Udo Helmbrecht
Heinz Thielmann
Albrecht Ziemer

Herausgeber

Elektronischer Personalausweis und E-Identity

2. Berliner Gespräch

MÜNCHNER KREIS
Übernationale Vereinigung für Kommunikationsforschung
Supranational Association for Communications Reseach

Das Buch enthält die Referate und Diskussionen des
2. Berliner Gesprächs „Elektronischer Personalausweis und E-Identity“
des MÜNCHNER KREIS am 6. Mai 2008

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 (ePA) und die Erarbeitung von E-Identity-Konzepten vor. Mit der Einführung des ePA soll ein kombiniertes Ausweissystem für Anwendungen im eGovernment und e-Business geschaffen werden, das eine verlässliche und einheitliche elektronische Identifizierung im Rahmen eines übergreifenden Gesamtkonzeptes ermöglicht.

Der MÜNCHNER KREIS hat dieses Thema in seinem 1. Berliner Gespräch am 26. März 2007 aus Politik, Wirtschaft und Wissenschaft aufgenommen. Die Ergebnisse aus Vorträgen und Diskussionen sind ausführlich dokumentiert (zu beziehen über die Homepage des Münchner Kreises: www.muenchner-kreis.de). Das Bundesministerium des Innern, das Bundesamt für Sicherheit in der Informationstechnik sowie die Wirtschaft haben inzwischen die Konzeption und Anwendungsszenarien des ePA vorangetrieben, so dass eine Zusammenführung und Diskussion des erreichten Standes sinnvoll erschien.

Es wurde deshalb ein 2. Berliner Gespräch zum Thema „Elektronischer Personalausweis und E-Identity“ am 6. Mai 2008 durchgeführt, bei dem nach Einführungs- und Übersichtsvorträgen insbesondere die Anwendungserprobungen zum elektronischen Personalausweis im Mittelpunkt gestanden haben. Im Rahmen der Veranstaltung wurden fünf charakteristische Anwendungsszenarien vorgestellt, die vor der breiten Einführung des ePA erprobt werden und maßgeblich noch in 2008 beginnen sollen. Sie sollen in ihrer Gesamtheit das wirtschaftliche und administrative Spektrum aufzeigen, das von der Einführung des ePA in den Bereichen eGovernment, Zutritt bei Großveranstaltungen, Nahverkehr, Zahlungsverkehr und eCommerce, aber auch im administrativen Bereich der Wirtschaft, besonders bei den KMU`s, erwartet werden kann.

Die Anwendungserprobungen umfassen sowohl die technischen Aspekte und Einsatzmöglichkeiten des ePA und der verschiedenen Lesegräte wie aber auch den verfahrensmäßigen und operativen Einsatz des Gesamtsystems elektronischer Personalausweis, Lesegerät und PC. Die Diskussion hat neben Ergänzungen und Korrekturen der bisherigen Planungen dieser Szenarien auch eine grobe Potenzialbewertung (Realisierbarkeit, Nutzeneffekt, Verbreitungsgrad/–wahrscheinlichkeit) der dargestellten Anwendungsszenarien ergeben und Anregungen für die nächsten Schritte der Umsetzung durch Politik und Wirtschaft ergeben. Der vorliegende Band enthält die Niederschriften der Referate und Diskussionsbeiträge.

Unser herzlicher Dank gilt den Referenten und 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

Prof. Dr. Jörg Eberspächer, Technische Universität München

Sehr geehrter Herr Staatsekretär Dr. Beus, sehr geehrte Damen und Herren des BMI und des BSI, sehr geehrte Damen und Herren der Bundestagsfraktionen, sehr geehrte Vertreter der Wirtschaft, der Wissenschaft und der Verbände, und nicht zuletzt sehr geehrte Referenten – ich darf alle herzlich begrüßen bei unserem zweiten Berliner Gespräch des Münchner Kreises. Mein Name ist Jörg Eberspächer. Ich bin im Vorstand des Münchner Kreises, aber hauptsächlich Professor an der TU München und kümmere mich normalerweise um die Infrastruktur der Telekommunikation.

Im Namen des Münchner Kreises, den viele von Ihnen aufgrund seiner vielfältigen Aktivitäten im Bereich der IuK und der Medien kennen aus den Konferenzen, die wir veranstalten, und aus anderen Aktivitäten, heiße ich Sie herzlich willkommen bei dieser Veranstaltung zum Thema „Elektronischer Personalausweis und E-Identity“. Ich soll Sie noch besonders grüßen von unserem Vorsitzenden, Herrn Prof. Picot, der wegen einer lange vorher anberaumten Sitzung heute nicht teilnehmen kann.

Meine Damen und Herren, viele von Ihnen waren vor einem Jahr, genau am 26. März letzten Jahres, schon hier versammelt, um bei unserem ersten Fachgespräch zu diesem Thema den Stand der Entwicklung zu erörtern und die Möglichkeiten der Nutzung des elektronischen Personalausweises zu diskutieren. Die Ergebnisse sind in einer Broschüre dokumentiert, genauso wie übrigens auch die heutigen Gespräche und Vorträge wieder in einem kleinen Bändchen dokumentiert werden.

Seither ist einiges geschehen. Das Bundesministerium des Inneren, das BSI sowie die Wirtschaft und viele andere, die an dem Thema interessiert sind, haben inzwischen die Konzeption und Anwendungsszenarien des elektronischen Personalausweises vorangetrieben, so dass eine Zusammenführung und Diskussion des erreichten Standes sinnvoll erschien. Gern haben wir vom Münchner Kreis uns bereit erklärt, dieses Gespräch wieder zu organisieren, in einem eingeladenen Kreise, wie Sie vom letzten Mal wissen. Wir machen sonst überwiegend öffentliche Veranstaltungen, doch für solch ein Thema wie unser heutiges ist es beim jetzigen Stand der Entwicklung sicherlich angebracht, die kritischen oder offenen Punkte im kleinen Kreise zu erörtern.

Wir haben das Programm in drei Teile geteilt. Im ersten Teil werden in Einführungs- und Übersichtsvorträgen die Grundlagen gelegt und der aktuelle Stand des elektronischen Personalausweises vorgestellt. Es wäre nicht fair und sogar unhöflich, wenn ich sagen würde, dass Sie die drei ersten Beiträge als „thematische Vorspeise“ betrachten sollten. Aber Vorspeisen – seien sie geistig oder kulinarisch -, machen Appetit auf mehr. Dieses „Mehr“ kommt dann im zweiten Teil bei den Berichten zu den Anwendungserprobungen, und das ist eigentlich das Thema heute, auf das wir uns fokussieren wollen. Wie Sie dem Tagesprogramm entnehmen können, haben wir dazu vier Einzelbeiträge vorgesehen, moderiert von Herrn Prof. Ziemer. Diese Anwendungen sollen vor der breiten Einführung des ePA, die wir alle erhoffen, erprobt werden und so bald wie möglich beginnen oder sie haben schon begonnen. Sie decken ein breites Spektrum von Bereichen aus dem wirtschaftlichen und administrativen Umfeld ab. Es sind zwar teilweise noch Pläne, aber praxisnahe Konzepte

und Szenarien, über die wir nachher noch mehr hören werden. Der dritte Teil besteht aus der Diskussion, die uns ganz wichtig ist und in die Sie natürlich einbezogen werden. Diese wird von Herrn Dr. Helmbrecht, dem Präsidenten des BSI und Herrn Prof. Thielmann, dem langjährigen Chef des Fraunhofer Instituts für Sichere Informationstechnologien, moderiert.

Mit den Herren Helmbrecht, Thielmann und Ziemer habe ich schon drei der Organisatoren und Treiber dieser Veranstaltung genannt. Ich sollte auf jeden Fall noch erwähnen, dass Herr Kowalski vom BSI und Herr Dr. Wolfenstetter von der Deutschen Telekom zur Vorbereitung enorm beigetragen haben. Ich möchte Ihnen allen an dieser Stelle danken für Ihre Initiative und das konsequente Verfolgen des Themas, das ja einen langen Atem erfordert. Der Münchner Kreis hat sich vorgenommen, am Ball zu bleiben, natürlich alles ist in enger Abstimmung mit dem Bundesministerium des Inneren. An dieser Stelle möchte ich dem Ministerium danken für die Offenheit der Gespräche im Vorfeld.

Danken möchte ich aber auch unseren Sponsoren, die das Zustandekommen des heutigen Abends unterstützt haben. Zu nennen sind hier die Firmen Gieseke & Devrient, Hewlett Packard, Secunet Security Networks, T-Systems Enterprise Services und Microsoft Deutschland. Ihre Hilfe ist sehr wichtig für die Durchführung dieses Berliner Gesprächs.

Ich darf jetzt zum ersten Redner des Abends überleiten. Wir freuen uns sehr, dass Herr Staatssekretär Dr. Hans Bernhard Beus zu uns gekommen ist. Er ist, wie Sie hoffentlich wissen, seit 1. Januar 2008 der Bundes-CIO. Offiziell heißt die Funktion: der Beauftragte der Bundesregierung für Informationstechnik. Damit fällt das heutige Thema in Ihren Zuständigkeitsbereich, und wir freuen uns auf Ihre Rede. Vielen Dank, Herr Staatssekretär, dass Sie zu uns gekommen sind.

2 Elektronischer Personalausweis und E-Identity
Keynote

Staatssekretär Dr. Hans Bernhard Beus, Bundesministerium des Inneren, Berlin

Zunächst einmal herzlichen Dank für die Möglichkeit, dass ich hier einige Worte zu Ihnen sage, zu diesem Thema, was uns in der Tat sehr bewegt und an dem wir arbeiten. Sie haben schon darauf hingewiesen, dass Sie es im letzten Jahr behandelt haben und dass mein Vorgänger, Herr Kollege Hahlen, damals dazu schon einiges gesagt hat.

Ich denke, dass ich deshalb die ganz grundlegenden Dinge nicht mehr auszuführen brauche, sondern mich darauf konzentriere, dass ich in einer Art Fortschrittsbericht das beschreibe, was in diesem Jahr passiert ist und was uns in der nahen Zukunft beschäftigen wird, d.h. also die Frage, was wir in dem letzten Jahr getrieben haben, wie wir weiter gekommen sind, und welche Fragen sich auch im Detail gestellt haben und wie wir sie beantworten wollen.

Vielleicht zum Verfahren: wir haben intensiv am Gesetzentwurf gearbeitet, der die Voraussetzung dafür ist, dass wir überhaupt mit dem elektronischen Personalausweis in der Realität starten können. Der Entwurf ist jetzt so weit, dass wir schon die Erwartung haben, ihn in den nächsten Tagen an die Ressorts und dann in die Länder und natürlich auch an die damit befassten Abgeordneten übersenden zu können. Das ist ein wichtiger Schritt, der dann auch öffentlich bekannt werden wird, der deutlich macht, dass wir das mit Energie verfolgt haben und jetzt einen wichtigen Schritt tun, der auf eine Kabinettbefassung nach unserer Vorstellung möglichst im Sommer zielt, um dann das Gesetzgebungsverfahren auch förmlich einzuleiten.

Sie kennen alle das Ziel, das wir mit dem Ausweis in diesem Segment Internet verfolgen. Ich will noch einmal darauf hinweisen; der Ausweis hat sozusagen zwei Aspekte, zwei Seiten. Einmal die traditionelle Aufgabe, die ein Personaldokument hat. Damit sind auch spezielle Fragen verbunden, vor allem die Anwendung biometrischer Daten. Das wird uns aber nicht heute Abend beschäftigen, sondern hier geht es um die Anwendung im Internet, wobei die biometrischen Daten keine Rolle spielen werden. Das muss man immer wieder betonen, weil das oft in der Öffentlichkeit nicht so klar ist, wie es Ihnen als Fachleuten klar ist.

Was wollen wir erreichen? Wir wollen ein Dokument haben, was vertrauenswürdig ist, was einfach ist und was wir sicher anwenden können. Mit diesen drei Eigenschaften wollen wir beim eGovernment und beim eBusiness ein deutliches Stück vorankommen. Ich denke, über den dort bestehenden Handlungsbedarf sind wir uns einig. Sie alle kennen die Landschaft, die sich entwickelt hat bei Online-Anwendungen mit PINs und Passwörtern und den verschiedenen Möglichkeiten, auch mit den Gefahren, die es in dem Bereich gibt und die sicher eher zunehmen als abnehmen. Wenn man die Erkenntnisse des BSI hört, ist man manchmal etwas verzweifelt, wie das weiter gehen soll, insbesondere wenn man Steigerungsraten sieht, die es bei Viren, Trojanern und ähnlichen Dingen gibt. Die sind wirklich exorbitant. Die Nachfrage nach sicherer Kommunikation im Internet und sicherer Authentisierung wird eher zunehmen als abnehmen. Das ist die Basis, auf der wir dieses Projekt betreiben.

Eine weitere Voraussetzung ist, und da gab es in den letzten Wochen eine neue Umfrage, dass die Nutzung des Internets doch auch in Deutschland deutliche Fortschritte macht, dass die

Zahlen der Nutzer deutlich steigen und wir da mehr aufholen, als wir das vielleicht bisher gedacht haben. Selbst die Gruppe derjenigen, für die eine solche Anwendung interessant sein wird, wird deutlich zunehmen.

Ein dritter wichtiger Punkt ist, dass wir mit diesem Personalausweis letztlich fast alle Bundesbürger erreichen, d.h. wir haben die Gruppe der ab 16-jährigen Menschen in unserem Lande, die dieses Dokument haben, die es auch fast täglich in der Hand haben werden und die in der Lage sind, wenn sie es in dem Bereich anwenden, um den wir uns heute kümmern – das Internet –, dieses nachhaltiger zu verändern, als wir uns das heute vorstellen können.

Ich denke, man muss sich dieses gesamtgesellschaftliche Potenzial immer wieder vor Augen führen, das dieses Projekt haben wird. Deshalb reicht es uns auch nicht, dass wir an dem Tag X, der nach unserer Vorstellung irgendwann im zweiten Halbjahr 2009 liegen wird, ein Dokument ausgeben und dem Bürger in die Hand drücken, sondern unser Ziel ist schon, dass es zu diesem Zeitpunkt auch möglichst viele Anwendungen gibt, sowohl im Bereich der öffentlichen Verwaltung, was wir als eGovernment bezeichnen, aber natürlich auch im Bereich des eBusiness. Ich denke, das ist entscheidend, um diesen elektronischen Personalausweis von Anfang an zu einem Erfolg zu machen. Wichtig ist dabei – und das ist sicher zum großen Teil unsere Aufgabe, aber wir erwarten natürlich, dass alle daran Beteiligten mitmachen – über das zu informieren, was dieser Personalausweis wirklich leisten wird. Das ist ein Punkt, um den wir uns in nächster Zeit in besonderer Weise kümmern müssen. Da ist einmal die Authentisierungsmöglichkeit, also der elektronische Identitätsnachweis, der zukünftig möglich ist, und dann im zweiten Feld auch die qualifizierte elektronische Signatur, die mit dem Ausweis verbunden werden kann, wenn der Inhaber dies wünscht. Beide Dinge müssen bekannt gemacht werden, für sie muss geworben werden. Da ist gerade ein Kreis wie Ihrer für uns ein wichtiger Multiplikator, um das in die breite Öffentlichkeit zu tragen.

Es ist im vorigen Jahr die Frage gestellt worden, wie wir das technisch umsetzen wollen. Wichtig ist immer zu betonen, dass es einen Identitätsnachweis auf beiden Seiten geben wird, die über diesen Ausweis in Kontakt treten werden. Es ist also nicht nur der Bürger, der sich auf diese Weise gegenüber seinem Geschäftspartner ausweisen kann, sondern es ist auch der Geschäftspartner, der an diesem Prozess nur teilnehmen kann, wenn er von einer staatlichen Stelle vorher dazu berechtigt worden ist. Der Bürger läuft also nicht in Gefahr, mit einem Geschäftspartner mit seinem elektronischen Ausweis in Kontakt zu treten, der vorher nicht von uns zertifiziert worden ist und der damit sozusagen nicht gewisse Qualitätskriterien erfüllt. Das ist deshalb wichtig, weil wir ja nur Erfolg haben werden mit dem Ausweis, wenn es uns gelingt, eine Vertrauensbasis bei denjenigen zu schaffen, die ihn anwenden sollen und das setzt auch voraus, dass ich mir einigermaßen sicher sein kann, dass der Geschäftspartner, mit dem ich zu tun haben werde und mit dem ich auf die Weise kommuniziere, die Anforderung erfüllt, die für solche Art von Kommunikation erforderlich sind.

Der Ausweis wird ermöglichen, und ich glaube, dass das ein Punkt ist, den wir immer wieder herausstellen müssen, differenzierter als bisher zu entscheiden, welche Daten ich von mir preisgeben möchte. Im Augenblick ist es so, dass – wenn ich jemandem meinen Personalausweis gebe – er in der Lage ist, alle dort abgedruckten Daten zu lesen und zur Kenntnis zu nehmen. Beim elektronischen Personalausweis wird es möglich sein, das zu differenzieren, d.h. ich kann auswählen, welche Daten ich meinem Geschäftspartner zukommen lassen möchte und werde das danach differenzieren, welche Daten für den Abschluss dieses Geschäftes oder für die Vornahme dieses Antrages im öffentlichen Bereich erforderlich sind. Ich kann sagen, es sollen der Name und die Anschrift sein, und das

Geburtsdatum hinzufügen, wenn ich das wünsche. Es kann die Frage des Geburtsortes sein, die ich beantworte oder nicht. Ich kann differenziert entscheiden, welcher Daten ich mich entäußere, und das ist gegenüber dem Status quo für den Nutzer ein Vorteil, den er hat und den wir ihm auch deutlich machen wollen.

Um das Ganze zu tun, muss ich eine PIN eingeben. Es gibt also außer der Karte noch ein weiteres Sicherheitselement, das im Prozess erforderlich ist. Wie ist das mit der PIN? Sie haben vielleicht von gewissen Problemen gelesen, die es bei der Gesundheitskarte gibt, unter anderem mit der PIN. Es wird beim elektronischen Personalausweis so sein, dass auch der Bürger, der Benutzer seine eigene PIN wählen kann, wenn er den Ausweis entgegen nimmt. Er ist also nicht festgelegt auf eine vorher eingegebene PIN, sondern er kann eine, die ihm besonders gut erinnerlich ist, wählen, um sie dann im Falle des Falles auch wirklich im Kopf zu haben und anwenden zu können. Ich glaube, dass man auch an diese Dinge denken muss, die im praktischen Leben eine Rolle spielen und die man sich vielleicht, wenn man das nur am Schreibtisch entwickelt, nicht so deutlich macht. Es ist aber ein wichtiger Punkt für die Benutzerfreundlichkeit.

Ich habe schon angesprochen, dass es die Möglichkeit geben wird, eine qualifizierte elektronische Signatur auf den Ausweis zu laden, wenn dies gewünscht wird. Es stellt sich dabei sicher die Frage, warum es das nicht von selbst gibt, warum es die Signatur nicht als Standardausstattung gibt. Sie wissen, dass sich da nichts geändert hat: Es ist das leidige Kostenargument. Wenn wir den Ausweis in allen Fällen mit dieser Signatur ausstatten würden, wäre der Preis, den der Bürger für den Ausweis zahlen müsste, doch ein Stück höher, ohne dass jeder von vornherein sagen könnte, dass er diese Signatur auch entsprechend anwendet. Deshalb haben wir uns entschieden, die Signatur nicht obligatorisch mit dem Ausweis zu verbinden, sondern das Angebot zu machen, sie darauf zu laden, wenn man glaubt, dass man dessen bedarf.

In der Einführungsphase wird es für uns wichtig sein, möglichst viele Ausweise an den Mann oder an die Frau zu bringen. Es wird die Möglichkeit geben, auch schon vor Ablauf des bisherigen Personalausweises den neuen elektronischen Ausweis zu beantragen und zu bekommen. Ein Verzicht auf diese freiwillige Umtauschmöglichkeit würde bedeuten, dass wir eine Umstellungsphase von zehn Jahren haben, bis sozusagen der gerade noch ausgestellte konventionelle Ausweis abgelaufen ist. Nach unserem Vorschlag wird es so sein, dass man, wenn man das wünscht, den elektronischen Ausweis sofort beantragen kann. Das ist wichtig.

Wichtig ist auch, dass wir möglichst viele Anwendungsmöglichkeiten zu diesem Zeitpunkt haben. Diese werden Lesegeräte voraussetzen, das ist klar. Die Lesegeräte werden relativ preiswert sein. Da wird keine Hürde bei der Anwendung liegen. Vielleicht gibt es den einen oder anderen Anwender, der bereit ist, seinen Kunden ein Lesegerät zur Verfügung zu stellen, um auf diese Weise den Start zu erleichtern. Wir werden kontaktlose Technologie in diesem Bereich anwenden. Das hängt einmal damit zusammen, dass wir sicherstellen müssen, dass die Ausweise zehn Jahre funktionsfähig sind, und da ist diese Technologie auf jeden Fall zu bevorzugen. Außerdem wird es möglicherweise in der Zukunft auch andere Möglichkeiten geben, sich mit dem neuen Ausweis einzuloggen, per Handy, PDA oder anderen Dinge, die wir heute noch nicht so absehen, wobei auch unter diesem Aspekt sicher der kontaktlose Chip vorzuziehen ist.

Über die Frage der Biometrie habe ich am Anfang etwas gesagt. Fingerabdrücke, Fotos und ähnliches sind im Bereich eGovernment und im eBusiness nicht von Bedeutung, sondern sind für die konventionellen Funktionen des Personalausweises wichtig.

Lassen Sie mich etwas sagen über die Frage, wie wir uns die Einführung des elektronischen Personalausweises vorstellen. Was tun wir von uns aus, um den Markt zu schaffen, so dass wir dort auch Nachfrage haben werden? Da besteht einmal ein guter Kontakt mit BITKOM, der für uns eine wichtige Funktion hat und mit dem wir im Vorfeld der Einführung Veranstaltungen und Workshops planen, um auf dieses Produkt aufmerksam zu machen, dafür zu werben und konkrete Anwendungsszenarien vorzustellen. Ich denke, es wird im Laufe des Abends auch noch eine Rolle spielen, wie das ablaufen kann. Wir haben enge Kontakte auch im Sinne der Verbraucher mit dem Verein „Deutschland sicher im Netz“, den wir als Partner in diesem Prozess gewonnen haben und mit dem wir versuchen wollen, auf die Verbraucher und ihre organisierten Verbände zuzugehen und dort zu überzeugen, dass der elektronische Ausweis ein gutes Produkt ist, was dem Verbraucher mehr Sicherheit und mehr Komfort bietet als die Techniken, die er bisher gekannt hat. Wir haben natürlich eine Reihe von engen Kontakten mit Fachverbänden, die an dieser Art von Technologie Interesse haben werden. Wir werden natürlich enge Kontakte haben mit unseren Banken, die im Online-Bereich sicher Interesse an dieser Technologie haben. Wir werden in unserem eigenen Bereich, also im öffentlichen Dienst, auf Länder und Kommunen zu gehen, um für den neuen Ausweis zu werben.

Ich denke, es sollte unser gemeinsames Ziel sein, dass wir versuchen, den gesamten Bereich der Anwendungsmöglichkeiten abzudecken und dafür gemeinsam einzutreten, dass möglichst mit Stichtag der Ausgabe des Ausweises diese Möglichkeiten zur Verfügung stehen. Sie wissen, es wird sicher noch einmal politische Diskussionen um den Ausweis geben, weniger in dieser Frage als in der Frage, wie das mit den biometrischen Daten ist. Das ist sicher okay. Es ist aber gleichzeitig wichtig, dass sich die potentiellen Nutzer im Internet immer deutlich machen, wie wichtig dieser neue Ausweis für sie ist. Und dass es ein Gleichgewicht in dieser Diskussion gibt, dass nicht nur über Risiken diskutiert wird, wie groß die auch immer sein mögen. Nach unserer Auffassung sind sie ja nicht vorhanden. Dass wir aber gleichzeitig die Chancen betonen, die dieser Ausweis in der Tat für Verwaltung und Geschäftsleben bietet. Wir denken schon, dass wir, wenn wir das gemeinsam richtig anpacken, mit dem neuen Ausweis einen großen Sprung nach vorn machen können. Dass wir Hindernisse, die wir bisher in der Authentisierung, in den Geschäftsprozessen haben, beiseite räumen können und dass wir dann durchgängige Prozesse sowohl in der öffentlichen Verwaltung als auch im eBusiness haben werden, die aufseiten der Bürger mehr Komfort, mehr Sicherheit, auch mehr Schnelligkeit bringen und aufseiten der Wirtschaft auch Kostenersparnisse nach sich ziehen werden. Das ist eine Situation, wo beide Seiten gewinnen können, wenn sie den elektronischen Personalausweis nutzen.

Und deshalb bin ich gern zu Ihnen gekommen – ich glaube, es ist kaum noch nötig, bei Ihnen dafür zu werben –, um auch zu hören, wo Sie noch Probleme sehen, auf die Punkte hinzuweisen, auf die wir achten müssen, vielleicht Anwendungen anzusprechen, die wir noch nicht kennen, die gesamte Bandbreite der Diskussion heute Abend noch einmal zu erleben.

Entscheidend wird in dem nächsten Jahr sein, dass wir das Projekt so auf die Schiene bringen, dass wir im zweiten Halbjahr 2009 damit starten können und im Jahr 2010 den wirklichen Betrieb haben werden und dann vielleicht bei einem Treffen des Münchner Kreises im Jahr 2010 sagen können, dass sich die Anstrengungen, die alle Beteiligten darauf verwandt haben, gelohnt haben.

3 Leistungsmerkmale des elektronischen Personalausweises

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

Zunächst möchte ich die Rolle des BSI beim elektronischen Personalausweis darstellen, Herr Kowalski wird dann über den fachlichen Stand des Projektes berichten. Das BSI ist als Bundesfachbehörde in dieses Projekt eingebunden ist. Die Chance, dies hat Herr Dr. Beus gerade ausgeführt, liegt darin, dass wir heute mit der Politik, mit Ministerien, den Behörden und auch mit der Industrie diskutieren können. Insofern kann ich Sie dazu nur anregen. Ich möchte noch eine Information vorab geben: wenn Sie in Ihre Unterlagen schauen, finden Sie Statements der Vortragenden. Wenn Sie zwischendurch mal hineinschauen, kann das für die Diskussion befruchtend sein.

Wir haben im letzten Jahr unseren Lagebericht zur IT-Sicherheit als BSI herausgegeben, und es ist leider ein Trend zu erkennen, der uns Sorgen bereitet (Bild 1).

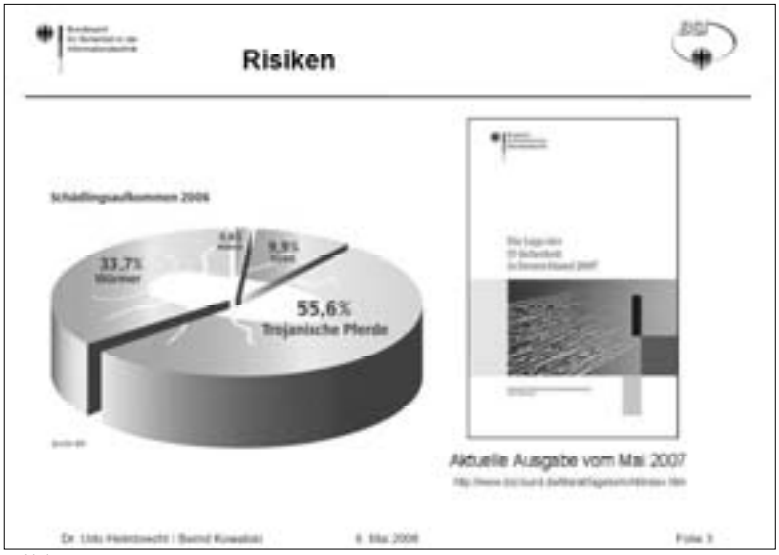

Bild 1

Es ist das Stichwort Trojanische Pferde oder umgangssprachlich kurz Trojaner. Leider haben wir feststellen müssen, dass es eine deutliche Zunahme bei der Verbreitung der Trojaner gibt. Wenn wir das einmal technologisch betrachten, bedeutet das, dass mit dem fortschreitenden Einsatz des Internet auch die verschiedenen technischen Schadszenarien zugenommen haben.

Computerviren haben wir mehr oder weniger im Griff. Das Thema Spyware ist eine weitere Herausforderung. Phishing kennen Sie aus dem Abgreifen von PIN und TAN zum Beispiel beim Online-Banking. Hierzu haben wir mit den Banken zum Teil schwierige, zum Teil erfolgreiche Diskussionen gehabt. Die Frage ist unter anderem, mit welchen Verfahren man dem Phishing begegnen kann. Es gibt neben der einfachen TAN-Liste die Verfahren iTAN, mTAN sowie weitere Lösungen wie zum Beispiel der Einsatz von Token.

Was uns im Moment Sorgen bereitet, sind die Bot-Netze. Diese Computer-Netze, die aus unbemerkt ferngesteuerten PCs bestehen, werden zu Angriffen auf die IT von Unternehmen und Organisationen eingesetzt. Denken Sie an den Angriff im letzten Jahr auf die IT-Strukturen in Estland. Diese Denial of Service-Attacke zeigt, dass das Internet mittlerweile mit krimineller Energie genutzt wird und dass im Web kriminellen Machenschaften stattfinden. Warum kommt das zustande, und warum dringt hier die Kriminalität ein? Viele eBusiness-Geschäftsmodelle sind erfolgreich, das zeigen die zunehmende Umsätze und die zunehmende Akzeptanz bzw. Nutzung elektronischer Plattformen.

Dies zieht aber auch Kriminalität an, und so finden wir im Internet natürlich auch Schattenseiten. Was früher Postkutschen- oder Bank-Überfälle waren, ist heute Phishing. Im Kern ist dies nichts anderes. Dies geschieht zum Ziele der Bereicherung jetzt mit dem Einsatz technologisch neuer Möglichkeiten. Was uns dabei zusammen mit dem Bundeskriminalamt Sorgen bereitet, ist die organisierte Internet-Kriminalität. Es gibt Beispiele, dass man im Internet durch Phishing, Spam, Bot-Netze oder über Erpressung bereits mehr Geld verdienen kann als mit Drogenhandel. Dieser Herausforderung durch die internationale Internetkriminalität müssen wir uns auch aus Sicht des Staates stellen.

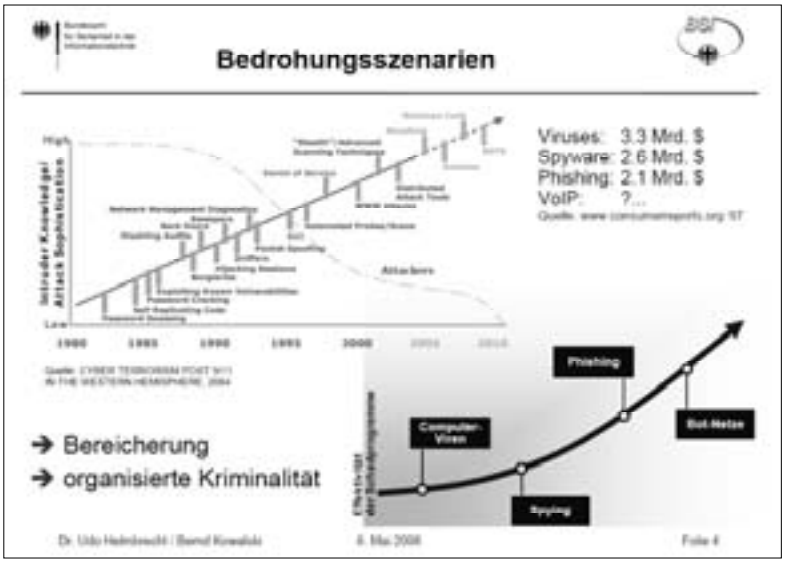

Bild 2

In der Statistik der amerikanischen Verbraucherorganisation Consumer Reports kann man verfolgen, wie sich die Schäden in den USA in den letzten Jahren entwickelten (Bild 2). Sie nehmen dramatisch zu, auch in Europa. Allein in Deutschland schätzen wir die Schadenshöhe auf 25 Millionen Euro. Was dabei künftig auch auf uns zukommen wird, sind neue Technologien wie Voice over IP. Hier treffen die klassischen Schadprogramme, wie Viren, Würmer und Trojaner und die Angriffsszenarien aus der Telekommunikation aufeinander. Insofern besteht hier Handlungsbedarf.

Es gibt aber auch Positives und das möchte ich hier in Verbindung mit den Chancen durch das Internet herausheben. Wenn Sie an Privatverkäufe im Internet denken, wobei sicherlich eBay das bekannteste Beispiel ist für Verkäufe über Webplattformen ist, so liegt Deutschland in der

EU an zweiter Stelle und damit weit über dem EU-Durchschnitt. Deutsche Firmen machen zurzeit pro Jahr etwa 500 Milliarden Euro Umsatz im Netz. Damit ist das eine signifikante Branche. Nach einer BITKOM-Studie aus dem April dieses Jahres sind bereits 41 Prozent der Privatpersonen im Internet als Einkäufer aktiv.

Bild 3

Das heißt, das Geschäftsvolumen ist vorhanden (Bild 3). In Verbindung mit den Risiken, die ich vorhin nannte, kommen wir nun zum Einsatzpotential des elektronischen Personalausweises und zur Frage: Wie können wir den elektronischen Personalausweis nutzen, um Transaktionen im Internet sicherer zu machen?

Die eCard-Strategie des Bundes beinhaltet eine Reihe von Projekten (Bild 4). Dazu zählt der elektronischen Reisepass, die Unionsbürgerkarte, die Aufenthaltstitel, die Gesundheitskarte, die eLena-Signatur oder ELSTER. Viele von Ihnen engagieren sich in Standardisierungs- oder Fachgremien wie dem Deutschen Industrieforum (DIF). Sie wissen daher, dass wir als BSI eine Middleware konzipieren, die der Wirtschaft ermöglicht, Geschäftsprozesse mit Anwendungen gegenüber dieser Middleware zu entwickeln, um die verschiedenen Kartensysteme zu nutzen.

Beim elektronischen Personalausweis wollen wir die Erfahrungen, die das BSI gemeinsam mit dem Innenministerium beim Reisepass gewonnen haben, nutzen.

Bild 4

Gestatten Sie mir hier eine Nebenbemerkung: Beim ePass haben wir die Diskussion in den Medien und der Öffentlichkeit um vermeintliche Schwachstellen des Passes erlebt. Es gab da auch kritische Diskussionen. Auch daraus haben wir gelernt, insbesondere dass man eine Kommunikationsstrategie für den elektronischen Personalausweis entwickeln und umsetzen muss.

Bild 5

Der elektronische Reisepass ist ein erfolgreiches Projekt (Bild 5). Im Chip des Passes sind als biometrische Merkmale das Gesichtsbild und Fingerabdrücke enthalten. Der Pass verfügt mit dem Zugriffsschutz und der Kryptographie über ein hohes Sicherheitsniveau. Insofern sind

wir sicherheitstechnisch auf einem sehr guten Weg. Was an Kritikpunkten zur IT-Sicherheit des Passes in der Presse stand, konnten wir letzten Endes entkräften.

Wir wollen nun beim elektronischen Personalausweis auf diese technischen Erfahrungen aufbauen, d.h. wir wollen den gleichen kontaktlosen Chip nehmen. Er ist bewährt und es gibt dazu bereits technische Lösungen (Bild 6).

Bild 6

Ich bitte nun Herrn Kowalski, über die technische Umsetzung zu berichten. Herr Kowalski ist im BSI Leiter der Abteilung Zertifizierung, Zulassung und Konformitätsprüfungen sowie Neue Technologien. Er ist vielen von Ihnen bekannt und derjenige, auf dessen Schultern das Projekt letzten Endes ruht.

Sehr geehrte Damen und Herren, ich werde Ihnen jetzt im zweiten Teil unseres Vortrages die technischen Funktionen des elektronischen Personlausweises etwas näher erläutern. Jeder redet darüber, aber was sich nun genau dahinter verbirgt, ist nicht so ganz einfach zu erläutern. Ich möchte auch darstellen, was eigentlich die Alleinstellungsmerkmale sind. Zuerst kann man sagen, ein elektronisches Dokument, der elektronische Personalausweis oder kurz ePA, ist eigentlich auch nur eine Chipkarte. Was unterscheidet ihn eigentlich von anderen Karten, die schon im Markt sind?

Bild 7

In Bild 7 können Sie zunächst sehr schön sehen, dass der neue elektronische Personalausweis konsequent auf der Systematik des bisherigen Ausweisdokumentes aufbaut. Sie sehen die hoheitlichen Funktionen die Identitätsfunktionen, wie sie es heute auch schon vom Personalausweis kennen. Auch im physikalischen Dokument sind das Passbild und Informationen über den Auszuweisenden abgedruckt. Die Identitätskontrolle bzw. Gesichtskontrolle wird auch weiterhin auf dieser Ebene stattfinden. Neu sind die elektronischen Funktionen der Biometrie, einmal das elektronisch gespeicherte Gesichtsbild und auch der Fingerabdruck, den Sie schon von dem Reisepass kennen. Insofern entsprechen diese neuen Funktionen denselben Vorgaben, wie das auch im Pass der Fall ist. Neu beim Personalausweis ist die Authentisierungsfunktion, die eID-Funktion und die optionale qualifizierte elektronische Signatur, die für die bekannten eBusiness und eGovernment Anwendungen verwendet werden sollen. Nur diese Funktionen sind dann letzten Endes in diesen Anwendungsbereichen nutzbar. Die hoheitlichen Funktionen bleiben weiterhin den hoheitlichen Personen vorenthalten.

Was unterscheidet den ePA zum Beispiel von der Gesundheitskarte? Die Gesundheitskarte ist ein hochkomplexes Instrument mit sehr vielen Anwendungsfunktionen und sehr stark erklärungsbedürftig. Diese Gestaltung ist dem Erfordernis im Gesundheitsbereich geschuldet, da man diese Funktionen für diese verschiedenen Anwendungsbereiche benötigt. Der Personalausweis hat eine lange Lebensdauer, und er hat eigentlich nur zwei wesentliche Funktionen, nämlich die eID-Funktion als Authentifikationsfunktion und die qualifizierte Signatur.

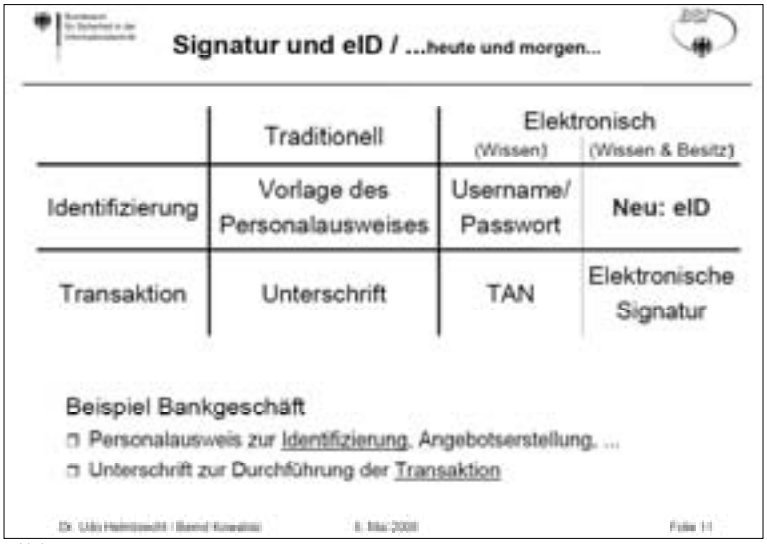

Bild 8

Hier sind diese beiden Funktionen noch einmal etwas stärker erläutert, auch an dem, was man heute im Markt kennt (Bild 8). Zunächst einmal die eID, die interne Beziehungsfunktion, kennen wir von der klassischen stationären Anwendung des Personalausweises. Zum Beispiel die Vorlage eines Ausweisdokumentes beim Ein-Checken in einem Hotel ist heute schon eher eine privatwirtschaftliche Anwendung. Elektronisch wird diese Identifikationsfunktion heute im Markt weitestgehend durch Username und Passwort abgedeckt, eine Sicherheitsfunktion, deren Nachteile bekannt sind und die ich hier nicht näher erläutern muss. Genau dort setzt der Personalausweis an. Hier hat die eID-Funktion mit ihrer Authentifikationsfunktion in Verbindung mit der PIN-Eingabe eine neue Qualität zu bieten. Der Ausweis soll also genau das können, was er bisher auch im klassischen stationären Fall konnte, nämlich die Identifizierung auch künftig elektronisch abwickeln.

Die zweite Sicherheitsfunktion, die Sicherung von Transaktionen von Dokumenten ist eine optionale Funktion. Sie wurde klassisch durch die Unterschrift auf Papier abgewickelt. Heute ist das TAN-Verfahren am weitesten verbreitet, also eine Transaktionskennung, die nur einmal gültig ist für die Transaktion, zum Beispiel einen Geldbetrag, den Sie überweisen. Dort gibt es aber keine direkte Integritätssicherung für diese Transaktion, sondern Sie müssen aufpassen, dass die TAN nicht in falsche Hände gerät und abgephisht werden kann, was heute ein häufiger Missbrauchsfall ist. Die elektronische Signatur des Ausweises schafft hier Abhilfe und jeder, der diese Funktion benötigt, kann sie sich optional beschaffen.

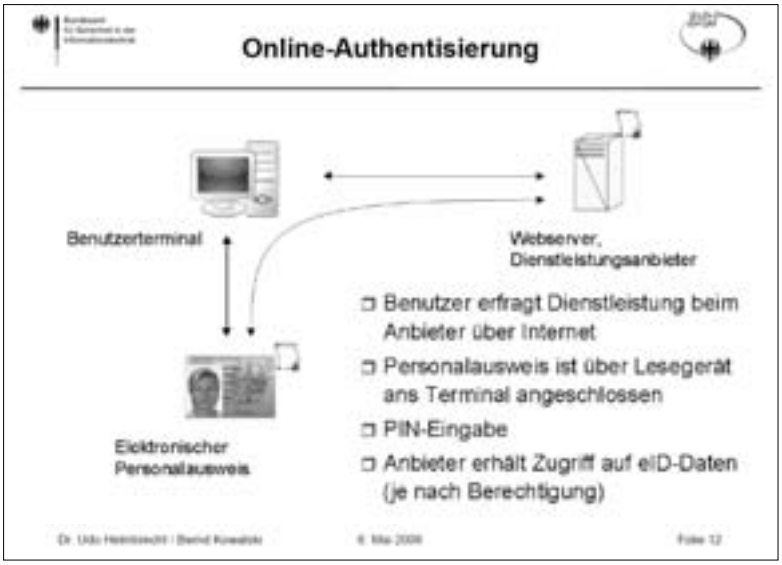

Bild 9

Hier eine kurze Darstellung der eigentlichen Sicherheitsfunktionen (Bild 9). Wie läuft so ein Prozess ab? Zunächst haben wir den ganz normalen Dienstzugang, den ein Benutzer zu seinem Dienstanbieter durchführt. Er loggt sich auf einem Webserver ein. Dann wird der Authentisierungsprozess angestoßen, zunächst will das Ausweisdokument, der ePA, wissen, ob dieser Dienstanbieter überhaupt berechtig ist, einen Authentisierungsprozess mit diesem Ausweis durchzuführen. Das kann der Ausweis aufgrund von vorhandenen Informationen, Schlüsseln auf dem Ausweis feststellen. Das Berechtigungszertifkat, rechts oben mit diesem kleinen Siegel hier dargestellt, des Dienstleistungsanbieters gibt ihm diese Gewissheit. Dann gibt der Benutzer seine PIN ein und startet damit den Authentikationsprozess. Das Ausweisdokument authentisiert sich damit auch gegenüber dem Diensteanbieter, so dass auch er gewiss sein kann, dass es sich um ein gültiges Dokument handelt und die weiteren Funktionen, die ich später noch näher erläutern will, können dann starten.

Sie sehen, hier haben wir eine direkte Authentifikation zwischen dem Anbieter und dem Benutzer. Das gibt es in den klassischen Anwendungsfällen bei Online-Diensten derzeit nicht, mit dem Berechtigungszertifikat. Insofern haben wir hier schon einmal eine neue technische Qualität, die wir nutzen können.

Nun zu den Aspekten des Datenschutzes. Der Zugriff auf die eID-Daten erfolgt nur nach Eingabe einer geheimen PIN. Es ist dann nicht möglich, den Ausweis in irgendeiner Form zu hinterlegen, so dass das Ausweisdokument sich sozusagen als technisches Dokument selbst identifiziert. Die Kontrolle der Datenvergabe ist damit an den Inhaber gebunden. Die Personenbindung der Authentisierung wird letzten Endes durch Eingabe der PIN durchgeführt. Es wird also die Person und nicht der Ausweis identifiziert. Das ist für einen Diensteanbieter von besonderer Bedeutung. Zugriff haben, wie eben gesagt, nur zertifizierte Diensteanbieter mit einem Berechtigungszertifikat. Die Überprüfung der Zertifikate erfolgt durch den Chip des Ausweisdokumentes. Es findet eine gegenseitige Authentisierung statt und damit ist das eine sehr wirkungsvolle Maßnahme gegen das verbreitete Phishing.

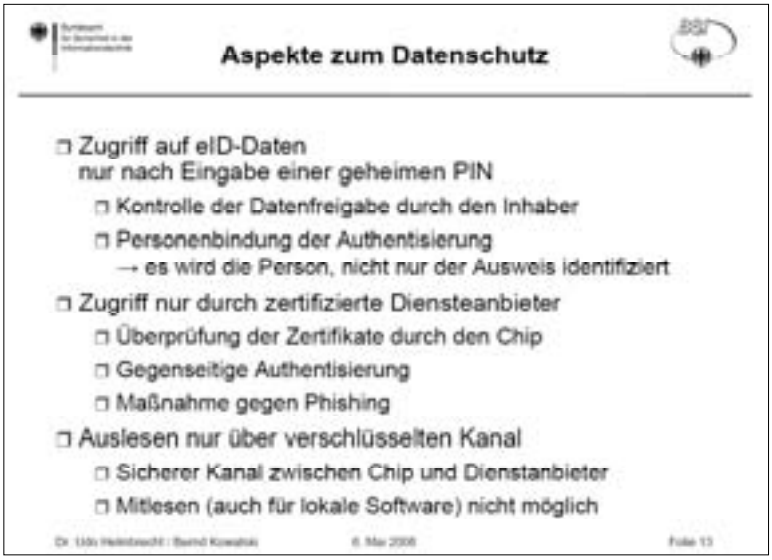

Bild 10

Das Auslesen erfolgt auch über einen verschlüsselten Kanal, so dass Kanalabhörmöglichkeiten hier nicht vorhanden sind (Bild 10). Zwischen dem Chip und Diensteanbieter erfolgt das direkt, d.h. die Software des Clientsystems ist nicht beteiligt. Das bietet eine weitere besondere Sicherheit. Auch das Mitlesen durch lokale Software ist damit nicht möglich. Damit ist eine ganze Reihe von Trojanerangriffen zumindest beseitigt.

Bild 11

Die Zugriffsrechte werden feldgenau ausgeführt (Bild 11). Was bedeutet das? Das Zertifikat eines Diensteanbieters weist genau aus, welche Berechtigung er hat, um welche Daten vom

Ausweis zu lesen. Ist es zum Beispiel die komplette Meldeadresse oder ist es Untermenge davon oder darf er nur eine Alersverifikation durchführen? Zusätzlich kann aber der Benutzer die vom Diensteanbieter dargestellten Anwendungsprofile, Zugriffsprofile reduzieren. Er kann einige Daten zusätzlich ausschalten, so dass der Benutzer letztendlich eine vollständige Kontrolle hat über die Daten, die sein Ausweis dem Diensteanbieter gegenüber offen legt.

Es gibt noch weitere Funktionen für die Datensparsamkeit. Einmal die Altersverifikation, wo nur das Alter geprüft wird und nicht die anderen Daten des Ausweisdokumentes freigegeben werden. Die Dokumentengültigkeit kann ebenfalls allein geprüft werden und schließlich gibt es das so genannte ausweis- und anwenderspezifische Kennzeichen. Ich werde Ihnen gleich noch sagen, worum es dabei geht. Es geht darum, dass eine pseudonyme Funktion angewendet werden soll, wenn zum Beispiel ein Ausweisinhaber sich bei einem Webdienst angemeldet hat. Dann muss er möglicherweise nur einmal am Anfang seine Identität preisgeben. Alle folgenden Authentifikationsvorgänge sollen dann pseudonym bzw. anonym durchgeführt werden können.

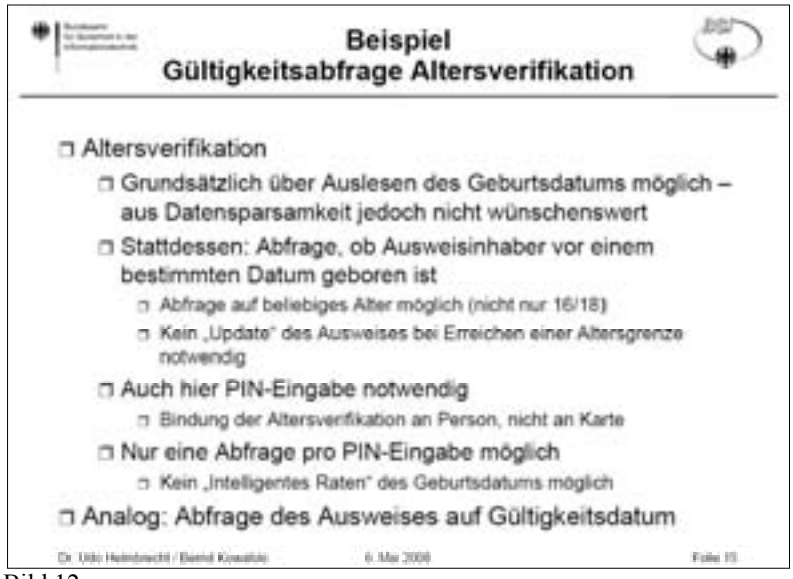

Bild 12

Bei der Gültigkeitsabfrage für die Altersverifikation könnte man grundsätzlich immer das Geburtsdatum ausgeben, falls ein Amt so etwas prüfen möchte (Bild 12). Das ist aber in Bezug auf die Datensparsamkeit nicht das wünschenswerte Ziel. Deswegen kann man auch abfragen, ob jemand ein bestimmtes Alter schon überschritten hat und damit die Altersgrenze vorweisen kann, um zum Beispiel Zugriff auf bestimmte Online-Inhalte zu erhalten. Es ist dafür aber auch kein Update des Ausweises notwendig. Diese Frage kann in Bezug auf ein beliebiges Alter durchgeführt werden. Auch hier ist die PIN- Eingabe wieder notwendig. Auch das ist für den Anbieter eine wichtige Funktion, dass es tatsächlich die Person ist, die sich dort mit ihrem Alter verifiziert und nicht eine Karte. Ganz anders als Sie das heute von den EC-Kartenautomaten und den dort benutzten Karten her kennen. Intelligentes Raten wird vermieden, indem Sie bei jeder Altersverifikation die PIN noch einmal extra eingeben müssen, so dass also ausgeschlossen ist, dass eine maschinelle Aufforderung zum Erraten des Geburtsdatums über den Anbieter nicht stattfinden kann. Analog funktioniert die Abfrage des Gültigkeitsdatums.

Bild 13

Die Pseudonymitätsfunktion durch Restricted Identity ist ein ausweis- und anbieterspezifisches Kennzeichen (Bild 13). Es dient dazu, dass ein Diensteanbieter einen Ausweis wieder erkennen kann, ohne dass er noch einmal die Identitätsdaten des Benutzers bzw. des Ausweisinhabers abfragen muss. Bei der Einrichtung eines Benutzerkontos, also bei dem ersten Kontakt eines Ausweisinhabers bei einem Online-Dienst werden diese Kontodaten angelegt, und es wird zunächst ein anbieterspezifisches Kennzeichen übertragen. Aus diesem Kennzeichen, was für jeden Anbieter, also Inhaber eines Berechtigungszertifikates einmalig ist, wird dann mit Hilfe eines Geheimnisses auf dem Ausweisdokument, ein so genanntes bereichspezifisches Kennzeichen dieses Benutzers, dieses Ausweisinhabers übertragen und dann beim Diensteanbieter gespeichert. Dieses einmalige Merkmal kann von niemand anderem, auch nicht von einem anderen Anbieter missbraucht werden in der Form, dass er auf den Benutzer zurückschließen kann. Das ist eine ganz wichtige Angelegenheit in Bezug auf die Erfüllung von Datenschutzanforderungen.

Der Ausweis liefert unterschiedliche Kennzeichen bei unterschiedlichen Diensteanbietern und damit ist der Benutzer bei unterschiedlichen Diensteanbietern, zum Beispiel bei eBay oder bei anderen Online-Diensteanbietern, mit unterschiedlichen Kennzeichen registriert. Das gilt natürlich auch für neue Registrierungen, die aber ein Dienstleister für verschiedene Dienstleistungen dann durchführen kann. Die Berechnung erfolgt über ein Chipgeheimnis, also über einen kryptografischen Schlüssel.

Bild 14

Zusammenfassung (Bild 14): Die eID-Funktion des Personalausweises dient der elektronischen Identitätsfeststellung mit einer Genauigkeit und einer Verbindlichkeit wie das heute mit anderen Ausweisdokumenten im Internet nicht möglich ist. Die Datenfreigabe erfolgt nur bei PIN-Eingabe. Damit ist der Personenbezug für die Aktionen, die ein Ausweisdokument auslöst, gewährleistet. Die gegenseitige Authentisierung, d.h. also die Bereitstellung eines Berechtigungszertifikates für die Diensteanbieter schafft eine neue Qualität, eine hohe Sicherheit gegen Phishing und damit auch eine hohe Sicherheit, so dass ein betrügender Diensteanbieter große Schwierigkeiten hat, seinen Betrug durchzuführen. Zumindest hat er ein großes Erkennungsrisiko.

4 Erwartungen der Wirtschaft an den elektronischen Personalausweis

Klaus-Dieter Wolfenstetter, Deutsche Telekom AG, Laboratories und BITKOM, Berlin

Der von der Regierung geplante elektronische Personalausweis, ich nenne ihn hier kurz: ePA, soll neben modernen hoheitlichen Funktionen, die der ePA als Reisedokument und Ausweisdokument benötigt, auch eine Funktion zum elektronischen Identitätsnachweis des Ausweisinhabers enthalten. Wir sprechen hier von der elektronischen Identifizierungsfunktion, der eID-Funktion des ePA. Diese soll die gegenseitige Authentisierung zwischen einem Diensteanbieter und einem Dienstenutzer (allgemein gesagt: einer Bürgerin bzw. eines Bürgers) ermöglichen. Vor allem, und das ist bei Ausweisen neu, soll dies auch bei Anwendungen, die online angeboten werden, möglich sein.

Damit diese neuen Möglichkeiten auch im privaten und geschäftlichen Einsatz bei den Anbietern und bei deren Kunden, also den Bürgern, die dann einen ePA haben werden, Akzeptanz finden, müssen die Einsatzfelder der eID-Funktion in Wirtschaft und Verwaltung ausgelotet und - soweit möglich - gefördert werden.

Der politische Rahmen wurde in der E-Government-Strategie im März 2005 und im Koalitionsvertrag vom 11. 11. 2005 gesetzt und schließlich als Projekt im Regierungsprogramm E-Government 2.0 vom September 2006 gestartet. Damit sah sich die IT-Industrie aufgefordert, ihrerseits ihre Rahmenbedingungen und Ziele zur Nutzung der eID-Funktion zu definieren und diese mitzugestalten. Dieses Ziel hat sich der Verband der IT-Branche BITKOM gegeben. Der BITKOM Fachausschuss Identitäten- und Rollenmanagement arbeitet seit über zwei Jahren intensiv an diesem Thema.

Zum Thema „Einsatzfelder des geplanten ePA in Verwaltung und Wirtschaft“ veranstaltete der Fachausschuß im Juni 2007 einen Workshop. Teilnehmer waren neben den Mitgliedern des Fachausschusses vor allem eingeladene Anwendungsanbieter, die in 4 Arbeitsgruppen ihre Anforderungen und Erwartungen an die eID-Funktion diskutierten und formulierten. Wir hatten die Arbeitsgruppen in Online-Handel, Banken und Versicherungen, Luftverkehr sowie regulierte Dienstleister gegliedert. Die Ergebnisse der 4 Arbeitsgruppen waren durchaus unterschiedlich. Ziele und Erfolgsfaktoren wurden diskutiert und schließlich von allen gemeinsam eine Vision und Mission erarbeitet. Nach einigen Abstimmungsrunden wurden die Ergebnisse des Workshop am 6.12. 2007 verabschiedet und veröffentlicht.

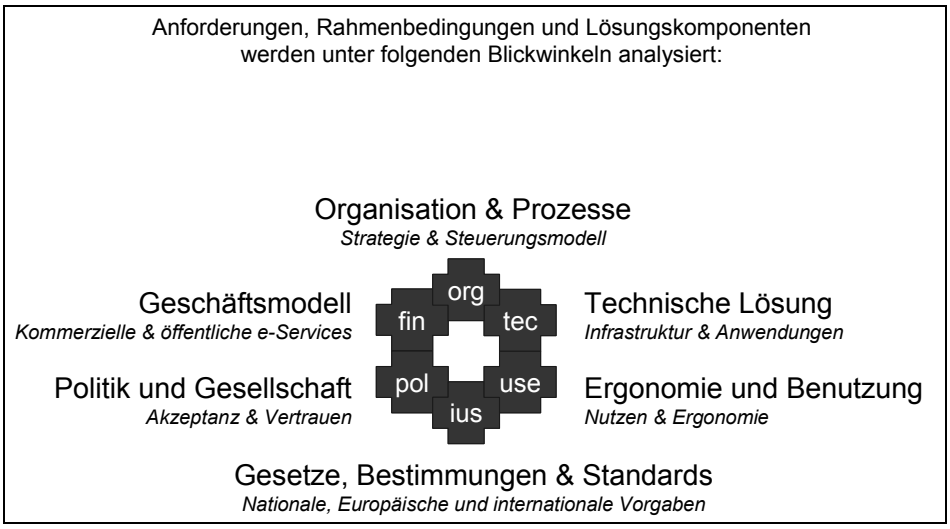

Bild 1: Erfolgsfaktoren für den Einsatz der eID

Nun zu den Ergebnissen selbst, die in 6 Erfolgsfaktoren gefasst wurden (Bild 1):

1. Geschäftmodelle: Mit dem ePA sollen Prozesse wie Erst-Identifikation, Registrierung, Authentisierung, Adress- oder Altersverifikation wirtschaftlich effizient, kostengünstig, komfortabel und kundenfreundlich - offline und online - realisiert werden. Rationalisierungseffekte und Kostenersparnisse in den Geschäftsprozessen sind signifikant.

