Möglichkeit ist in den frühen 1980er-Jahren von David Chaum entwickelt worden: die blinde Signatur.

Kurz&bündig

In der Theorie kann anonymes E-Voting mithilfe von blinden Signaturen relativ einfach realisiert werden. In der Praxis sieht es etwas komplizierter aus und die Situation muss hier differenzierter betrachtet werden. Insbesondere muss bei einer konkreten Realisierung eines E-Voting-Systems darauf geachtet werden, dass nicht über verdeckte Kanäle Informationen über stimmberechtigte Personen z. B. in Tokens hineincodiert werden können. Ähnlich wie in der realen Welt ist auch in der digitalen Welt die Nichtexistenz von verdeckten Kanälen schwierig nachzuweisen. Dazu müsste das realisierte E-Voting-System mit all seinen Kommunikationsmöglichkeiten von einer unabhängigen Stelle untersucht und analysiert werden. Das ist auf der einen Seite zwar aufwändig und teuer, auf der anderen Seite scheint es aber auch erforderlich zu sein, damit anonymes E-Voting mehr ist als eine zugegebenermassen schöne mathematische Illusion.

Mithilfe von RSA kann eine Nachricht m – interpretiert als Zahl zwischen 0 und n-1 – digital signiert werden. Die digitale Signatur lautet $s \equiv m^d \pmod n$. Zur Erzeugung von s benötigt der Signierer den privaten Schlüssel d. Die Signatur s wird dann üblicherweise zusammen mit der Nachricht m dem Empfänger zugestellt, so dass dieser $m' \equiv s^e \pmod n$ bilden und verifizieren kann, ob m' und m übereinstimmen. Offenbar wird für diesen Signaturverifikationsschritt nur der öffentliche Schlüssel des Signierers (in allerdings authentischer Form) benötigt. Bei dieser vereinfachten Darstellung haben wir verschwiegen, dass üblicherweise nicht Nachrichten, sondern Hashwerte von Nachrichten signiert werden, und dass die Sicherstellung der Authentizität von öffentlichen Schlüsseln in der Praxis schwierig ist und eine Public-Key-Infrastruktur (PKI) erforderlich macht.

Im Normalfall wird bei der Erzeugung einer digitalen Signatur verlangt, dass der Signierer die zu signierende Nachricht im Klartext sieht (ähnlich wie man bei einem Unterzeichner eines Vertrages verlangt, dass dieser den Inhalt des Vertrags gelesen und verstanden hat). Bei einer blinden Signatur weicht man von dieser Anforderung ab. In der Tat zeichnet sich eine blinde Signatur gerade dadurch aus, dass der Signierer die zu signierende Nachricht im Klartext nicht sieht. Auf den ersten Blick wird man überrascht sein und sich fragen, was man damit tun kann. In der Tat liegen Anwendungen für blinde Signaturen nicht gerade auf der Hand. Chaum hat als erster das Potenzial von blinden Signaturen erkannt und deren Einsatz nicht nur für E-Voting propagiert, sondern auch für viele andere Anwendungen, die sich durch spezielle Anonymitätsanforderungen auszeichnen (wie z. B. anonymes elektronisches Geld).

Eine blinde Signatur zeichnet sich gerade dadurch aus, dass der Signierer die zu signierende Nachricht im Klartext nicht sieht.

Im Falle von RSA kann eine blinde Signatur dadurch erzeugt werden, dass sich ein Teilnehmer anstelle von m den Wert $m' = mr^e \pmod n$ signieren lässt – d.h. er multipliziert die Nachricht vor der Signaturerzeugung mit r^e an. Dabei ist r eine beliebige und zufällig gewählte Zahl kleiner als n. Der Signierer bildet dann $s' = m'^d \pmod n$, und dieser Wert entspricht offenbar $(mr^e)^d \equiv m^d r^{ed} \equiv m^d r^1 \equiv m^d r \pmod n$. Wenn der Signierer dem Teilnehmer s' zurückgibt, kann dieser s (als Signatur von m) dadurch erzeugen, dass er $s'/r \equiv m^d r/r \equiv m^d \pmod n$ bildet, d.h. s' durch r modulo n dividiert. Man beachte, dass bei diesem Verfahren der Signierer nie die Nachricht m im Klartext sieht, sondern nur eine mit einer vom Teilnehmer gewählten Zufallszahl r «geblindete» (Dummy-)Nachricht m'. Wenn also später jemand den Signierer fragt, für wen er m signiert hat, kann dieser die Frage nicht beantworten, weil er «nur» m' signiert hat (und m gar nie gesehen hat).

Andere digitale Signatursysteme (als RSA) kennen ähnliche Möglichkeiten, blinde Signaturen zu erzeugen. In der Tat gibt es für fast jedes digitale Signatursystem mittlerweile eine «blinde» Variante, d.h. eine Variante, die blinde Signaturen unterstützt.

Anonymes E-Voting

Mithilfe von blinden Signaturen kann man anonymes E-Voting technisch relativ einfach realisieren. Wie bereits erwähnt besteht die Grundidee darin, dass man für eine stimmberechtigte Person die Kontrolle der Stimmberechtigung von der abgegebenen Stimme entkoppelt und logisch trennt. Konkret bedeutet das, dass sich die stimmberechtigte Person gegenüber einem Berechtigungsserver authentifiziert und autorisiert, und dass im positiven Fall der Berechtigungsserver ein Token ausgibt, das die Person zur einmaligen Stimmabgabe berechtigt. Das Token ist blind signiert, d.h. wenn jemand das Token verifiziert, wird er zwar sehen, dass das Token vom Berechtigungsserver ausgestellt bzw. signiert worden ist (und damit gültig ist); er wird aber nicht erkennen und auch den Server nicht fragen können, an wen das Token ursprünglich ausgestellt worden ist (weil der Server das Token nie im Klartext gesehen hat). Entsprechend kann die Person das Token einsetzen, um sich gegenüber einem Abstimmungsserver als stimmberechtigt auszuweisen, und trotzdem anonym bleiben. Die Stimmabgabe erfolgt von der Berechtigungskontrolle entkoppelt und logisch getrennt, und dadurch wird Anonymität sichergestellt.

