Udo Helmbrecht
Heinz Thielmann
Albrecht Ziemer

Herausgeber

Elektronischer Personalausweis und E-Identity

MÜNCHNER KREIS
Übernationale Vereinigung für Kommunikationsforschung
Supranational Association for Communications Reseach

Das Buch enthält die Referate und Diskussionen des
Berliner Gesprächs „Elektronischer Personalausweis und E-Identity“
des MÜNCHNER KREIS am 26. März 2007

Vorwort

Die Bundesregierung hat im September 2006 das Programm „E-Government 2.0“ veröffentlicht, in dem vier Handlungsfelder ausgewiesen sind. Das Handlungsfeld „Identifizierung“ sieht die Einführung eines elektronischen Personalausweises im Jahr 2008 und die Erarbeitung von E-Identity-Konzepten vor. Mit der Einführung des elektronischen Personalausweises soll ein kombiniertes Ausweissystem für Anwendungen im E-Government und E-Business geschaffen werden, das eine verlässliche und einheitliche elektronische Identifizierung im Rahmen eines übergreifenden Gesamtkonzeptes ermöglicht.

Der MÜNCHNER KREIS hat in seiner bewährten Tradition, aktuelle Innovationsthemen aufzugreifen um sie zwischen Wissenschaft, Wirtschaft und Politik interdisziplinär zu diskutieren und gegebenenfalls Handlungsoptionen für alle Beteiligten abzuleiten, in Berlin ein Fachgespräch durchgeführt. Dabei haben Vertreter des Bundesministeriums des Innern und des Bundesamtes für die Sicherheit in der Informationstechnik sowie Fachleute aus Unternehmen, Verbänden und der Wissenschaft Informationen zum Stand der Entwicklung und den Perspektiven gegeben und diskutiert. Der vorliegende Band enthält die Niederschriften der Referate und Diskussionsbeiträge.

Unser herzlicher Dank gilt den Referenten und engagierten Teilnehmern sowie vor allem auch den Förderern, deren finanzielle Unterstützung die Durchführung dieser Veranstaltung ermöglicht hat.

Udo Helmbrecht Heinz Thielmann Albrecht Ziemer

Inhalt

1 Begrüßung und Einführung

Prof. Dr. Arnold Picot, Universität München

Meine sehr verehrten Damen und Herren, ich begrüße Herrn Staatssekretär Hahlen vom Bundesministerium des Inneren sowie Sie alle, die Sie von verschiedenen Bereichen des Parlaments, der Wirtschaft, der Wissenschaft und auch anderen Feldern der Politik und der Verbände heute Abend zu uns gekommen sind. Wir freuen uns sehr, dass dieses Thema eine so erhebliche Resonanz in einem Diskussionskreis gefunden hat, der hoffentlich dann auch wichtige Anstöße für die weitere Entwicklung geben kann.

Der Münchner Kreis hat sich heute mit Ihnen in Berlin versammelt und setzt damit seine Tradition fort, Veranstaltungen auch in Berlin abzuhalten. Er heißt zwar Münchner Kreis, ist aber überregional und übernational ausgerichtet. Seit über 30 Jahren agiert er an den Schnittstellen zwischen Politik, Wirtschaft und Wissenschaft im Bezug auf Themen der Informations-, Kommunikations- und Medientechnik und ihrer Anwendungen in der Gesellschaft. So hat er zum Beispiel zu Fragen des Telekommunikationsgesetzes, zu Fragen der Medien- und Frequenzpolitik, zu e-Government hier in Berlin und auch früher in Bonn getagt. Er wird nächsten Monat mit dem Deutsch-Japanischen Symposium zu Vernetzung und Konvergenz wieder hier in Berlin zu Gast sein. Aufgabe des Münchner Kreis ist es, den Weg des Wandels zur vernetzten Informations- und Wissensgesellschaft durch vorausschauende Analyse und kritisch-konstruktive Expertendiskussion zu gestalten. Das Thema, welches wir heute behandeln, passt zentral zu dieser Aufgabe.

Der elektronische Personalausweis ist, wie Sie alle wissen, im September des letzten Jahres von der Bundesregierung im Programm des Bundes zum Thema E-Government 2.0 angekündigt worden. Unter den Zielen dieses Programms heißt es unter anderem, dass Bürgerinnen und Bürger sowie Unternehmen online Dienstleistungen des Staates und der Wirtschaft zuverlässig nutzen und sichere elektronische Geschäftsbeziehungen aufbauen können sollen und dass dafür der elektronische Personalausweis eine wichtige Aufgabe erfüllt. Er ist ein staatlich bereitgestelltes Hochsicherheitsdokument, das die Anforderungen für eine sichere und einfache Identifizierung und Authentifizierung erfüllt. Das gilt insbesondere auch für den elektronischen Handel zu vertretbaren Kosten für die Nutzerinnen und Nutzer. Ab 2008 wird daher der Bund den elektronischen Personalausweis bereit stellen und dies dann weitergehend ermöglichen. Es heißt in dem Programm, dass mit dem elektronischen Personalausweis die erforderliche sichere harmonisierte Online-Authentifizierungsfunktionalität für E-Government und E-Business geschaffen und der bewährte bisherige Personalausweis zu einem kombinierten Ausweissystem weiter entwickelt wird.

Dabei wird mit dem Einsatz des elektronischen Personalausweises ein höheres Datenschutzniveau ermöglicht als mit dem herkömmlichen Personalausweis, da für die Identifizierung jeweils nur die erforderlichen Daten zur Verfügung gestellt werden. Und schließlich sollen mit der Einführung dieses Ausweises in 2008 auch privatwirtschaftliche E-Business Anwendungen durch die Wirtschaft zur Verfügung stehen, die diese elektronische Identifizierung verwenden. Das ist eine sehr interessante und auch innovative Perspektive, die der Bund hier aufzeigt und die natürlich in eine Welt hinein wirkt und in einer Welt entstehen soll, in der es bereits bestimmte Alternativen gibt zur Lösung der Identifizierungsfrage und auch der Bezahlung im E-Business (Kreditkarten u. a.). Es ist nun sehr spannend zu

überlegen, wie ein elektronischer Personalausweis erst einmal im E-Government selbst und dann über das E-Government hinaus eine Positionierung finden kann und wie diese dann technologisch, geschäftsstrategisch, rechtlich und datenschutzmäßig aussieht.

Deswegen bin ich sehr froh und sehr dankbar, dass wir heute Abend einen Expertenkreis versammeln konnten, der uns Informationen, Statements und Thesen zu dieser Entwicklung vorträgt, und damit die Diskussion beflügelt.

Ich möchte, ehe ich überleite zu unserem Programm, vor allen Dingen denjenigen danken, die dieses Programm ermöglicht haben. Das sind zuförderst Herr Dr. Helmbrecht vom Bundesamt für die Sicherheit in der Informationstechnik, Herr Kollege Thielmann vom Fraunhofer Institut für Sicherheit in der Telekommunikation und Herr Prof. Ziemer, der bis vor kurzem der Technikchef des ZDF war und dem Münchner Kreis, wie auch die anderen genannten, verbunden ist. Sie haben zusammen mit anderen dieses Programm entwickelt, und es ist sehr erfreulich, dass verschiedene, auch hier anwesende, Firmen und Organisationen dann das Zustandekommen der heutigen Gesprächsrunde unterstützt haben. Ich nenne ausdrücklich als Förderer des heutigen Abends das Fraunhofer-SIT (Institut) in Darmstadt, Giesecke&Devriant aus München, Netsecure Deutschland GmbH in Unterföhring, SCM Microsystems in Ismaning, Secunet Security Networks AG in Essen, der TÜV Rheinland Secure IT-GmbH in Köln und Utimaco Software AG in Oberursel. Ihnen allen einen ganz herzlichen Dank für die Unterstützung.

Meine Damen und Herren, ich darf nun überleiten zu unserem ersten Orientierungsgeber, wenn ich das so sagen darf, nämlich dem Staatssekretär aus dem Bundesinnenministerium Herrn Johann Hahlen. Er ist für dieses Feld im Bundesinnenministerium zuständig und wird uns unter dem Thema „Der elektronische Personalausweis - Sicherer eCommerce –politische Zielsetzung“ den Rahmen aufspannen, innerhalb dessen sich diese zukünftigen Entwicklungen abspielen werden. Herr Hahlen ich danke Ihnen sehr, dass Sie heute Abend zu uns gekommen sind, und wir sind gespannt auf Ihr Statement.

Staatssekretär Hahlen:
(Der Vortrag von Staatssekretär Hahlen ist unter Ziffer 2 abgedruckt).

Prof. Picot
Meine Damen und Herren, vielleicht gibt es noch die eine oder andere Frage, die Sie direkt an Herrn Staatssekretär Hahlen stellen möchten? Ich darf vielleicht mit einer Frage von mir aus anfangen. Sie haben gesagt, dass vielleicht auch die Chance bestünde, die elektronische Signatur auf eine breitere Basis zu stellen und haben darauf hingewiesen, dass sich dafür eine Zusatzdienstleistung anböte, die der Bürger getrennt bezahlen müsste. Nun muss der Bürger aber natürlich auch einen elektronischen Personalausweis bezahlen, wenn er zum Einwohnermeldeamt geht. Hier hätte ich zwei Anschlussfragen, nämlich einmal: Gibt es in Ihrem Hause bereits Vorstellungen, in welcher Höhe sich dieser Zusatzbeitrag für den Bürger bewegen würde, um den elektronischen Personalausweis zu erhalten? Und die andere Frage: Wäre es auch eine Überlegung Wert, zu analysieren, ob man die elektronischen Signaturen nicht in ein Paket beim Einwohnermeldeamt mit reinpackt, so dass man sozusagen die Gebühren für den ePA entsprechend ein bisschen aufstockt und dann dieses Identifizierungsinstrument schrittweise bundesweit und flächendeckend zur Verfügung hat?

Staatssekretär Hahlen:
Die letzte Frage ist natürlich eine besonders pfiffige Frage. Sie können das natürlich auch noch mit einem Los der Klassenlotterie oder was weiß ich noch verbinden. Dann hätten Sie

noch einen zweiten oder dritten Mehrwert mehr. Da bitte ich Sie um Verständnis, wir werden bei unserer Gebühr nur die Leistung in Rechnung stellen können, die der Bürger eben aus Sicherheitsgründen für diesen biometrischen Personalausweis aufwenden muss. Wir müssen davon ausgehen – ich lege mich jetzt nicht auf einen Euro fest -, dass aber der biometrische Personalausweis sich in ähnlicher Weise verteuert wie es der elektronische Pass getan hat, sprich: er wird wahrscheinlich gut doppelt so teuer werden wie gegenwärtig ein Personalausweis ist. Das ist so die Zielvorstellung, die mir vorschwebt. Das hängt auch davon ab, welches Muster und in welcher Ausstattung usw. das dann produziert wird. Mehr kann ich Ihnen beim besten Willen nicht sagen. Aber sicher wird nicht das Package Personalausweis + verpflichtende Signatur sein. Das wäre zwar eine sehr interessante Idee, aber das werden wir nicht machen können, weil das doch zwei verschiedene Stiefel sind.

Prof. Picot:
Noch weitere Fragen bitte sehr. Vielleicht können Sie sich kurz vorstellen.

Herr Mock-Hecker, Dt. Sparkassenverlag Stuttgart:
Ich hätte ein Frage zum „Rollout“. Zunächst einmal halte ich es für wirklich sehr wichtig, dass ein elektronischer Personalausweis mit einer elektronischen Authentifizierungsfunktion tatsächlich relativ schnell ins Feld kommt, weil es einfach wichtig ist für viele Businessprozesse, um, wie Sie sagten eine wirklich zuverlässige Identifizierung darstellen zu können und es wird sicherlich auch an vielen Stellen Prozesskosten einsparen.
Deshalb die Frage, wie schnell glauben Sie, wird denn der Rollout dieses elektronischen Personalausweises sein?

Staatssekretär Hahlen:
Das ist relativ einfach sich vorzustellen. Die Ausweise sind, wenn ich das richtig im Kopf habe, zehn Jahre gültig. Wir werden einen Umwälzungsprozess haben, wenn Sie mich fragen, wird es maximal zehn Jahre dauern. Dann haben wir eine Vollausstattung bis zum Jahr 2019. Wenn aber das Kind attraktiv ist und ich glaube, das Kind ist durchaus attraktiv, dann wird der ein oder andere Bürger, die eine oder andere Bürgerin schon mal früher zur Gemeinde gehen und einen neuen Personalausweis beantragen. Das ist so das Szenario.

Herr Mock-Hecker:
Noch eine Frage habe ich, weil wir natürlich als Sparkassen im Online-Banking auch schon die Erfahrung gemacht haben, dass neben der Karte noch ein bisschen mehr Infrastruktur für den Kunden zählt. Anwendungen auf der einen Seite, aber zum Beispiel auch ein Kartenleser. Wenn er sich im Internet von zuhause sicher identifizieren lassen will, braucht er einen Kartenleser. Und da sehe ich momentan eine Entwicklung, die mir etwas Sorge bereitet. Wir haben die Bankkarten an unsere Kunden ausgegeben. Für unsere Kunden ist das Thema Online-Banking ein immer wichtigeres Thema. Wir haben nun festgestellt, dass die Chipkartenleserabsätze im letzen Jahr ganz erheblich angestiegen sind. Jeder weiß warum. Nun bekommen wir die Gesundheitskarte. Auch dort mag der eine oder andere Nutzer mal gerne einen Chipkartenleser zu Hause haben, um die Daten zu lesen. Wenn wir jetzt alle parallel versuchen, jeder seinen eigenen Chipkartenleser dem Bürger zu verkaufen, dann kriegen wir alle die Quittung zurück, ob das Banken, Gesundheitswesen oder in dem Fall der Staat ist. Der Nutzer wird dies nicht mitmachen. Damit eben genau das nicht passiert, müssen wir es dem Bürger vereinfachen die Karten zu nutzen. Meine Frage: Was planen Sie in diesem Zusammenhang? Wahrscheinlich noch nichts, aber meine Anregung wäre, dass wir uns zusammensetzen sollten.

Staatssekretär Hahlen:
Da haben Sie mit Sicherheit Recht, aber jetzt führen Sie ein bisschen auf dieses technologische Glatteis. Wir haben da noch Interessengegensätze auszufechten. Wir haben einmal unsere Grenzpolizei, unsere Bundespolizei, die sagen wird: Ich brauche etwas, was mit einem Mal lesbar ist, etwas, was möglichst kontaktlos arbeitet. Dann gibt es andere, zu denen Sie gehören und die sagen, wir brauchen etwas, was in ein Lesegerät reinkommt. Darüber müssen wir uns noch unterhalten.

Prof. Rossnagel, Universität Kassel:
Wenn die Wirtschaft an diesen Personalausweis andocken soll, dann kann sie das ja nur, wenn sich alle in Deutschland sich den relativ schnell besorgen. Die Frage ist deswegen: Was passiert mit den ausländischen Mitbürgern? Bekommen die ein ähnliches Dokument?

Staatssekretär Hahlen:
Das ist eine Frage, auf die ich nicht eingerichtet bin. Aber wir haben hier Herrn Engel oder Herrn Schallbruch sitzen. Und vielleicht kann Herr Schallbruch etwas dazu sagen?

Herr Schallbruch:
Die Europäische Union wird für die langfristigen Aufenthaltstitel von Ausländern einen Aufenthaltstitel in Kartenform einführen. Die entsprechende Richtlinie ist gerade in der Entstehung in Brüssel. Wir haben uns in Brüssel dafür eingesetzt und auch erreicht, dass diese Aufenthaltstitel in Kartenform, in Form einer Aufenthaltskarte genau die gleiche technische Spezifikation erfüllen kann wie der elektronische Personalausweis, d.h. die sich langfristig in Deutschland aufhaltenden Ausländer mit einem langfristigen Aufenthaltstitel bekommen dann ein Dokument, was vielleicht ein bisschen anders ausschaut, was eine andere Rechtsqualität hat, was aber die gleichen technischen Funktionalitäten haben wird.

Frau Linde, Bundesverband Deutscher Banken:
Herr Prof. Picot hatte ja bereits das Geschäftsmodell angesprochen, das der Ausgabe des elektronischen Personalausweises zugrunde liegen soll. Sie hatten in Ihrem Vortrag angedeutet, dass für die verschiedenen Funktionen des elektronischen Personalausweises verschiedene Preismodelle vorgesehen werden sollen. Die Frage ist, ob für den Einsatz der Authentifizierungsfunktion im elektronischen Geschäftsverkehr Teile der Kosten von denjenigen getragen werden sollen, die den Personalausweis in ihren Anwendungen einsetzen? Dieses Modell war in der Vergangenheit von der Kreditwirtschaft im Signaturbündnis der Bundesregierung vorgestellt worden. Dort hatten wir dafür plädiert, dass derjenige, der eine Infrastruktur aufbaut, nicht 100% der Kosten tragen möge, sondern dass eben auch derjenige, der von dieser Infrastruktur profitiert, einen Teil der Kosten übernehmen sollte. Uns wurde jetzt zugetragen, dass dieses Geschäftsmodell, das wir seinerzeit für die Banken-Signaturkarte vorgeschlagen hatten, von Seiten der öffentlichen Hand auf den elektronischen Personalausweis angewendet werden soll. Wie ist hierzu der aktuelle Stand der Überlegungen?

Staatssekretär Hahlen:
Ich glaube, dass die Infrastruktur, die wir hier einrichten, jedenfalls das, was die Sicherheitstechnik und die Vorrüstungen bei den Personalausweisbehörden angeht, auf Kosten der Steuerzahler geht.

Prof. Picot:
Ich darf dann mich noch einmal in Ihrer aller Namen herzlich bedanken für Ihren wichtigen Input und die Diskussion und möchte gleich überleiten zur ersten Vertiefung dessen, nämlich

zur technischen Basis, von der letztlich alles dann ausgehen wird, Herr Dr. Helmbrecht, Präsident des BSI, Sie haben das Wort.

Dr. Helmbrecht:
(Der Vortrag von Dr. Helmbrecht ist unter Ziffer 3 abgedruckt.)

Prof. Picot:
Vielen Dank, Herr Helmbrecht. Das waren sehr klare und sehr Perspektive gebende Statements. Ich denke, dass vielleicht doch noch die eine oder andere Frage da ist, um besser zu verstehen, welchen Stand auch technisch das Projekt jetzt erreicht hat und wo Sie im Moment stehen. Ich weiß nicht, ob hier im Moment noch Informationsbedarf im Raum ist. Ich darf auch mit einer ganz laienhaften, kleine Frage beginnen: Man hat vor ein, zwei Jahren irgendwie lesen können in allen möglichen Gazetten, dass es ziemlich einfach wäre, irgendwelche biometrischen Daten zu übertölpeln, indem man also irgendwelche Gummifinger oder sonstige Dinge benutzt, um diese Geräte zu foppen. Ich weiß nicht, wie das heute aussieht. Es hat sich ja einiges auf dem Gebiet getan. Es wird weltweit auch benutzt, auch in den Vereinigten Staaten. Aber wie sicher ist man da heute, dass das nicht umgangen wird mit irgendwelchen einfachen Tricks?