2. Technische Lösung: Die nötige Infrastruktur (z. B. das Zertifikatsmanagement, die Kartenleser, die Middleware zwischen den Komponenten) ist finanzierbar, ist aufgebaut und wird betrieben. Idealerweise sind alle Neugeräte gleichzeitig mit der Einführung des ePA mit Lesegeräten und den nötigen Software-Komponenten ausgerüstet.

3. Gesetze, Bestimmungen und Standards: Der rechtliche Rahmen für sichere Transaktionen mit dem ePA ist mit der Industrie abgestimmt (z. B. die Frage, welche Identitätsdaten (Attribute) für die kommerzielle Nutzung sinnvoll und rechtlich zulässig sind). Der Datenschutz und die Haftungsfragen bei sorgsamer Benutzung des ePA und insbesondere etwaige Haftungsbeschränkungen sind geklärt.

4. Organisation und Prozesse: Betriebs- und Geschäftprozesse sind angepasst. Prozessanpassungen und -vereinfachungen, wie beispielsweise beim PostIdent-Verfahren, werden umgesetzt. Wo immer anwendbar, ist der ePA europaweit und international interoperabel.

5. Politik und Gesellschaft: Die eID Funktion des ePA wird vermarktet. Pilotversuche mit Musteranwendungen werden durchgeführt und gefördert. Bestimmungen und Anliegen des Datenschutzes und Verbraucherschutzes sind berücksichtigt.

6. Benutzung und Ergonomie: Der ePA wird wie andere Karten nach Eingabe einer PIN (also in gewohnter Weise) genutzt. Der ePA gibt das Gefühl von Sicherheit, ist einfach handhabbar, sowie vielseitig und verbindlich einsetzbar.

Als gemeinsame Vision von IT-Industrie und Service-Providern wurde schließlich formuliert: Der ePA identifiziert mich als Bürger und Geschäftspartner gleichermaßen in der realen wie in der virtuellen Welt.

BITKOM hat also versucht, bei Anwendungsanbietern (wie etwa eBay, Schufa, Lotto-Toto, Versicherungen, Fraport, Home Shopping provider etc.) das Interesse an der eID-Funktion zu wecken mit dem Ziel, jene in ihre Workflows zu integrieren, und damit die genannten Effizienzsteigerungen zu erzielen, oder sich damit sogar neue Geschäftsfelder zu erschließen. Auch wenn am WS selbst kein Vertreter des Bürgers teilnahm, so war doch der Blick immer auch auf den Bürger, also den Kunden der Anbieter, gerichtet. Der User spielt in den diskutierten Use Cases natürlich für den Erfolg der Geschäftsmodelle eine entscheidende Rolle.

Darüber hinaus wurde im Januar 2008 vom BITKOM eine Umfrage gestartet, die sich direkt an den Bürger richtete: Gefragt war nach dem Anteil der Internet-Nutzer, die einen elektronischen Personalausweis zur Identifikation nutzen würden.

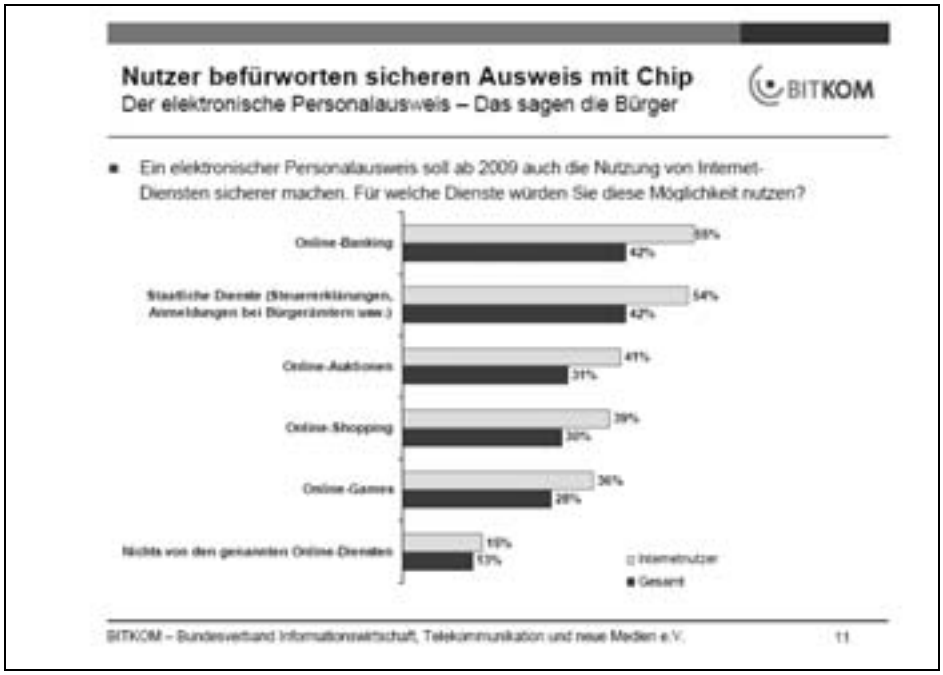

Bild 2: Surfer wollen sicheren Ausweis mit Chip

Das Ergebnis ist viel versprechend, wie sie im Bild 2 erkennen können: Es wurde auch gefragt, welche Kosten die Nutzer auf sich nehmen würden, um das erforderliche Lesegerät anzuschaffen. Immerhin erklärten sich 60 % der Befragten bereit, dafür 20 € zu bezahlen. Ob das ausreichen wird, um auch die Hotline und den Support zu finanzieren, muss geprüft werden.

Das frühe und konsequente Engagement des BITKOM wurde auch vom letzten IT-Gipfel, der am 10. Dezember 2007 in Hannover stattfand, wahrgenommen. Die dortige AG4, die

den Titel trägt: „Sicherheit und Vertrauen im Internet und in der IT“, hat den BITKOM beauftragt, weiterhin Einsatzszenarien und Geschäftmodelle zu erörtern sowie die notwendigen Schritte für einen flächendeckenden Einsatz in der Wirtschaft zu erarbeiten.

Dieser Auftrag mündete in eine Road Map für das Jahr 2008, die inzwischen mit den geplanten WSs des BMI abgestimmt ist (Bild3).

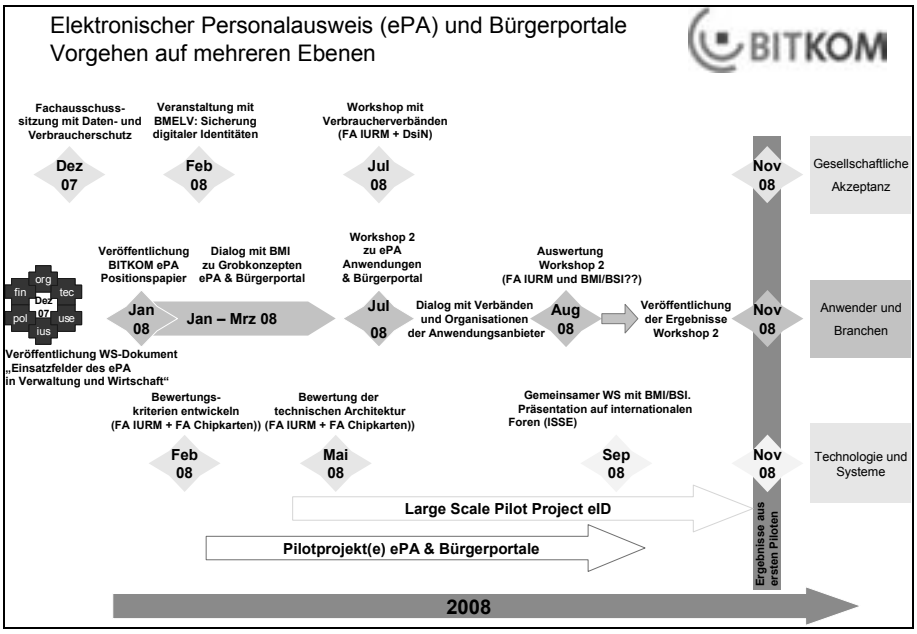

Bild 3: Road Map: Nutzung der eID-Funktion

Der Dialog mit Anbietern, Anwendern, Verbraucherschutz, Datenschutz, Wissenschaft und Wirtschaft wird fortgesetzt. Insbesondere wird am 16. Juli in der Hauptstadtrepräsentanz der Deutschen Telekom ein zweiter WS mit dem Titel „Einführungsstrategie der eID-Funktion des ePA stattfinden“. Wie im vergangenen Jahr wird eine Workshop-Methode von HP eingesetzt werden.

Ich komme nun zum Schluss: Der ePA und die mögliche Nutzung seiner eingebauten eID Funktion werden eine hohe Verbreitung finden. Er wird zu einer höheren Sicherheit führen. Er wird aber bestehende Kartensysteme nicht ablösen. Die Vereinigung dieser Eigenschaften macht ihn im Vergleich zu anderen Karten wie z. B. Bankenkarten oder SIM bzw. UICC-Karten im Mobilfunk, einzigartig. Seine Gestaltung und Nutzung geht alle an. Und Fragen, die alle betreffen, können nur alle zusammen beantworten. Deshalb ist der schon genannte öffentliche Dialog wichtig, auch in Form von Foren wie am heutigen Abend.

5 ANWENDUNGSERPROBUNGEN ZUM ELEKTRONISCHEN PERSONALAUSWEIS

Moderation: Prof. Dr. Albrecht Ziemer, Konstanz

Prof. Ziemer:
Sehr geehrter Herr Staatssekretär, sehr geehrte Herren Abgeordnete, meine Damen und Herren. Wir kommen jetzt zum Tagesordnungspunkt, der sich mit den Anwendungserprobungen des elektronischen Personalausweises beschäftigt. Hier wollen wir Ihnen insgesamt vier mögliche, vier geplante, vier vorbereitetet Pilotprojekte vorstellen und wollen Ihnen in Abfolge dessen, was bislang gesagt worden ist, deutlich machen, dass im Vorfeld der Gesamteinführung des elektronischen Personalausweises mit diesen Piloten die Zeit genutzt werden kann und genutzt werden sollte.

Ich will auf die Kriterien, die diesen Feldversuchen zu Grund liegen sollen, noch einmal ganz kurz eingehen, bevor ich dann zu den Rednern der einzelnen Feldversuche komme. Es geht einmal darum, bei den Feldversuchen in der Regel hohe Fallzahlen zu erreichen. Es hat keinen Zweck, irgendwelche akademischen Besonderheiten deutlich zu machen, sondern es sollen Feldversuche sein, die die breite Einführung, die breite Erprobung und die breite Anwendung insgesamt mit vorsehen und sich auf sie abstützen. Es sollen auch keine Showcases sein, sondern es sollen echte praxisbezogene Feldversuche sein. In diesen Feldversuchen geht es insbesondere auch darum, und das ist ein weiteres Kriterium, die so genannte medienbruchfreie Interaktion deutlich zu machen. Das sind an sich die Besonderheit und der große Vorteil des elektronischen Personalausweises, dass er das zulässt. Das ist sein ganz großer Vorteil in punkto Sicherheit und in punkto Funktionalität.

Die Feldversuche sollen als weiteres Kriterium die direkten Vorteile für den Nutzer aufzeigen. Sie sollen deutlich machen, dass über den Nutzen Akzeptanz erzeugt und entstehen wird und dass sich diese Nutzerakzeptanz aus dem Gesamtsystem ergeben wird.

Weiterhin geht es darum, dass das Gesamtsystem elektronischer Personalausweis und Eingabegeräte, also Lesegeräte, in einem Zusammenhang gezeigt werden. Der elektronische Personalausweis ist hier und heute mehrfach dargestellt worden. Man muss aber wissen, dass all die Funktionalitäten, die man von ihm erwartet, eben auch einer Eingabe und einer Auslesung bedürfen und dass es von dorther immer ein Gesamtsystem ist, das in der Betrachtung berücksichtigt und gewertet werden muss.

Die Feldversuche sollen sich außerdem sowohl an "einfache Bürger" wie aber auch an geschulte Anwender wenden. Das ist, gerade wenn ich an das Projekt T-City in Friedrichshafen denke, von großer Wichtigkeit, dass auch professionelle Benutzergruppen für ihre Geschäftsfälle Vorteile aus dem System ePA erwarten können. Die Feldversuche sollen zudem die Datensicherheit im Gesamtsystem deutlich machen. Es muss herausgestellt werden, Herr Staatssekretär Beus, Sie hatten bereits darauf hingewiesen, dass hoheitliche Daten wie die Biometrie von den geschäftlichen Anwendungen grundsätzlich zu trennen sind und für diese nicht zur Verfügung stehen. Es muss in den Feldversuchen deutlich gemacht werden, dass zwischen den beiden Bereichen getrennt werden kann.

Schwerpunkt in der geschäftlichen Nutzung des ePA ist die Identifizierung und die Authentifizierung. Insgesamt geht es um die Sicherheit internetbasierter Transaktionen im geschäftlichen Verkehr und um die Übertragung dessen, was der heutige Personalausweis in der realen Welt bedeutet auf die virtuelle Welt des Internets mit Hilfe des elektronischen Personalausweises.

Weiterhin, und auch das ist schon gesagt worden, geht es um eine schnelle Durchdringung mit dem ePA. Es sollte nicht zehn Jahre dauern bis der letzte klassische Personalausweis sozusagen im Shredder gelandet ist, sondern die Feldversuche sollen das Potenzial aufzeigen, wie eine Welle der Akzeptanz diesen Durchdringungsvorgang beschleunigen kann.

Ein letzter Punkt gilt der Frage: wer zahlt eigentlich? Der Bürger zahlt nach Gesetz für die Grundversion, für den ePA selber. Doch das Gesamtsystem einschließlich Lesegerät erzeugt Zusatzkosten und wie steht es mit ihrer Abdeckung, können sie verursachungsgerecht zugewiesen werden? Dies wird sicherlich, gerade wenn es um das Lesegerät geht, eine Diskussion sein, die mit der schnellen Durchdringung und der Akzeptanz im Zusammenhang stehen wird.

Ich gehe nun noch kurz auf die Typologien der Lesegeräte ein. Es wird einfache Lesegeräte geben müssen, die nur Identifikation und Authentifizierung möglich machen. Es wird aber auch eine gehobene Typologie von Lesegeräten geben, die dann zusätzlich auch die Signaturfähigkeit ermöglichen werden. Über PIN–Eingabe, wie vorhin mehrfach von Herrn Dr. Helmbrecht und Herrn Kowalski erwähnt. Insgesamt geht es darum, in beiden Fällen sichere und medienbruchfreie Kommunikationsräume zu schaffen.

Die vier Piloten, die nun vorgestellt werden, beinhalten sozusagen in einem gewissen Raster entweder teilweise oder zur Gänze die eben von mir noch einmal zusammengefassten Stichworte. Sie umfassen die Bereiche Finanzwirtschaft, das kommunale eGovernment, Verkehrsbetriebe und ein so genanntes Bürgerbüro.

Ich darf nun zum ersten Feldversuch kommen. Herr Dr. Büger, Sie wollen uns den Feldversuch aus der Finanzwirtschaft vorzustellen. Herr Dr. Büger ist von der Deutschen Bank, ist dort zuständig für die technologische Entwicklung und die Sicherheitstechnologie im Bankwesen. Herr Dr. Bürger hat an der Universität Gießen Mathematik studiert und ist auch im Fachgebiet Mathematik promoviert worden. Ich darf Sie bitten, uns Ihren Feldversuch vorzustellen.

Dr. Büger
(Der Vortrag ist unter Ziffer 5.1 abgedruckt)

Prof. Ziemer:
Vielen Dank Herr Dr. Büger. Ich würde vorschlagen, dass wir insbesondere die wohlwollende und interessierte Begleitung später in der Diskussion noch einmal vertiefen, denn eigentlich möchten wir da schon ein bisschen mehr von der Finanzwirtschaft erwarten, es sollte über das reine Wohlwollen hinausgehen. Es sollte etwas rüberkommen, das den Kriterien, die ich eingangs zusammengefasst hatte, entspricht und ich würde die Kollegen, die die Diskussion später leiten, bitten, dieses noch einmal zu vertiefen.

Der nächste angedachte Feldversuch betrifft das Gesamtgebiet kommunale eGovernment-Services und hier die Einbettung des ePA in das Projekt T-City in Friedrichshafen. Ich darf dazu jetzt Herrn Dr. Kaack bitten und ihn vorab kurz vorstellen. Herr Dr. Kaack ist

promovierter und studierter Physiker, war bei SEL, BMW, AEG und debis. Bei debis waren Sie für Marketing und Vertrieb zuständig und sind jetzt über innovative Geschäftsmodelle, die dann auch eine Weile Ihr Interessensgebiet waren, interimistischer Leiter des Projektes T-City in Friedrichshafen geworden. Damit liegt es nun ganz in Ihren Händen, das System ePA dort zu integrieren und zum Einsatz kommen zu lassen. Wir freuen uns auf Ihren Vortrag.

Dr. Kaack
(Der Vortrag ist unter Ziffer 5.2 abgedruckt)

Prof. Ziemer:
Vielen Dank, Herr Dr. Kaack. Sie haben einen ganzen Strauß von hochinteressanten Möglichkeiten aufgezeigt und ich finde, eine relativ kleine Stadt mit 58.000 Einwohnern besagt nicht, dass diese Möglichkeiten nicht große Skaleneffekte haben werden und sehr treffgenau in das Gesamtszenario passen können. Also, noch einmal herzlichen Dank und auch hier werden wir sicherlich in der späteren Diskussion noch vertiefend darauf eingehen können.

Ein weiteres, ich hätte fast gesagt, plakativ auf der Hand liegendes Anwendungsgebiet ist der gesamte Bereich der Verkehrsbetriebe. Es gibt den Verkehrsverbund Rhein-Ruhr, der sich mit dieser Thematik seit geraumer Zeit beschäftigt und Herr Zeino-Mahmalat wird uns für den Verkehrsverband Rhein-Ruhr und dort speziell das Kompetenzcenter Elektronisches Feldmanagement die Möglichkeiten zeigen, die sich hinsichtlich des Einsatzes des elektronischen Personalausweises ergeben können

Kurz zu seiner Person. Herr Zeino-Mahmalat hat Politikwissenschaften, Soziologie und Wirtschaftswissenschaften an der Universität Siegen studiert. Zunächst als freier Journalist tätig, ist er 2001 zum Verkehrsverbund Rhein-Ruhr gekommen. Dort war er zunächst stell-vertretender Pressesprecher und ist jetzt Leiter des eben genannten Kompetenzcenters Elektronisches Feldmanagement und hat damit den Zuständigkeitsbereich für die uns hier und heute bewegenden Dinge.

Herr Zeino-Mahmalat
(Der Vortrag ist unter Ziffer 5.3 abgedruckt)

Prof. Ziemer:
Vielen Dank Herr Zeino-Mahmalat. Sie haben aufgezeigt wie ein Kerngeschäft mit großer wirtschaftlicher Bedeutung durch den ePA unterstützt werden kann. Der Personennahverkehr ist ein Wirtschaftsfaktor, aber er ist auch für unseren Alltag etwas Elementares und Unverzichtbares und da auf diesem Wege zu Vereinfachungen zu kommen, wäre eine ganz großartige Sache.

Der letzte angedachte Feldversuch betrifft neue Prozesse im Bürgerbüro. Das sind Gedanken und Strukturen, die gegenwärtig von der Stadt München vorgedacht werden. Herr Hanfstengl ist in München Leiter des Bürgerbüros. Zu ihm gehören das zentrale Kreisverwaltungsreferat und sechs Bürgerbüros in Außenstellen mit insgesamt 220 Mitarbeiterinnen und Mitarbeitern. Das Aufgabenspektrum umfasst vom Einwohnermeldewesen über die Beantragung von Ausweisdokumenten eigentlich alles, was man sich als Bürger einer Stadt von einem Bürgerbüro wünscht. Es geht nun darum, typologische Ansatzpunkte für den Einsatz eines elektronischen Personalausweises zu finden. Wir sind gespannt auf Ihre Ausführungen.

Herr Hanfstengl
(Der Vortrag ist unter Ziffer 5.4 abgedruckt.)

Prof. Ziemer:
Vielen Dank, Herr Hanfstengl. Sie haben uns in das Herz des eGovernment hineingeführt, nämlich den Bürger da abzuholen, wo er ist, zuhause, rundum betreubar, 24 Stunden ansprechbar und nicht in einer Warteschleife. Er kann handeln, er kann interagieren.

Wir sind damit am Ende dieses Tagesordnungspunktes angekommen, in dem wir Ihnen vier mögliche Feldversuche vorstellen wollten. Ich möchte auf eine Zusammenfassung verzichten, weil wir jetzt noch eine ausführliche Diskussion haben werden, in der wir alle Möglichkeit und Gelegenheit haben, diese Feldversuche und ihr Potenzial zu vertiefen. Ich möchte mich bei den Vortragenden noch einmal recht herzlich bedanken und darf hiermit zum nächsten Punkt der Tagesordnung überleiten, zu unserer Diskussion. Nochmals vielen Dank Ihnen allen!

5.1 Einsatzmöglichkeiten des ePA in der Finanzwirtschaft

Dr. Matthias Büger, Deutsche Bank AG, Frankfurt

Es ist eine besondere Freude und Ehre für mich, am heutigen Tage zu Ihnen zu sprechen, wobei ich eine kleine Erwartung an dieser Stelle ein bisschen dämpfen muss. Aber das ist vielleicht im Ausblick auch gar nicht problematisch. Ich kann noch keinen Piloten oder einen Feldversuch in dem Sinne vorstellen. Wenn wir das Wort Pilot verwenden, meine ich, dass es da konkret etwas gibt in das man eine Karte steckt und das funktioniert. Das haben wir nicht für den Personalausweis, aber wir haben Signaturkarten, die konkret in Anwendungen funktionieren.

Als ich angefragt worden bin – ich schaue in die Richtung von Herrn Kowalski –, am Rande des IT Gipfels, den wir auch mit viel Freude und Interesse begleiten, bat er mich, ich solle etwas sagen zu den Einsatzmöglichkeiten des elektronischen Personalausweises in der Finanzwirtschaft. In dem Wort Einsatzmöglichkeiten steckt das Wort Möglichkeiten, d.h. es geht um Dinge, die ich für möglich halte. Es heißt natürlich auch, dass es Sachen sind, die nur „möglich“ sind und also noch nicht entsprechend umgesetzt. Aber daran, dass sie real werden, wollen wir gemeinsam arbeiten.

Zunächst will ich anfangen mit dem großen Bild, was Sie sicherlich nicht überraschen wird und das viele kennen. Ich habe die Überschrift bewusst an der Stelle so gewählt und sage ganz klar: Authentisierung ist für die Finanzwirtschaft und für das Bankgeschäft ganz wesentlich. Ich glaube sogar, dass es hier eine Ähnlichkeit gibt zwischen dem eBanking und dem eGovernment, was sie sogar von vielen anderen Branchen unterscheiden mag. Wenn Sie bei eBay etwas kaufen, bei Amazon etwas kaufen, dann kommt am Ende noch jemand, der das körperlich bringt. Dann ist sozusagen die Sache abgeschlossen, wenn der Postbote vorbeikommt. Es ist noch etwas Körperliches, was wirklich von rechts nach links geht. Letztendlich ist es bei uns die Tatsache, dass man am Ende sich über einen bestimmten Geschäftsvorfall, den man abschließt wie bei einer Transaktion, entsprechend einig ist und danach eine Willenserklärung abgibt und sagt: ja, bitte Bank, führe dieses Geschäft durch! Aufgrund dieser Willenserklärung führen wir das Geschäft entsprechend durch. Genau so sagen Sie auch im eGovernment, dass Sie etwas Bestimmtes vornehmen möchten, eine Anmeldung, eine Ummeldung. Sie erklären, dass bestimmte Daten, z.B. in der Steuererklärung, ihre Richtigkeit haben. Insoweit haben wir hier durchaus eine Ähnlichkeit.

Ich habe es in drei Bereiche unterteilt, die uns als Finanzwirtschaft wichtig sind und die durchaus auch unterschiedlich zu bewerten sind und wo man unterschiedliche Ansätze benötigt. Zum einen der gesamte Bereich der Kontoeröffnung, dass, wenn Sie zum ersten Mal einen Vertrag entsprechend abschließen. Und das ist im Übrigen ein durchaus interessanter Bereich, denn es sitzt vielleicht jemand am Samstagabend um 23 Uhr auf der Couch und sagt, dass er einen bestimmten Betrag auf seinem Konto anlegen möchte. Er schaut sich unterschiedliche Angebote an und sieht bei dem einen oder anderen Angebot, dass das seine Hausbank nicht hat und möchte es abschließen. Er möchte nicht warten, bis am Montagmorgen die Bank öffnet oder bis am Dienstag ein Post-Ident möglich ist, sondern er möchte es in dem Moment durchführen. Hier sind ganz klar eine sichere Identifikation und Vertragsabschluss, durchaus zwei getrennte Dinge. Ganz wichtig sind auch die rechtlichen Anforderungen, die wir hierbei als Kreditwirtschaft zu beachten haben. Das sind im

wesentlichen Kreditwesengesetz (KWF), Geldwäschegesetz (GWG) und Abgabenordnung (AO).

Bei bestehenden Kundenverbindungen unterscheidet man zwischen der Weitergabe Information und einer Transaktionen. Bei Information denkt man zunächst einmal, dass dies nicht sehr kritisch ist. Es passiert ja nichts, es fließt kein Geld. Das ist richtig, aber auch mit der Information müssen wir natürlich sehr vorsichtig umgehen. Wer möchte schon, dass sein eigener Kontostand, sein Depotstand in irgendwelche fremde Hände gelangt? Also, insoweit ist auch die reine Information, eben die Abfrage von Umsätzen und Kontoständen durchaus etwas sehr wichtiges und auch ein sehr schützenswertes Gut. Auf der anderen Seite – und das behalte ich immer im Auge – geht es auch um Ausgabe von Belegen, zum Beispiel Steuerbescheinigungen u.ä., die der Kunde benötigt und die weiter gegeben werden müssen. Das ist auch etwas, das ich sicher nicht mit dem Personalausweis selbst, aber mit dem gesamten Verfahren zu tun hat. Wir brauchen Zertifikate, die ausgegeben werden für Institutionen – und das sollte sich in einem solchen Rahmen auch lösen lassen.
Zuletzt erwähne ich dann noch die Transaktionen: Überweisungen oder Online-Brokerage, Wertpapiergeschäft.

Ich will kurz auf die beiden großen Punkte eingehen: Kontoeröffnung, Kontoinformation und Transaktion.

Was ist der Nutzen eines Personalausweises im Bereich der Kontoeröffnung? Hier sehe ich ganz deutliche und ganz klare Vorteile, nämlich genau in dem, was Herr Prof. Ziemer auch gesagt hat, in der Ablösung manueller Prozesse. Genau darum muss es gehen. Manuelle Prozesse sind aufwendig, sie sind für den Kunden teuer, sie sind auch für uns teuer – vorausgesetzt die Regularien werden entsprechend angepasst. Das ist meine Bitte, die ich an der Stelle formulieren möchte, auch an den Regulator, die Bundesregierung, aber selbstverständlich dann auch an die Legislative. Die Regularien, die die Finanzwirtschaft betreffen, eben Geldwäschegesetz, Abgabenordnung, Kreditwesengesetz, auch so anzupassen, dass mit einem solchen elektronischen Personalausweis dann auch eine Kontoeröffnung möglich ist und es nicht heißt, das ist ein Antrag, aber am Ende muss doch eine Kopie des Personalausweises vorliegen, weil das in einem dieser nämlichen Gesetze drinsteht. Oder derjenige muss den dort persönlich jemand vorgelegt haben, was er natürlich im elektronischen Verfahren nicht getan hat. Dies entsprechend nachzuziehen, ist etwas Notwendiges, sonst haben wir einen Schritt getan und können den zweiten an dieser Stelle nicht gehen. Ein weiterer Vorteil, den ich auch durchaus für unser Haus sehe, ist mehr Wettbewerb. Ganz einfach, der Kunde ist um 11 Uhr abends im Internet, kann viele Angebote sehen. Da ich ein großer Verfechter der Marktwirtschaft bin, ist das etwas, was grundsätzlich zu begrüßen ist. Die Kostenersparnis liegt hier auf Seiten der Banken und damit auch auf Seiten unseres Hauses dann und nur dann, wenn die teuren Medienbrüche hier vermieden werden können, d.h. wenn wir die gesetzlichen Anpassungen haben, auf teure Verfahren verzichten können, haben wir hier auch einen ganz klaren Nutzen geschaffen. Bei der erstmaligen Kontoeröffnung haben wir ein ganz eindeutiges Potenzial, was wir sehen.

Zweiter Punkt sind Kontoinformation und Transaktion, also das, was Sie aus dem klassischen Online-Banking kennen. Selbstverständlich besteht auch hier die Möglichkeit, den elektronischen Personalausweis einzusetzen. Der Unterschied zur Kontoeröffnung ist der, dass es hier bereits Verfahren gibt, die medienbruchfrei, auf eine elektronische Art und Weise das aktuell abbilden. Auf Verfahren ist Herr Kowalski auch schon in seinem Vortrag eingegangen, Thema PIN/TAN. Ich vermute, fast jeder hier im Raum hat schon einmal ein PIN/TAN-Verfahren verwendet. Ich habe gerade die neuesten Zahlen von einem Kollegen des

Bankenverbandes gehört, dass für so ungefähr rund 35 Millionen Konten in Deutschland Online-Banking freigeschaltet sind. Bei uns im Bereich der privaten Banken ist der Anteil bei über 50%, also schon sehr hoch. Im Bereich Sparkasse und Volks- und Raiffeisenbank ein wenig geringer. Aber insoweit haben wir hier sehr etablierte Verfahren. Verfahren, die Stärken und Schwächen haben, wie das alle diese Verfahren haben. Deren Stärken und Schwächen wir auch kennen, und wo wir uns als Kreditwirtschaft noch immer darum bemühen, diese Verfahren fortzuentwickeln. Sie kennen die iTAN, die unser Haus anbietet. Es gibt in anderen Häusern mTAN oder TAN-Generatoren. Es gibt unterschiedlichste Formen dort. Wir haben auch Karten im Einsatz. So haben wir im Rahmen des Signaturbündnisses, das wir gemeinsam mit der Bundesregierung betrieben haben, auch ein Signaturkarte für den Einsatz für Online-Banking. Insgesamt kann man aber sagen, dass dort etablierte Verfahren bestehen, die auf jeden Fall eines sind, nämlich kostengünstig. Auch die Fraud-Rates sind zumindest nach dem Stand heute und in der Vergangenheit nicht so, dass sie kostenmäßig ein massives Problem darstellen, was zum Glück ja auch schön für unseren Standort ist. Wir werden auch alles dafür tun, dass das entsprechend so bleibt.

Die Folgerung ist an der Stelle, dass wir hier verhältnismäßig wenig Kostenersparnis haben im Vergleich zu der Ablösung der manuellen Prozesse bei der erstmaligen Anmeldung, gleichzeitig aber natürlich den Kundennutzen sehen. Der Kunde kann auch durchaus mehrere Bankverbindungen haben und wenn unser Kunde sagt, dass er sich gern mit dem Personalausweis einloggen möchte, weil er sich dann nur eine PIN merken muss, nämlich die für den Personalausweis. Damit kann er bei fünf unterschiedlichen Banken seine Konten bedienen. Warum nicht? Warum sollte ich meinen Kunden an der Stelle daran hindern? Und wenn ich an die 55% denke, die sich nach der soeben vorgestellten Untersuchung den Einsatz des Personalausweises beim Online-Banking wünschen, werden wir unseren Kunden dort selbstverständlich entgegenkommen. Es wäre auch ein Anachronismus, wenn wir das an der Stelle nicht täten. In dem Sinne sehe ich ganz klar den entsprechenden Kundennutzen. Und wenn der Kunde das entsprechend will, selbstverständlich. Ich warne nur davor, an der Stelle zu hohe Gewinne oder Kostenersparnisse einzurechnen. Das ist aber vielleicht auch gar nicht das Notwendige an dieser Stelle.

Damit will ich zu meinem Fazit und zum Ende meiner Vorstellung hier kommen und zusammenfassen.

Erstens, ganz klar: Authentisierung ist für die Finanzwirtschaft grundsätzlich ein wichtiges Thema. Es war ein wichtiges Thema und wird auch ein grundsätzlich wichtiges Thema bleiben, weil es bei jeder Transaktion, bei jeder Information, die ich habe, wesentlich ist zu wissen, wer an der anderen Seite der Leitung ist. Authentisierung ist das ganz wichtige Thema. Ob die qualifizierte Signatur und an welcher Stelle, ist eine ganz andere Frage. Wenn ich weiß, wer ins Online-Banking hineingegangen ist und wer den Klick macht, ist mir das doch durchaus ausreichend. Ich kann auch bestimmte Verträge mündlich machen. Ich muss nicht alles schriftlich machen. Ich muss nur wissen, wer sicher an der anderen Stelle der Leitung ist. Wenn ein Personalausweis das bietet, dann ist mir das für 99,9% meiner Geschäftsvorfälle ausreichend. Und wo es um die ganz großen Summen geht, sind die Vorgänge ohnehin anders organisiert: Unsere Händler im Bereich Investmentbanking machen Geschäfte am Telefon, weil sie sich persönlich kennen. Die haben wiederum völlig andere Mechanismen.

Zweitens: Einsatz des elektronischen Personalausweises bei der Kontoeröffnung. Hier sehe ich einen sehr großen wirtschaftlichen Nutzen. Ich weiß, dass wir hier noch einige Hürden haben, aber wir ja auch noch eine gewisse Zeit, in der wir diese Hürden aus dem Weg räumen

können. Ich würde einfach die Bitte äußern, dass wir die gesetzlichen Anforderungen entsprechend nachziehen, damit wir dies auch durchführen können. Auch für eine Kreditwirtschaft wäre das sicherlich ein bohren dicker Bretter, wenn Sie erstmals ein Konto eröffnen, ohne eine handschriftliche Unterschrift hinterlegt zu haben, weil es eine rein elektronische Unterschrift ist. Das wäre ein völlig neuer Vorgang für eine Kreditwirtschaft. Aber auch das sind alles Dinge, an die wir uns schlicht heran wagen werden.

Drittens: Einsatz bei Online-Banking und Brokerage. Den sehe ich primär unter dem Gesichtspunkt der Kundenfreundlichkeit. Selbstverständlich sehe ich das an dieser Stelle und kann auch insoweit für unsere eigene Fachabteilung sagen, mit der ich mich im Vorfeld auseinander gesetzt habe, dass unser Kunde, wenn er es will, nicht notwendigerweise nur unsere Medien nutzen können sollte. Wenn er einen Personalausweis hier an der Stelle nutzen möchte und sagt, das ist das Medium, mit dem ich das tun möchte, werden wir uns dem mit Sicherheit nicht in den Weg stellen. Oder anders herum: wir werden das gerne fördern.

Bis auf weiteres werden wir natürlich parallele Systeme haben. Das heißt, eine vollständige Ablösung wird es sicherlich nicht geben. Wir werden parallel diese Welten durchziehen müssen. Das hat in den Prozessen manche Schwierigkeiten, auch weil bestimmte Dinge parallel sind. Es ist etwas, dem man entsprechend ins Auge sehen muss.

Insoweit sehe ich als Quintessenz für die Finanzwirtschaft. In jedem Fall kann ich es für unser Haus versprechen, aber ich denke auch, so wie ich alle Kollegen aus anderen Gremien der Finanzwirtschaft kenne, kann ich sogar für die Gesamtfinanzwirtschaft sagen, dass wir die Entwicklung des elektronischen Personalausweises weiterhin wohlwollend und mit Interesse begleiten werden. Inwieweit es jetzt ein Pilot, ein Feldversuch oder ähnliches wird, hängt einfach von dem Konkreten ab, was wir an der Stelle haben. Insgesamt halten wir die Entwicklung einer solchen Infrastruktur, die Identifikation ermöglicht und dann sichere Authentisierung erlaubt, für etwas, was sehr wichtig ist auch für den Finanzsektor und was wir an der Stelle sehr begrüßen.

5.2 Einsatz elektronischer Identitäten im Rahmen des T-City Projektes

Dr. Jürgen Kaack, FN-Dienste GmbH, Friedrichshafen

Ich bin für das Projekt T-City von Seiten der Stadt Friedrichshafen verantwortlich. Als Vertreter der Stadt bin ich in Ihrem Kreis vor dem Hintergrund der überschaubaren Einwohnerzahl von Friedrichshafen mit gerade mal rd. 58.000 vielleicht ein Exot, da eine mittelgroße Stadt nicht der typische Testkandidat für den elektronischen Personalausweis ist. Allerdings, Herr Prof. Ziemer hat es gerade erwähnt, wir setzen in Friedrichshafen das Projekt T-City um. Ich möchte im Rahmen des Vortrags zeigen, wo wir in T-City Friedrichshafen Ansätze für den Feldversuch mit dem elektronischen Personalausweis sehen.

Bild 1

Zunächst einige kurze Hintergrundinformationen (Bild 1). T-City ist hervorgegangen aus einem Städtewettbewerb, den die Deutsche Telekom durchgeführt hat und an dem sich von 450 möglichen mittelgroßen Städten 52 beteiligt haben. Unter diesen 52 ist dann Friedrichshafen im Februar letzten Jahres als Sieger hervorgegangen. Friedrichshafen ist heute die T-City und ein derartiges Projekt gibt es in der Tat nur einmal, zumindest in Deutschland. Auch im Vergleich zu anderen Ländern ist das Projekt in Friedrichshafen weitgehend einmalig.

Die konkrete Projekt-Phase startete dann im August letzten Jahres mit der Unterzeichnung der Rahmenvertrags zwischen der Stadt Friedrichshafen und der Deutschen Telekom. Auf der Grundlage dieses Vertrages konnte die Arbeit im Projekt aufsetzen. Eine wesentliche Voraussetzung für die Umsetzung der Breitbandanwendungen war der Ausbau der Festnetz- und Mobilfunk-Infrastruktur. Wir haben als einzige Stadt dieser Größenordnung in Deutschland, vielleicht sogar in Europa in Friedrichshafen eine flächendeckende VDSL Infrastruktur und zusätzlich ein schnelles HSDPA Mobilfunknetz. Mit dieser Infrastruktur als Grundlage können sehr viele Breitbandanwendungen getestet werden. Denn nicht die

Infrastruktur ist der eigentliche Kern von T-City, sondern die Anwendungen auf dieser Infrastruktur. Insofern bietet T-City eine Innovationsplattform. Es ist Chance, Angebot und die Möglichkeit, neue Anwendungen in sehr unterschiedlichen Einsatz-Feldern und Lebenslagen zu erproben.