Fussnoten

1 David Chaum, Blind signatures for untraceable payments, Advances in Cryptology – Proc. of CRYPTO '82, Springer-Verlag (1983), 199–203.

2 Ron Rivest, Adi Shamir und Len Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol. 21 (1978), No. 2, 120–126.

Theorie und Praxis

Aufgrund des Gesagten ist in der Theorie anonymes E-Voting technisch möglich. In der Praxis sieht es allerdings komplizierter aus und hier muss die Situation auch differenzierter betrachtet werden. Wenn man zur Erzeugung von blinden Signaturen z. B. probabilistische Signaturverfahren einsetzt (d.h. Signaturverfahren, die zur Signaturerzeugung Zufallszahlen einsetzen), kann der Berechtigungsserver über die Wahl der Zufallszahlen einen verdeckten Kanal realisieren, d.h. er kann dann in eine (blinde) Signatur hineincodieren, an wen er ein Token ausgibt. Diese Identifizierungsinformation kann später zur Auswertung von Stimmverhalten herangezogen werden. Die stimmberechtigte Person hat kaum eine Möglichkeit, die Existenz eines solchen Kanals zu erkennen. Entsprechend wird man an dieser Stelle den Einsatz probabilistischer Signaturverfahren unterbinden und den Einsatz deterministischer Verfahren (wie z. B. «normales» RSA) verlangen. Das ist auch deshalb erwähnenswert, weil viele digitale Signatursysteme ihre Sicherheit gerade darauf stützen, dass die zu signierenden Nachrichten mit geschickt gewählten Zufallswerten auf eine bestimmte Blockgrösse erweitert werden. Zudem wird man sicherstellen müssen, dass im (in den) eingesetzten E-Voting-Protokoll(en) keine anderen verdeckten Kanäle implementiert sind. Das ist im Allgemeinen schwierig sicherzustellen, weil verdeckte Kanäle auf sehr vielfältige Art und Weise realisiert werden können (eine ähnliche Problematik hat man z. B. auch im Zusammenhang mit «Side channel»-Angriffen). So könnte die Client-seitige Software z. B. versuchen, Informationen über eine stimmberechtigte Person in ein Token hineinzucodieren, um so einen verdeckten Kanal zu realisieren. Eine einfache Möglichkeit wäre z. B. ein Feld im Token zu definieren, das immer chiffriert oder als reserviertes Feld deklariert wird. Weniger offensichtlich wäre es, wenn man mit Hilfe von steganografischen Verfahren Informationen über eine stimmberechtigte Person in ein bestehendes Feld eines Tokens hineincodieren würde. Der Fantasie sind hier kaum Grenzen gesetzt.

Vor diesem Hintergrund erscheint es relativ schwierig, die Existenz verdeckter Kanäle grundsätzlich ausschliessen zu können. Man wird den Entwicklern von E-Voting-Systemen und Lösungen relativ viel Vertrauen entgegenbringen müssen. Zum Teil wird man dieses Mass an Vertrauen dadurch reduzieren oder relativieren können, dass man verlangt, dass eine Implementierung einsehbar und öffentlich überprüfbar sein muss (im Extremfall z. B. als Open Source Software). Dennoch wird man gut beraten sein, die Existenz von verdeckten Kanälen zur Unterwanderung der Anonymität nicht kategorisch zu verneinen. Die Frage nach der Existenz solcher Kanäle lässt sich letztlich nur für eine konkrete Realisierung beantworten. Zudem muss sich die Beantwortung dieser Frage auf eine in jedem Fall aufwändige und teure Untersuchung stützen. Dieser Aufwand ist bis heute nicht getrieben worden, und so wird es wohl aufgrund fehlender wirtschaftlicher Anreize auch bleiben. Man beachte, dass der Staat eine solche Untersuchung nicht durchführen kann, weil es letztlich darum geht, die Nichtexistenz von verdeckten Kanälen zu zeigen und man solche Kanäle primär von staatlicher Seite vermuten würde. Jede Untersuchung von dieser Seite wäre deshalb nicht neutral und würde kaum akzeptiert.

Zur Beantwortung der Frage, ob verdeckte Kanäle realisiert worden sind, sind in jedem Fall aufwändige und teure Untersuchungen erforderlich.

Schlussfolgerungen

In der realen Welt müssen wir die Annahme machen, dass Stimmzettel nicht markiert und/oder aufgrund ihrer unterschiedlichen physikalischen (Struktur-)Eigenschaften registriert sind. Im Prinzip müssen wir die analoge Annahme auch in der digitalen Welt machen: Zur Stimmabgabe berechtigende Tokens dürfen keine Informationen über ihre Besitzer enthalten. Zudem dürfen auch sonst keine verdeckten Kanäle vorhanden sein. Nur unter solchen Annahmen kann man argumentieren, dass anonymes E-Voting technisch möglich ist und keine mathematische Illusion darstellt. Die Annahmen selbst gilt es aber immer auch kritisch zu hinterfragen – wenigstens solange Anonymität im E-Voting ein berechtigtes Anliegen und erstrebenswertes Ziel darstellt. ■

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §