



**Netzkongress 2006**  
**Regieren und Verwalten in der Wissensgesellschaft**

**Thesenpapier 4**  
**„Neue Wege der Identifikation“**

**Hinweis:**

Dieses Thesenpapier wurde entwickelt auf dem Cisco Systems Netzkongress vom 17.-18. Januar 2006 in Fulda, unter Mitwirkung aller Teilnehmer aus der Arbeitsgruppe „Neue Wege der Identifikation“ unter Leitung von Klaus Lenssen, Business Development Manager Security und Government Affairs, Cisco Systems GmbH.

## Inhaltsverzeichnis

1.	Einladung – pro und kontra Digitale Signatur .....	4
2.	Status Quo – rechtliche und wirtschaftliche Aspekte .....	5
2.1	Politik im Zugzwang .....	5
3.	Praxisbeispiele .....	7
3.1	Belgien – Identifikation per Chipkarte .....	7
3.2	HamburgGateway .....	8
3.3	Erfahrungen aus Bremen .....	9
4.	Kritische Erfolgsfaktoren – Schlussfolgerungen .....	11

## 1. Einleitung – pro und kontra Digitale Signatur

E-Government steht und fällt mit der Möglichkeit, bestehende Verwaltungsprozesse effektiv auf eine elektronische Prozesskette abzubilden. Als größte Hürde wurde die Anforderung „persönliche Unterschrift“ angenommen. Sie lässt sich zwar mit den Mitteln der Kryptografie nachbilden, jedoch ist die Bereitstellung der hierfür notwendigen flächendeckenden Infrastrukturen nicht trivial und kostenintensiv.

Den rechtlichen Rahmen für die digitale Signatur als virtuelles Pendant zur physischen Unterschrift schuf der Gesetzgeber bereits 1997 mit dem so genannten Signaturgesetz. Anfang vergangenen Jahres traten dann eine Reihe von Änderungen in Kraft, die in erster Linie auf Verfahrensvereinfachungen bei der Erteilung qualifizierter Zertifikate abzielen. Die Bundesnetzagentur verwaltet die Root-CA für Deutschland, Zertifikate für Bürger werden jedoch nur von ausgewählten, kommerziellen Unternehmen kostenpflichtig ausgegeben.

Zweifellos sind komplizierte Rahmenbedingungen mit Schuld daran, dass die digitale Signatur bei der deutschen Bevölkerung bislang auf wenig Gegenliebe gestoßen ist. Angesichts der Tatsache, dass jeder Bürger durchschnittlich nur 1,5 mal im Jahr eine Behörde kontaktiert (einer dieser Fälle ist die jährliche Einkommensteuererklärung), erscheint die Kosten-Nutzen-Relation zudem äußerst fragwürdig.

Da der Fokus bisher ausschließlich darauf lag die persönliche Unterschrift in elektronischer Form abzubilden, wurde einem wesentlichen Problem wenig Beachtung geschenkt – ist die Unterschrift wirklich zwingend notwendig für E-Government? Vermutlich nicht, denn einfache Auskünfte werden auch über das Telefon oder per E-Mail erteilt und für Verwaltungsvorgänge, in denen sensible persönliche Daten bearbeitet werden, ist die Feststellung der Identität wichtig, nicht die Unterschrift. Welche Instanz übernimmt jedoch die Funktion der zweifelsfreien, zentralen Identitätsfeststellung in Deutschland, wo das Meldewesen Ländersache ist? Außerdem sind datenschutzrechtliche Fragen zu klären, weil beispielsweise nach dem Volkszählungsurteil von 1983 ein „einheitliches Ordnungsmerkmal“ nicht zulässig ist.

Daraus darf aber nun keinesfalls der Schluss gezogen werden, dass öffentliche Serviceangebote im Internet verschoben werden müssten bis zum Sankt Nimmerleinstag. Authentifizierung und (virtuelle) Unterschrift sind ja zwei sehr verschiedene Dinge: Für etliche Verwaltungsverfahren reicht die einfache Identitätsfeststellung eines Antragsstellers vollkommen aus. Das digitale „Gegenzeichnen“ einer Anfrage ist theoretisch in vielen Fällen überflüssig. Wie das Praxiskapitel 3 nachfolgend aufzeigt, macht sich die Hansestadt Hamburg diesen Umstand zunutze und geht pragmatische Alternativwege jenseits der digitalen Signatur. Zuvor jedoch soll die Verantwortung der Gesetzgebung für dieses wichtige Thema angesprochen werden.