T-City ist eigentlich kein Technologieprojekt und auch kein „klassisches“ Telekommunikations-Projekt, das mit einer fertigen Technik auf den Markt kommt. Es ist ein Gemeinschaftsprojekt zunächst einmal zwischen der Stadt Friedrichshafen und der Deutschen Telekom, in den Projekten aber jeweils auch von Partnern aus der Stadt mit entsprechenden Umsetzungspartnern bei der Deutschen Telekom. Dieses Vorgehen macht T-City tatsächlich einmalig.

Mit einer Laufzeit bis 2012 können wir nicht nur Dinge auf den Weg bringen, sondern auch beobachten, wie die einzelnen Projekte wirken bzw. wie sich der Nutzen in der Praxis tatsächlich darstellt.

Bild 2

Wenn man neue Projekt-Ideen bewertet, dann sind nicht alle zur Umsetzung geeignet (Bild 2). Ein T-City Projekt sollte Telekommunikations- und IT-Technologien verwenden. Für uns steht aber immer der Nutzen für die Zielgruppe im Vordergrund und nicht die Technologie. Das ist auch im Hinblick auf den geplanten Feldversuch von Bedeutung, auf den ich nachher eingehen möchte. Wir suchen natürlich insbesondere nach solchen Projekten, die Innovation und Strahlkraft bringen und damit die Möglichkeit beinhalten, bei einem Erfolg bundesweit in anderen Städten eingesetzt zu werden. Ein wesentliches Element ist dabei, wie schon erwähnt, die aktive Mitwirkung von Partnern aus der Region.

Über diesen Projektzeitraum hinweg und bedingt durch neue Technologien sowie Wechselwirkungen zwischen den Anwendungen erwarten wir, dass sich Anwendungen verändern. Hierfür sind wir vorbereitet. T-City ist eine ideale Plattform, um auch veränderte

Ideen aufzugreifen und um zu setzen. Das ist ein Grund, warum wir uns in Verbindung mit T-City Projekten auch mit dem Thema der elektronischen Identitäten beschäftigen.

Damit keine Projekte verfolgt werden, die keinen ausreichenden Nutzen bringen oder vielleicht nur einer theoretischen Idee folgen, ist ein Business-Plan eine notwendige Voraussetzung für T-City-Projekte. Nur so können wir letztlich Nachhaltigkeit absichern. Wir wollen bei T-City keine technologischen Labor-Versuche realisieren, nur weil die erforderliche Technologie verfügbar ist oder weil sie theoretisch interessante Chancen bietet, sondern Projektidee umsetzen, bei denen ein Erfolg konkret absehbar ist. Wie bei allen Innovationen wird man dabei nie von vorhersagen können, welche Projekte die Erwartungen dann tatsächlich erfüllen. Das kennt man ja auch von Unternehmensgründungen. Aber wir wollen die Chancen doch zumindest bestmöglich prüfen und absichern.

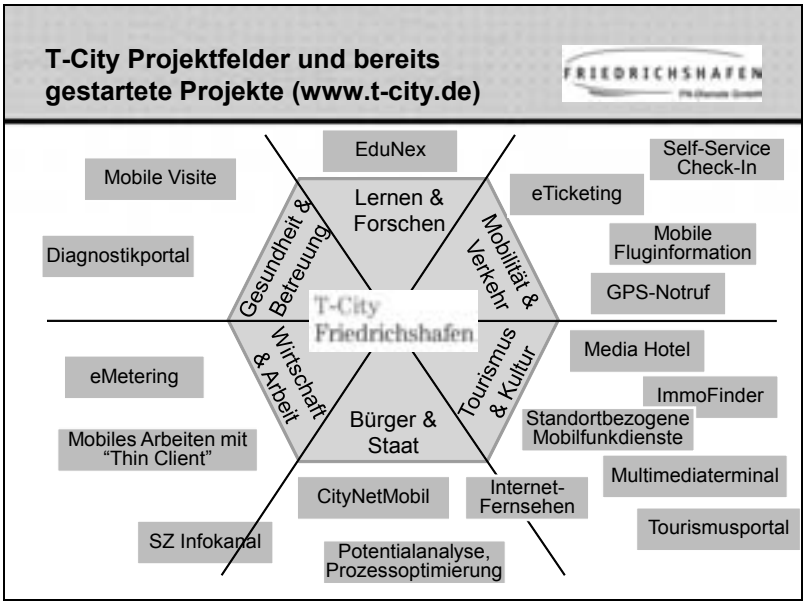

Bild 3

Mit dem Chart zu den Projektfeldern möchte ich Ihnen kurz zeigen, in welcher Breite wir bei der Projektarbeit tätig sind (Bild 3). Wir haben unsere Aktivitäten in sechs Projektfelder gegliedert, die als eine Hilfe für die Strukturierung dienen, nicht als Ausgrenzung. Es mag durchaus Themen geben, die nicht eindeutig in das eine oder andere Projektfeld passen. In diesem Fall treffen wir eine bestmögliche Zuordnung. Wir decken grundsätzlich alle Bereiche ab, die ein Bürger in seinen Lebenslagen betreffen oder die ein Unternehmen bewegen. Im Projektfeld „Lernen & Forschen decken wir alle Bereiche vom Vorschulbereich bis zur Erwachsenenbildung ab. Das Projektfeld "Verkehr & Mobilität" verfolgt insbesondere den Aspekt der Mobilität, weil wir das gesamte Spektrum der Bewegung von Personen und Gütern einbeziehen wollen. Der Bereich „Tourismus & Kultur" ist für eine Stadt wie Friedrichshafen mit einer ausgeprägten Tourismusindustrie natürlich von hoher Bedeutung. Das Projektfeld „Bürger & Staat" umfasst soziale Bereiche und den Themenkomplex eGovernment. Weitere Projektfelder sind „Wirtschaft & Arbeit" sowie „Gesundheit & Betreuung".

Die in dem Chart gelb unterlegten Felder stehen für Projekte, die entweder schon in der Umsetzung sind oder in der konkreten Vorbereitung. Seit Ende Sommer letzten Jahres haben 17 Projekte auf den Weg zur Umsetzung gebracht. Ich gehe davon aus, dass die Breite der Themen in den nächsten Monaten mit neuen Projekten weiter anwachsen wird.

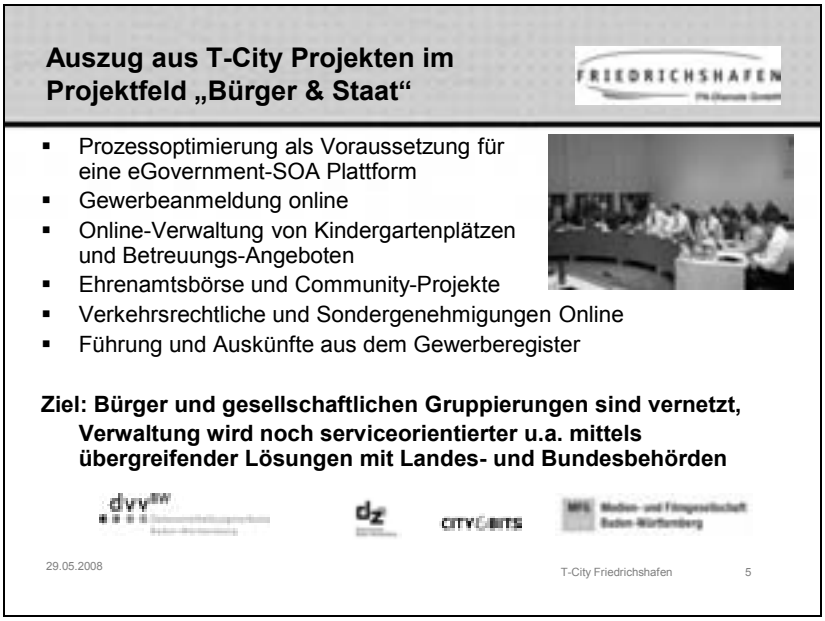

Bild 4

Ausgehend von der Darstellung des T-City Vorhabens möchte ich auf das Kernthema dieses Vortrags zurückzukommen mit der Frage: Wo lassen sich elektronische Identitäten einsetzen? Im Bereich unseres Projektfeldes „Bürger & Staat“ haben wir uns mit der Prozessoptimierung in der Verwaltung beschäftigt (Bild 4). Das zugehörige Projekt der Prozessanalyse und der Neugestaltung von Abläufen steht kurz vor seinem Abschluss. Eine Erkenntnis aus dem Projekt ist zu identifizieren, welche Verfahren sich durch eine Digitalisierung optimieren lassen. Für die Umsetzung wird eine Gesamtarchitektur gestaltet mit einer SOA-Plattform. In Verbindung mit der Neugestaltung der Prozesse kann der Einsatz von elektronischen Identitäten den Vorteil bieten, eine medienbruchfreie Umsetzung zu ermöglichen. Dies schafft die Voraussetzung für einen höheren Nutzen.

Verfahren wie die Gewerbeanmeldung online, aber auch auf den ersten Blick eher „kleinere“ Themen wie eine digitalisierte Organisation einer Ehrenamtsbörse oder die Kindergarten-Verwaltung sind hier zuzurechnen. Dies sind Ansätze, die im kommunalen Umfeld verankert sind und ihren jeweiligen Randbedingungenfolgen entsprechend umgesetzt werden müssen.

Die Zielsetzung in dem angesprochenen T-City Projekt ist es, die Bürger und die gesellschaftlichen Gruppierungen stärker untereinander zu vernetzen, unter Nutzung der in Friedrichshafen vorhandenen Breitbandinfrastruktur, aber eben auch unter Nutzung von realen nutzenstiftenden Anwendungen. Auf diesem Wege soll die Verwaltung aus Sicht des Bürger und der Unternehmen serviceorientierter und effizienter werden. Für die Umsetzung suchen wir die enge Zusammenarbeit mit dem Land Baden-Württemberg und mit dem Bund, um so die Entstehung von Insellösungen zu vermeiden.

Bild 5

Ein weiteres Projektfeld, das unter dem Aspekt der Nutzung elektronischer Identitäten interessant erscheint, ist „Wirtschaft & Arbeit“ (Bild 5). Das Projekt eMetering zur quasi online Messung und Erfassung von Strom und Gas ist eines der ersten Projekte aus diesem Projektfeld. Ein weiteres Projekt zur Realisierung der Voraussetzungen für vernetztes und mobiles Arbeiten bietet interessante Ansätze zur Integration von elektronischen Identitäten zu. Hier geht es ja unter anderem um mobiles Arbeiten und Kollaborationsgruppen, bei denen Arbeitsgruppen zusammenwirken sollen, die nicht am selben Standort sind und teilweise nicht mal zum gleichen Unternehmen gehören. Hierfür sind eindeutige Identitäten wichtig, z.B. zum Schutz sensibler Daten. Die Großunternehmen setzen zu diesem Zweck heute eigene Signaturkarten ein, in der Regel sind dies proprietäre Systeme, die nicht von Dritten verwendet werden können. Ein generell nutzbares System, das offen ist für die Einbindung Unternehmensfremder, bietet Vorteile.

Generell wollen wir in diesem Feld weitere Verfahren testen. Eine Ausschreibungsplattform für Handwerker und Dienstleister eröffnet ein weiteres Einsatzfeld. In die Thematik eBusiness werden nach unserer Überzeugung zunehmend auch kleinere Unternehmen einbezogen. Die verfolgte Vision lässt sich zusammen fassen mit: „Die Arbeitsmethoden der Zukunft erproben und sehen, welche Akzeptanz zur Annahme besteht.“

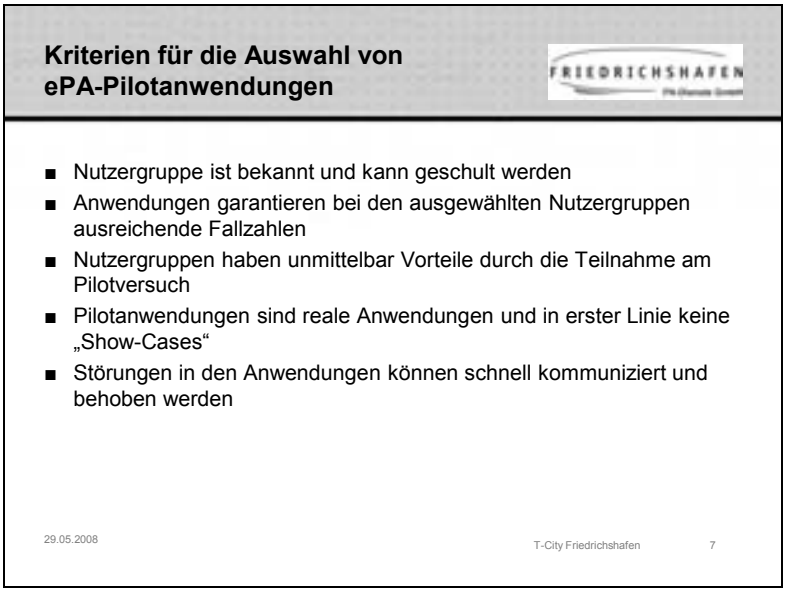

Bild 6

Analog zu den Kriterien für T-City Projekte sehen wir auch die Kriterien für ePA-Pilotanwendungen (Bild 6). Hier ist zunächst an zu merken, dass der Einsatz elektronischer Identitäten nicht als eigenes T-City Projekt zu verstehen ist. Wohl aber kann die Erprobung auf Ergebnissen der erwähnten T-City Projekte aufsetzen.

Damit ein Pilotversuch mit elektronischen Identitäten erfolgreich verlaufen kann, müssen die potenziellen Nutzergruppen bekannt oder identifizierbar sein. Wir halten es nicht für sinnvoll in einem Pilotversuch mit im Vorfeld unbekannten Nutzern zu starten, die nicht geschult und qualifiziert werden können. So lassen sich die Ergebnisse auch begleitend auswerten.

Auch hier wurde schon mehrfach erwähnt, dass für einen Pilotversuch ausreichend hohe Fallzahlen notwendig sind. Ein Pilotversuch wird scheitern, wenn einzelne Nutzer die elektronischen Identität selten oder nur in Einzelfällen einsetzen. Für den Test benötigen wir solche Gruppen, die tatsächlich häufiger elektronische Identitäten verwenden. Die Analyse der möglichen Zielgruppen führt schnell zu gewerblichen und kommerziellen Gruppen, die ihre Identität häufiger im Rahmen ihrer normalen Geschäftstätigkeit nachweisen müssen. Ein mögliches Beispiel habe ich schon erwähnt, die Einrichtung Arbeitsgruppen mit Vertretern unterschiedlicher Unternehmen.

In Analogie zu Anforderungen an T-City Projekte ist es genauso wichtig, dass die Teilnehmer bei diesem Feldversuch schon während der Pilotphase einen sofortigen Nutzen erfahren. Entsprechend ist für uns wichtig, dass wir reale Anwendungen erproben. Showcases wollen wir nicht bauen und dies ist auch bei T-City Projekten nicht vorgesehen. Wir gehen davon aus, dass sich solche konkreten Anwendungen auch identifizieren lassen. Für reale Anwendungen im operativen Betrieb ist es unabdingbar, das mögliche Störungen schnell erkannt und beseitigt werden.

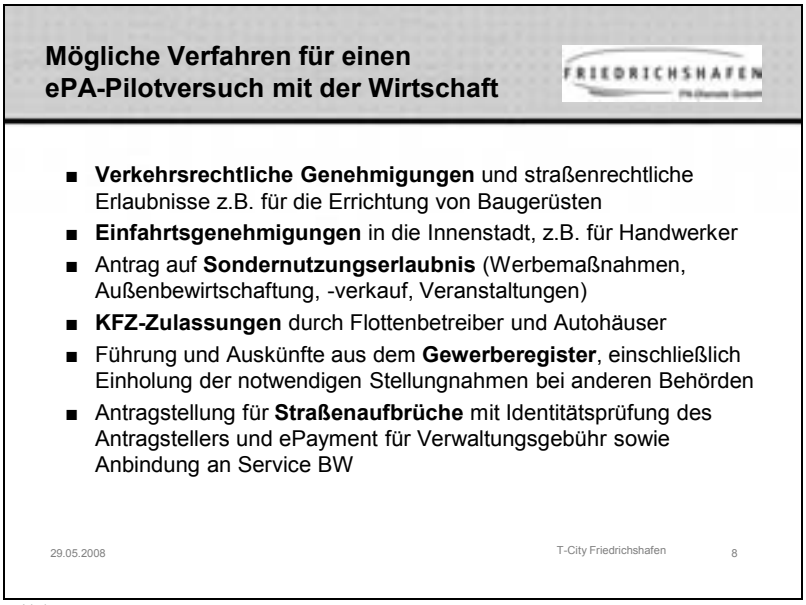

Bild 7

Bild 7 gibt Beispiele für Anwendungen, die uns als für einen Pilotversuch geeignet erscheinen. Sie finden hier Verwaltungsvorgänge und Anwendungen, die im privatwirtschaftlichen Bereich genutzt werden. Für Handwerksbetriebe, Kleinunternehmen fallen Anwendungen wie z.B. verkehrsrechtliche Genehmigungen häufig an. Selbst eher einfache Verfahren, wie die Genehmigung zur Errichtung von Baugerüsten erfordern heute einen Gang zum Rathaus. Diese Wege lassen sich durch einen automatisiertes und digitalisiert Verfahren einsparen. Mit solchen Anwendungen lassen sich die benötigten Fallzahlen erreichen. Ähnliches gilt für Einfahrtsgenehmigungen in die Innenstadt, die heute ebenfalls im Rathaus beantragt werden muss. Sondernutzungserlaubnisse sind weitere möglicherweise geeignete Anwendungen. Eine weitere in Betracht kommende Anwendung ist das Ersuchen um Auskünfte aus dem Gewerberegister. ePayment kommt als sinnvolles Ergänzungsmodul zu den genannten Anwendungen hinzu. Erst in Verbindung mit ePayment kann ein Verfahren komplett online abgewickelt werden.

Wenn Sie die ausgewählten Beispiele betrachten, die wir hoffentlich bis Anfang nächsten Jahres so weit vorbereitet haben werden, dass sie in einen Pilotversuch eingebracht werden können, stellen Sie fest, dass sie sich mit Identifikation und Authentifizierung beschäftigen. Die digitale Signatur steht bei uns derzeit nicht im Vordergrund und kommt möglicherweise erst später als Anforderung hinzu.

Ich möchte diesen Aspekt noch mal zusammen fassen: Für die ePA-Pilotanwendung sehen wir die Möglichkeit sie auf einzelne T-City Projekte aufzusatteln. Es sind derzeit aber keine T-City Projekte im eigentlichen Sinn. Ich gehe aber davon aus, dass sich der Pilotversuch mit elektronischen Identitäten gut in vorhandene Projekte einbettet werden kann und die Möglichkeit gegeben ist, dies auch in Friedrichshafen auf der Basis realer Anwendungen durch zu führen.

Bild 8

Innovationsvorhaben und Pilotversuche müssen sich in die Gesamtziele „Erhöhung von Lebensqualität für Bürger und Erhöhung der Standortqualität für Unternehmen“ einbetten (Bild 8). Ein weiteres Ziel ist die Steigerung der Vernetzung zwischen Bürgern, Unternehmen und der Verwaltung.