Dr. Helmbrecht:
Der Punkt, auf den man hinweisen muss, ist: Was ist das Ziel? Worüber rede ich? Und ich benutze manchmal das Wort "abstruse Szenarien", über die man redet, wenn man an solchen Stellen noch manche Dinge kritisiert. In welcher Absicht kritisiert man das? Wenn man heute den Pass nimmt, dann haben wir gesagt, wir haben das Passdokument mit den bekannten Sicherheitsfeatures, beim Personalausweis ist es dasselbe, und wir wollen das Sicherheitsniveau erhöhen. Also, wir bauen zusätzliche Sicherheits-Features hinein. Das ist das grundsätzliche Prinzip, das wir immer haben, ob Sie den Geldschein nehmen, den Sie stetig verbessern, oder ob Sie andere Dokumente haben, die Sie verbessern. Es geht um eine Verbesserung und es geht jetzt nicht darum zu sagen, ich habe ausschließlich die Sicherheit in einem Chip. Das heißt also, wenn Sie sich den Grenzprozess anschauen, dann ist es so, dass der Grenzbeamte den Pass mit einem zusätzlichen Sicherheitsmerkmal, was der Fingerabdruck und das Gesichtbild sein werden, prüft. Damit kann man diese neuen Sicherheitsmerkmale mit den klassischen Sicherheitsmerkmalen kombinieren. Das muss man berücksichtigen, wenn man sich fragt, was realistisch ist.
Ich gebe ein Beispiel, das als Horrorszenario durch die Presse geistert. Ich könne irgendwo Ihren Pass auslesen und dann irgendwo nachschauen, das ist der Herr Picot, und dann hab ich Sie entdeckt. Wir haben alles dafür getan, dass man die Informationen im ePass praktisch nicht auslesen kann.
Weitere Beispiele sind: Wenn Sie mein Gesichtsbild haben wollen, fotografieren Sie mich. Wenn Sie meinen Fingerabdruck haben wollen, nehmen Sie mein Glas mit. Das heißt, ich brauche, wenn ich von jemandem einen Fingerabdruck haben will, nicht den Umweg über den Pass zu gehen. Wenn ein Terrorist jemanden irgendwo angreifen will, dann muss er nicht so umständlich die Daten aus dem Pass mit riesengroßen Antennen auslesen. Mit einer speziellen Antenne können Sie das vielleicht auf einige Meter Distanz machen. Allerdings ist die Vorstellung absurd, dass jemand an der Passkontrolle ohne aufzufallen mit einer großen Antenne vorbeigeht und Ihren Pass ausliest.
Das sind die Diskussionen, die dem BSI das Leben schwer machen, weil die Frage immer ist: Ist es eine Diskussion gegen den Chip im Pass oder eine Diskussion um die Technik? Ich diskutiere gern mit Universitätsprofessoren über die Entropie des Schlüssels. Ist der Schlüssel lang genug? Wie ist die Kryptografie? Ich mag es aber nicht, wenn man mit dem Ziel diskutiert, weil man den Chip oder das Speichern der Fingerabdrücke nicht mag, und sich

daher unrealistische Szenarien ausmalt. Wenn Sie das so mitnehmen und immer vergleichen, was ist eine technische Argumentation und was ist eine Argumentation gegen den ePass an sich, dann kann man sehr schnell die Spreu vom Weizen trennen.

Prof. Picot:
Hier sind im Moment keine dringenden Wortmeldungen. Wir kommen zum nächsten Vortrag. Herr Vater ist Vorsitzender der Arbeitsgruppe 2 des Deutschen Industrieforums, das sich schwerpunktmäßig mit der technischen Ausstattung der Nutzerseite des Elektronischen Personalausweises befasst. Herr Vater, bitte.

Herr Vater
(Der Vortrag von Herrn Vater ist unter Ziffer 4 abgedruckt.)

Prof. Picot:
Vielen Dank. Meine Damen und Herren, ich schlage vor, dass Sie etwaige Fragen oder Kommentare speichern, weil wir nachher noch eine Diskussionsrunde haben und wir jetzt die nächsten beiden Beiträge gleich anschließen.
Ich bitte den nächsten Präsentator, Herrn Dr. Groß-Selbeck von eBay seinen Vortrag zu halten. Herr Dr. Groß-Selbeck ist seit fünf Jahren bei eBay. Davor war er in verschiedenen Funktionen bei anderen Unternehmen, auch bei Beratungsunternehmen. Er war im Ausland für eBay, ist seit kurzem zurückgekehrt und ist der Geschäftsführer für den eBay Marktplatz in Deutschland. Er ist also berufen uns zu sagen, ob und wie der eCommerce im Internet mithilfe dieser Perspektiven des elektronischen Personalausweises tatsächlich befördert, verbessert und vereinfacht, vielleicht auch noch weniger kostspielig gemacht werden kann..

Dr. Groß-Selbeck:
(Der Vortrag von Dr. Groß-Selbeck ist unter Ziffer 5 abgedruckt.)

Prof. Picot
Ich bitte nun Herrn Hans Peter Heidebach von der Landeshauptstadt München, der aus dem Blickwinkel der kommunalen Anwender oder der öffentlichen Anwendung des E-Government uns einige Punkte zur Diskussion stellen möchte. Er ist Leiter der Abteilung Wirtschaft und beschäftigungspolitischer Grundsatzfragen bei der Landeshauptstadt München und sozusagen der ordnungspolitische Wirtschaftsminister von München. Ich freue mich sehr, Herr Heidebach, dass Sie heute hier sind und uns die Perspektive Ihres Hauses vermitteln.

Herr Heidebach:
(Der Vortrag von Herrn Heidebach ist unter Ziffer 6 abgedruckt.)

Prof. Picot:
Vielen Dank, Herr Heidebach. Das ist eine sehr wichtige Abrundung und Fundierung unseres ganzen Themas gewesen und ich schlage vor, dass wir jetzt in die Diskussion einsteigen.

(Die Niederschrift zur Diskussion ist unter Ziffer 7 abgedruckt.)

2 Der ePA „Sicherer eCommerce“ – politische Zielsetzung

Staatssekretär Johann Hahlen, Bundesministerium des Innern, Berlin

Herzlichen Dank, Herr Prof. Picot, für diese freundliche Begrüßung und den Rahmen, den Sie uns für dieses Gespräch heute Abend bieten. Wenn ich Sie hier an dieser schönen Tafel in diesem schönen Raum sehe, dann stelle ich mir diese Frage: „Was haben Regenwolken und Dinneransprachen denn gemeinsam?“ Sie haben das gemeinsam: Wenn sie vorbei sind, kann es noch ein schöner Abend werden. Deshalb möchte ich versuchen, mich etwas kürzer zu fassen.

Der elektronische Personalausweis, „Sicherer E-Commerce“ - politische Zielsetzung?, haben Sie mich gefragt. Herr Prof. Picot hat schon berichtet, was wir vorhaben. Sie wissen vielleicht, dass schon rund 3 Millionen der elektronischen Pässe ausgegeben sind und zwar mit einer halben biometrischen Ausstattung: das Foto in diesen 3 Millionen ausgegebenen Pässen ist schon digitalisiert und in dem Chip elektronisch gespeichert. Wir sind gerade dabei, in Testregionen seit Anfang März dieses Jahres die zweite Hälfte der Biometrie, nämlich die Aufnahme von beiden Fingerabdrücken in den elektronischen Pass zu testen. Denn wenn von Elektronik die Rede ist – wir denken vielleicht an die Mautbrücken – gibt es mitunter Probleme. Bei dem elektronischen Pass hat es bis jetzt solche Probleme nicht gegeben, und ich bin auch sicher, dass das weiter so gehen wird.

Nach dem Vorbild des Passes will die Bundesregierung jetzt einen elektronischen Personalausweis einführen, der auch beide biometrischen Merkmale enthalten soll, nämlich einmal das Lichtbild und zum anderen die beiden Fingerabdrücke. Insofern wird die Biometrie, was wir möglicherweise von Herrn Helmbrecht und anderen Fachleuten heute Abend noch näher hören werden, dieselbe sein wie bei unserem elektronischen Reisepass. Aber der Personalausweis wird mehr leisten. Weshalb wir auch sehr dankbar sind, dass wir die Gelegenheit haben, heute in den Diskurs mit Ihnen zu treten. Wir wollen mit diesem elektronischen Personalausweis nicht nur die Behörden der Republik, die Grenzbehörden primär, in die Lage versetzen, sehr viel sicherer die Menschen zu identifizieren bei diesen hoheitlichen Akten, die es da gibt, sondern wir haben die Vorstellung auch vor dem Hintergrund, dass der Personalausweis gewissermaßen ein Ausstattungsmerkmal in Deutschland ist, dass dieser Personalausweis den Bürgerinnen und Bürgern auch in ihrem täglichen privaten Leben zugute kommen soll, wie das ja auch jetzt schon der Fall ist. Wenn ich ein Bankkonto eröffnen möchte, muss ich auch meinen Personalausweis vorzeigen, obwohl die Bank mit dem hoheitlichen Akt nichts zu tun hat. Wir gehen davon aus, dass der elektronische Personalausweis genau so im Geschäftsleben eine Bedeutung für die Identifizierung der Bürgerinnen und Bürger erlangen soll, und darauf setzen wir eigentlich auch neben der Anwendung im hoheitlichen Bereich unsere ganzen Erwartungen. Ich glaube, dass wir da im gewissen Umfang eine Marktlücke abdecken. Wir nutzen immer intensiver die elektronischen Möglichkeiten des Internets, sei es im Privaten, dass wir Nachrichten austauschen, dass wir irgendwelche persönlichen Erlebnisse ins Internet stellen, sei es, dass wir aus dem Internet unser Wissen beziehen, sei es aber auch, dass wir wirklich im Geschäftsverkehr ein Auto mieten, ein Buch bestellen oder einen sonstigen Geschäftsvorfall tätigen. Immer stehen wir vor dem Problem, wie wir uns gegenseitig in dieser Cyberwelt identifizieren und authentifizieren. Und da glauben wir, dass der elektronische

Personalausweis in diese Marktlücke hineinkommt und es den Bürgerinnen und Bürgern erlauben wird, sich sehr zuverlässig zu authentifizieren in dieser elektronischen Cyberwelt des Internet.

Das bitte ich auch wirklich sehr ernst zu nehmen, denn damit bringt der Staat eine gewisse infrastrukturelle Vorleistung und es wäre sehr traurig, wenn diese infrastrukturelle Vorleistung, die wir mit dem elektronischen Personalausweis beabsichtigen, nicht dann auch von den Bürgerinnen und Bürgern und vor allem natürlich von der Geschäftswelt aufgegriffen würde. Ich bin aber sehr zuversichtlich, dass das der Fall sein wird, weil wir in eine Marktlücke hineinstoßen.

Lassen Sie mich in dem Zusammenhang noch eine ganz wichtige Feststellung machen. Diese biometrischen Merkmale, die wir in dem elektronischen Personalausweis haben, werden für private Geschäftsvorfälle nicht nutzbar gemacht. Hier sind wir mit den Vertretern des Datenschutzes einig. Wir halten uns für verpflichtet, dass diese biometrischen Daten in der Tat auf den hoheitlich notwendigen Bereich und die hoheitlich notwendige Nutzung beschränkt bleiben. Der große zusätzliche Vorteil des elektronischen Personalausweises ist, dass er ein elektronisches Ausweisen im Internet und dazu mit einer persönlichen und dem jeweiligen Ausweisinhaber zuzuteilenden und nachzufragenden PIN ausgestattet sein wird. Damit ist aus meiner Sicht eine zuverlässige Authentifizierung in der virtuellen Welt zu gewährleisten.

Wir wollen auch einen zweiten Schritt tun. Wir wollen neben der Funktion des Authentifizierens den Bürgerinnen und Bürgern die Möglichkeit geben, diese Infrastruktur, nämlich den elektronischen Personalausweis, für die elektronische Signatur zu nutzen. Die elektronische Signatur wird auch durch die Einführung des Personalausweises nicht gratis sein, sondern sie wird unverändert von den Providern nur mit Gebühren angeboten werden können. Aber wenn die Bürgerin oder der Bürger das möchte und wir nehmen an, dass das dann in sehr viel größerem Umfang der Fall sein wird als das bisher ist, wird er diesen elektronischen Personalausweis zusätzlich mit der dann von seinem Provider nachgefragten elektronischen Signatur versehen können. Wenn dann, und das sind in der Regel Rechtsvorfälle, die elektronische Signatur vom Gesetzgeber oder vom Vertragspartner erwartet wird, kann sie gegeben werden.

Wir glauben, dass auf diese Weise sich auch Skaleneffekte erzielen lassen, denn die elektronische Signatur ist deshalb in der Republik bislang nicht zu der Erfolgsgeschichte geworden, wie wir uns das gern wünschten, weil das Ganze noch zu teuer ist, weil es noch zu wenig nachgefragt wird. Ich bin aber überzeugt davon, wenn es über den elektronischen Personalausweis in dieser breiten Möglichkeit angeboten wird, werden sich auch da die Preisverhältnisse deutlich ändern.

Das ist der Rahmen, den ich Ihnen anzubieten hatte. Sie werden vielleicht noch fragen, wie lange es dauern wird. Der Zeitplan ist relativ einfach darzustellen. Wir haben die Absicht, die rechtlichen Vorbereitungen, d.h. wir brauchen eine gesetzliche Absicherung für den elektronischen Personalausweis, bis Mitte oder Ende des Jahres zu einer Kabinettsentscheidung über einen entsprechenden Gesetzentwurf zu kommen. Wenn wir den Gesetzentwurf dann im Gesetzgebungsverfahren hätten, ab Anfang 2008, meinen wir, dass das Gesetzgebungsverfahren bis Mitte 2008 abgeschlossen sein könnte. Wir werden natürlich während dieser Zeit schon mit Tests und Prototypen unsere Übungen machen. Wenn alles gut läuft, könnte ich mir vorstellen, dass der elektronische Personalausweis in der Fläche Ende

2008, Anfang 2009 hier in der Republik seine Einführung erlebt. Ich glaube, dass das, was ich Ihnen jetzt vorgestellt habe, keine Vision ist, sondern ein durchaus realistisches Szenario ist.

Ich fasse noch einmal zusammen: Der elektronische Personalausweis wird dieselbe Biometrie haben wie der elektronische Pass. Der Personalausweis soll neben der hoheitlichen Nutzung, und zwar hier mit den biometrischen Merkmalen, aber den Bürgerinnen und Bürgern auch die Authentifizierung in der Cyberwelt ermöglichen. Und er soll den Bürgerinnen und Bürgern die elektronische Signatur populär und deutlich preiswerter machen. Ich glaube, dass das ein Angebot an unsere Gesellschaft ist, das Sicherheitsinteressen der Sicherheitsbehörden gerecht wird und zugleich als Kundendienst und als Dienst an den Unternehmen in dieser Republik gedacht ist. Ich bin sehr dankbar dafür, dass viele intensiv an der Technik arbeiten. In diese schwierigen Gebiete möchte ich mich als Jurist nicht hinein begeben. Ich habe mir hier in die Tasche zwei Prototypen einstecken lassen, werde die Ihnen aber nicht vorzeigen, damit mir nicht vorgeworfen wird, dass ich für irgendeinen Prototyp Reklame mache. Im Übrigen wünsche ich Ihnen einen guten Abend und bedanke mich für Ihr Interesse.

3 Technische Übersicht über Lösungen zu ePA und E-Identity

Dr. Udo Helmbrecht, Bundesamt für Sicherheit in der Informationstechnik, Bonn

Es freut mich, bei der heutigen Veranstaltung zahlreiche bekannte Gesichter zu sehen. Ebenso freue ich mich auch über die vielen neuen Kontakte, die ich heute aufnehmen kann. Mit dem heutigen Gespräch des Münchner Kreises wollen wir sowohl ein Diskussions-Forum zum Thema "Elektronischer Personalausweis und E-Identity" als auch ein Forum für die Arbeit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bieten.

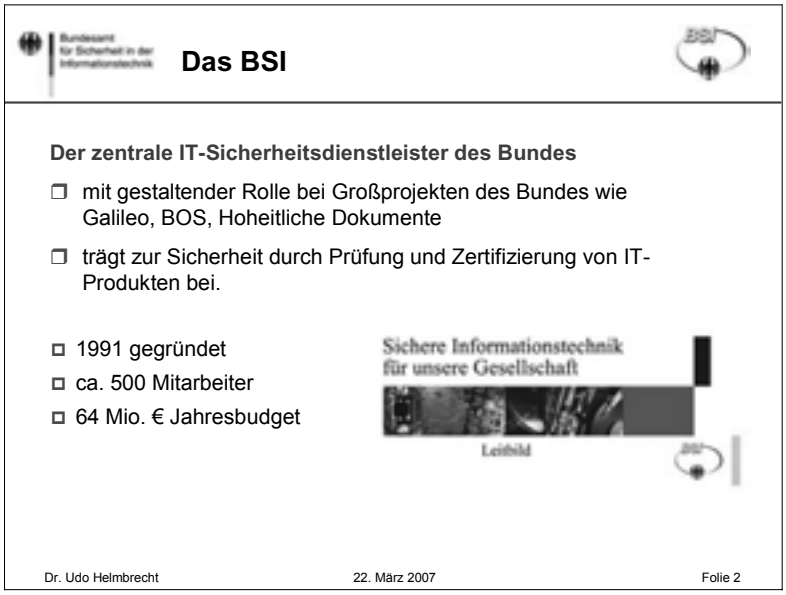

Bild 1

Lassen Sie mich zunächst in einigen Worten die Aufgaben des BSI darstellen (Bild 1). Überall dort, wo IT-Sicherheit in der Gesellschaft erforderlich ist, ist das BSI tätig. Das BSI sorgt zum Beispiel beim Mobilfunk Galileo, beim BOS-Digitalfunk für Behörden mit Sicherheitsaufgaben oder beim elektronischen Reisepass (ePass) für IT-Sicherheit in der Gesellschaft. Zudem stehen wir der Industrie als Partner bei Fragen zur IT-Sicherheit zur Seite. Desweiteren informieren wir die Bürgerinnen und Bürger darüber, was sie für ihren Informations- und Datenschutz im Internet tun können. Wir vermitteln ihnen auch Sicherheitsaspekte im Internet und Lösungen zur elektronischen Identität. Damit wollen wir ihr Vertrauen in innovative IT-Sicherheits-Lösungen made in Germany gewinnen. Wir erläutern hierzu die vielfältigen Sicherheitskonzepte und Lösungen, die das BSI und seine Partner für die Anwendungen entwickelt und zum Teil als neue sicherheitstechnische Standards etabliert haben. Das Ziel ist, dass die Belange des Datenschutzes erfüllt sind und die Bürgerinnen und Bürger dieser Infrastruktur vertrauen können.

Die aktuelle Diskussion über die Sicherheit in der IT ist geprägt durch Themen wie Computerviren, das Ausspähen im Netz, Identitätsdiebstahl und Phishing. Kriminelle Angriffsmethoden, zum Beispiel durch Bot-Netze mit ferngesteuerten Computern, gefährden die Akzeptanz und den Erfolg von Geschäftsmodellen im Internet. Denn diese Geschäftsmodelle funktionieren nur dann, wenn die entsprechende Infrastruktur auch sicher benutzt werden kann.

Eine Aufgabe des BSI ist die Vermittlung von Know-how zum Thema Sicherheit im Internet und in der IT. Wir versuchen das Bewusstsein für die Aspekte der IT-Sicherheit in Fachkreisen und in der breiten Öffentlichkeit zu schaffen und wir informieren darüber, was wir für diese Sicherheit tun. Das Ziel ist eine sichere IT-Infrastruktur.

Bild 2

Eine sichere IT-Infrastruktur ist auch im Bereich der e-Identity ein wichtiges Thema (Bild 2). Welche Rahmenbedingungen müssen für den sicheren Einsatz einer e-Identity geschaffen werden? Erforderlich sind sichere Verfahren zur Authentifikation und eine sichere Infrastruktur. Denn wir benötigen auch in der elektronischen Welt eine Identität und damit verbunden die Sicherheit, dass hier niemand unter falschem Namen aktiv werden kann.

Heute erleben wir im Internet gefälschte E-Mail-Adressen und E-Mail-Anhänge, die Schadprogramme enthalten. Wirkungsvolle Sicherheitstechnik dagegen haben wir bereits heute. Das sind Signaturen und die Verschlüsselung. Würden wir in großem Umfang signierte E-Mails nutzen, hätten wir viel weniger Probleme mit Spam. Die entscheidende Frage ist, wer die Kosten trägt, damit diese Lösungen in der Fläche und über die kritische Masse hinaus eingesetzt und für den breiten Einsatz attraktiv werden. Mit dem Signaturbündnis liefert der Staat bereits eine Vorarbeit für den Aufbau einer Infrastruktur. Damit schaffen wir eine Ausgangsbasis, um diese Technologie auch an den Kunden bringen zu können.

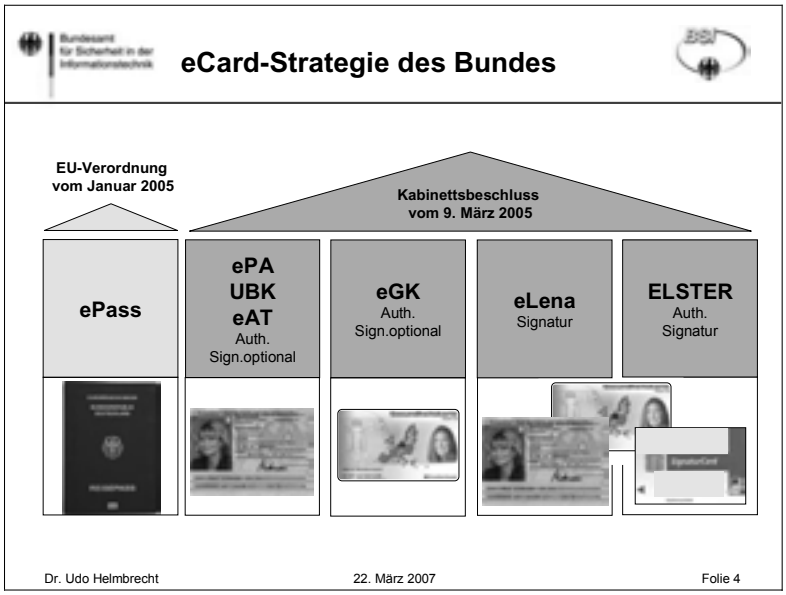

Bild 3

Welche Ergebnisse hat eine Bestandsaufnahme zum Thema E-Identity? Eine entsprechende EU-Verordnung besteht. Der ePass ist seit 2005 eingeführt und geht im November 2007 in seine zweite Stufe, bei der die Fingerabdrücke auf dem Chip des ePasses gespeichert werden. Eine ganze Reihe von Entwicklungen resultieren aus der eCard-Strategie der Bundesregierung, die 2005 beschlossen wurde (Bild 3). Das ist zum Beispiel der elektronische Personalausweis (ePA) oder die Unionsbürgerkarte (UBK, European Citizen Card). Mit diesen Vorhaben soll Europa vorangebracht werden. Das BSI trägt auch hier durch Standardisierung, wie bei der elektronischen Gesundheitskarte eGK und beim ePass dazu bei, diese Vorhaben sicher zu gestalten und umzusetzen.