## 2. Status Quo – rechtliche und wirtschaftliche Aspekte

### 2.1 Politik im Zugzwang

Ein gravierendes Problem bei der Einführung von Online-Diensten stellt die gegenwärtige Rechtslage in Deutschland dar: Als Relikt aus der Vergangenheit sind die allermeisten der heute gültigen Gesetze nicht von modernem Prozessdenken geprägt. An einen Verwaltungsservice via Internet dachten die Autoren seinerzeit noch weniger. Zudem verlangt der Gesetzestext in vielen Fällen explizit die eigenhändige Unterschrift – obgleich auch bei herkömmlicher Arbeitsweise ohne weiteres darauf verzichtet werden könnte.

Bleiben all diese Gesetze wie sie sind, müssten beim Umstieg vom Papierformular auf das digitale Medium in jedem dieser Fälle elektronische Zertifikate mit implementiert werden. Kosten würden die Effekte schmälern. Daraus ergibt sich eine klare Forderung an die Legislative, unnötigen bürokratischen Ballast so schnell wie möglich abzubauen. Sonst droht Deutschland beim elektronischen Geschäftsverkehr noch weiter ins Hintertreffen zu geraten.

Viele unserer Nachbarn, wie z.B. Belgien und Österreich, gehen mit gutem Beispiel voran. So nimmt beispielsweise Belgien die Einführung einer einheitlichen Identitätskarte zum Anlass, überkommene Verwaltungsvorschriften systematisch abzubauen. Weil die belgische ID Card ein integraler Baustein der landesweiten E-Government-Kampagne ist, wird sie als Praxisbeispiel in Kapitel 3 vorgestellt.

Unbeschadet der laufenden Aktivitäten zur Förderung elektronischer Zertifikate (z.B. durch das 2003 gegründete „Signaturbündnis“, einer Gemeinschaftsinitiative von Bundesregierung, Wirtschaftsverbänden und Unternehmen) trifft das Chipkartenmodell in Deutschland derzeit auf erheblichen Widerstand: Die Vision einer universellen Signaturkarte, die im Idealfall Zugang zu jedem E-Government- und E-Commerce-Angebot schafft, wirft eine Reihe bis heute ungelöster datenschutzrechtlicher Fragen auf. Hinderlich wirkt in diesem Kontext zudem, dass viele relevante Zuständigkeiten auf Bund, Länder und Gemeinden verteilt sind.

Das Institut für Informationsmanagement Bremen (ifib GmbH) – ein gemeinnütziges Forschungs- und Beratungsinstitut, das der Bremer Universität zugeordnet ist – erhofft sich in diesem Zusammenhang, dass eine Neuordnung des Meldewesens neuen Schwung in die Entwicklung verwaltungsübergreifend nutzbarer Identifikationsverfahren bringt. Die Thüringer Landesbeamten haben jetzt sogar dezidiert die bundesweite Einführung eines elektronischen Personenregisters angemahnt. Das Personenstandswesen wird in Deutschland seit 1876 in Papierform dokumentiert. Durch das elektronische Register ließen sich laut Bundesverband der Deutschen Landesbeamten Einsparungen von rund 41 Millionen Euro pro Jahr realisieren. Auch könnte ein elektronisches Verzeichnis mit Daten zu Familienstand, Geburt und Tod den Bürgern helfen, schneller an verschiedene Urkunden zu kommen.

## 3. Praxisbeispiele

### 3.1 Belgien – Identifikation per Chipkarte

Ähnlich wie in Deutschland verteilen sich Verwaltungskompetenzen breit auf regionale und kommunale Behörden. Sozialversicherung und Steuer sind beinahe die einzigen Themen, bei denen belgische Bürger direkt mit der föderalen Verwaltungsinstantz konfrontiert werden. Seit 2001 zieht nun der Zentralstaat mit den 10 Provinz- und 589 Kommunalverwaltungen an einem Strang, um eine landesweit einheitliche E-Government-Plattform aufzubauen: Gegenstand der Initiative ist es, möglichst viele öffentliche Dienstleistungen für Bürger und Unternehmen elektronisch bereitzustellen.