5.3 Einsatz des ePA für die Online-Kundenbetreuung im ÖPV

Nils Zeino-Mahmalat, Verkehrsverbund Rhein-Ruhr, Gelsenkirchen

Kurz zu meiner Person. Es war schon als Journalist das wirkliche Leben. Ich hatte als freier Journalist die Chance für die Westfälische Rundschau aus der alten Bundeshauptstadt Bonn noch mit zu berichten, bin dann beim Verkehrsverbund als Pressesprecher gelandet und habe hausintern gewechselt und leite jetzt das Kompetenzcenter Elektronisches Fahrgeldmanagement. Dahinter verbirgt sich das eTicket im ÖPV. Vielleicht ein paar Worte zum Hintergrund, warum ich mich eigentlich mit dem Thema beschäftige, was uns beim ePA interessiert. Wir haben einen Hintergrund, wo wir herkommen, weil wir schon eine elektronische Welt haben.

Zur Institution: das Kompetenzcenter Elektronisches Fahrgeldmanagement ist eine Einrichtung des Landes Nordrhein-Westfalen beim Verkehrsverbund Rhein-Ruhr. Das Land Nordrhein-Westfalen hat Interesse daran, dass elektronische Verfahren im Ticketing landesweit einheitlich aufgebaut werden und dass das Know how gebündelt ist. Dass nicht jeder Verkehrsverbund in Nordrhein-Westfalen, nicht jedes Verkehrsunternehmen, eine eigene Know-how-Kompetenz aufbauen muss. Wir beraten alle Verkehrsbetriebe und Verbünde in unserem Bundesland.

Was machen wir bisher? Wir haben eine Geschichte im Bereich des eTickets. Wir haben im Jahr 2003 angefangen, unsere Tickets zu elektronisieren, sie völlig zu virtualisieren. Sie existieren für Abonnement Kunden nur noch auf Chipkarten als Datensatz. 2003 haben wir angefangen. Wenn man jetzt die Verkehrsverbünde Rhein-Ruhr - die Region im Ruhrgebiet, Bergisches Land, Wuppertal, Großraum Düsseldorf, ein bisschen Niederrhein ist dabei, die Verkehrsgemeinschaft Niederrhein ist der restliche Niederrhein und den Verkehrsverbund Rhein Sieg, dahinter verbirgt sich der Großraum Köln, Bonn – zusammennimmt, so haben wir jetzt 1,5 Millionen Kunden mit Chipkarten ausgestattet. Abonnementkunden – das kann man sich vorstellen wie ein Zeitungsabonnement, wenn Sie das einmal abgeschlossen haben, läuft das immer – ist unser stärkstes Kundensegment. Im VRR beispielsweise werden drei Viertel aller Fahrten von Abonnementkunden unternommen. Allein in diesem Segment setzen wir rund 450 Millionen Euro im Jahr um. Das heißt, es ist für uns keine Spielwiese mehr, es ist unser Hauptgeschäft.

Kommen wir gleich zum Thema Technik und Kompatibilität, denn das ist der Bereich, wo wir angefangen haben, uns mit dem ePA zu beschäftigen. Was setzen wir ein? Für die etwas Technik-Affineren: Wir haben eine kontaktlose Chipkarte nach ISO 14443. Das betonen wir ganz deutlich, um auch klar zu machen, dass wir kein proprietäres System einsetzen, sondern wir haben einen offenen Standard, weil wir kompatibel sein wollen zu anderen Systemen und da wird später auch der ePA ein ganz interessanter Punkt sein.

Für das eTicketing im ÖPNV gibt es einen deutschen Standard, die VDV-Kernapplikation. VDV ist die Abkürzung für Verband Deutscher Verkehrsunternehmen. Aber der hat diese Kernapplikation nicht allein erfunden. Das war ein Forschungsprojekt der Bundesregierung. Da hat der Bund doch einiges Geld investiert, dass es einen Standard gibt, der wirklich die Plattform ist, dass im deutschen ÖPNV alles gleichermaßen abgewickelt werden kann. Es ist ein sehr komplexer Standard, der beispielsweise die Abläufe einer Chipkarte bis in jedes Bit und Byte beschreibt. Das ist ein unheimlicher Vorteil, wenn man anfangen möchte, im

Massenmarkt aufzutreten, dass man kann quasi ein Lastenheft aus dem Schrank nehmen kann und sagen: „Lieber Hersteller, bau mir eine Chipkarte, die kompatibel ist zu allem, was es sonst noch in Deutschland geben wird."

Dann habe ich das Stichwort ePassport Conformity Test aufgeschrieben. Als wir angefangen haben, in Massen unsere Chipkarten produzieren zu lassen, ist immer die Frage aufgetaucht: Was gibt man einem Hersteller für Qualitätskriterien mit an die Hand? Wir haben gesagt, wir müssen etwas nehmen, was Basis hat und an was man sich auch getrost anlehnen kann. Wir haben uns an den ePassport Conformity Test gehalten, d.h. unsere Chipkarten mussten den passieren, sonst hätte uns die Firma nicht beliefern dürfen.

Jetzt gibt es eine weitere Entwicklung. Da bin ich sehr froh, dass wir eine sehr gute Zusammenarbeit mit dem BSI haben. Da schon einmal Dank an Herrn Kowalski und seine werten Kollegen, die uns immer unterstützt haben bzw. wir sie auch unterstützen und mit Ratschlägen versorgen durften bei der Entwicklung der technischen Richtlinie RFID. Da ist ganz wichtig gewesen, Technologien, die sich entwickeln einmal in der ÖPNV-Welt und dann im Bereich ePass und ePA, auf die gleiche Plattform zu stellen. Denn spätestens beim technischen Equipment würde man sich sehr ärgern, wenn es nicht zusammen passt.

Wo konvergiert das eigentlich alles? Wo wachsen unsere Welten zusammen zwischen den hoheitlichen Dokumenten und dem eTicket? Und zwar wachsen sie nicht nur beim Thema Authentisierung zusammen, sondern auch anschließend beim Equipment, was eingesetzt wird.

Wo sind wir heute? Wir schreiben unsere eTickets auf Chipkarten, aber nur in Kundencentern. Das ist für uns eine sichere Umgebung, wo wir auch eine sichere Authentisierung durchführen können. Ein neuer Kunde legt seinen Personalausweis auf den Tisch, die Kollegen machen eine Kopie und dann kann man sagen, dein Abonnement ist geschlossen und schreibt das eTicket auf eine Chipkarte und reicht dem Kunden diese. Das heißt, wir sind begrenzt auf unsere eigenen Kundencenter. Wenn wir aus diesen Kundencentern rauswollen, stellt sich ganz schnell die Sicherheitsfrage und auch eine Technologiefrage. Wenn wir allein in kleine Verkaufsstellen wollen, die gehören uns nicht. Das sind Kioske. Wenn ich an Firmenkunden denke, die Jobtickets haben, bzw. wenn ich an einen Endkunden denke zu Hause, dann habe ich die Authentisierungsfrage, aber ich habe auch eine Equipmentfrage. Was hat denn der Kunde zu Hause für ein Equipment, über das beides geht, das eTicket und zur Authentisierung der ePA? Da glauben wir, dass das die einzige Möglichkeit ist, dass man diese beiden Welten zusammenführt.

Hier haben wir ganz groß die 14443, die ISO-Norm, die uns ganz wichtig ist, um einmal zu zeigen, dass das, was man als Equipment draußen einsetzt, wirklich diese offene Norm erfüllen muss. Wenn man jetzt einen eTicket-Vertrieb zum Kunden nach Hause bringt, dann sagt man aus ÖPV-Sicht, der Kunde muss sich den Leser wahrscheinlich selbst beschaffen und der muss sehr preisgünstig sein. Vorhin sind einmal die 20 Euro gefallen. Ich wollte eigentlich 9,90 Euro reinschreiben, um deutlich zu machen, dass ich mit 10 Euro nicht im Zweifelsfall 11,30 Euro meine. 9,90 Euro sind auch machbar. In Korea ist unser Leser bereits im Einsatz zu dieser preislichen Größenordnung. Und bereits vor einem Jahr auf der CeBIT haben drei Hersteller gesagt, dass sie in der Lage wären, im Massenmarkt für 10 Euro zu produzieren.

Dann ist die spannende Frage der Kompatibilität. Nur wenn es diesen Leser im Massenmarkt zu diesem Preis gibt, werden unsere Kunden als ÖPV-Kunden sich den Leser zulegen und dann das eTicket kaufen. Dann ist es für uns wichtig, dass über denselben Leser auch der ePA

kommt, weil sonst der Geschäftsprozess abbricht. Ich kann dem Kunden nicht zumuten, dass er über einen Leser oder über ein Verfahren seine Authentisierung macht und ein anderes Verfahren ggf. mit weiterem Equipment unser Ticket bezieht.

Dass das machbar ist, würde ich Ihnen gern in einer kleinen Demo zeigen.

Ich habe hier einen relativ einfachen Kontaktlosleser. Da ist im Prinzip nicht vielmehr drin als eine Antenne, die eine Chipkarte auslesen kann. Ich habe freundlicherweise von einem Industriepartner, NXP Semiconductors, Unterstützung bekommen.

Das ist also eine Demoversion eines elektronischen Personalausweises, und die spannende Frage ist jetzt: Wie sieht ein solcher Prozess konkret aus? Hier ist also eine Website aufgebaut und ich kann zum Beispiel sagen: Ich bin ein neuer Kunde, ich habe ein Kundenmedium und möchte mich neu registrieren lassen, d.h. ich gehe jetzt darauf, dass ich ein neues Benutzerkonto anlegen möchte. Die erste Frage ist dann die der Authentisierung. Wir haben hier die Imaginären Verkehrsbetriebe IVB genommen, um da neutral zu sein. Die Verkehrsbetriebe möchten wissen, ob meine Daten, mein Name, Adresse etc wirklich echt sind. Ich lege den ePA auf den Leser, gebe meine PIN ein und starte die Authentisierung. Die Anwendung zieht aus der Karte meinen Namen – jetzt habe ich Ihnen gerade meine Privatanschrift verraten – und ein Bild. Als nächstes muss ich die AGBs akzeptieren. Bei den heutigen Authentisierungsprozessen machen Sie einfach ein Häkchen. Und was macht der Bertreiber in Wirklichkeit? Der loggt vielleicht Ihre IP mit und ärgert sich anschließend, wenn der Prozess schief gegangen ist. Hier kann man jetzt wirklich sagen: Ja, ich akzeptiere die AGB, ich lege den Personalausweis wieder auf, sofern ich den da nicht noch liegen habe, und dann akzeptiert er meinen Zugang. Als nächstes könnte ich jetzt beispielsweise sagen: Okay, jetzt bin ich authentisiert, das Verkehrsunternehmen kennt mich, und jetzt möchte ich einen Fahrschein kaufen. Unser Programmierer hat das hier ‚Berechtigung' genannt, in unserem internen Jargon heißt ein eTicket ‚Berechtigung'. Jetzt bekomme ich die Tickets zur Auswahl, die es gibt. Ich könnte sagen: ich möchte ein Ticket2000. Das ist ein Standardprodukt bei uns. Das möchte ich jetzt kaufen und wähle es aus. Jetzt will er noch einmal wissen, ob ich wirklich sicher bin, dass ich dieses kaufen will. Das akzeptiere ich noch einmal mit meinen ePA. Jetzt ist der Kaufprozess abgeschlossen und es kommt der spannende Punkt. Ich nehme meinen ePA herunter, lege ein VDV-Kernapplikation konformes Nutzermedium auf denselben Leser, das ist der wichtige Punkt, und schreibe das eTicket darauf. Das ist der Dreh- und Angelpunkt, dass der Kunde wirklich sagen kann: Ich habe mir einmal einen Leser beschafft und der funktioniert auf derselben Plattform.

Einmal ist kritisch gefragt worden, wo denn jetzt der konkrete Pilot ist. Wir haben ohne ePA, also nur für den Prozess, ein elektronisches Ticket im Internet zu verkaufen, einen Piloten vereinbart mit den Verkehrsbetrieben der Stadt Düsseldorf. Das ist die Rheinbahn. Da ist der Pilotauftakt im Juni, und wenn uns die Möglichkeit gegeben wird, in diesem Piloten den Authentisierungsprozess - der ein bisschen fummelig ist bei uns -, sauber abbilden zu können, indem man uns unterstützt hat, in den Prozess den ePA einzubinden, sind wir dem gegenüber offen und würden uns freuen, wenn das geht.

5.4 Neue Prozesse im Bürgerbüro

Anton Hanfstengl, Kreisverwaltungsreferat der Landeshauptstadt München

Mein Vortrag dreht sich um das Thema ‚Neue Prozesse im Bürgerbüro'. Richtigerweise müsste es eigentlich heißen: ‚Anwendungsmöglichkeiten des elektronischen Personalausweises am Beispiel des Dienstleistungsangebots im Bürgerbüro München'. Der Teilnehmerkreis kommt, wie ich der Einladung entnehmen kann, aus der ganzen Republik, aber ich gehe davon aus, dass der Begriff „Bürgerbüro" in fast allen Städten bekannt ist. Es heißt manchmal ein wenig anders, wird z.B. Bürgerservicedienste genannt und bietet unterschiedliche Dienstleistungen, aber letztendlich ist das Kerngeschäft des Bürgerbüros, das regelmäßig den Meldebereich, das Passwesen und die Lohnsteuerangelegenheiten umfasst, doch in allen Städten wieder gleich. Insoweit ist das Beispiel das ich Ihnen heute darstellen möchte auch übertragbar.

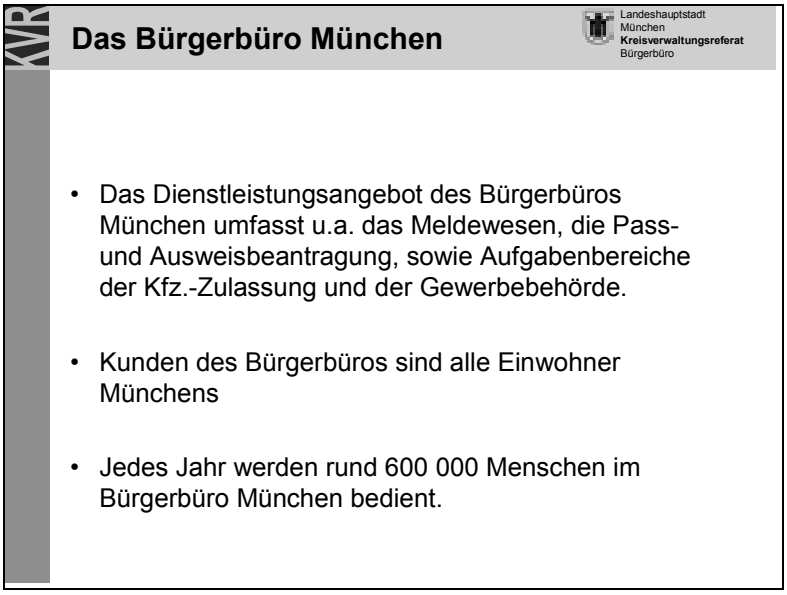

Bild 1

Im Bürgerbüro München sind das Meldewesen, die Pass- und Ausweisbeantragung, sonstige Aufgabenbereiche der Kfz-Zulassung und der Gewerbebehörde zusammengefasst (Bild 1). Nachdem es auch um Zahlen geht; im Jahr suchen rund 600.000 Menschen das Bürgerbüro persönlich auf. Hier erhoffen wir uns vom elektronischen Personalausweis den Durchbruch, um in eine durchgängige Online-Sachbearbeitung einzusteigen.

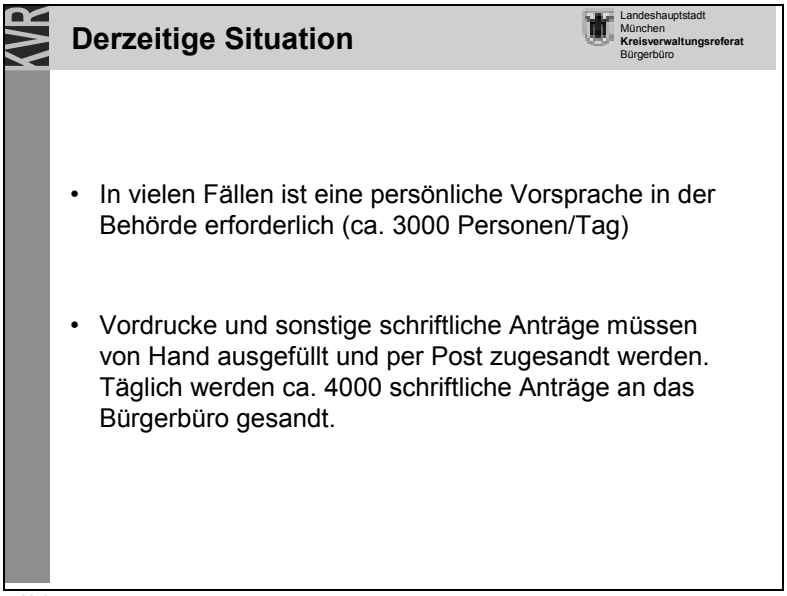

Bild 2

Die derzeitige Situation stellt sich folgendermaßen dar (Bild 2): Im Bürgerbüro der Landeshauptstadt München werden täglich rund 3000 Personen bedient. Daneben wird eine Vielzahl schriftlicher Anträge gestellt, die bearbeitet und wieder zurückgesandt werden müssen. In vielen Fällen ist eine Identifizierung oder die Unterschrift nötig. Die weiteren einschränkenden Faktoren kennen Sie bestimmt aus eigener Erfahrung. Wir haben einschränkende Öffnungszeiten, in den Städten unterschiedlich gestaltet, die letztendlich nicht die Wünsche einer modernen Gesellschaft erfüllen können. Heutzutage möchte jeder Mensch ganz gerne seine Angelegenheiten rund um die Uhr erledigen können. Darüber hinaus gibt es oftmals lange Wartezeiten und auch lange Bearbeitungszeiten.

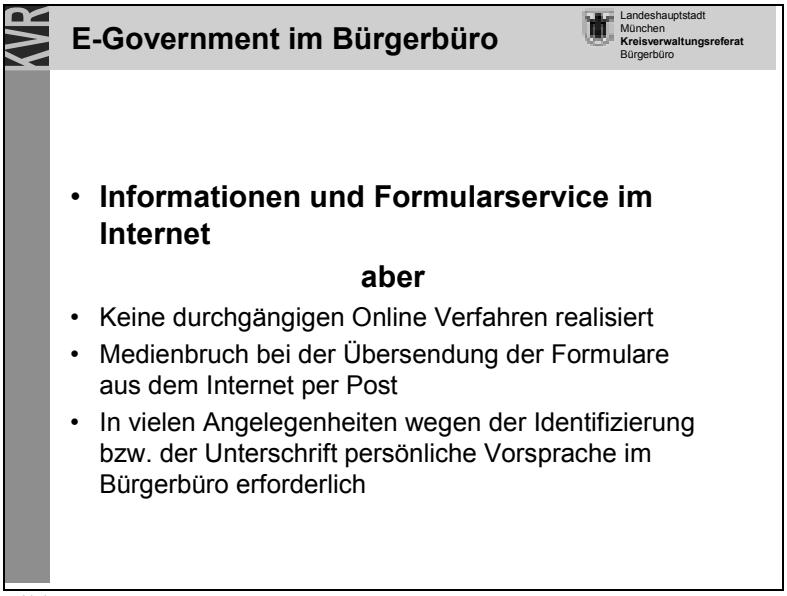

Bild 3

Die Bestrebungen und die Intensionen der Städte sind fast überall gleich. Man versucht den Menschen die erforderlichen Informationen möglichst schon im Vorfeld zukommen zu lassen. In fast allen Städten stehen schon viele Informationen im Internet. Auch der Formularservice steht oftmals im Internet zur Verfügung. Letztendlich ist aber bei allen Vorgängen immer noch ein Medienbruch vorhanden, so dass günstigstenfalls das Formular am PC im Internet ausgefüllt werden kann, dann aber ausgedruckt und wieder per Post an die Behörde geschickt werden muss (Bild 3). Uns geht es darum, diesen Vorgang aufzulösen und eine rechtsverbindliche elektronische Kommunikation zwischen den Menschen und der Behörde zu ermöglichen.