Weitere Aktionsfelder des BSI sind die elektronische Gesundheitskarte, aus dem Bereich der Finanzverwaltungen das Thema ELSTER oder die Jobkarte. Dabei muss es sich nicht immer um eine einzelne Karte handeln.

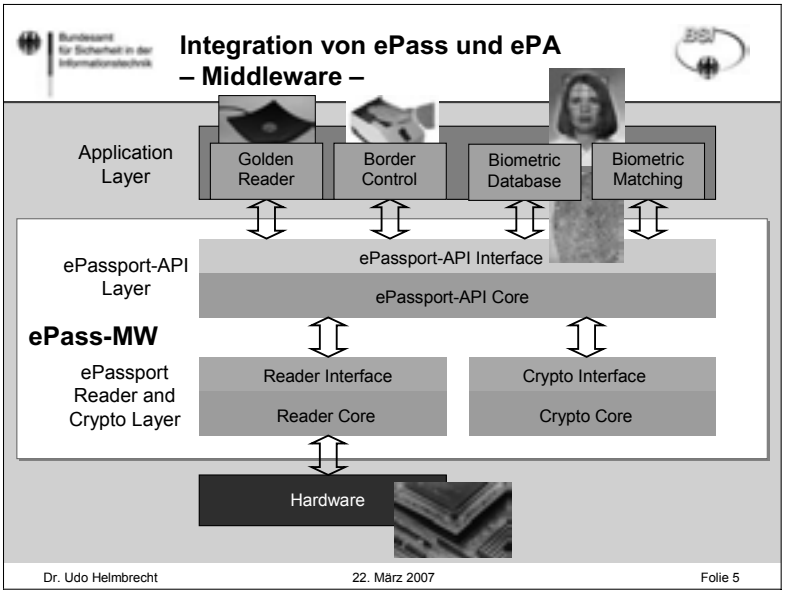

Bild 4

Ich möchte Ihnen verdeutlichen, dass wir uns im Rahmen der eCard-Strategie des Bundes auch mit der Middleware beschäftigen (Bild 4). Die Konzeption und verbindliche Vereinbarung dieser Verbindung zwischen IT und Anwendungen ist das Modell, wie wir als BSI diese Vorhaben steuern. An dieser Stelle treffen die IT, also die Hardware und ihre spezifischen Programme, mit den Anwendungen zusammen. Dieses komplexe Zusammenspiel von Hardware zur Erfassung und Übermittlung der E-Identity mit den unterschiedlichsten Anwendungen muss reibungslos funktionieren. Auf der Cebit 2007 konnten Sie eine solche Lösung sehen. Mit dem Golden Reader Tool hat das BSI den Standard für die Spezifikationsüberprüfung der elektronischen Reisepässe gesetzt. Derzeit wird dieses Verfahren bei der Grenzkontrolle an den Flughäfen pilotiert.

Ich möchte die Gelegenheit des heutigen Fachgesprächs auch nutzen, um unseren Abteilungsleiter Herrn Bernd Kowalski vorzustellen. Er leitet die Abteilung, die zuständig ist für die Zertifizierung und Konformitätsprüfungen und ist eine wichtige Stütze für die Arbeit des BSI. Eine seiner Aufgaben ist, die Sichtweise der Industrie und ihrer Vertreter und die Anforderungen des Staates zusammenzubringen. Sie kennen ihn sicherlich aus dem Deutschen Industrieforum, aus dem Signaturbündnis und anderen Diskussionsrunden zum Thema IT-Sicherheit. Die Vereinbarungen, die wir dort treffen, werden in den Projekten dort umgesetzt und setzen sich von der Hardware bis zu den Anwendungen fort. Beispiele sind die elektronische Gesundheitskarte, die europäische Bürgerkarte oder die Job-Card ELENA.

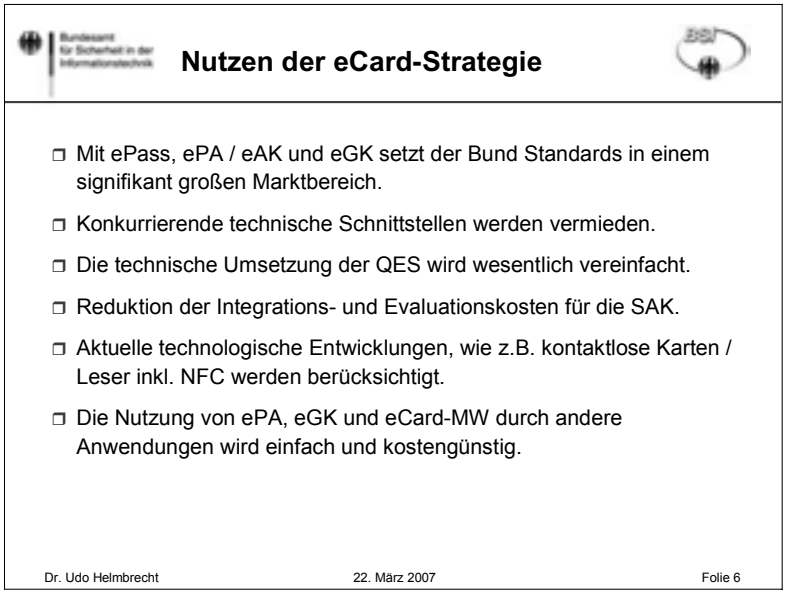

Bild 5

Wenn man über Nutzen und Risiken in einem solchen Kreis diskutiert, wird sehr schnell klar, welche enormen Chancen sich durch die eCard-Strategie eröffnen (Bild 5). Staat und Industrie müssen sich im Klaren sein, wer an welchen Stellen voranschreiten muss und wie wir die Vorteile und Möglichkeiten den Kunden darstellen. Das Wichtige ist, dass wir hier schauen, an welchen Stellen wir voranschreiten müssen und vor allem auch an welchen Stellen wir überlegen müssen, wie wir das zum Kunden bringen. Diese Veranstaltung ist sicherlich für uns eine gute Möglichkeit, weil wir aus Sicht des Staates mit unseren eGovernment-Projekten aus der Bundesverwaltung in die Länderebenen gehen. Wir haben dieses Thema bei BundOnline gehabt. Wir gehen nun mit eGovernment 2.0 den nächsten Schritt. Die Dynamik, die entsteht, muss genutzt werden, damit die staatlichen Prozesse in die Businessprozesse der Industrie übergehen.

Als BSI versprechen wir uns eine Kombination aus den Geschäftsmodellen der Wirtschaft mit den Prozessen der Verwaltung. Sie können von uns erwarten, dass der Staat durch den elektronischen Personalausweis die Identität einer Personen mit dem Dokument garantiert, besonders im Internet. Das BSI verantwortet den Prozess, sodass Sie sicher sein können, dass jemand, der sich mit seinem elektronischen Personalausweis ausweist, auch die Person am PC ist und nicht jemand anderes.

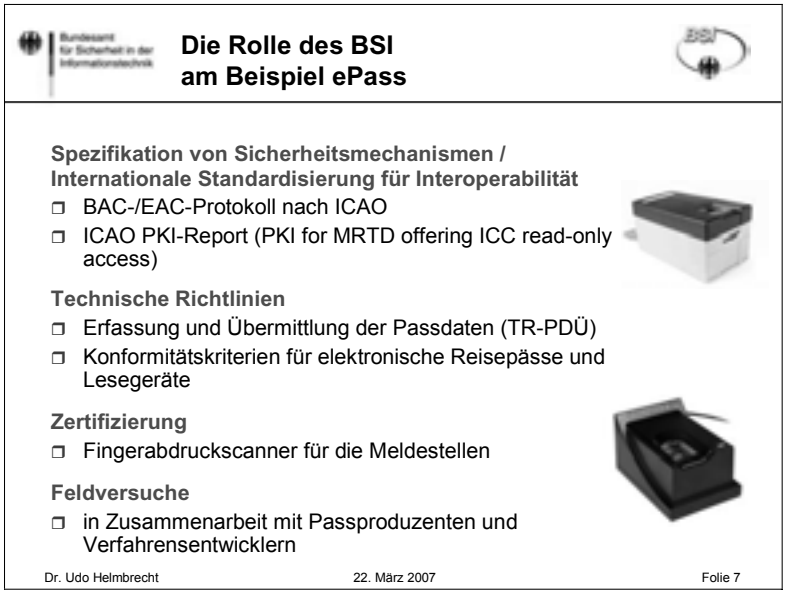

Bild 6

Wir haben die Erfahrung aus dem ePass-Projekt und wir verfügen über die entsprechenden Kartenlesegeräte (Bild 6). Aktuell führen wir zusammen mit der Industrie die ersten Feldtests für den ePass der Stufe zwei mit den gespeicherten Fingerabdrücken durch. Herr Staatssekretär Hahlen hat dies bereits erwähnt. Im September werden wir diese Erfahrungen aus dem Feldtest in die weiteren Schritte beim ePass-Projekt einbringen. Der nächste konsequente Schritt ist, diese Erfahrung aus dem ePass auch in andere Projekte einzubringen.

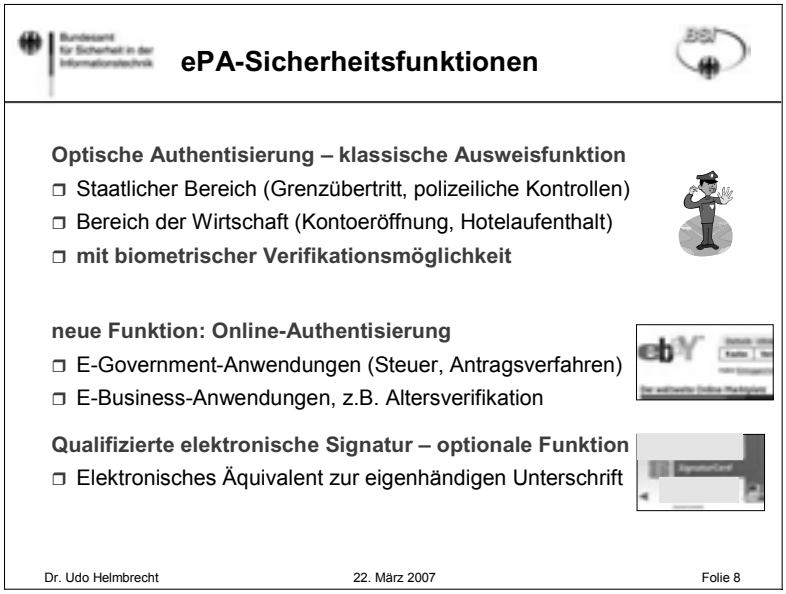

Bild 7

Die Erfahrungen, die wir im staatlichen Bereich mit dem Reisedokument ePass gemacht haben, nutzen wir auch für den neuen Personalausweis und seine Anwendungen beziehungsweise Geschäftsmodelle (Bild 7). Ob das Auktionen sind, ob das an anderer Stelle Business-to-Business- oder Business-to-Citizen-Prozesse sind. Insofern ist das für uns einfach eine konsequente Weiterentwicklung dessen, was wir heute tun.

Die Botschaft lautet: Auf Seiten der Technik haben wir das Projekt ePersonalausweis und damit die E-Identity im Griff. Wir sind von dem hohen Sicherheitsstandard und dem Daten- und Informationsschutz durch Kryptografie und Verschlüsselung, den wir beim ePass haben, überzeugt und integrieren diese auch in den neuen elektronischen Personalausweis. Damit bieten wir der Wirtschaft, wenn sie diese Anwendung nutzt, das gleiche, hohe Sicherheitsniveau, das wir auf der staatlichen Seite haben.

4 Zugangsgeräte wie Lesegeräte und Terminals für den ePA

Siegfried Vater, Vorsitzender der AG2 des Deutschen Industrieforums, Erfurt

Ich freue mich, dass ich die Möglichkeit habe, hier einen Statusbericht unserer Arbeitsgruppe im Deutschen Industrieforum abzugeben. In dieser Arbeitsgruppe beschäftigen wir uns speziell mit den Lesegeräten und Terminals, die künftige Besitzer des neuen ePA für dessen vielfältige Nutzung benötigen werden - auch mit dem im vorherigen Vortrag angesprochenen Kontext der E-Card-Strategie, die ja im weitesten Sinne ein Software-Interface für unsere Applikationen darstellt.

Das Deutsche Industrieforum hat vom BMI und BSI die Aufgabenstellung bekommen, sich mit der Leser- und Terminalseite der benötigten Infrastruktur zu beschäftigen. Das ist ein sehr wesentlicher Punkt, weil wir gerade auch bei der Einführung der E-Passports gesehen haben, wie wichtig es ist, dass alle Karten in allen möglichen Teilen der Welt sicher gelesen werden. Interoperabilität ist demzufolge ein wichtiges Thema und kann nur gewährleistet werden, wenn man den gesamten Komplex Karte, Terminal und Applikation betrachtet. Für uns Firmen, die wir führend an diesen Technologien arbeiten, ist es das Ziel, eine Infrastruktur basierend auf internationalen Standards zu definieren, die es unserem Wirtschaftsstandort ermöglicht, einen Export der neuen Technologien zu gewährleisten. Das Deutsche Industrieforum hatte schon vor zwei, wenn nicht sogar drei Jahren, eine Arbeitsgruppe gestartet, die sich speziell mit den Fragen der Karte beschäftigt hat. Das ist an sich schon ein komplexes Thema, da die Karte eine Prozessorplattform darstellt, in der alle sicherheitsrelevanten Applikationen laufen.

Das Speichern und Verarbeiten der Schlüssel ist dabei ein ganz wichtiges Thema und nur ein Beispiel. Wir haben vor ca. anderthalb Jahren angefangen, uns mit dieser Leser - und Terminalinfrastruktur zu beschäftigen. Dies ist sehr wichtig, damit wir ab 2008 – wenn die Infrastruktur eigentlich schon verfügbar sein soll – garantieren können, dass die Anwender zuhause Applikationen, basierend auf dem elektronischen Personalausweise auch sicher nutzen können.

Die Aufgabe der Arbeitsgruppen des Deutschen Industrieforums ist es, eine Infrastruktur für den Personalausweis zu schaffen, die zwei Seiten verkörpert. Dies ist zum einen die Funktionalität gemäß des bereits verfügbaren ePassports. Das ist dann im Prinzip gemeint mit der ICAO-Funktion – die hoheitliche Funktion - die 1:1 vom ePassport für den elektronischen Personalausweis übernommen wird. Daher haben wir auch vom Zeitplan eine logische Abfolge: der nächste Schritt für den ePassport ist die Einführung der Biometrie-Fingerprints mit dem Enhanced Access Code, danach erfolgt die Ausgabe der ersten ePAs, basierend auf dieser Technologie.

Unser erklärtes Ziel ist es, eine offene Plattform zu definieren, die es ermöglicht, dass zum Beispiel Entwickler von Software, aber auch von Lesern, von Karten und Kartenbetriebssystemen im weitesten Sinne unabhängig voneinander arbeiten können. Dies ist im Moment teilweise nicht gegeben, was ältere Smartcard-Technologie / Standards betrifft. Ich will nicht zu technisch werden, aber es gibt Situationen, wo zum Beispiel jemand, der eine Applikation schreibt, ziemlich viele Details von der Leserseite oder eben auch von der Kartenseite wissen muss und umgekehrt. Daher ist es unser Ziel, die Dinge voneinander

abzukoppeln, das heißt, klare Schnittstellen zu definieren, so dass die Entwicklung von Karte, Leser und Applikation völlig unabhängig voneinander erfolgen kann. Das ist möglich, indem – basierend auf der E-Card-Strategie – ein Interface geschaffen wird, welches strukturiert genug ist, um beispielsweise eine Applikation zu entwickeln, ohne die Leser- und Kartenseite kennen zu müssen.

Weitere wichtige Aspekte sind die Funktionalität, die Sicherheit und die Kosten. Wir haben die Aufgabenstellung und die Erwartung, dass Menschen zuhause in der Lage sein müssen, ihren neuen elektronischen Personalausweis, aber auch andere Karten, wie Gesundheitskarte oder Jobcard sinnvoll nutzen zu können. Es wird erwartet, dass Plattformen definiert werden, die für den häuslichen Bereich einfach zu gebrauchen sind. Darüber hinaus gibt es auch sicherheitsrelevante Anwendungen, gerade die hoheitliche Anwendung, wo Sicherheitsfunktionen implementiert sein müssen, um den hohen Anforderungen gerecht zu werden.

Für verschiedene sicherheitsrelevante Anwendungen wird sich die Notwendigkeit ergeben ein Protection Profile zu erstellen. Das Protection Profile definiert man für spezifische Anwendungen, zum Beispiel die hoheitliche Anwendung oder die qualifizierte elektronische Signatur. Damit schafft man auch eine Plattform, die Geräte, Karten und auch Software unter Umständen zertifizierbar macht. Das gewährleistet, dass im Umkehrschluss für den Enduser – der nicht alle technischen Details versteht – einfach nachzuvollziehen ist, für welche Applikation, für welchen Sicherheitslevel, welche Zertifizierung notwendig ist.

Die Hauptfunktion des Personalausweises ist die hoheitliche Anwendung. Das heißt alle Funktionen, die im elektronischen Passport schon implementiert sind, werden auch im elektronischen Personalausweis vorhanden sein. Diese Applikation basiert auf den internationalen Standards, die die ICAO für ePassports festgeschrieben hat.
Unsere angestrebte Infrastruktur setzt auf den existierenden Lösungen auf. Das heißt, es ist wirklich wichtig zu sagen, dass wir im Sinne der Interoperabilität keine Insellösungen schaffen wollen und auch gar nicht können, sondern wir müssen die internationalen Standards nutzen und weiterentwickeln, um die Technologie für alle Beteiligten attraktiv zu machen.

Für die hoheitliche Anwendung haben wir folgende Dinge zu berücksichtigen: Die Personalisierung der Dokumente, wie auch deren Ausgabe. Ein anderes Beispiel ist die Grenzkontrolle, im Fall des Personalausweises innerhalb Europas. Das schliesst natürlich auch mobile Kontrollgeräte ein, die von Polizei, Grenzschutz usw. nutzbar sind.

Zur hoheitlichen Funktion – und das ist ein wesentlicher positiver Aspekt des neuen ePA's - besteht die Möglichkeit, in einem separaten Bereich des Personalausweises allgemeine Anwendungen zu laden. Hier müssen wir versuchen Dinge zu berücksichtigen, die wir im Moment noch nicht kennen. Wir haben in einem früheren Vortag gehört, dass die Lebensdauer eines Personalausweises zehn Jahre ist und dass sich auch die Ausgabe in Deutschland über zehn Jahre erstrecken wird. Insofern ist es nahezu unmöglich, im Moment schon alle Aspekte zu berücksichtigen, die vielleicht in fünf oder mehr Jahren eine Rolle spielen werden. Unser Verständnis an der Stelle ist, dass wir durch die modulare Struktur und durch die klar definierten Schnittstellen der Plattform dafür sorgen, dass wir auch in Zukunft ohne Probleme entsprechende Erweiterungen vornehmen können.

Eines der wichtigsten Themen ist zweifellos die Authentisierung und Identifizierung über das Internet mit dem neuen ePA – und das ist natürlich für den Heimanwender ein angestrebter Zusatznutzen des Dokuments. Dabei muss die Applikation nicht immer bis zum

Sicherheitslevel einer qualifizierten elektronischen Signatur gehen. Es kann auch einfach nur sein, dass man komfortabel – ohne sich verschiedene Passwörter merken zu müssen – die verschiedensten Websites nutzen kann, bei denen man sich normalerweise registrieren bzw anmelden muss.

Zur qualifizierten elektronischen Signatur haben wir bereits Erläuterungen in einem früheren Vortrag erhalten. Das ist definitiv eine Applikation, die im Personalausweis vorbereitet sein wird und von einem TrustCenter frei geschaltet werden muss, je nachdem, ob der Anwender / Kunde dies wünscht. Andere Dinge, die in der Zukunft sicherlich eine Rolle spielen werden, sind bestimmte Zugangskontrollen oder Kundenbindungsprogramme auf Basis des Personalausweises.

Wichtig für den Erfolg des elektronischen Personalausweises ist, dass wirklich die Erfahrung und auch die Technologie des ePassports genutzt wird und damit auch die Lernkurve, die wir als Industrie vollzogen haben, was Interoperabilität betrifft. Hier laufen nicht nur im Deutschen Industrieforum, sondern auch in technischen Arbeitsgruppen des DIN wie auch ISO viele Aktivitäten, wo die beteiligten Firmen sicher stellen, dass Standards fertig gestellt oder erweitert werden – sehr viel existiert an der Stelle schon – die die Interoperabilität von Karten und Lesern ermöglichen.

Unsere Arbeitsgruppe nähert sich diesem Szenarium über User Cases, das heißt, wir schauen, was zum Beispiel für eine Heimanwendung erforderlich ist. Und noch einmal, hier ist ganz klar das Ziel, dass wir am Ende eine sinnvolle Technologie zu einem Preis verfügbar machen müssen, in der der Anwender zuhause einen echten Vorteil und einen Nutzen davon hat.

Wir haben einen Status erreicht, wo wir erste Implementierungen bezüglich einer erweiterten Spezifikation machen, die die Zertifizierung der zukünftigen Plattform ermöglicht. Viele führende Firmen sind involviert.

Die Spezifikation, die wir im Moment in einer Demo-Implementierung testen, ist im Prinzip schon auf dem Weg zu einem internationalen Standard. Die erste, fast fertige Version ist auf ISO-Level unter der nochmaligen Durchsicht. Damit haben wir bald die Chance, sicherzustellen, dass wir die Hardware der Leserseite zertifizieren können. Hier sind wir einen großen Schritt vorangekommen. Dies betrifft den ePassport, aber eben auch die Plattform für den elektronischen Personalausweis. Das war eines unserer erklärten Ziele: die Internationalen Standards an dieser Stelle entsprechend voranzubringen.

Wir haben nun eine Situation erreicht, wo wir denken, dass zuerst natürlich aus unserer Sicht hier in Deutschland, aber auch weltweit, End-User zuhause diese Technologie nutzen. Nach unseren Informationen haben wir im Moment weltweit ca. 30 Millionen Leser installiert. Fast zu 100% sind das Anwendungen, die sicherheitsrelevante Applikationen in Firmen oder Institutionen betreffen, aber eben nur sehr wenig Anwender zuhause. Hier erwarten wir uns, dass durch den Personalausweis mit der Funktionalität, die gegeben sein wird, wirklich ein Wechsel eintrifft, der über einen Nutzen, den ein Endanwender zuhause hat, die Verbreitung von solchen Lesern in großem Volumen ermöglicht. Der Gedanke ist auch, dass man mit dem Gesamtkonzept und mit der Gesamtlösung anderen Staaten eine Technologie anbieten kann, die einfach zu nutzen bzw nachzunutzen ist.

5 Wie moderne Technologie Vertrauen und Sicherheit im Online-Handel fördern kann

Dr. Stefan Groß-Selbeck, eBay Deutschland

Der elektronische Personalausweis kann dazu beitragen, den Handel im Internet einfacher und sicherer zu machen – wie, das will ich am Beispiel eBay erläutern. Zuvor möchte ich als Geschäftsführer von eBay in Deutschland ein paar grundsätzliche Anmerkungen zu diesen Themen machen.

Für unseren weltweiten Online-Marktplatz sind Sicherheit und Vertrauen von fundamentaler und strategischer Bedeutung, seit es uns gibt. Das wird niemanden überraschen, der unser Geschäftsmodell kennt, denn dieses beruht darauf, dass zwei Menschen, die sich noch nie gesehen haben und wahrscheinlich auch nie sehen werden, genug Vertrauen zueinander entwickeln, um miteinander zu handeln. Dabei kennen sie voneinander nicht mehr als den Nutzernamen, also ein Pseudonym, und einige weitere wichtige Informationen wie zum Beispiel das Bewertungsprofil. Kurz: Sie wissen nicht sehr viel, zumal es beim Online-Handel ja fast immer um Distanzgeschäfte geht, bei denen einer von beiden in Vorleistung geht. Das ist bei eBay typischerweise der Käufer, der dem Verkäufer den Kaufpreis überweist. Das macht er natürlich in der Erwartung, dass der Verkäufer die Ware so, wie er sie beschrieben und wie das Foto sie gezeigt hat, auch schickt. Es braucht schon sehr viel Vertrauen, damit das funktioniert. Die gute Nachricht ist: Es funktioniert gut. Der Online-Marktplatz eBay wächst und wächst, allein in Deutschland zählen wir inzwischen über 20 Millionen Nutzer. Das Handelsvolumen liegt bei über acht Milliarden Euro pro Jahr. Das ist schon eine richtige kleine eBay-Wirtschaft, die da entstanden ist. Und man kann sehr schön sehen, was passiert, wenn man Menschen einen Marktzugang eröffnet – und nichts anderes tun wir. Es gibt in Deutschland über 64.000 Menschen, die davon leben, dass sie auf eBay verkaufen, etwa weil sie sich ein Kleinstunternehmen aufgebaut haben. Das unterstützen wir unter anderem durch Schulungsveranstaltungen. Es gibt eBay Universities und weitere Fortbildungsmöglichkeiten für unsere Nutzer. Wir informieren Existenzgründer und helfen ihnen bei allen relevanten Fragen vom Steuerrecht bis hin zum professionellen Verkaufen. Ich finde es immer wieder auch für mich persönlich inspirierend, mit diesen Nutzern zu sprechen, weil man eine enorme unternehmerische Energie spürt, die frei wird, wenn Menschen plötzlich Zugang zu einem Markt bekommen.

Man könnte also sagen: Das ist doch alles wunderbar, es funktioniert. Die Wahrheit freilich ist etwas komplizierter, wie wir aus einer Vielzahl von Studien wissen. Aus unserer jüngsten eBay/TNS Infratest-Studie zum Thema „Sicherheit im Online-Handel“ etwa wissen wir, dass mangelndes Vertrauen in die Sicherheit von Internet und Online-Handel nach wie vor unser größtes Wachstumshemmnis darstellt. Und das betrifft gar nicht so sehr diejenigen, die das Internet gar nicht benutzen, weil sie ihm ohnehin grundsätzlich nicht trauen. Nein, sogar bei so genannten „Heavy Usern“, die sehr viel online handeln, gibt es eine Art psychologische Hemmschwelle im Kopf, die sie daran hindert, mehr als einen bestimmten Betrag beim Online-Kauf auszugeben. Beim einen liegt die Grenze vielleicht bei 500 Euro, beim anderen bei 5.000. Aus der eben genannten Studie wissen wir, dass deutsche eCommerce-Nutzer im Durchschnitt maximal 600 Euro für den Kauf eines Artikels im Internet auszugeben bereit sind.

Wie viel jeder einzelne letztlich bereit ist, auszugeben, ist individuell sehr unterschiedlich und hängt davon ab, wie viel Vertrauen er Internet und Online-Handel schenkt. Fest steht: Es gibt einen direkten Zusammenhang zwischen dem vorhandenen Vertrauen und der Bereitschaft, auch höhere Summen beim Einkauf im Internet zu investieren. Von daher ist es ein für unser Geschäft entscheidender Faktor, dieses Vertrauen in die Sicherheit des Online-Handels zu stärken. Davon hängt auch ab, ob wir die Möglichkeiten der Informationstechnologie für Wirtschaft und Gesellschaft voll nutzbar machen.

Probleme mit der Sicherheit gibt es viele: Datensicherheit, Identitätsschutz, Schutz vor Betrug, Jugendschutz etc. Das sind alles wichtige Themen. Mir liegt daran, darauf hinzuweisen, dass man nun zwei Dinge tun muss. Das eine ist, an den Technologien zu arbeiten, vor diesen Gefahren schützen. Für sehr viele der genannten Risiken gibt es effektive Technologien. Aber das allein reicht nicht aus. Was Sie ebenfalls brauchen, ist das Vertrauen der Nutzer. Das hängt zwar entscheidend von deren Sicherheit beziehungsweise deren Sicherheitsempfinden ab, meint aber noch etwas anderes. Die technischen Voraussetzungen für größtmögliche Sicherheit zu schaffen, genügt nicht.

Wir kennen das aus der eigenen eBay-Welt. So ist beispielsweise der deutsche eBay-Marktplatz sicher, oder sagen wir, recht sicher. Auch im Vergleich zu eBay-Marktplätzen in anderen Ländern steht er objektiv gut da. Das Vertrauen der Nutzer in den nationalen Marktplatz aber fällt in Deutschland niedriger aus als in anderen Märkten. Warum? Hat das kulturelle Gründe? Sind die Deutschen besondere Sicherheitsfanatiker? Ich weiß es nicht. Fest steht, dass es uns offenbar nichts nutzt, „nur“ objektiv für Sicherheit zu sorgen. Wir müssen das Vertrauen der Menschen gewinnen, und das hat eben auch eine subjektive und emotionale Komponente. Deswegen widmen wir dem Thema Sicherheit und Vertrauen in Deutschland so viel Aufmerksamkeit. Wir bemühen uns fortlaufend um Aufklärung, um ein Bewusstsein für die Risiken und Schutzmechanismen zu schaffen. Wir klären die Nutzer auf über die Instrumente, die sie zu ihrer Sicherheit einsetzen können. Und wir sagen ihnen, wie sie sich verhalten sollen, um Risiken begegnen zu können oder von vorneherein auszuschließen.

Man kann sich im Internet sicher bewegen, wenn man einen „gesunden Internetverstand“ entwickelt. So, wie es einen gesunden Menschenverstand gibt, gibt es auch einen gesunden Internetverstand. Dazu gehört zum Beispiel, dass ich auf eine E-Mail hin nicht irgendwo im Internet meine persönlichen Daten eingebe. Das muss man lernen. Das muss man wissen. So kann man sich schützen. Mit diesen Informationen kann man Sicherheit beziehungsweise Vertrauen und somit die Voraussetzung dafür schaffen, das Potenzial von Internet, eCommerce und allen anderen Anwendungen der Informationstechnologie in unserem Land auszuschöpfen. Also, Sicherheit ist wichtig. Aber Vertrauen ist mindestens genauso wichtig.

Wie gehen wir nun mit den Themen digitale Identitäten und elektronischer Personalausweis um? Inwiefern könnten wir davon profitieren? Zunächst einmal: Für uns gibt es im Wesentlichen zwei unterschiedliche Aufgaben in diesem Bereich. Da ist zum einen die Verifizierung bei der Anmeldung, zum anderen die Authentisierung bei der Rückkehr auf die Seite, also beim Einloggen. Das sind die beiden wesentlichen Prozessschritte und Themen, bei denen der elektronische Personalausweis für uns interessant sein könnte. Der Nutzen einer digitalen Signatur ist für mich weniger ersichtlich, denn wie in der Offline-Welt nur wenige Verträge schriftlich oder gar mit notarieller Beurkundung geschlossen werden, reichen auch online in den meisten Fällen formlose Verträge. Der Vertrag ist in aller Regel wirksam, wenn die Handelspartner verifiziert und authentisiert sind – in der digitalen Signatur sehe ich für den eBay-Marktplatz in seiner aktuellen Form keinen großen Zusatznutzen. Wohl aber bei der Verifizierung und Authentisierung der Nutzer mittels eines elektronischen Ausweises.

Wie verfahren wir heute bei der Verifizierung? Der übliche „Use Case“ ist der, dass sie auf eBay etwas kaufen oder verkaufen wollen und sich dazu bei uns registrieren müssen, das heißt, sie geben ihre persönlichen Daten an. Wir wollen in einem nächsten Schritt sicherstellen, dass Sie wirklich derjenige sind, der Sie zu sein vorgeben. Wir führen die Verifizierung in mehreren Stufen durch. Als Erstes gleichen wir die angegebenen Daten mit der Datenbank der SCHUFA ab. Und das nicht etwa, um die Kreditwürdigkeit zu prüfen, sondern einfach um festzustellen, ob es eine Person gibt, auf welche die Daten passen, also ob der Name zur Adresse passt. Das ist die wesentliche Kontrolle. Das ist nicht hundertprozentig sicher, aber es ist eine erste Stufe, die wir brauchen, um Fantasieanmeldungen auszuschließen.

Ist dieser Abgleich nicht erfolgreich, weil die Daten nicht zusammenpassen oder weil es sie nicht in der Datenbank gibt, erfolgt im zweiten Schritt eine Verifizierung über Briefpost. Wir schicken Ihnen ein Passwort an Ihre Postanschrift, und nur mit diesem Passwort können Sie Ihr Mitgliedskonto aktivieren. Das ist auch nicht vollkommen sicher, weil Sie sich natürlich eine falsche Adresse zulegen könnten, doch schafft das schon eine erhebliche Hürde gegen Missbräuche.

Die dritte Stufe, die wir anbieten, ist die Nutzung des Post-Ident-Verfahrens, ein Dienst der Deutschen Post, bei dem ein Postangestellter die Identität anhand des Personalausweises überprüft. Das ist die sicherste, aber auch aufwändigste und teuerste Form der Verifizierung. Dieses Verfahren kostet eine nicht unerhebliche Gebühr, vor allem ist es aber auch mit deutlichem zeitlichem Aufwand für den Nutzer verbunden. Dennoch fordern wir diese Form der Verifizierung von bestimmten Nutzergruppen, etwa von Verkäufern, die besonders viel verkaufen und die wir deshalb PowerSeller nennen. Sie müssen bestimmte qualitative und quantitative Kriterien erfüllen und bekommen unter anderem ein Logo von eBay, das sie benutzen dürfen, wenn sie ihre Waren anbieten. Seit kurzem knüpfen wir die Vergabe dieses Logos daran, dass der Verkäufer das Post-Ident-Verfahren durchlaufen hat. Seitdem kennen wir gesichert die Identitäten unserer über 10.000 PowerSeller, die trotz Kosten und Aufwand großes Interesse an dem Logo haben. Denn PowerSeller zu sein, verschafft Verkäufern einen Wettbewerbsvorteil auf unserem Marktplatz. Unsere Mitglieder kaufen gerne bei PowerSellern, weil sie wissen, dass Anbieter mit PowerSeller-Logo erfahrene eBay-Verkäufer sind – und man ihnen besonders vertrauen kann.

Zurück zur Verifizierung. Die große Herausforderung für uns besteht nicht so sehr in den Kosten der Verfahren. Die entscheidende Frage lautet: Wie bereit sind die Nutzer, diese Verfahren anzuwenden? Das Post-Ident-Verfahren als strengste und sicherste Verifizierungsform zur Grundvoraussetzung für jeden zu machen, der auf eBay etwas verkaufen möchte, wäre im Markt schlicht nicht durchsetzbar. Denn für die Akzeptanz vor allem der gelegentlichen Nutzer ist es entscheidend, dass es für sie einfach ist, etwas bei eBay zum Verkauf anzubieten. Deswegen wäre es aus unserer Sicht nicht angemessen, jeden per Post-Ident-Verfahren zu identifizieren. Für jemanden, der in großem Umfang professionell bei eBay verkauft, ist das Durchlaufen des PostIdent-Verfahrens sicher zumutbar – aber eben nicht für jeden eBay-Verkäufer. Wir halten hier eine Staffelung für sinnvoll und notwendig. Das belegt ein weiteres Beispiel: Wenn wir das doch relativ einfache Briefpost-Verfahren anwenden, liegen die Abbruchraten bei rund 40 Prozent. Das heißt: Von 100 Leuten, die den Anmeldeprozess beginnen, uns ihre Adresse geben und denen wir dann per Post ein Passwort zuschicken, werden nur 60 tatsächlich Kunden bei eBay. Das geschieht, weil es den Leuten einfach zu kompliziert wird. Die Kosten, die wir für die Briefpost und den dahinter liegenden Prozess aufwenden müssen, sind auf gut Deutsch „Peanuts“ im Vergleich zu den Kosten, die

dadurch entstehen, dass wir von den 100 Kunden 40 verlieren, bevor sie bei eBay überhaupt aktiv werden. Darin besteht die große Herausforderung: Wie schaffen wir es, Authentisierungsverfahren anzubieten, die so einfach sind, dass die Nutzer sie definitiv anwenden? Das ist der entscheidende Punkt, mit dem wir uns intensiv beschäftigen müssen. Natürlich würden wir gerne jeden Nutzer, der auf dem eBay-Marktplatz unterwegs ist, zu 100 Prozent sicher identifizieren. Nur müssen wir das auf eine Art und Weise realiseren, die dem Geschäftsmodell nicht schadet.

An dieser Stelle kommt der elektronische Personalausweis ins Spiel – wenn er hohe Sicherheit und leichte Handhabung bietet. Aber es gibt noch offene Fragen, beispielsweise: Wird es genug Lesegeräte geben? Sind sie einfach zu bedienen? Wenn Bedingungen wie diese beim elektronischen Personalausweis erfüllt sind – wunderbar, denn dann kann er als wesentlich effizientere Alternative neben das Post-Ident-Verfahren treten, da er genauso sicher, ja vielleicht sogar noch sicherer ist. Wenn er dazu noch einfacher funktioniert, ist er mehr als willkommen. Aber die Anwendung muss einfach sein. Um die freiwillige Nutzung des Verfahrens zu fördern, müsste man einen Anreiz setzen. Man könnte zum Beispiel sagen: Wer sich durch den elektronischen Personalausweis identifiziert, bekommt ein Logo, an dem erkennbar ist, dass er sich identifiziert hat. Das schafft einen Wettbewerbsvorteil. Aber auch mit einem elektronischen Personalausweis sehe ich nicht, dass wir eine solche Verifizierung für alle Nutzer zur Pflicht machen können – selbst wenn in zehn Jahren jeder einen solchen Personalausweis und ein entsprechendes Lesegerät hat. Denn was machen die Ausländer? Was machen Firmen, die sich registrieren wollen? Es gibt Fälle, die einen Zwang zum digitalen Personalausweis nicht klug erscheinen lassen. Es kann deswegen nur über den Anreiz funktionieren: Die Verifizierung muss dem Nutzer einen Vorteil bieten.

Verifizierung ist das eine Thema. Das andere Thema ist die Authentisierung. Der Ablauf ist folgendermaßen: Der Nutzer hat sich registriert. Er kommt wieder. Er loggt sich ein. Wie stelle ich nun sicher, dass derjenige, der sich einloggt, auch wirklich der ist, der er zu sein vorgibt? Heute gibt es zwei Technologien, die das sicherstellen. Die eine ist Standard, nämlich ein Passwort. Sie haben einen Nutzernamen und ein Passwort, mit dem hoffentlich jeder verantwortungsvoll umgeht. Es gibt allerdings immer noch Leute, die mit einem Post-it ihr Passwort an den Computer kleben. Das ist natürlich alles andere als sicher. Wenn man jedoch verantwortungsvoll mit dem Passwort umgeht, bietet es eine gewisse Sicherheit, wenngleich keine absolute. Etwas anderes, das wir seit kurzem anbieten, ist die so genannte Zwei-Faktor-Authentifizierung per Sicherheitsschlüssel. Zwei-Faktor heißt, dass ich über zwei Dinge verfügen muss, um mich einzuloggen: Eines, das ich physisch bei mir habe, und eines in meinem Kopf. Gespeichert habe ich mein Passwort, physisch bei mir ein Gerät. Dieses generiert alle 30 Sekunden einen 6-stelligen Code. Einloggen kann ich mich, indem ich den jeweils aktuellen Code zusammen mit meinem Passwort eingebe. Die beiden voneinander unabhängigen Faktoren bieten doppelte Sicherheit: Verliere ich den Sicherheitsschlüssel, fehlt immer noch mein Passwort. Stiehlt jemand mein Passwort, nutzt ihm das ohne den Code des Sicherheitsschlüssels auch nichts.
Der Sicherheitsschlüssel, den wir anbieten, kostet 4,95 Euro, wobei die Anschaffung von uns subventioniert wird. Das Echo unserer Nutzer auf das Angebot ist sehr positiv und die Nachfrage erheblich. Es gibt offenbar ein großes Interesse an sicheren Verfahren, die wie in diesem Fall vor Identitätsdiebstahl schützen. Anstelle unseres Sicherheitsschlüssels kann eine ähnliche Zwei-Faktor-Authentisierung sicher auch mit Hilfe eines digitalen Personalausweises realisiert werden, wenn dieser über eine Schnittstelle als zu einer Person gehörig identifiziert werden kann. Insofern liegt hier sicher ein weiteres Potential für den neuen Ausweis. Wir sind bereit, weiter in solche Verfahren zu investieren. Auch hier gilt aber wohl: Ohne die Bereitschaft des Kunden, solche Verfahren anzuwenden, wird es nicht gehen.

