Übertriebene **Sorge**

Bei der praktischen Umsetzung von e-Government ist der Einsatz qualifizierter elektronischer Signaturen selten nötig, im schlimmsten Fall sogar kontraproduktiv. Diese These vertritt der e-Signatur-Experte Dr. Johann Bizer von der Universität Frankfurt am Main.

e-Government in Deutschland leidet immer noch am fehlenden Vertrauen der Nutzer in die Sicherheit der elektronischen Kommunikation. Woran liegt das?

In der elektronischen Kommunikation fehlen die aus der konventionellen Kommunikation wohlvertrauten Sicherheitsanker. Das Medium ist flüchtig. Die Nutzer müssen lernen, anstelle eines Originals mit zahlreichen originalen Kopien umzugehen und diese von anderen Versionen zu unterscheiden. Die wohlvertraute Gewissheit des Papiers und der eigenhändigen Unterschrift fehlen, das irritiert die Menschen. Man sollte die Enttäuschung in die hohen Erwartungen aber nicht auf das fehlende Vertrauen der Nutzer schieben. Vielleicht fehlt es auch nur an einfachen Inhalten und Anwendungen, die den Nutzern einen unmittelbar einsichtigen Vorteil bieten.

„Die e-Signatur ist nur ein Werkzeug."

Zur Person

Dr. Johann Bizer ist Jurist und Herausgeber der Fachzeitschrift „Datenschutz und Datensicherheit - DuD":
• www.dud.de

Welche Rolle spielt hierbei der Einsatz elektronischer Signaturen?

Elektronische Signaturen helfen ein Grundproblem elektronischer Kommunikation in offenen Netzen zu lösen, nämlich die Authentifizierung eines bislang unbekannten Kommunikationspartners. Kernstück des Verfahrens ist nicht die Signatur, sondern das zugehörige Zertifikat, indem ein Dritter bescheinigt, ein bestimmter Prüfschlüssel gehört zu einer bestimmten Person. Der Haken an der Sache ist nur, dass der Absender Aufwand und Kosten des Signaturverfahrens tragen muss, damit der Empfänger ihn sicher authentifizieren kann. Warum aber sollte der Absender daran ein Interesse haben?

Wie beurteilen Sie Pläne der Bundesregierung, für die Bundesverwaltung die elektronische Signatur flächendeckend bis Ende 2003 einzuführen?

Man könnte fast den Eindruck gewinnen, als wäre für die Bundesregierung die e-Signatur bereits die Anwendung des Internets schlechthin, obwohl es doch nur ein Werkzeug ist. Für die normale innerministerielle Kommunikation braucht man keine Hochsicherheits-Signaturen. Es reichen fortgeschrittene Signaturen mit Softwarezertifikaten.

Dr. Johann Bizer

Viel wichtiger ist stattdessen eine hochwertige Verschlüsselung der e-Mail-Kommunikation, damit die Kommunikation innerhalb der Regierung nicht eine Einladung an die Nachrichtendienste der Welt ist. Bedenklich ist allerdings die zunehmende Zahl an Anwendungen, in denen die qualifizierte elektronische Signatur den Bürgern abverlangt wird. Den Vogel hat der Gesetzgeber mit der gesetzlichen Anordnung abgeschossen, dass elektronische Rechnungen bei der Vorsteuer nur anerkannt werden, wenn sie eine akkreditierte elektronische Signatur tragen: Das nennt man eine Strategie der „Zwangsbeglückung". Der Effekt wird sein, dass KMUs ihre Rechnungen in Zukunft ausdrucken und lieber per Post versenden als sich auf Verfahren einzulassen, die der Rechnungsempfänger nicht beherrscht.

Was bedeutet dies für den Einsatz elektronischer Signaturen in den digitalen Rathäusern?

Man muss die Kommunikation zwischen dem Bürger und seiner Verwaltung als eine geschlossene Benut-

zergruppe interpretieren. Hierzu benötigt man aber keine qualifizierten elektronischen Signaturen. Stattdessen beginnt die Kommunikation mit der Gemeinde mit der Anmeldung, bei der der Bürger eine Kommunikationsnummer oder ein Softwarezertifikat auf einem Datenträger ausgehändigt bekommt, mit deren Hilfe er während der weiteren Kommunikation identifiziert werden kann. Die offiziösen Szenarien gehen demgegenüber von der unzutreffenden Annahme aus, der antragstellende Bürger sei regelmäßig „ein Wesen von einem anderen Stern", zu dessen elektronischer Authentifizierung der Bürger einen maximalen Sicherheitsaufwand zu leisten habe.

Welche Alternativen gibt es zum Einsatz elektronischer Signaturen, die auf Smart Cards basieren?

Smart Cards sind als Datenträger der Signaturschlüssel für qualifizierte elektronische Schlüssel erforderlich und verteuern automatisch das Angebot. Die Alternative sind entweder softwarebasierte Signaturverfahren, die das Signaturgesetz im Einklang mit der europäischen Signaturrichtlinie als „fortgeschrittene elektronische Signaturen" bezeichnet. Eine Variante ist die Verwendung von Smart Cards niedrigerer Sicherheitsanforderungen. Die Sicherheitslücke könnte durch zusätzliche Umgebungsbedingungen abgesichert werden. Dazu können eine Inhaltsverschlüsselung, die Verwendung von Kennziffern oder von Browserzertifikaten gehören.

„Die Wahrscheinlichkeit von Missbrauch und Schadensfällen wird völlig überschätzt."

Wie wird die (rechts)sichere, allgemein akzeptierte Kommunikation zwischen Behörde und Bürger beziehungsweise Wirtschaft in fünf Jahren aussehen?

Das typische Verwaltungsverfahren beginnt mit dem Abruf eines Formulars vom Server der Verwaltung. Nun will der Bürger eine Leistung beantragen. Lösung 1 ist konventionell: Das Formular wird ausgefüllt, unterschrieben und mit der Post weggeschickt. Dieses Modell ist aus der Sicht des Bürgers sicher, aber es erhöht den Aufwand für die Verwaltung. Demgegenüber passen sich die nächsten drei Lösungen nahtlos in den Workflow der Kommune ein, begnügen sich aber mit einem niedrigeren Sicherheitsniveau: In Lösung 2 wird das Formular elektronisch ausgefüllt, mit einem Browserzertifikat autorisiert und an die Gemeinde versandt. In Lösung 3 wird ohne Autorisierung gleichzeitig eine elektronische Lastschrift erteilt und die Verwaltungsleistung erst nach erfolgreicher Buchung der fälligen Verwaltungsgebühr beglichen. In Lösung 4 bekommt der Bürger seine Leistung nur, wenn er den Antrag mit einer qualifizierten elektronischen Signatur versehen hat. Soweit für die Leistung gleichzeitig eine Verwaltungsgebühr anfällt, könnte die Authentifizierung auch über den Bezahlvorgang erfolgen. Die vierte Lösung ist daher die unwahrscheinlichste.

Interview: Sabine Schutz