Serviceverbesserung, Standortvorteile im internationalen Wettbewerb sowie massive Kosteneinsparungen durch effizientere Verwaltungsabläufe sind die vordringlichen Ziele des Projekts „Belgian Government Federal Portal Secure e-Government Services to Citizens Project“. Interessanterweise macht die informations- und netzwerktechnische Basis nur gut 20 Prozent des Gesamtprojekts aus; 80 Prozent entfallen auf die Neugestaltung von Verwaltungsprozessen, die Anpassungen von Gesetzen sowie auf Umstrukturierungen.

Grundlage für das belgische E-Government ist das Hochverfügbarkeitsnetzwerk FEDMAN (Federal Metropolitan Area Network) mit integrierten **Sicherheitsfunktionen**, darunter eine zentrale Firewall, VPN-, sowie Anti-Virus- und Intrusion-Detection-Systemen. Die Zugangs-Sicherheitsarchitektur gliedert sich in vier Ebenen: vom einfachen öffentlichen Zugang über zwei passwortgeschützte Zugriffsvarianten bis hin zur Electronic Identity Card „eID“ für rechtsverbindliche Transaktionen über elektronische Kommunikationskanäle.

#### **Zwei Kernlehren aus Belgien**

- 1) Das Hauptgewicht des Projekts – rund 80 Prozent – liegt auf Gesetzesanpassungen und der Vereinfachung und Optimierung von Verwaltungsprozessen; nur 20 Prozent fließen in Technologie.
- 2) Erfolgskritisch ist ein effektives, zentrales Back-Office und die Bereitstellung von Shared Services.

Da es erklärtes Ziel des Projekts ist, einer digitalen Spaltung der belgischen Gesellschaft entgegenzuwirken, arbeitet die Regierung eng mit der Industrie zusammen. So sollen beispielsweise alle im Handel erhältlichen Computer künftig über einen eingebauten Kartenleser verfügen. Bereits heute nutzen mehr als eine Million Belgier eine eID-Karte. Pro Monat kommen etwa 150.000 weitere hinzu. Die belgische Regierung schätzt, dass bis Ende 2009 rund 8,2 Millionen aller über 12jährigen Bürger eine Identitätskarte besitzen werden. Die Chipkarte kann beispielsweise für Online-Steuererklärungen, die Anforderung amtlicher Dokumente wie Heirats- und Geburtsurkunden sowie für diverse kommunale Services eingesetzt werden. Auch Privatunternehmen sollen künftig an der Sicherheitsinfrastruktur von eID partizipieren können. Perspektivisch bedeutet das für belgische Bürger: nur noch eine Identifikationskarte für alle Onlinedienste – egal, ob öffentlich oder kommerziell.

### 3.2 HamburgGateway

Wie gesagt: In Deutschland haben Chipkarten mit digitaler Signatur für die breite Masse der privaten Anwender noch zu wenig Nutzen, um akzeptiert zu werden. Hamburg stellt sich den Problemen rund um die Identifikation und Authentifizierung deshalb mit einem überraschend einfachen Ansatz: Die Dienste der Stadt werden nach Schutzbedarf klassifiziert; statt digitaler Zertifikate werden primär Benutzername und Passwort verwendet. Für einfache Anwendungen reicht lediglich eine einmalige Registrierung im Internet aus, Verfahren der Sicherheitsstufe 2 erfordern die Vorlage des Personalausweises bei der Registrierung im Kundenzentrum.

Das digitale Tor zum Onlineservice der Hansestadt, das *HamburgGateway*, ist seit 2003 geöffnet: HamburgGateway bietet gebündelten Zugang zu Leistungen wie Authentisierung und Benutzerverwaltung, Abwicklung von Online-Zahlungen sowie Kundenanfragen und deren Beantwortung via Web. Vorteilhaft für Hamburgs Bürger und Unternehmen: Das Stadtportal ist sieben Tage in der Woche 24 Stunden erreichbar, wobei die Kommunikation mit den Kunden über verschlüsselte **SSL-Verbindungen (SSL = Secure Socket Layer)** erfolgt. Kann eine Anfrage einmal nicht sofort beantwortet werden (zum Beispiel, weil Backend-

systeme nicht verfügbar sind oder ein Sachbearbeiter zuvor tätig werden muss), wird der Kunde per E-Mail informiert, sobald eine Antwort vorliegt.