Und dafür sind aus meiner Sicht zwar auch die damit verbundenen Kosten, vor allem aber die Einfachheit der Nutzung maßgeblich.

Lassen Sie mich zusammenfassen, welche Anforderungen wir an einen elektronischen Personalausweis stellen, damit er interessant werden und aus unserer Sicht funktionieren kann: Zunächst hängt es von der Verbreitung der Lesegeräte ab, die an verschiedenen Orten zur Verfügung stehen müssen, weil ich mich vielleicht heute morgen zuhause, mittags im Büro und abends mobil von unterwegs einloggen will. Auch die Kosten müssen überschaubar bleiben. Und die Verifizierung und Authentisierung müssen für alle potenziellen Nutzer möglich sein – auch Ausländer und juristische Personen. Es gilt zu klären, ob es dafür Lösungen gibt. Wichtig wäre, dass die technischen Spezifikationen frühzeitig verfügbar sind, damit man sich entsprechend darauf einstellen und passende Anwendungen schaffen kann. Internationale Kompatibilität ist für eBay ganz wichtig, denn einen wesentlichen Teil unseres Geschäftsvolumens verbuchen wir international, ja global. Wie aber kann das funktionieren? Gelingt es hier, gemeinsame internationale Standards zu schaffen? Schließlich bleibt die Frage – und das ist aus meiner Sicht der wichtigste Punkt: Wie hoch ist die Wechsel- und Nutzungsbereitschaft der Kunden? Von der hängt letztlich ab, inwiefern wir die Lösung von Problemen bei Identifizierung und Authentisierung vorantreiben können.

6 Anwender-Szenarien im kommunalen Bereich (E-Government)

Hans Peter Heidebach, Landeshauptstadt München

Es gibt 12.504 Gemeinden in Deutschland. Alle werden durch den elektronischen Personalausweis in ihrem E-Government betroffen sein. Zunächst eine Begriffsklärung: Ich lehne mich beim kommunalen E-Government an eine Definition des Bundesministeriums für Wirtschaft und Technologie an, die lautet: Alles Regieren und Verwalten mit Unterstützung der Informations- und Kommunikationstechnologien gehört zu E-Government.

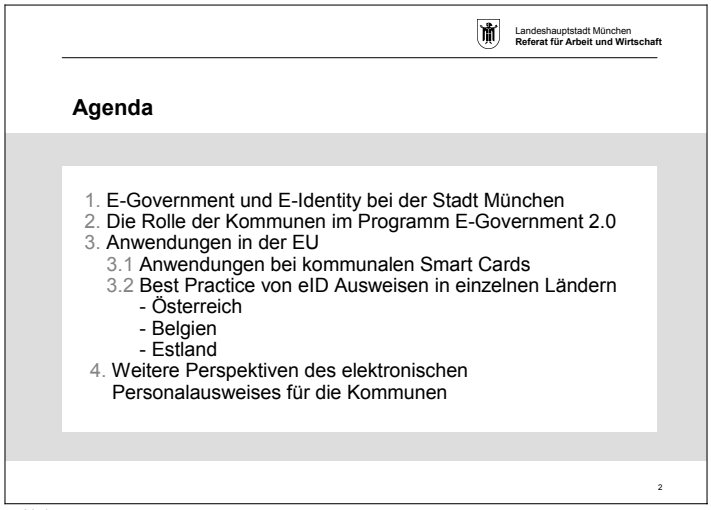

Bild 1

Kurz zu meiner Agenda (Bild 1): Zuerst möchte ich Sie über den Stand der Umsetzung von E-Identity bei den Kommunen am Beispiel der Stadt München informieren, dann geht es um die Bedeutung des neuen Bundesprogramms 'E-Government 2.0' für die Kommunen. Drittens geben die bestehende Smart Card Projekte von europäischen Städten Anregungen zu möglichen Anwendungen für den elektronischen Personalausweis. Außerdem gibt es bereits Erfahrungen mit nationalen elektronischen Ausweisen in anderen Ländern wie Österreich, Belgien und Estland. Und im letzten Punkt ist ein Resümee zu ziehen für die weiteren Anwendungsperspektiven bei den Kommunen in Deutschland.

Derzeit liegt der Schwerpunkt des E-Government bei den meisten Kommunen immer noch auf der Information über Web-Portale. Mit dem Aufkommen der elektronischen Signatur erwarteten damals die Kommunen einen großen Schub hin zur Online-Abwicklung für Transaktionen, die mit Unterschriften verbunden sind. Leider haben sich die Signaturkarten nicht richtig durchgesetzt.

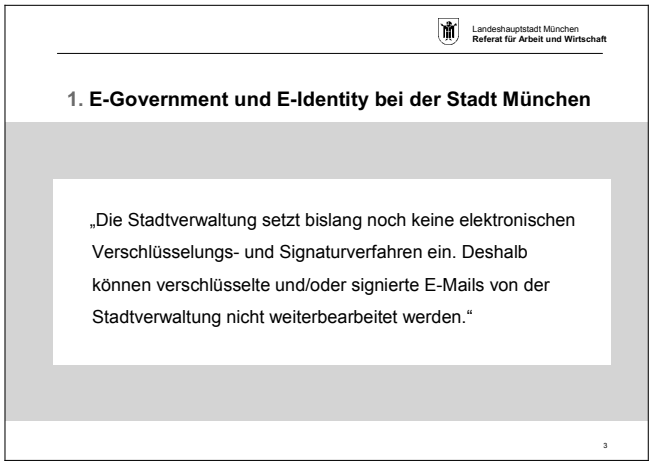

Bild 2

Das in Bild 2 dargestellte Zitat ist aus dem aktuellen München Portal entnommen. Wie fügt sich dieser lapidare Befund über den Münchner Umsetzungsstand in das Gesamtkonzept von E-Government in München ein?

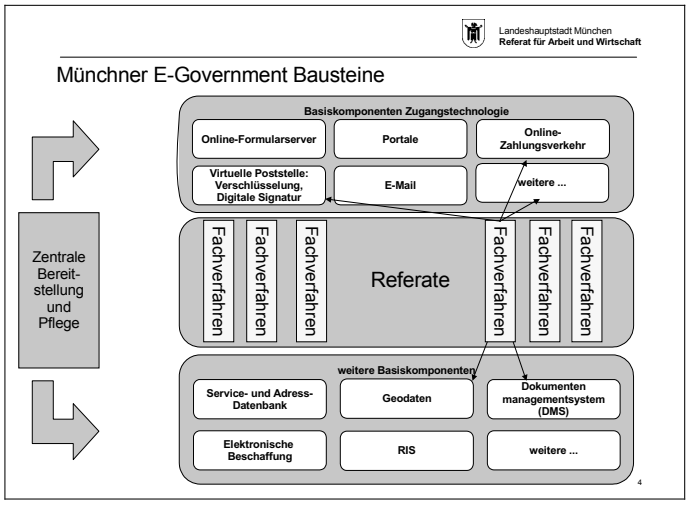

Bild 3

Hierzu folgender Überblick in Bild 3: Dazu ist anzumerken, dass die Signatur mit der virtuellen Poststelle ein Baustein im Aufbau ist, außer einem kleinen internen Pilotprojekt bewegt sich hier noch wenig. Im Aufbau sind auch noch die zentrale Service- und Adressdatenbank, die elektronische Beschaffung und das Dokumenten-Management-System, integriert in einer Lösung für bayerische Kommunen insgesamt. Aktuell hat in München die Umsetzung einer einheitlichen E-Payment-Plattform für die ganze

Stadtverwaltung Priorität. Sie soll endlich den obsoleten Medienbruch bei der Zahlung per Nachnahme für Online - Leistungen beseitigen. RIS bedeutet hier übrigens öffentliches Stadtratsinformationssystem.
Mit dem Stand der Verwendung der elektronischen Signatur dürfte es bei vielen deutschen Städten ähnlich bestellt sein. Außer einzelnen Kartenprojekten, so im Nürnberger Raum die RegioSign Card, hat sich kaum etwas entwickelt.

Man wartet auf bundesweite Anwendungen zur elektronischen Identifizierung und Authentisierung, die alles vorwärts bringen. Doch hat auch der Bund seit Jahren hier Baustellen offen:

- Seit 2004 gibt es Überlegungen, einen **e**lektronischen Personalausweis einzuführen. Das war damals für den März 2007 vorgesehen.
- Dann gibt es das bundesweite Jobcard Projekt. Das Konzept ist seit fünf Jahren in der Diskussion.
- Immer noch müssen die Unternehmen 60 Millionen Einkommensbescheinigungen p. a. in Papierform an andere Stellen, auch an die Kommunen weiterleiten.
- Eine dritte bundesweite Chip-Karte, bei der es stockt, ist die Gesundheitskarte. Sie soll die bestehende Krankenversicherungskarte ersetzen und ihre Einführung war bereits für den 1. Januar 2006 geplant.
- Mit dem neuen Programm E-Government 2.0 des Bundes ist zu hoffen, dass nun ein erfolgreicher Anschub für die Umsetzung dieser Konzepte erfolgt und neue Potentiale erschlossen werden.

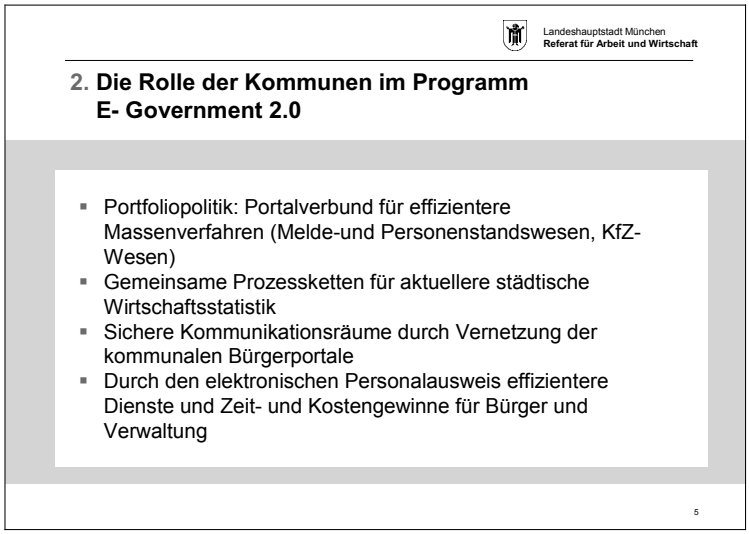

Bild 4

Die Kommunen sind von allen strategischen Zielen dieses Programms betroffen (Bild 4):

In der Portfoliopolitik macht ein Portalverbund Massenverfahren schneller und kostengünstiger. In München z. B. sind bei rund 1,3 Mio. Einwohnern jährlich 165.000 Zu- und Wegzüge zu registrieren, über 13.000 Geburten und 105.000

Neuanmeldungen von Kraftfahrzeugen. Das sind alles Bereiche, die am Front End zum Bürger bei den Kommunen angesiedelt sind. Wobei mancher Bürger natürlich erwartet, dass ihm der traditionelle Weg zur kommunalen Behörde weiterhin auch offen steht.

Bei gemeinsamen Prozessketten können Statistikmeldungen der Unternehmen an die Landesämter und von dort an die städtische Wirtschaftsstatistik, automatisiert ohne Verzögerung zugeleitet werden. Meldedaten müssen weniger redundant gehalten werden.

Für sichere Kommunikationsräume für den Bürger müssen die bestehenden Bürgerportale der Kommunen untereinander vernetzt werden, natürlich auch mit den Landes- und Bundesportalen.

Alle drei genannten Punkte stehen und fallen mit der Einführung einfacher Verfahren für eine sichere elektronische Identifizierung für alle Bürger. Für die Kommunen als vollziehende Behörden gibt es noch keine Ausführungsbestimmungen zu den neuen Personalausweisen in 2008. Man sammelt aber mit den Reisepässen Erfahrung, da müsste die Umstellung ohne größere Schwierigkeiten vonstatten gehen.

Der elektronische Personalausweis eröffnet neben vielen kommerziellen Möglichkeiten auch für die Kommunen und kommunale Unternehmen wie den Stadtwerken schnellere und Kosten sparende Möglichkeiten der Transaktion mit dem Bürger, mit der Wirtschaft und natürlich innerhalb der Verwaltung. Die Jobcard - Funktion, die Steuererklärung, alles lässt sich dann durchgängig elektronisch erledigen.

Im Rahmen des E-Government 2.0 Programms wurde auch das Konzept einer Ausländerkarte vorgestellt, vergleichbar mit dem deutschen elektronischen Personalausweis. Eine derartige Karte würde die Kontrolle der Aufenthaltsberechtigung für beide Seiten deutlich schneller machen und den Aufwand in den Ausländerämtern reduzieren. München z. B. hat derzeit die Akten von über 300.000 nichtdeutschen Einwohnern zu verwalten.

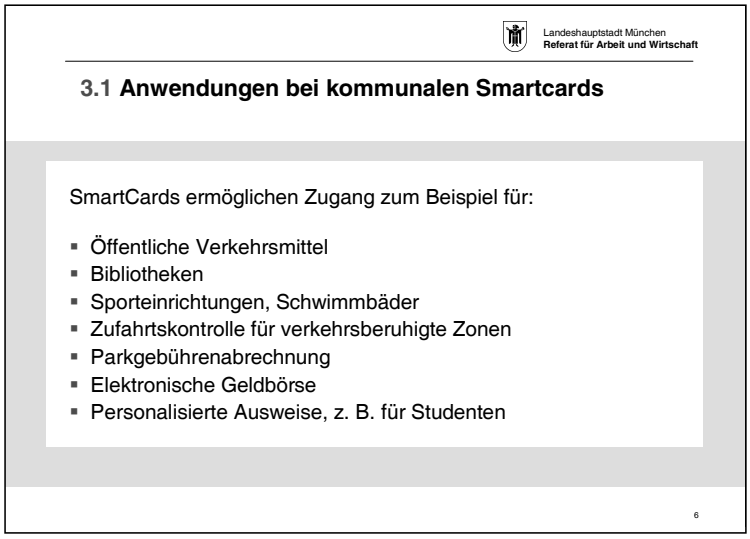

Bild 5

Welche Möglichkeiten bietet der neue Ausweis grundsätzlich noch für die Kommunen (Bild 5)? Hier liefern zunächst Städte Anregungen mit Smartcard-Projekten, die von Hongkong bis Amsterdam bereits umgesetzt sind. Diese Chipkarten werden vor allem für den öffentlichen Verkehr genutzt, für den Eintritt in städtischen Schwimmbädern, Sportstadien, Bibliotheken, für die Zufahrtskontrolle von Anwohnerverkehr in verkehrsberuhigte Zonen, Parkgebührenabrechnung und als personalisierte Ausweis wie den Studentenausweis. Die Karten enthalten in der Regel auch eine elektronische Geldbörse.

In den meisten EU-Ländern laufen inzwischen jedoch Überlegungen für die Einführung nationaler elektronischer ID-Ausweise und es gibt auch mit diesen Ausweisen bereits konkrete Erfahrungen.

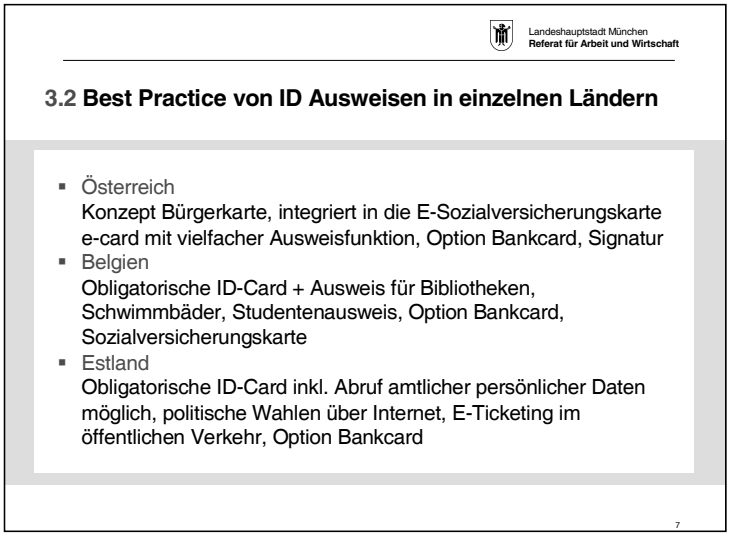

Bild 6

Hier möchte ich beispielhaft auf Österreich, Belgien und Estland eingehen (Bild 6):

> In Österreich wurde 2003 das Konzept Bürgerkarte eingeführt. Die Karte erlaubt zunächst einen sicheren Zugang zu elektronischen Diensten der Behörden. Sie kann auch als besonderer Ausweis dienen z. B. als Beschäftigter des öffentlichen Dienstes, als Parlamentsmitglied oder als Studentenausweis und lässt sich mit einer Bankcard verbinden. Die Funktion der Bürgerkarte ist inzwischen in der neuen eCard, der österreichischen elektronischen Sozialversicherungskarte integriert. Bis Oktober 2006 waren etwa 8,2 Millionen eCards mit Bürgerkartenfunktion herausgegeben, aber nur rd. 8.500 Halter hatten die kostenpflichtige Signatur dazugenommen - so das Fraunhofer Institut für Offene Kommunikationssysteme. Mit einer derartigen Zurückhaltung wird man unter Umständen auch in Deutschland rechnen müssen.

In Belgien wird eine obligatorische e-ID Card bereits seit 2003 herausgegeben. Die Karte enthält elektronische Identifizierungs- und Authentisierungsfunktionen im Chip und optional eine digitale Signatur. Sie kann auch als Ausweis für kommunale Dienste wie Bibliotheken, Schwimmbäder, als Zugangskarte für Gebäude, oder als Studentenausweis eingesetzt werden, mit integrierter Bankkartenfunktion und möglicher Sozialversicherungsfunktion.
Die optionale aber kostenlose Signaturfunktion haben rd. 90 % der Nutzer akzeptiert. Andererseits hat nur ein kleiner Teil der Nutzer ein Lesegerät, sodass man diese Zusatzfunktion nur ungenügend wahrnimmt.

Estland startete bereits 2002 mit der Ausgabe von elektronischen ID cards für Alle. Sie ist in eine Bankcard integrierbar. Man hat damit über ein Bürger-Portal einen Online-Zugang, man kann Online mit den eigenen amtlich gespeicherten Personendaten Formulare abrufen, man kann aber auch einsehen, welche Behörde und für welchen Zweck die persönlichen Daten angefordert hat. Nicht zuletzt kann man mit der Karte auch an Wahlen über Internet teilnehmen. Bei den letzten Kommunalwahlen in 2005 haben nur rund 1 % der Wähler elektronisch gewählt, bei den Parlamentswahlen Anfang dieses Monats waren es immerhin bereits rund 3,5 %. In Tallinn wurde die e-Karte auch an ein Ticketsystem des städtischen öffentlichen Verkehrsverbundes angeschlossen. Die Kontrolle in Bus oder Tram erfolgt durch mobile Lesegeräte. Die e-ticketing Funktion erwies sich als attraktiv. Innerhalb von zwei Monaten votierten dazu über 80.000 Nutzer.

Längerfristig strebt die EU auch eine Konformität der nationalen Personalausweise an. Sie würde das Ummelden des Wohnsitzes von einem EU-Land zu einem anderen erleichtern. Die Arbeitsaufnahme in einem anderen Land wäre ebenfalls erleichtert. Man hätte einen automatischen Transfer der Sozialdaten und den direkten Zugang zum Arbeitsmarkt bei der Arbeitssuche von zu Hause aus.

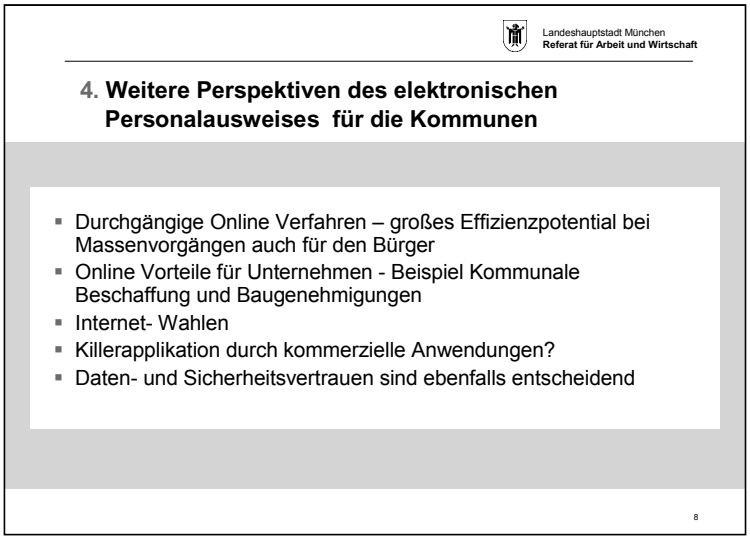

Bild 7

Ich komme zu den weiteren Perspektiven (Bild 7):

Alle massenhaft anfallenden Vorgänge, wie Umzugs- und Wohnungsmeldungen, KfZ-Anmeldungen, das ganze Ausweismeldewesen stellen bei den Kommunen große Potentiale der Rationalisierung dar, wenn durchgängig Online - Transaktionen möglich werden. Für Unternehmen könnte die Signaturfunktion im Beschaffungsbereich besonders nützlich sein und speziell für Bauträger, um zum Beispiel den Stand der Baugenehmigungen verfolgen zu können.

Wahlen, die ja von den Kommunen zu organisieren sind, bedeuten immer einen großen personellen Aufwand. Hier könnten Internet-Wahlen mit elektronischem Personalausweis für eine Entlastung sorgen. Das würde auch schnelle Wahlergebnisse bringen. Wie allerdings das Beispiel Estland zeigt, begegnet dieses Verfahren noch Vorbehalten.

Echte „Killerapplikationen“ des neuen Personalausweises bei den Bürgern dürften sich am ehesten zusammen mit kommerziellen Diensten einstellen. Das E-Ticketing in Tallinn im Verkehrsverbund ist dafür auf kommunaler Ebene ein gutes Beispiel. Jedoch lassen sich Entwicklungen in anderen Ländern nicht ohne weiteres auf Deutschland übertragen. Bei einem elektronischen Personalausweis, wird die gesamte erwachsene Bevölkerung erfasst. Da könnten sich mit der in Deutschland besonders sensiblen Haltung zum Umweltschutz noch stärkere Vorbehalte entwickeln als beim elektronischen Reisepass.

Deutschland liegt in der Umsetzung der Technik in Europa allenfalls im Mittelfeld. Andererseits liegen deutsche Firmen mit der Chipkartentechnologie, mit Verschlüsselungs-, Sicherheits- und Biometrieverfahren sowie der Lesegerätetechnik mit an der Weltspitze. Diese neue Branche muss ihre Innovationsfähigkeit auch auf dem heimischen Markt weiter entwickeln können. Sorgfältige Informationskampagnen sollten anlaufen, damit das Potential des neuen Ausweises für die Bürger, die ganze Wirtschaft und die Verwaltung voll genutzt wird.

7 Diskussion mit weiteren Anwendungsbeispielen und Folgeaktivitäten

Moderation: Prof. Dr. Heinz Thielmann, Heroldsberg und
Prof: Dr. Albrecht Ziemer, Konstanz

Prof. Ziemer:
Wir wollen in den letzten Punkt unseres Abends, die Diskussion, einsteigen. Wir hoffen, dass es nicht nur eine Diskussion ist, die Fragen stellt und beantwortet, sondern wir wollen sie interaktiv dahingehend gestaltet wissen, dass Sie vielleicht auch zu weiteren Anwendungsbeispielen kommen. Vorhin ist uns von eBay gesagt worden, dass es da etwas gibt. Auch die Stadt München hat deutlich gemacht, dass es Anwendungsbeispiele gibt. Also, wenn wir jetzt die Diskussion haben, haben wir auch die Erwartung, dass sich in die Diskussion Phantasie mit einschleicht und mit der Phantasie auch Anwendungsbeispiele genannt werden. Uns ist in den Vorträgen das System des elektronischen Personalausweises vorgestellt worden und wir haben dabei gelernt, dass es eben nicht nur der elektronische Personalausweis ist, sondern dass zu dem elektronischen Personalausweis auch ein Lesegerät gehört. Und nicht nur ein Lesegerät, wie man es sich früher bei der Polizei oder beim Einwohnermeldeamt vorstellt, sondern auch ein Lesegerät zuhause. Letztendlich wird das auch die Basis dafür sein, dass sich die geschäftliche Phantasie für den Einsatz des elektronischen Personalausweises in nicht hoheitlichen Aufgaben entwickeln kann.

Uns ist von Ihnen, Herr Staatssekretär, der staatliche Wille noch einmal deutlich gemacht und unterstrichen worden, dass diese Infrastruktur, die hier geschaffen wird, eben nicht nur für hoheitliche Aufgaben genutzt werden soll, sondern sich ins Geschäftsleben hinein verbreitern soll. Sie haben gesagt, der Staat sei hier in Vorleistung getreten und es ist die Aufgabe derer, die Nichthoheit wollen, dass sie diese Vorleistungen auch für geschäftliche Zwecke nutzen, sie in ihre Geschäftsideen mit einbinden und sie in ihren Geschäftsideen zum Leben erfüllen. Dabei habe ich aus den Vorträgen gespürt, sind es nicht nur Bezahlvorgänge, um die es geht, sondern es sind Sicherheitsvorgänge vielfältiger Art. Immer da, wo Authentifizierung und Identifizierung verlangt wird, Grundlage des Geschäftes ist – eBay hat es noch einmal deutlich gemacht – ist eben ein Einsatz dieses elektronischen Personalausweises zu denken. Wenn man das mit einer Endsumme darstellt, geht es darum, dass Sicherheit im Geschäftsleben gewünscht wird. Aber Sicherheit darf das Geschäftsleben nicht komplizieren, sondern Sicherheit muss das Geschäftsleben schneller und im Alltag lockerer, aber natürlich auch sicherer machen, dauerhaft sicher gestalten und Vertrauen schaffen.

Im Vordergrund der Diskussion steht das Wecken von Phantasie und Gegenstand der Diskussion ist es, mit dieser Phantasie die staatliche Vorleistung zu nutzen. Dazu sind Sie jetzt herzlich aufgefordert, mit Ihren Fragen und mit Ihren Beiträgen zu uns zu stoßen.

Herr Thielmann, Sie wollen jetzt freundlicherweise sozusagen den „Einpeitscher“ übernehmen, damit eine lebhafte Diskussion in Gang kommt.

Prof. Thielmann:
Meine Damen und Herren, bitte melden Sie sich einfach. Es gibt sicher noch Fragen aus den letzten drei Vorträgen. Die Fragen dazu hatten wir ja zurück gestellt. Ansonsten haben Sie sicher einzelne Frage vorgemerkt, und bevor wir lange reden, möchten wir Sie zu Wort kommen lassen.

Herr Lothar Lux, Datev Nürnberg:
Ich bin etwas ratlos, wenn ich hier diese Veranstaltung Revue passieren lasse, weil ich gelernt habe, dass wir eine neue Infrastruktur machen, wieder eine Infrastruktur. Wir haben schon jede Menge Infrastrukturvorleistungen gesehen. Bis jetzt ist eigentlich nichts richtig weiter gegangen. Die Frage, den zweiten Schritt zu tun, eine Infrastruktur auszurollen und dann gleich die Zertifikate mit herauszugeben. Ich weiß nicht, wo jetzt der Unterschied liegt. Ob das Ding jetzt Gesundheitskarte heißt, Jobcard und sonstige Card. Ich sehe da keinen Unterschied und bin deswegen ratlos, was wir jetzt mit dem neuen Personalausweis dann wieder machen, wo denn dann die Geschäftsfelder sind.
Sie sollen es nicht sein lassen, Sie sollen aber auch den zweiten Schritt gehen, weil dann ein Unternehmen davon ausgehen kann, dass die Zertifikate draußen beim Kunden sind. Und dann kann man sich Prozesse überlegen. Dann kann man sich Geschäftsmodelle überlegen, weil es dann eine Zielgruppe gibt. Da meine ich ganz speziell die Zertifikate. Da rede ich überhaupt nicht über die Kartenleser. Der Kartenleser kann ich mir irgendwo bei eBay oder beim Conrad holen. Wer einmal bei der Post war und ein Postidentverfahren durchlaufen hat, weiß, was das für einen Spaß macht. Ich gehe eigentlich hin, hole meinen Personalausweis und bekomme doch wieder nur die Hälfte von dem, was ich eigentlich brauche, und das kann es nicht sein. Sorry, dass ich das ein bisschen überspitzt sage, aber wir sind in dem Geschäft schon seit vier, fünf Jahren. Wir haben unser Trustcenter gehabt. Wir haben es jetzt ausgesourct, weil wir eigentlich keine kommerzielle Anwendung sehen.

Prof. Thielmann:
Vielen Dank, Herr Lux. Sie brauchen sich nicht zu entschuldigen. Es ist sehr gut, wenn wir ein bisschen Würze in die Diskussion hier hineinbringen. Ich denke, das war zunächst mal an die Adresse des BMI gerichtet. Es wurde vorhin gesagt, das BMI wolle die Infrastruktur bereitstellen, aber keine kommerziellen Anwendungen mit finanzieren. Ich möchte eine Frage an die von Herrn Lux anschließen, ob es nicht andere vertrauenswürdige Instanzen gibt außer den Einwohnermeldeämtern, die den Personalausweis mit einem Paket von anderen Angeboten verkaufen können? Herr Schallbruch, bitte.

Herr Schallbruch, BMI:
Wenn Sie von Zertifikaten sprechen, meinen Sie ja Zertifikate für die qualifizierte elektronische Signatur. Zertifikate wird der elektronische Personalausweis in jedem Fall enthalten, wahrscheinlich sogar bis zu 3 verschiedene Zertifikate: Darunter ein Zertifikat für die Authentisierungsfunktion mit der man sich ausweisen kann. Das ist die Funktion eines Personalausweises. Die Funktion einer qualifizierten elektronischen Signatur dagegen ist eine eigenhändige Unterschrift zu ersetzen. Das wiederum wird nicht in jedem Fall beim elektronischen Geschäftsverkehr oder auch bei elektronischen Behördengängen benötigt werden. Herr Groß-Selbeck hat als Beispiel eBay genannt und hat gesagt, dass eBay nicht ein so großes Interesse an der qualifizierten elektronischen Signatur hat, weil die Verträge nicht schriftlich geschlossen werden. Wenn Sie sich das Bund-Online-Dienstleistungsportfolio ansehen, fast 500 Online-Dienstleistungen des Bundes, werden Sie feststellen, dass in diesem Portfolio eine kleine zweistellige Zahl um die 30 Dienstleistungen enthalten sind, die eine eigenhändige Unterschrift benötigen. Bei einer eigenhändigen Unterschrift soll es aber dann natürlich auch eine besondere Leistung sein, nämlich ein Dokument, das eigenhändig unterschrieben ist, soll dauerhaft überprüfbar sein. Da ist die Leistung dahinter, dass man viele Jahre sehen kann, wer das unterschrieben hat.

Das ist aus unserer Sicht eine völlig andere Leistung, eine völlig andere Bedarfslage als das Ausweisen. Der Staat hat nach unserer Auffassung zuförderst die Pflicht, den Menschen eine

Infrastruktur zu bieten, mit denen sie sich authentifizieren, also ausweisen können. Wir wollen mit dem elektronischen Personalausweis auch elektronische Betrügereien verhindern, Phishing verhindern. Wir wollen verhindern, was Sie sich in der polizeilichen Kriminalstatistik im Augenblick sehr genau anschauen können, dass nämlich die Kriminalität im Internet ein einziger großer Identitätsbetrug ist. Die steigenden Kurven sind alles Identitätsbetrügereien. Und da geht es nicht darum, dass jemand Verträge, die schriftlich geschlossen werden müssen, irgendwie unter falschem Namen, mit anderen falschen Zertifikaten oder sonst was schließt, sondern es geht darum, dass die Identität unklar ist. Das sehen wir als die Aufgabe des Staates, hier für Klarheit zu sorgen. Und wir halten es nicht für sinnvoll, dass wir den Bürgerinnen und Bürgern vermeidbare Zusatzkosten, zum Beispiel für die qualifizierte elektronische Signatur, auf die normale Personalausweisgebühr umlegen, die sie nicht unbedingt brauchen. Wir werden im Übrigen aber, wie ja auch die Gesundheitskarte, den Personalausweis so vorbereiten, dass wenigsten die Karte und auch die Technologie für die qualifizierte elektronische Signatur genutzt werden können. Das heißt, auch für die qualifizierte Signatur wird ein Kostenvorteil entstehen, auch wenn der Staat es nicht vorfinanziert und auch nicht den Bürgern auf die Personalausweisgebühren umlegt.

Prof. Thielmann:
Vielen Dank, Herr Schallbruch. Ich denke, wir sind uns alle einig hier im Raum, dass der elektronische Personalausweis als solches kein Diskussionsthema ist und dass es sinnvoll ist, ihn einzuführen und dass er auch in zehn Jahren eine Flächendeckung bringen wird. Die Frage, über die wir heute hier eigentlich diskutieren sollten, ist, wie wir Anwendungen darum herum finden und schaffen können, die sich selbst finanzieren und die die Zielsetzung der Bundesregierung, nämlich der zusätzlichen e-commerce Nutzung zum Selbstgänger machen. Wir wissen alle, dass man Killerapplikationen nicht planen kann, sondern dass sie irgendwann von ungeplanten Ideen kommen. Aber wie können wir Pakte finden, die vielleicht ein Potenzial haben, dass sich andere Anwendungen auf dem Personalausweis realisieren lassen?

Prof. Grimm, Universität Koblenz-Landau:
Ich habe eine Sachfrage in Bezug auf den elektronischen Personalausweis und damit verbunden eine Anregung für eine Anwendung, die sich eher an dem eBay-Modell orientiert. Erst einmal die Sachfrage. Wird der elektronische Personalausweis so ausgerüstet sein, dass er sich ausweisen kann als Karte ohne Signaturfunktion? Die Tatsache, dass dort Zertifikate drauf sind, reicht mir nicht aus für eine entfernte sichere Identifizierung. Im ersten Angang würde man dafür die Signatur einsetzen. Es gibt sicher Möglichkeiten, wie man zusätzliche Merkmale einbringen kann, dass die Karte sich als Karte identifizieren kann. Das ist die Sachfrage.
Jetzt die Anregung. Ich sehe es nicht als gutes allgemeines Geschäftsmodell an, das man nur mit der Karte auftritt und immer mit derselben eindeutigen bürgerlichen Identität sich gegenüber allen in jedem einzelnen Geschäftsmodell neu identifiziert, allein schon aus Datenschutzgründen. Man würde eine ungeheure Masse an Datenspuren erzeugen. Was ich aber als sehr sinnvoll ansehe, so wie wir das vom eBay-Modell her im Grunde genommen als Anregung bekommen haben, ist, dass man sich in einem ersten Schritt gegenüber eBay sicher identifiziert und dass von da ein pseudonymes Modell innerhalb von eBay greift, d.h. die verwalten ihr Identitätsmodell so wie sie das bisher auch gemacht haben, und viele andere Anwender machen das auch. Z.B. auch bei der Deutschen Bahn agiert man innerhalb des virtuellen Systems mit Pseudonymen. Also der allererste Schritt, der erste Identifizierungsschritt ist einer über die bürgerliche Identität und von da an geht es dann mit Pseudonymen weiter.

Prof. Ziemer:
Wer kann darauf antworten? Bitte Herr Helmbrecht.

Dr. Helmbrecht:
Ich glaube Herr Grimm sprach vor allen Dingen die Funktion der Pseudonymität an. Die bietet der Ausweis unmittelbar nicht. Aber der Ausweis bietet Möglichkeiten, durch eine Erstregistrierung, z.B. über einen weiteren Dienstleister, Pseudonyme zu realisieren. Dann kann auf jeden Fall auf seine Identität zugegriffen werden, ohne dass er sie bei einem Standardgeschäft offenbaren muss. Das ist ja auch die Funktion des klassischen Ausweises: Öffnung eines Bankkontos oder eines Versicherungsvertrages, dass man sozusagen in der Erstinitialisierung dann die Identität wirklich klar nachweisen muss und danach bauen sich weitere Geschäftsprozesse auf dieser Funktion auf. Dann ist man im System.

Prof. Grimm:
Ja, so war die Anregung. Da sind wir völlig d'accord, jetzt aber dieser erste Schritt. Wie identifizieren Sie sich mit der Karte ohne die Signaturfunktion?

Dr. Helmbrecht:
Ohne Signaturfunktion? Über ein Authentifikationsverfahren, wo Zertifikate herausgegeben werden über eine Route-Instanz, die dann eine Rückführung auf den Herausgeber des Ausweises ermöglicht.

Prof. Ziemer:
Die nächste Frage, Frau Linde.

Frau Linde:
Zum Beitrag von Herrn Lux folgende Verständnisfrage: Welche Standardausrüstung ist für den elektronischen Personalausweis geplant? Die qualifizierte Signatur wird eine Option darstellen, die der Bürger beantragen kann oder nicht. Unklar ist noch, ob Sie die Authentisierungszertifikate standardmäßig auf jeden elektronischen Personalausweis aufbringen werden mit der dazu gehörigen PIN zur Aktivierung dieses Schlüssels. Aus unserer Sicht kann das Henne-Ei-Problem nur dann gelöst werden, wenn durch die öffentliche Hand die komplette Infrastruktur bereit gestellt wird, damit hierauf die Anwendungen aufsetzen können. Wie sehen Ihre Planungen hierzu aus?

Dr. Helmbrecht:
Dieser zweite Teil, diese Bürgerkartenfunktion soll gerade elektronisch das abbilden, was der klassische Ausweis kann, nämlich die originale Meldeadresse, den Namen und die Adresse des Inhabers auch elektronisch nachzuweisen. Deswegen muss natürlich die Authenfikationsfunktion mit einem entsprechenden Zertifikat von Anfang an auf der Karte sein.

Prof. Ziemer:
Muss und wird.

Herr Mock-Hecker, Dt. Sparkassenverlag:
Ich muss immer wieder feststellen, dass, wenn in irgendwelchen Runden über Signaturen oder Authentifikation gesprochen wird, es dann sehr schnell ziemlich technisch wird. Dies ist eigentlich genau das, was der Nutzer nicht möchte. Wenn Sie heute in ein Auto einsteigen, überlegen Sie sich eigentlich wie Ihr Motormanagement funktioniert? Aber wir diskutieren schon wieder darum, wie er sich denn jetzt genau authentifiziert. Ich würde doch sagen, da

funktioniert. Wir müssen uns auch nicht überlegen, welche Anwendungen, an denen sich jemand authentifizieren kann, es noch zu definieren gilt. Diese Anwendungen werden entstehen, wenn sie sinnvoll sind. Insbesondere dann, wenn die Infrastruktur mit dem Personalausweis einfach ausgerollt wird. Aber man muss sich überlegen, wie wir es für den Nutzer ganz einfach machen diese Infrastruktur zu verwenden, weil sich darüber letztendlich entscheiden wird, ob er sie einsetzt oder nicht.
Dies bedeutet auch, dass er für verschiedene Einsatzzwecke verschieden Karten haben wird. Ich bin der festen Überzeugung, dass er auf Dauer verschiedene Karten haben wird, weil er dann auch einfacher auseinander halten kann für was er welche Karten verwendet. Der nächste Punkt, der dann gelöst werden muss, ist, dass die Infrastruktur die er zu Hause hat, eben der Chipkartenleser, auch tatsächlich die verschiedenen Karten (Bankkarte, Gesundheitskarte, Personalausweis) akzeptiert. Technisch machbar ist alles, nur was kostet es wieder? Also, wir brauchen Einfachheit, Usability, auch bei den Kosten. Es muss einfach billig sein, sonst läuft da nichts. Und deshalb ist es ganz wichtig, dass wir die verschiedenen Projekte Gesundheitskarte, Bankkarten und Personalausweis auf der Chipkartenleserseite zusammenführen. Nicht auf der Kartenseite. Dies würde dazu führen, dass jeder bei jedem mitredet. Das ist nicht der Punkt. Der Punkt ist, wie wir es zusammen dem Nutzer einfach machen, dass, wenn er sich einen Leser kauft, weil er gern irgendeine Authentifikation bei irgendeinem Anbieter, zum Beispiel bei eBay, durchführen will, dass er dann diesen Leser, wenn er sich morgen überlegt, dass er gerne wissen würde, was der Arzt bei ihm alles auf die Gesundheitskarte geschrieben hat, ebenfalls verwenden kann und er sich nicht nochmals ein Chipkartenleser anschaffen muss. Das ist ein ganz kritischer Punkt. Wie machen wir es dem Nutzer ganz einfach an dieser Stelle? Etwas wird durch diesen elektronischen Personalausweis schon sehr einfach: Ich brauche keine Postidentverfahren mehr, um mich irgendwie im Netz zu authentifizieren, weil dies der Personalausweis schon leistet. Aber die andere Seite der Kompatibilität der Karten am Chipkartenleser müssen wir ebenfalls betrachten und das ist wichtiger als darüber nachzudenken welche Authentifikationsverfahren gewählt wurden oder welche Anwendungen wir noch alles brauchen könnten. Diese werden automatisch kommen, wenn wir die Nutzung einfach machen.