Durch Firewalls gliedert sich die Architektur in unterschiedliche Sicherheitszonen – so genannte demilitarisierte Zonen – und einen geschützten Bereich für Backendsysteme. Im Backend laufen die bestehenden Fachverfahren unverändert weiter. Als einheitliches Schnittstellenformat setzt Hamburg auf XML: Auf dieser Basis wird für jedes Fachverfahren ein Adapter als Bindeglied zur Präsentationsschicht entwickelt. Ähnlich wie beim vernetzten Melderegister sorgt der Universalstandard XML also auch in Hamburg für die Integration bestehender Systeme und Verfahren bei gleichzeitigem Investitionsschutz.

Von Januar bis August 2005 stieg die Zahl der Firmenanfragen an das Hamburger Melderegister von 2.280 auf 3.635; bei externen Behördenanfragen war der Sprung noch deutlicher: von 1.724 auf 7.314. Insgesamt erteilte Hamburg bereits deutlich mehr als eine Million Melderegisterauskünfte online über das HamburgGateway.

Durch die Anwendung von für den Benutzer einfachen Verfahren wurde das HamburgGateway zum Erfolgsmodell. Andere Bundesländer interessieren sich stark für den Ansatz, einige kooperieren bereits mit Hamburg und nutzen die zentralen Authentisierungsdienste.

### **3.3 Erfahrungen aus Bremen**

Das Institut für Informationsmanagement Bremen (ifib GmbH) hat die Erfahrungen des Bundesprojekts Media@Komm im Hinblick auf Identifikationsproblematik im E-Government genauer unter die Lupe genommen: Die Resultate zeigen, dass sich der Charakter des Projekts mehr und mehr in Richtung einer Förderinitiative „Virtuelles Rathaus“ wandelte. Die Erprobung elektronischer Signaturen rückte in den Hintergrund. Zwar setzte die Förderung des Standards OSCI (Online Services Computer Interface) eine der für das deutsche E-Government wesentliche Entwicklungen in Gang, doch spielen digitale Signaturen im Nachfolgeprojekt MEDIA@Komm-Transfer keine herausgehobene Rolle mehr.

In mehr als drei Jahren Förderlaufzeit wurde das Kontingent kostenlos nutzbarer Signaturen in Bremen nicht annähernd ausgeschöpft. Auch verschob sich der Fokus weg von den Bürgerdiensten und hin zu mehr Services für professionelle Anwender: Obwohl sich 90 Prozent der Angebote an Bürger richteten, entfielen 90 Prozent der Transaktionen auf Unternehmen und professionelle Mittler wie Anwälte und Notare.

Für die Identifikation im Netz zeichnen sich bei den verschiedenen Zielgruppen klare Unterschiede ab: Im professionellen Bereich kann die elektronische Signatur als Erfolgsmodell gelten. Erhebliche Skepsis meldet das ifib aber bezüglich der Frage an, ob und wann sich digitale Signaturen im privaten Umfeld durchsetzen werden. Zu fragen bleibt dabei allerdings, ob dies für effektive öffentliche Bürgerservices überhaupt notwendig ist. Die einseitige Orientierung auf Signaturen verstellt mitunter den Blick auf das eigentliche Problem im E-Government: nämlich einfache und kostengünstige Verfahren zur elektronischen Identifikation.

Schon aus wirtschaftlichen Gründen – so die Schlussfolgerung des ifib – sollte sich die deutsche Verwaltung auf einen gemeinsamen Weg der Online-Identifizierung einigen. Behörden- oder landesspezifische Lösungen sind langfristig keine Alternative. Denn sie stehen letztlich vor dem ähnlichen Grundsatzproblem wie elektronische Signaturen: Bürger wollen die schnelle Erledigung ihrer Anliegen, ohne sich erst langwierig um einen Zugang zum jeweiligen Online-Angebot bemühen zu müssen. Zudem stehen unterschiedliche Identifikationsverfahren verwaltungsübergreifenden Angeboten im Sinne des „One-Shop-Government“ im Wege. Außerdem geben die vergleichsweise seltenen Behördenkontakte (durchschnittlich 1,5 pro Jahr) kaum Anlass zu der Erwartung, dass sich digitale Signaturen bei Privatanwendern allein durch E-Government durchsetzen werden. Als eher diffus bewertet das ifib die Rolle von Signaturen bei laufenden Chipkartenprojekten auf Bundesebene wie der Job- oder Gesundheitskarte. Eine neue E-Government-Phase hingegen könnte eine Neuordnung des deutschen Meldewesens im Zuge der Föderalismusreform einläuten, regt das ifib an.

## 4. Kritische Erfolgsfaktoren – Schlussfolgerungen

In Deutschland hat sich die Vision einer einzigen Signaturkarte für sämtliche Anwendungen bisher nicht erfüllt – und wird sich auch in absehbarer Zukunft nicht erfüllen. Davon darf sich E-Government aber nicht aufhalten lassen: Wie das Beispiel Hamburg zeigt, gibt es interessante Authentifizierungsalternativen. Nicht zuletzt, weil ohnehin nur für relativ wenige Verfahren digitale Signaturen tatsächlich notwendig sind.

E-Government definiert sich im Wesentlichen über G2B- (Government to Business) und G2G- (Government to Government) Kommunikation; Privatpersonen spielen als Kunden derzeit eine eher untergeordnete Rolle. Unter dem Win-Win-Aspekt sollten neue Angebote daher vorrangig auf Unternehmen und Behörden zugeschnitten sein. Dass sich dadurch schnell sichtbare Effekte einstellen, illustriert das Beispiel Hamburg ebenfalls eindrucksvoll.

Wie eingangs erwähnt: Es muss zwischen Authentifizierung und digitale Signatur unterschieden werden. Das Kernproblem aussichtsreicher E-Government-Projekte sind nicht die Signaturen, sondern robuste, sichere und kostengünstige Authentifizierungsverfahren. Allerdings benötigt Deutschland dafür einheitliche elektronische Identifikationsmöglichkeiten für jeden Bürger als einen Shared Service, der für alle Verwaltungseinheiten zentral bereitzustellen ist – womit sich der Kreis zum Generalthema des diesjährigen Netzkongresses von Cisco schließt.

Abschließend sei betont, dass es hierbei nicht allein darum geht, wann dieses oder jenes Verwaltungsverfahren gestrafft und wie viel Kosten dadurch im Einzelnen eingespart werden können. Es geht heute vielmehr darum, dass Deutschland den Anschluss im Bereich E-Government nicht verpasst. Datenschutzrechtlich einwandfreie elektronische Identitäten als Basis für Authentifizierungsmechanismen sind der Grundbaustein für eine anpassungs- und wettbewerbsfähige Verwaltung – und damit Voraussetzung für die Zukunftssicherheit unseres Landes.

## Impressum

Cisco Systems GmbH  
Am Söldnermoos 17  
85399 Hallbergmoos

Tel.: 00800-9999-0522  
info-center@cisco.com  
Internet: [www.cisco.de](http://www.cisco.de)

### Cisco Systems, Inc. – Unternehmensprofil

Cisco Systems, Inc. ist weltweit führender Anbieter von Networking-Lösungen für das Internet. Mit 34.000 Mitarbeitern weltweit setzt sich Cisco dafür ein, Netzwerke mit eingebauten Services intelligenter, schneller und beständiger zu machen.

Die europäische Unternehmenszentrale von Cisco ist in London. Die deutsche Cisco Systems GmbH wurde im April 1993 als 100%ige Tochtergesellschaft der Cisco Systems, Inc. gegründet. Die GmbH verstärkt die Präsenz des Unternehmens in Deutschland und hat die Aufgabe, die Vertriebspartner bei Marketing und Vertrieb sowie im technischen Support und Channel-Management zu unterstützen. In Deutschland werden die Networking-Komponenten von den zertifizierten Partnern und über autorisierte Distributoren vertrieben. Geschäftsstellen bestehen derzeit in München, Berlin, Hamburg, Düsseldorf, Eschborn bei Frankfurt und Stuttgart. In Deutschland sind insgesamt rund 600 Mitarbeiter beschäftigt.

Copyright © 2005 Cisco Systems, Inc. Alle Rechte vorbehalten. Cisco IOS ist ein Warenzeichen von Cisco Systems. Cisco Systems und das Cisco-Systems-Logo sind in den USA und anderen Ländern eingetragene Warenzeichen von Cisco Systems, Inc. Alle anderen namentlich erwähnten Warenzeichen sind Eigentum der betreffenden Inhaber.