Prof. Thielmann:
Vielen Dank, Herr Mock-Hecker, vielleicht können wir das gleich noch einmal diskutieren, nämlich wer muss dafür sorgen, dass wir es einfacher machen? Wie kommen wir dazu? Zunächst Herr Binnebößel, bitte.

Herr Ulrich Binnebößel, Hauptverband des Deutschen Einzelhandels:
Ich möchte ein simples Beispiel bringen über die Begeisterung, die ich empfinde, wenn es zu dem elektronischen Personalausweis kommt. Es ist ja so, Herr Prof. Picot hat es eingangs erwähnt, dass wir uns eine möglichst sichere Identifikation des Kunden zu vertretbaren Kosten wünschen, und ich möchte hinzufügen, in möglichst schneller Art und Weise. Das, habe ich gelernt, wird es geben. Ich komme jetzt zu dem „klassischen Distanzhandel“, also nicht, was man unter Online-Handel oder eBay versteht, sondern die „klassische“ Distanz, also der Bereich über die Theke oder das heutige Kassenband hinweg. Der Einzelhändler kennt ja oftmals gar nicht mehr seinen Kunden. Er hat also eine gewisse Distanz zu ihm. Das verstehen wir heute unter „klassischem Distanzhandel“. Der neue Personalausweis ist geeignet dazu, diese Distanz zu überwinden, d.h. also, der Händler hat durch diesen Personalausweis die Möglichkeit, seinen Kunden kennen zu lernen. Dazu ein klassisches Beispiel: das beliebteste unbare Zahlungsmittel im Einzelhandel ist heute die Lastschrift. Sie kennen es alle, das Bezahlen per Bankkarte und Unterschrift. Bei diesem Zahlungssystem hat der Händler keine Information über den Kunden außer seiner Bankleitzahl und der Kontonummer; er hat auch keine Zahlungsgarantie. Er hat allerdings jetzt mit dem

Personalausweis die Möglichkeit, die Kontaktdaten zu gewinnen und dadurch wiederum auch eine Möglichkeit, diese Zahlung ein Stück sicherer zu machen. Wir können davon ausgehen, dass durch diese zusätzliche Sicherheit auch die Zahlungssysteme generell günstiger werden. Die Alternativen sind Kreditkarten, Electronic Cash und andere, die für den Handel extreme Kosten verursachen. Als Hintergrundinformation dazu: es gibt Branchen im Handel, die eine Umsatzrendite von unter einem Prozent haben. Da sind selbst 0,3% eines Zahlungssystems hohe Kosten, die genau überlegt werden wollen. Und wenn wir jetzt die Möglichkeit haben, eine solche Anwendung mit dem elektronischen Personalausweis zu nutzen, dann können Sie sicher sein, dass der Handel begeistert ist, wenn es solche Möglichkeiten gibt.

NN:
Meine Erfahrung ist, dass Kunden grundsätzlich von sich aus nicht bereit sind, ohne weiteres Daten von sich preiszugeben. Und wenn auch noch die Aussicht besteht, dass er den nächsten Newsletter von seinem freundlichen Händler bekommt, dann erhöht das nicht unbedingt die Bereitschaft. Deswegen habe ich gerade gezuckt, als Sie das sagten, und das hat auch mit Usability zu tun, also dass wir die Hemmschwelle für jeden so niedrig wie möglich machen und ungewollter Zusatznutzen sind da vielleicht eher kontraproduktiv.

Herr Ulrich Binnebößel:
Vielleicht darf ich gerade darauf antworten. Es ist sicherlich richtig, dass es gewisse Hindernisse gibt, die aber auch rechtlich gelöst werden können. Ich bin jetzt gar nicht auf die Möglichkeit eingegangen, Killerapplikationen auf dem Ausweis zu installieren oder den Ausweis für andere Dinge wie z.B. Kundenkarten zu nutzen. Es ist klar, dass auch das Vertrauen natürlich eine große Rolle spielen wird. Ich denke aber, dass wir das als Aufgabe des Handels ansehen können, dieses zu schaffen. Es ist natürlich auch eine Freiwilligkeit gegeben. Die Alternative ist zumindest bei uns im „klassischen Distanzhandel“ das Bargeld, das als Alternative immer noch hoch angesehen wird. Ich denke, dass die Zahlung mit Hilfe des Ausweises eine Möglichkeit wäre, um ein zweites quasi staatliches System neben dem Bargeld zu etablieren und man es durchaus dem Markt oder der Akzeptanz überlassen kann, ob es angenommen wird oder nicht. Ich denke, dass der Handel eine gute Chance haben würde - im Übrigen auch als Alternative zu etablierten Zahlungsmitteln, um eventuelle Kostensteigerungen im Zaum zu halten, die vorstellbar sind, wenn man die Entwicklungen im europäischen Zahlungsraum berücksichtigt, der auch wieder weitere Hindernisse hervorrufen kann. Es klang vorhin schon an, dass Ausländer, aber auch Touristen in Deutschland dann auch die Möglichkeit haben müssten, dieses System nutzen zu können. Aber da ist eine europäische Bürgerkarte, die mit den vorhandenen Schnittstellen auch funktioniert, eine gute Lösung.

Prof. Ziemer:
So richtig nach vorne stützende, strömende Beispiele haben wir bislang noch nicht gehört. Eigentlich haben wir erst einmal wieder aufgearbeitet, was an Bedenken gekommen ist. Herr Lux, Sie haben das angestoßen. Gibt es da nicht einmal die Phantasie, die gekommen ist, dass man sagt: Mensch, wenn wir das haben, fällt uns das und das ein? Eines ist deutlich geworden, dass die Lesegeräte zum einen ein wesentliches Merkmal sind und zum anderen sich nicht nur auf den elektronischen Personalausweis beziehen dürfen, sondern eigentlich alles verarbeiten müssen. Dass man nicht zuhause eine ganze Batterie von den Dingern hat, sondern man will seine Patientendaten und dies und jenes wissen. Das müsste eigentlich von einem Gerät ausgehen.
Aber jetzt wollen wir doch die Zukunft und nicht die Vergangenheitsbewältigung bei uns sehen.

Prof. Alexander Roßnagel, Universität Kassel:
Wir überlegen von der Universität aus, den Personalausweis einzusetzen für universitäre Anwendungen, also Anmeldungen am Rechnerpool oder als Studentenausweis und ähnliche Dinge. Meine Frage ist: Kann man auf den Chip noch weitere Daten privater Anwendungen laden? Wenn das der Fall wäre, wäre das für uns ein Stück leichter, als wenn alles im Hintergrundsystem ablaufen müsste.

Herr Kowalski, BSI:
Man könnte das natürlich können, weitere Daten auf den Chip zu laden. Aber stellen sie sich vor, dass man das für den einen Anwendungsfall machen würde. Dann gäbe es gleich 100 weitere Anwendungsfälle, wo man das machen will. Ich denke, man soll bei dem einen Konzept bleiben, der elektronische, der Bürgerkartenteil des Personalausweises sollte ein Abbild der klassischen Funktion sein, den Bürger mit sehr einfachen überschaubaren Funktionen zu identifizieren. Wir dürfen nicht vergessen, dass der Ausweis eine Lebensdauer von zehn Jahren hat. Man sollte auch dort Funktionen haben, die diese Zeit überdauern können.

Prof. Thielmann.
Die Frage wäre natürlich, ob man einen zweiten Chip auf den Ausweis bringen kann.

Prof. Ziemer:
Oder man könnte sich einen beschreibbaren Bereich vorstellen. Das macht auch ein rechtliches Fass auf. Oder sehe ich das falsch? Ein technisches oder ein rechtliches? Ich sehe auch ein rechtliches; Wettbewerbsverzerrung und was nicht alles da entstehen kann, aber….

Herr Kowalski, BSI:
Ganz kurz einige zusätzliche Daten. Wir haben jetzt auf der CeBit in Hannover einen Stand, wo wir e-Government-Projekte des Bundes gezeigt haben, u. a. auch den elektronischen Reisepass und elektronischen Personalausweis. Und da kamen viele Menschen und haben Fragen gestellt, auch viele junge Leute, die u. a. die Frage gestellt haben, ob man nicht den Speicherplatz auf dem Personalausweis so groß machen könnte, dass man da dann auch Fotos und MP3-Files und solche Dinge abspeichern könnte. Da bräuchte man keinen UBS-Stick. Wir haben dann diese Frage andiskutiert und es tun sich in der Tat da auch ein paar rechtliche Fragen auf. Weil sich da natürlich sofort die Frage der Haftung und was mit diesen Daten ist stellt usw. Und es tut sich zusätzlich auch wiederum die Frage des Vertrauens auf. Wir haben jetzt eine Diskussion beim elektronischen Reisepass darüber erlebt, dass dieser Pass kontaktlos auslesbar ist, wer unter welchen Umständen mit was für Berechtigungen usw. diesen Pass auslesen. Allein wegen der Tatsache, dass er kontaktlos auslesbar ist, werden diese Fragen gestellt. Wenn wir das auf den Personalausweis übertragen, würde ich prophezeien, dass allein wegen der Tatsache, dass wir einen beschreibbaren zusätzlichen Speicherplatz irgendwo auf diesem Personalausweis haben, eine ähnlich gelagerte Diskussion bekommen, ob denn die Daten im Personalausweis dann nicht auch überschrieben werden können. Deshalb muss man da sehr genau darüber nachdenken. Es ist technisch grundsätzlich natürlich möglich.

Prof. Thielmann:
Diese Frage ruft die Rechtsexperten auf den Plan. Prof. Roßnagel hat dazu sicher eine kompetente Antwort. Bitte Herr Roßnagel.

Prof. Roßnagel:
Ja, meine zweite Frage betrifft die Aufgaben des Staates in dem Kontext. Herr Schallbruch hat zu Recht darauf hingewiesen, dass der Staat hier die Aufgabe hat, ein Authentisierungsmittel zur Verfügung zu stellen. Ich würde das gern ergänzen um die Feststellung, dass der Staat auch die Aufgabe hat, dem Bürger die Möglichkeit zu geben, beweissichere Dokumente zu erstellen, auch elektronisch. In der Rechtsprechung hat sich gerade an eBay-Fällen in den letzten Jahren eine Meinung herausgebildet, dass der Nachweis einer Willenserklärung elektronisch mit Passwort allein nicht ausreicht – dadurch entsteht kein nachweissicheres Dokument –, sondern dass hier die elektronische Signatur genau das richtige Mittel ist. Wenn Sie sich überlegen, wie oft Sie unterschreiben, dann sind höchstens 5% der Unterschriften, die Sie tagtäglich geben, rechtlich verpflichtend. 95% der Unterschriften geben Sie ausschließlich deswegen, weil Sie dem Gegenüber ein verlässliches Beweismittel geben wollen. Und deswegen ist die elektronische Signatur so wichtig. Nicht, weil wir so viele unterschriftspflichtige Dokumente haben, die wir ersetzen wollen, sondern weil wir im elektronischen Bereich die gleiche Rechtssicherheit in Form von Beweissicherheit haben wollen.
Wenn wir die elektronische Signatur über den Personalausweis verbreiten wollen, ist das ein sehr hilfreiches, nützliches Mittel. Aber allein die Infrastruktur reicht nicht, es ist schon mehrfach darauf hingewiesen worden. Wir brauchen auch Anwendungen dafür. Ich will nur darauf hinweisen, dass wenn wir zum Beispiel für das Handelsregister und das Unternehmensregister vorgesehen hätten, dass nicht nur die Anmeldungen durch die Notare, sondern auch die jährlichen Berichte, die man dorthin schicken muss, signiert sein müssten, dann hätten wir auf einen Schlag in allen Unternehmen der Bundesrepublik elektronische Signaturverfahren zur Verfügung. Würden wir die monatliche Umsatzsteuererklärung mit elektronischer Signatur fordern, würden auch alle Unternehmen entsprechende Signaturen haben. Die Kosten für diese sind vergleichbar gering. Und wir hätten die Skaleneffekte, die wir jetzt haben wollen. Also, der elektronische Personalausweis und solche ähnlichen Anwendungen – das zusammen bringt tatsächlich die Lösung, dass die elektronische Signatur in die Fläche kommt und dass sie entsprechend genutzt werden können. Ansonsten befürchte ich, dass wir genau solche Ergebnisse bekommen, wie sie von Österreich geschildert wurden, 3 Millionen Karten, aber nur 8.500 Zertifikate. Das wäre ein ungutes Verhältnis, wenn wir das erreichen würden.

Staatssekretär Hahlen:
Herr Roßnagel, im Grundsatz bin ich ganz bei Ihnen, wenn Sie darauf hinweisen, dass die handschriftliche Unterschrift bei uns im Alltagsleben diese ganz unterschiedlichen Funktionen hat und man von daher in der Tat darüber nachdenken sollte, dass wir diese unterschiedlichen Funktionen dann auch im Internet und im eCommerce und überhaupt in dem Verkehr über diese elektronischen Mittel, vielleicht so haben sollten. Ich gehe aber nicht so weit zusagen, dass man die qualifizierte elektronische Signatur auf dem Ausweis braucht, sondern ich bin der Auffassung, dass wir durch die Möglichkeit der Authentifizierung, und zwar der sicheren und verlässlichen Authentifizierung schon einen Durchbruch bekommen. Damit ist das eigene Handeln im Internet gegenüber dem Distanzpartner, wer das auch immer ist, sei es der Geschäftsmann, sei des der Privatmann, von einer ganz anderen Qualität als jetzt. Das ist nahezu so, als wenn Sie wirklich zum Einzelhändler an die Theke gehen und ihm gegenüber stehen. Da ist nun auf der einen Seite ist der Herr Roßnagel und auf der anderen Seite ist der Herr Hahlen. Beide wissen, dass das der eine und das der andere ist. Das ist schon ein himmelweiter Unterschied zum jetzigen Zustand im Internet, und von daher glaube ich, dass das der entscheidende Durchbruch ist. Es mag sein und ich hoffe das auch, dass wir auf diese Weise die qualifizierte elektronische Signatur nach vorne bringen. Das ist überhaupt keine Frage. Aber zum Beispiel, was Sie gesagt haben, bei der Gewerbe- oder

vorzuschreiben, hielte ich für ein Übermaß. Seien wir froh, dass wir das nicht vorgeschrieben haben. Wir neigen sonst in Deutschland immer dazu, perfektionistisch zu sein, und ich finde es immer am putzigsten, wenn man Briefe bekommt, wo man unterschreiben und noch einen Stempel daneben drücken muss. Das ist der Bürokratismus in Deutschland, wo man denkt, dass es mit einem Gummistempel daneben noch „besonders" unterschrieben ist. Lassen Sie uns nicht diesen Weg gehen. Ich bin der Überzeugung, dass wir durch die sichere Authentifizierung schon den Durchbruch bekommen.

Herr Chiachiarella, Gesamtverband der Deutschen Versicherungswirtschaft:
Ich wollte einen weiteren Aspekt in die Diskussion um die Lesekartengeräte einbringen. Selbstverständlich ist es im Bereich von Internet- oder Direktversicherungen erforderlich, dass Interessenten und Kunden eine entsprechende Lesekartengeräteinfrastruktur nutzen können und im Zugriff haben.
Sie alle kennen den Versicherungsberater, der heute schon mit einem modernen Laptop ausgestattet zu Ihnen nach Hause kommt und Sie dort vor Ort mit technischer Unterstützung eingehend berät. Unser Wunsch ist, dass der geplante elektronische Personalausweis dort auch für Geschäftprozesse eingesetzt werden kann, und zwar ohne dass durch die heute noch bestehenden papiergebundenen Verfahren Medienbrüche entstehen. Sollte dies möglich werden, so überlegt die Versicherungswirtschaft sicherlich sehr konkret, ob und inwieweit die Außendienstmitarbeiter neben den Laptops mit moderner Kommunikationstechnologie auch mit entsprechender Lesekarteninfrastruktur ausgestattet werden. Damit könnten wir die erforderliche Infrastruktur nicht nur zum Kunden bringen, sondern ihm auch den Umgang mit den modernen Möglichkeiten erläutern. Ob und inwieweit das letztendlich technisch und rechtlich abgesichert durchgeführt werden kann, muss selbstverständlich noch intensiv diskutiert und abgeklärt werden.
Allerdings kann man doch zum jetzigen Zeitpunkt bereits fragend feststellen, dass wenn der Gesetzgeber sagt, dass für die Abgabe der Steuererklärung die Authentisierungsfunktion des Personalausweises ausreicht, warum dies bei E-Business-Anwendungen nicht ähnlich sein sollte? Daher auch das Angebot aus der Versicherungswirtschaft, den neuen elektronischen Personalausweis an den Stellen auch einzusetzen, an denen uns das zur Geschäftsprozessunterstützung möglich ist.
Wir sind der Auffassung, dass 1,5 bis 1,7 eGovernment-Anwendungen pro Jahr und Bürger alleine nicht ausreichen, um eine wirkliche Akzeptanz bei der Bevölkerung zur flächendeckenden Nutzung des ePA zu erreichen und halten daher den Ansatz der Verwendung des ePA für E-Businessprozesse für zielführend. Sicherlich gibt es auch heute Abend noch viele Dinge und Argumente, die gegen das sprechen, was ich hier vorgetragen habe. Aber gerade daher halte ich es für richtig und wichtig über vernünftige Visionen zu sprechen, wie wir alle gemeinsam den Wirtschaftsstandort Deutschland nicht nur erhalten sondern zielgerichtet fördern und ausbauen können. Die Hindernisse die dabei bestehen müssen natürlich nicht nur einfach aus dem Weg geräumt werden, es müssen vielmehr sichere und alle Interessen wahrende Lösungen gefunden werden. Diese allerdings müssen konstruktiv sein. Lassen Sie mich mit folgender Bemerkung schließen: Ich finde es ganz positiv, dass die Bundesregierung hier eine flächendeckende Infrastruktur bereitstellen wird, die sich vom Grundsatz her für die Verwendung von eGovernment und E-Businesslösungen anbietet. Zu diesem Thema stehen wir auch im engen Dialog mit dem BMI und werden diesen auch konstruktiv fortführen, um hier gemeinsam eine weitere Erfolgsgeschichte für Deutschland zu gestalten.

Prof. Picot:
Herr Groß-Selbeck hat uns vorhin berichtet, dass 20 Millionen Menschen in Deutschland eBay nutzen, mehr oder weniger häufig, und dass Verifizierung benötigt wird. Wenn der

elektronische Personalausweis nun eingeführt wird und eBay würde den Kunden sagen, wenn Sie sich bei uns über den elektronischen Personalausweis identifizieren lassen, dann haben Sie irgendwelche Vorteile, was auch immer das sein mag. Auf diese Weise könnten die zehn Jahre Einführungszeit verkürzt werden. Wenn dann von den 20 Millionen fünf Millionen sofort den ePA haben wollten, was passiert dann? Ist das administrativ machbar? Ist das von der Industrie zu schaffen? Sind Hersteller und Standardisierung in der Lage, ein Standardlesegerät in einer relativ überschaubaren Zeit für die Endgeräte in den zu bringen? Wir haben zwei Lesegerätetypen gesehen, die an einer Leine hängen. Das kann ja allenfalls eine erste Lösung sein. Sehr bald muss im Notebook, im PDA, oder in welchem Endgerät auch immer, eine integrierte Lesekomponente verfügbar sein. Was muss passieren, damit wir dahin kommen? Das ist zudem ja auch eine internationale Frage.

NN:
Wir haben bis jetzt einen Personalausweis mit visuellen Merkmalen. Wir befinden uns in einer Welt, die sich sehr stark auch außer dem Visuellen in der realen Welt sich weiter in die virtuelle Welt entwickelt. Dafür ist der neue elektronische Personalausweis gedacht, dass er diese Welt mit abdeckt. Da haben wir heute Abend erstens gehört, dass er in dieser Funktion das sein soll, was wir heute im elektronischen Reisepass haben. Das soll auch mit abgedeckt werden, weil wir dieses Dokument auch als Reisedokument verwenden. Zweitens haben wir gehört, dass wir eine Art Bürgerzertifikat haben wollen, damit wir uns in dieser virtuellen Welt, von der ich eben gesprochen habe, auch klar unsere Identität authentifizieren können, was ich für sehr wesentlich halte. Wir sind zukünftig in der Lage, wirklich zu sagen, dass es der Kunz und das ist der Hinz. Wenn ich mich beispielsweise bei eBay einklinke, weiß ich wirklich, dass Sie bei eBay sind, und sie holen sich über ein Trustcenter ein Zertifikat, damit auch sozusagen diese Kommunikation aufgebaut werden kann. Wir haben auf der CeBit auch eine entsprechende Präsentation gehabt, wo wir dargestellt haben, wie einfach so etwas letzten Endes für den Bürger geht. Da bin ich bei Ihnen. Es muss „keep it simple and stupid“ auch von der wirklichen Praktikabilität für den Bürger sein.
Jetzt komme ich zum dritten Thema. Natürlich wird diese Karte auch darüber hinaus eine Thematik abdecken können, die wir unter digitaler Signatur mit dem entsprechenden Gesetz im Hintergrund haben. Aber das brauchen wir nur für eine ganz bestimmte Art von Rechtsgeschäft, wo wirklich diese Signatur da ist.
Jetzt komme ich zu Ihrer Frage. Ich benutze ein kleines Gerät in meinem Laptop seit ungefähr viereinhalb Jahren, wo ich beispielsweise meinen ganzen Email-Verkehr über ein Virtual Private Network in der Firma mache. Das gibt es schon seit Jahren. Das kostet 15 oder 12 Euro. Wir haben auch entsprechende Hybridkartenleser. Wir wissen ja heute noch nicht, ob der elektronische Personalausweis kontaktlos sein wird oder nicht. Aber es gibt diese Hardware bereits, und die ist auch nicht so teuer. Wir brauchen für diese Art von Lesegeräten auch nicht die Klassifikation 3, die ich beispielsweise bei digitaler Signatur brauche, weil die sehr viel teurer sind. Ich denke, das ist schon auf dem Markt und ist auch erschwinglich. So etwas kostet vielleicht zum Schluss wenn die Menge stimmt, 20 oder 25 Euro, ein Hybridkartenleser. Das heißt, es ist da.
Und jetzt komme ich zum Schluss noch einmal zu den Applikationen. In dem Moment, wo wirklich diese Authentifizierung der Identität in der virtuellen Welt auch möglich sein wird, bin ich überzeugt davon, was sie auch gesagt haben in Ihrem speziellen Fall, dass die Applikationen wirklich fast von selber kommen. Diese Applikationen für die entsprechenden Signaturgeschäfte sind relativ limitiert und bleiben auch relativ limitiert. Aber was wir unbedingt brauchen, ist, dass wir uns zukünftig in der virtuellen Welt auch wirklich identifizieren können und wirklich eine Authentizität dahinter haben.

Herr Robert Schneider, SCM:
Wir sind im Geschäft dieser Lesegeräte weltweit tätig. Es ist ein mühsames Geschäft, und im Gegensatz zu den Smartcard-Herstellern haben wir den Nachteil, dass die Geräte keiner kaufen will, sondern das das immer der Konsument, der Endanwender, machen soll. Das ist natürlich ein schwieriges Geschäft. Wenn Sie eine Smartcard beim Endanwender in den Markt bringen wollen, ist es natürlich ein Vielfaches der Kosten. Am einfachsten sind natürlich die Infrastrukturkosten, wenn sie ein Bundle machen, d.h. Sie verkaufen es mit der Smartcard. Das wäre natürlich die billigste Methode, weil man auch sofort die Stückzahlen definieren kann, und nur so bekommt man die Preise runter. Der erste große Durchbruch der Smartcardleser, dieser Klasse 1, ganz einfach ein kontaktbehafteter Leser übrigens, kam aus den USA von der Regierung, dem Department of Defence. Die haben 4 Millionen Leute mit einer ID-Card ausgerüstet und 2 Millionen Leser. Diese Leser sind dann von 25 Dollar auf heute 10 Dollar Verkaufspreis gesunken. Es gibt aber kein weiteres Projekt, und man braucht wirklich Projekte in dieser Größenordnung, damit man die Kosten runter bringt.
Einfach zu sagen, jeder bekommt diese Karte, die im Prinzip ja auch ein paar Dollar oder Euro kostet, aber der Leser wird irgendwo schon gekauft und irgendwo gibt es die Killerapplikation. Das wäre natürlich schön, wenn die Killerapplikation da wäre, das heißt der Konsument sagt, dass es ihm egal ist, ob er 30 Dollar ausgebe. Das ist auch die Lösung und ist hier natürlich die Gretchenfrage. Wenn es die gibt, ist der Konsument gern bereit. Was sind denn 30 Dollar für den Konsumenten, die er ausgibt in fünf Jahren? Gar nichts. Das ist doch kein Betrag. Aber warum soll er sie ausgeben? Wenn hier die Regierung oder die großen Applikationen, eBay gehört inzwischen auch dazu, eine Forderung hat, wird das einfach passieren.

NN:
Aber ich möchte sicher ein, dass ich mit irgendjemand kommunizieren kann. Ich glaub in der Zukunft, das wird nicht morgen sein. Die Zukunft wird sein, dass wir mehr Sicherheit brauchen, soviel wie in großen Unternehmen mit großen Netzwerken relativ wenig auf Sicherheit geachtet wird. Und ich sage voraus, wir werden in der Zukunft mehr und mehr solche Angriffe haben. Natürlich muss man andere Technologien haben, aber in summa möchte jeder, wenn er ins Internet geht, eine gewisse Sicherheit haben. Ich glaube, das wird kommen. Ich gebe Ihnen Recht, das ist ein Prozess, der seine Zeit braucht, aber dieses wird kommen. Und dafür brauchen wir eine grundlegende Basis. Diese Basis ist für mich zum Beispiel ein sicherer Ausweis, der die Identität bewahrt.

Herr Kowalski:
Das ist sicherlich ein erster ganz wichtiger Schritt. Was ich noch sagen wollte: Die kontaktlose Technologie hinkt natürlich schon fünf bis zehn Jahre hinterher von den Kostenreduzierungen, auch beim Leser. Das heißt, ein kontaktloser Leser ist heute Faktor 3 der Herstellkosten wie ein kontakbehafteter Leser. Das muss man natürlich auch noch berücksichtigen. Heute einen kontaktlosen Leser unter 40 Euro zum Endanwender zu bringen, ist fast nicht möglich. Natürlich kostet er in der Herstellung 13 Euro. Aber bis er natürlich irgendwo in einem Retailkanal steht, muss ja jeder etwas damit verdienen. Das ist natürlich auch noch einen ganz schöne Hürde, und diese Infrastrukturkosten darf man nicht unterschätzen. Wir sind eben da noch nicht am Ziel.

NN:
Wir haben in dem Zusammenhang überlegt, was machen wir heute möglichst schnell, um zu einem kontaktlosen Leser zu einem Preis von 10 Euro zu kommen? Als wir da saßen, kam noch ein Vertreter vom VDV dazu, der gerade in Korea gewesen war und ein USB-ähnliches

also unter unserem Preis. Es ist ganz einfach; Asiaten sind wesentlich experimentierfreudiger. Das Ganze war aus irgendwelchen Gründen nicht richtig sicher, aber es hat zumindest funktioniert, und die Token hatten eben nicht das Format einer Checkkarte, sondern waren rund. Das ist genau der Punkt. Die kontaktlose Technik eröffnet ganz neue Möglichkeiten. Wir werden in fünf Jahren eben nicht mehr PC Desktops haben, wo wir dann große Leser daneben stellen, sondern wir haben mobile Geräte, mit denen wir alle diese Geschäfte machen wollen. Und da passt kein herkömmliches Format. Sie müssen einfach nahtfrei arbeiten können. Das wird auch die Lesertechnik revolutionieren, denn RFID ist eben nicht nur dazu in der Lage, Chipkarten zu lesen, sondern auch Kommunikation mit ganz anderen Endgeräten zu betreiben. Zum Beispiel waren die Compact Flash Leser von Anfang an wegen der Verbreitung der Fotoapparate für neun oder zwölf Euro im Markt und auch relativ aufwendig herzustellen. Bei dem kontaktlosen Leser gibt es nur einen einzigen Chip. Der Philips-Vertreter auf unserem Stand wollte wissen, welche Firma den Chip für den koreanischen Leser geliefert hat, das war ein Philips-Chip.

Prof. Thielmann:
Jetzt haben wir noch Herrn Mock-Hecker und dann Herrn Roßnagel.

Herr Mock-Hecker:
Zur Leserinfrastruktur: Dies ist genau der Punkt, man möchte gerne einen einfachen Leser haben, der im Notebook steckt und dann läuft mit einer Karte alles was man braucht. So eine Karte verwenden wir auch als Mitarbeiterkarte im DSV. Man steckt die Karte in ein Notebook, gibt die PIN ein und man authentifiziert sich automatisch an allen Anwendungen. Nur geht das nicht beim Homebanking, weil niemand weiß wie der Rechner beim Kunden zuhause aussieht, konkret: wie sicher er ist. Wenn der Kunde die PIN über die Rechner-Tastatur eingibt, Herr Kowalski, Sie wissen das auch, kann diese irgendwo ganz anders landen als man denkt. Das ist ein Problem, wenn man einfache Leser verwendet. Wenn man sich sicher authentifizieren will, benötigt man gleich die nächste Stufe, Klasse 2. Hierfür braucht man eine Tastatur, die vielleicht nicht in den beschriebenen Token hineinpasst. Wenn man aber Sicherheit haben will kostet dies mehr Geld. Das ist die eine Seite. Die andere Seite, die positive Nachricht ist, dass die Sparkassen schon eine Menge Karten im Feld haben. Natürlich ist unser Online-Banking sehr sicher, aber auch wir sehen, dass der Sicherheitswunsch unserer Kunden steigt und wir auf Dauer ein Maximum an Sicherheit bieten wollen. Auch wir sind daran interessiert Leser, in diesem Fall Klasse 2, zusammen mit unseren Karten ins Feld zu bringen. Wir können zum Beispiel das Thema Online-Banking mit Lesern bundeln und dabei stellt sich die Frage, ob man dieses Bundle nicht gleich als Teil eines Konto-Package vermarktet. Muss der Kunde für den Leser gleich 80, 50 oder 40 € zahlen oder er bekommt ein Konto-Package angeboten, das diesen Leser für einige Cent mehr im Monat beinhaltet. Somit kann sehr wohl, insbesondere wenn wir uns da abstimmen, eine sichere Leserinfrastruktur entstehen, die erheblich größer ist als die aktuelle. Wir haben heute immerhin in der Sparkassen Finanzgruppe 9 Mio. Online-Banking Kunden.

Prof. Thielmann:
Das sind nicht die gleichen wie beim e-commerce, z.B. eBay?

Herr Mock-Hecker:
Doch. Auch da kann man dann wieder zusammenarbeiten, um das letztendlich hinzubekommen. Wir müssen zusammenarbeiten, und zwar nicht in Arbeitskreisen zum Spezifizieren, sondern in Arbeitskreisen, um bestimmte Dinge in die Welt zu setzen. Dort müssten wir loslaufen.

Prof. Roßnagel:
Ich wollte ganz kurz auf Herrn Hahlen reagieren. Es ist ein ganz großer Vorteil und Fortschritt, wenn wir Identifizierung haben, die über das Internet möglich ist, die sicher ist. Das ist ohne jeden Zweifel. Die andere Frage ist aber, ob ich denn mit der Identifizierung auch ein Dokument sicher machen kann. Und da muss ich sagen, dass das nicht der Fall ist. Also, ich identifiziere mich irgendwo, aber das heißt noch lange nicht, dass das Dokument danach dann unveränderlich ist. Es ist veränderlich, und wenn ich das vor Gericht vorlege, ist es kein taugliches Beweismittel. Ich brauche einfach die qualifizierte Signatur, um ein Dokument überprüfen zu können. Und Sie hatten in Ihrem Eingangsvortrag auch darauf hingewiesen, dass der elektronische Ausweis ein Mittel sein soll, um die elektronische Signatur in den Markt zubringen. Ich finde es ganz hervorragend, dass das jetzt versucht wird und ich wollte nur darauf hinweisen, dass man dafür dann auch Anwendungen braucht, damit am Schluss es nicht nur ganz wenige sind, die das hobbymäßig nutzen.
Noch ein kurzer Hinweis. Wir haben auch eine entsprechende Regelung in unseren Prozessordnungen, die qualifizierte Signaturen entsprechend beweissicher machen. Das ist bei allen anderen Sicherungsmitteln nicht der Fall, ausschließlich bei der qualifizierten Signatur.

Dr. Groß-Selbeck:
Sie wollten noch ein positives Statement. Eine gute Nachricht ist, dass wir wissen, dass Konsumenten prinzipiell bereit sind, für mehr Sicherheit auch mehr zu bezahlen Das kann man messen. Das kann man sehen. Es ist ja alles transparent, und im Internet gibt es diese Preisvergleiche, die Ihnen ein Produkt von zehn verschiedenen Händlern zeigen. Da können Sie genau sehen, dass die Preisunterschiede erheblich sind. Und die Zahlen zeigen, dass die Leute nicht immer das Billigste nehmen, sondern sie nehmen das, wo sie den besten Mix haben aus vernünftigem Preis und Sicherheit. Seriosität, vor allem auch die Marke des Händlers spielt eine große Rolle, weil eine Marke ein Sicherheitsgefühl gibt. Die Leute sind durchaus bereit, eine Prämie für mehr Sicherheit zu bezahlen Da bin ich sehr bei meinem Vorredner. Wie können wir es denn schaffen, und das schaffen wir wahrscheinlich nur gemeinsam, etwas zu machen, was den Konsumenten anspricht. Ein Lesegerät für 30 Euro ist per se nicht so wahnsinnig schmackhaft. Wenn ich es aber schaffe, daraus ein Paket zu schnüren, ein Paket, das einen Bankenaspekt hat und vielleicht einen eBay-Aspekt und noch ein paar andere Aspekte von großen Anwendungen,, kann daraus vielleicht etwas werden. Der Konsument findet das interessant und ist auch bereit, dafür etwas zu zahlen. Im Moment vermarkten wir diesen eBay spezifischen Token eben als eine Krücke. Den subventionieren wir. Wir verkaufen den für 4,95 €. Die Warenkosten liegen wesentlich höher. Sie sehen, es gibt eine Bereitschaft der Kunden 4,95 zu zahlen. Es gibt eine Bereitschaft von uns, da zu investieren. Da kann man sich schon etwas ausdenken. Und wenn Sie die großen Zahlen haben, wie 9 Millionen Bankkunden und 20 Millionen eBay-Kunden, kann man wahrscheinlich daraus etwas stricken, was die Kunden auch überzeugt und daraus entsprechend ein Paket wird.

Frau Linde:
Eigentlich nur eine kleine Ergänzung zu dem, was Herr Mock-Hecker gesagt hat, damit nicht ein Gerücht im Raum stehen bleibt. Es ist möglicherweise die Strategie der Sparkassen, hier ein Kontopackage zu machen. Es ist aber mitnichten die Strategie der Kreditwirtschaft. Im Bereich der privaten Banken gibt es mindestens 9 Millionen Online-Kunden. Ich glaube, durchaus mehr; in der gesamten Kreditwirtschaft haben wir je nach Statistik an die 33 bzw. 37 Millionen. Es ist eben tatsächlich so, dass die Kosten für den Kartenleser nach wie vor ein Showstopper sind, um hier auch wirklich die Chipkarte als Authentifikationsverfahren im Online-Banking einzusetzen. Zumindest bei unseren Mitgliedsinstituten ist das nach wie vor eine Sorge, und das wollte ich hier noch einmal sagen.

NN:
Lassen Sie mich vielleicht auch noch ein positives Wort sagen, mit sehr viel Anstrengung eine vielleicht nicht optimale Lösung zu finden, aber wir müssen uns einfach mal dazu durchringen, eine Lösung zu haben. Auch als Vertreter der Branche aus Hochsicherheitsbereichen habe ich Einiges erlebt, auch im Bereich der Kartenleser. Herr Mock-Hecker, Sie kennen das, dass wir versuchen, gerade auch mit Lösungen, die aus dem Hochsicherheitsbereich kommen, nämlich mit Virtualisierungstechnik, Kosten massiv reduzieren zu können. Wir glauben wirklich, dass man mit Virtualisierungstechnik so etwas wirklich Card3-Leser auf den Preis von Card1 reduzieren kann. Da sind wir sehr sicher, und da wird früher oder später auch die Bundesnetzagentur mitmachen und so etwas erkennen. Wir sollten auch nicht diese Sicherheit – das haben wir auch früher schon mit Herrn Rossnagel diskutiert – der elektronischen Signatur dann hinterher auf die Sicherheit der PIN Eingabe zurückführen, denn da steckt wesentlich mehr Sicherheit dahinter. Das ist genau die Authentisierung, um es jetzt nicht zu technisch zu machen.
Wir haben früher Kartenleser gehabt, die 1300 DM kosteten. Da haben wir versucht, digitale Signatursysteme einzuführen und fanden diese Summe ganz interessant für den Bürger und dachten, dass das jeder zweite kaufen wird. Heute diskutieren wir, dass wahrscheinlich keiner 30 Euro für einen Card3-Leser ausgeben wird und dass da die Infrastrukturkosten zu hoch sind. Da muss noch ein bisschen Zeit ins Land gehen lassen und da müssen sich noch einige Dinge von selbst einwickeln. Die entwickeln sich. Ich war seinerzeit dabei, als man http und html spezifiziert hat. Die Weiterarbeit wurde mehrfach vom Konzil abgelehnt, weil man den weiteren Vorteil dieser Technologie nicht erkennen konnte. Wir hätten heute also keine Internetapplikationen, so etwas wie eBay würde es nicht geben, wenn die Leute damals zurückgeschreckt wären, eine sicherlich nicht perfekte Lösung so lange zu diskutieren, bis sie dann einsatzfähig gewesen wäre. Also warten wir es ab. Man muss sich den Hochsicherheitsbereich anschauen und was da alles schon existiert, gerade hier in Deutschland. Da können wir eine Vorreiterrolle spielen, und vielleicht nicht alles so perfekt machen, wie wir es mit der qualifizierten Signatur etwas überzogen haben - ich habe da wirklich Erfahrungen – und haben vielleicht einen Zeitvorsprung, denn wir hatten einfach verspielt, sowohl weltweit wie auch in der EU. Jetzt lassen Sie uns hier vorankommen und gerade auch Softwaretechnik einführen. Gerade das BSI ist hier sehr bemüht, Schnittstellen zu definieren, wo verschiedenste Datenlesegeräte mit verschiedensten anderen Applikationen, Bordercontrol vom Reisepass wie irgendwelche weiteren Karten aus dem Gesundheitswesen oder sonst etwas an Applikationen herangeführt werden. Und wenn diese Schnittstellen dann existieren, da bin ich ziemlich sicher, wird man auch plötzlich Anwendungen erleben, die wir uns heute gar nicht vorstellen können.

Prof. Thielmann:
Vielen Dank. Ich denke, wir machen langsam Schluss mit der Diskussion. Ich glaube, das Experiment, das wir als Münchner Kreis das Thema aufgegriffen haben, ist uns einigermaßen gelungen – vor allen Dingen in der Neutralität, die der Münchner Kreis hier hat, nicht als Hersteller- oder Anwenderverband, sondern, wie Herr Prof. Picot heute Abend gesagt hat, zwischen Politik, Wirtschaft und Wissenschaft. Wie wir das Thema weiter entwickeln können – es gibt viele Anregungen aus der Diskussion – müssen wir uns überlegen. Wir können keine Organisation und Arbeitskreise etablieren wie andere Verbände. Das wollen wir auch nicht. Wenn Sie Vorschläge haben, wie wir das weiter betreiben können, vielleicht in einem zweiten Abend im Spätsommer oder im Herbst, wäre das eine Möglichkeit.

Anhang

Liste der Referenten und Moderatoren

Dr. Stefan Groß-Selbeck
Geschäftsführer
eBay GmbH
Marktplatz 1
14532 Europarc Dreilinden
stefan.gross-selbeck@ebay.de

Prof. Dr. Dres. h.c. Arnold Picot
Universität München
Institut für Information, Organisation
und Management
Ludwigstr. 28
80539 München
picot@lmu.de

Staatssekretär Johann Hahlen
Bundesministerium des Innern
Alt-Moabit 101 D
10559 Berlin
sthn@bmi.bund.de

Prof. Dr.-Ing. Heinz Thielmann
Eichenstr. 11
90562 Heroldsberg
heinz.thielmann@t-online.de

Hans Peter Heidebach
Verwaltungsdirektor
Landeshauptstadt München
Ref. für Arbeit u. Wirtschaft
Herzog-Wilhelm-Str. 15
80331 München
hp.heidebach@muenchen.de

Siegfried Vater
Vorsitzender der AG2 des DIF
SCM Microsystems
Oskar Messter Str. 13
85737 Ismaning
svater@scmmicro.de

Dr. Udo Helmbrecht
Präsident
Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
Udo.Helmbrecht@bsi.bund.de

Prof. Dr.-Ing. Dr.-Ing. E.h. Albrecht
Ziemer
Grüngang 5
78464 Konstanz
ziemer.a@zdf.de