Zum Anwendungspotenzial des elektronischen Personalausweises im Bürgerbüro habe ich die nächste Folie vorbereitet. Sie sehen hier noch einmal unser Dienstleistungsangebot und welche Vorgänge oder welche Dienstleistungen sich für ein durchgängiges Onlineverfahren anbieten würden. Das fängt bei der schon genannten An-, Um- und Abmeldung an und hört bei der Gewerbeummeldung auf. Dazwischen finden sich viele Vorgänge, z.B. die Beantragung von Führungszeugnissen und ähnliche Dinge, die für manche Menschen durchaus des Öfteren notwendig werden. Insofern könnte dort auch ein Anwendungsgebiet für den elektronischen Personalausweis liegen.

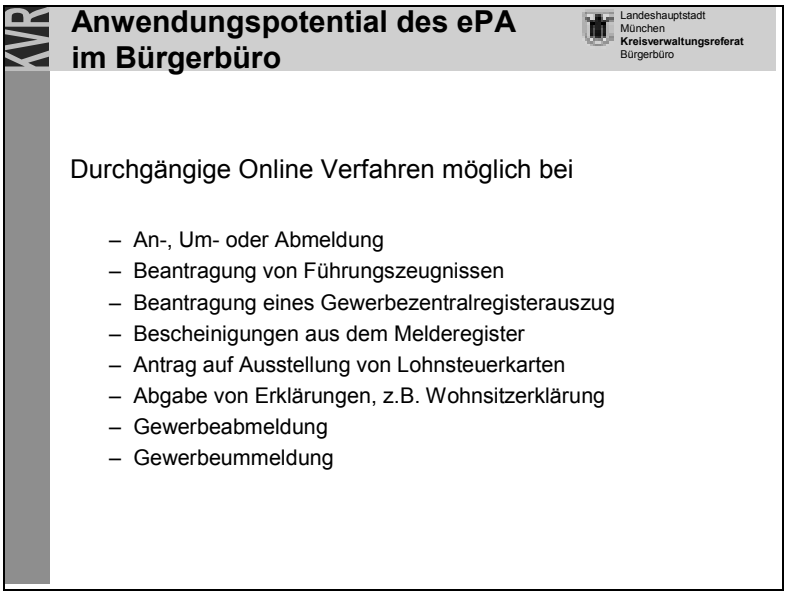

Bild 4

Die Vorteile bei durchgängigen Online-Verfahren sind leicht einsehbar (Bild 4). Die Kunden könnten, um bei dem vorherigen Beispiel zu bleiben, von zuhause oder auch von unterwegs ihr Führungszeugnis beantragen. Man ist unabhängig von einschränkenden Öffnungszeiten und auch die Wartezeiten im Amt würden sich verringern oder ganz wegfallen. Auch für die Verwaltung könnten sich dadurch erhebliche Rationalisierungsmöglichkeiten ergeben.

Im Bild 5 sind die Voraussetzungen für einen Feldversuch aufgeführt. Es sind koordinierte Aktionen der Anbieter der Fachverfahren, gemeint ist damit die eingesetzte Software im Bürgerbüro, erforderlich. Es gibt für die Meldebehörden ein bestimmtes Programm. Es gibt für die Passbeantragung ein bestimmtes Programm, das mit der Bundesdruckerei kommunizieren muss. Es sind also bestimmte Vorgaben der IT und Anpassungen in der IT erforderlich, um einen Feldversuch in diesem Bereich überhaupt erst möglich zu machen. Das sind gleichzeitig auch die Hindernisse, die einen Feldversuch in der Praxis noch behindern und die man in der nächsten Zeit lösen müsste.

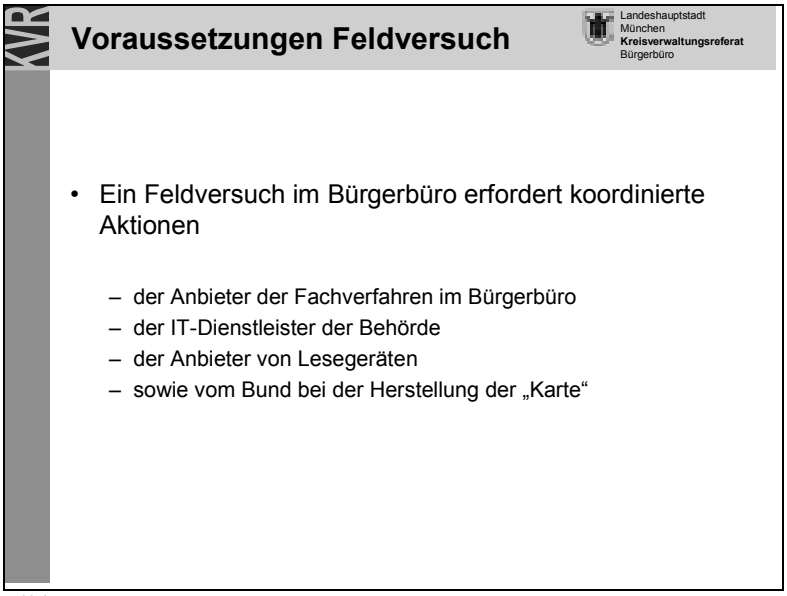

Bild 5

Zunächst einmal geht es heute aber nur um ein Anwendungsszenarium. Aus Sicht des Bürgerbüros wäre ein Feldversuch jedoch durchaus sehr sinnvoll. Zu berücksichtigen wäre bei einem Feldversuch der Zeit- und Arbeitsaufwandes für die Anpassung eines elektronischen Zugangs zur Stadt München. Auch der schon erwähnte Zeit- und Arbeitsaufwand für die Anpassung der Fachverfahren wird eine Rolle spielen. Hier ist das Bürgerbüro auch auf Dritte angewiesen. Die Softwareanbieter müssten die Authentifizierungsmöglichkeiten in ihre Programme mit einbinden, damit in der Praxis ein Versuch überhaupt erst möglich wird. Und letztendlich muss eine Akzeptanz bei den Bürgern für einen Feldversuch erreicht werden. Insofern muss es um Angebote gehen, die tatsächlich mehrere Menschen auch mehrmals benötigen.

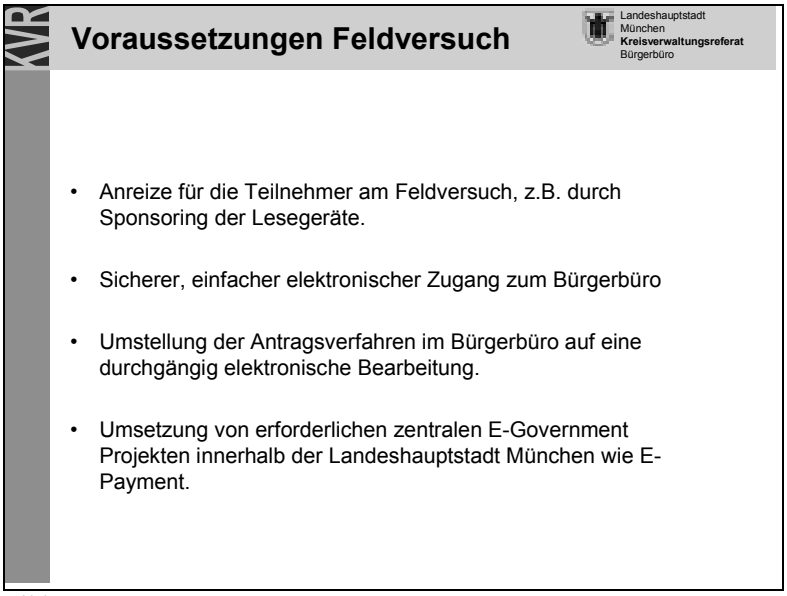

Bild 6

Anreiz um dies etwas zu forcieren wäre zum Beispiel ein Sponsoring der Lesegeräte (Bild 6). Dies ist auch von meinen Vorrednern schon erwähnt worden. Ein sicherer und einfacher elektronischer Zugang zur Behörde ist dabei genauso erforderlich, wie eine einfache Benutzerführung durch die Antragsformulare. Als Hausaufgabe der Landeshauptstadt München ist auch noch die Realisierung eines E-Payment Verfahrens erforderlich, um in Online-Verfahren die Gebühren auch online erheben zu können.

Das gesamte Dienstleistungsangebot des Bürgerbüros wäre jedoch für einen Einstieg in den Feldversuch zu umfangreich, so dass wir nicht in der Lage sein würden, alle Dienstleistungen für eine Online-Anwendung umzustellen. Insoweit lautet unser Vorschlag dahingehend, mit einzelnen Dienstleistungen aus dem Bürgerbüro zu beginnen (Bild 7). Wir denken an den Antrag auf ein Führungszeugnis, Bescheinigungen aus dem Melderegister, Antrag auf Ausstellung einer Lohnsteuerkarte. Hier wäre es vorstellbar, dass die Anpassung der Fachverfahren nicht zu umfangreich ist und dass auch rechtliche Hindernisse wie zum Beispiel eine Unterschrift nicht zwingend erforderlich sind. Wir reden trotzdem von nicht unerheblichen Fallzahlen. Beim Führungszeugnis sind es in München zum Beispiel immerhin noch 40.000 Anträge im Jahr.

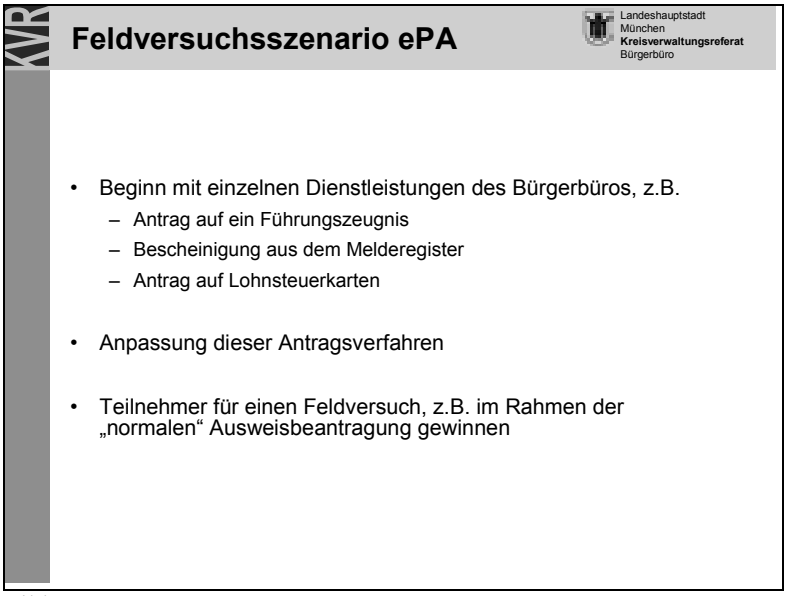

Bild 7

Ein weiteres Thema ist auch die elektronische Signatur und deren Umsetzung. Damit möglichst viele Menschen diese Option nutzen wäre die Frage zu stellen, ob die Kosten für die Eintragung dieser Option im elektronischen Personalausweis nicht von „Sponsoren“ übernommen werden könnten. Weiterhin könnten - eventuell über den Gebührenrahmen - Anreize geschaffen werden, um für Online-Verfahren geringere Gebühren zu verlangen Meines Erachtens sind solche Anreize erforderlich damit die Menschen am Feldversuch teilnehmen und den elektronischen Personalausweis –nach seiner Einführung- nicht erst zum Ende des Ablaufs vom alten Personalausweis beantragen sondern vielleicht auch schon zu einer früheren Zeit.

Es ist heute schon einige Male dargestellt worden, wie ein elektronischer Zugang zu den Anbietern denn ausschauen könnte, bzw. wie das Szenario eines Feldversuchs ausschauen könnte. (Bild 8) Auch für uns geht es darum wie das technisch funktionieren könnte. Die Firma SCM Microsystems hat uns freundlicherweise einige Bilder zur Verfügung gestellt.

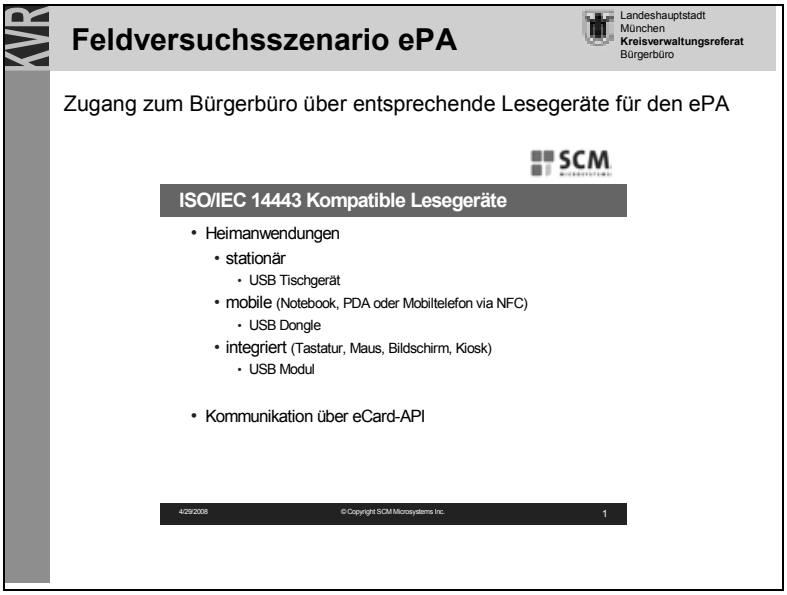

Bild 8

Man könnte also von zuhause oder von unterwegs, – da war der vorhergehende Beitrag sehr anschaulich- die Kommunikation mit dem Anbieter der Dienstleistung über den elektronischen Personalausweis starten.

Das nachfolgende Bild 9 zeigt die Geräte.

Bild 9

In Bild 10 wird ein Gesamtsystem der Heimanwendung dargestellt.

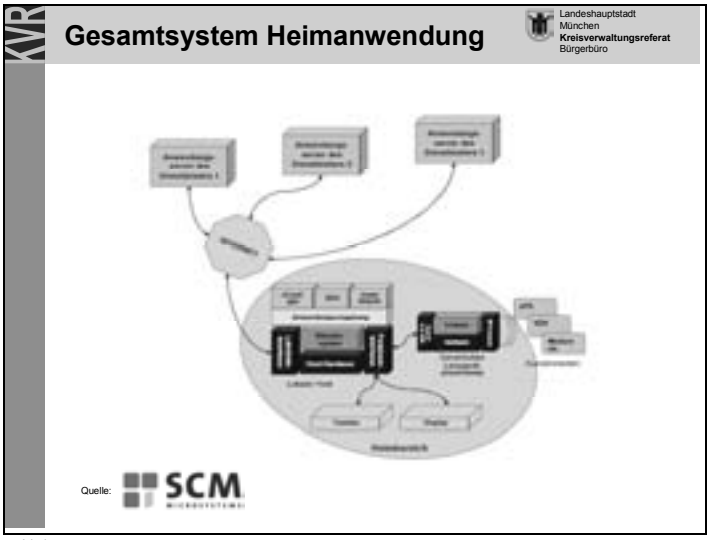

Bild 10

Damit bin am Ende meines Vortrags angekommen. Herzlichen Dank für die Aufmerksamkeit.

6 Handlungsbedarf und nächste Schritte Diskussion

Moderation:
Dr. Udo Helmbrecht, Bundesamt für Sicherheit in der Informationstechnik, Bonn
Prof. Dr. Heinz Thielmann, Emphasys, Heroldsberg

Prof. Thielmann:
Vielen Dank, Herr Ziemer, vielen Dank Herr Staatssekretär Dr. Beus, vielen Dank an alle Redner von heute Abend. Herr Dr. Helmbrecht und ich haben nun die ehrenvolle Aufgabe, für eine Stunde die Diskussion gemeinsam zu moderieren. Mein Name ist Heinz Thielmann, ich bin vorhin bereits vorgestellt worden.
Was wir gehört haben, sind zunächst einmal die allgemeinen Einführungen von Herrn Staatssekretär Dr. Beus, Herrn Dr. Helmbrecht, Herrn Kowalski und Herrn Wolfenstetter. Dann diese vier Anwendungsszenarien. Ich bin schon gefragt worden, warum diese vier, ob es nicht auch andere gibt. Sicher gibt es andere, aber wir mussten uns natürlich irgendwie beschränken. Es gibt sicher Anwendungen im Bereich Handel, Schufa, Deutsche Post, Lotto, Notare. Wir haben einige Vertreter aus diesen Anwendungsbereichen, die hier teilnehmen. Es sind auch einige Statements eingereicht worden, Beispiel Herr Osthaus von eBay, der mehr auf die Kommunikationsthemen und auf die allgemeine Vorbereitung des Themas hinweist. Auch andere Statements werden wir in der Dokumentation mit veröffentlichen. Ich möchte Sie gerne bitten, wenn Sie aus der Diskussion heute eigene Vorstellungen entwickeln, dass Sie diese noch als Statement beim Münchner Kreis einreichen. Dann würden wir Ihren Beitrag mit zur Dokumentation dazu nehmen. Das ist auch hilfreich für das BMI, BSI und die Umsetzung.

Was wir jetzt in der nächsten Stunde versuchen wollen zu erreichen, ist, dass wir ganz konkret zu einigen Vorschlägen kommen für Handlungsempfehlungen für das Innenministerium und die politischen Entscheidungen, für Handlungsempfehlungen für die Technik und die Lösungsanbieter. Konkrete Anwendungserprobungen herauszufinden, die eben nicht nur wohlwollendes Begleiten bedeuten – Herr Prof. Ziemer hat es vorhin angesprochen -, sondern die ein konkretes Mittun bedeuten. Dass wir die Marktpotenziale noch einmal diskutieren. Ein Punkt für die Bürgerbüros, der vorhin bei uns am Tisch angesprochen wurde, ist die Frage der Portalfunktion in der öffentlichen Verwaltung, die es ja heute noch nicht gibt. Wo sind konkrete Anwendungen für den modernen Staat?

Es gibt eine ganze Menge von Punkten, die wir diskutieren sollten. Aber es wäre schön, wenn wir nach einer Stunde erreichen könnten, dass wir auch in der Dokumentation einige Dinge festmachen können, die für uns alle, für das Innenministerium, für die politischen Entscheidungsträger, für die Technik und für die potenziellen Anwender hilfreich sind als Handlungsempfehlungen, um dann von da aus weiterzumachen.

Nach der kurzen Einführung möchte ich an Herrn Dr. Helmbrecht übergeben, damit wir die Diskussion mit Ihnen gemeinsam eröffnen.

Dr. Helmbrecht:
Vielen Dank. Gibt es spontane Wortmeldungen zu den bisherigen Vorträgen?

Prof. Popescu-Zeletin, Fraunhofer Fokus, eGovernment Labor:
Ich fand den heutigen Abend sehr lehrreich. Es gibt einen Punkt, den ich mich eigentlich immer gefragt habe, warum er nicht dabei ist. Der Bund hat das Deutschland-Online Projekt gestartet. Das sind im Grunde genommen eine Reihe von Projekten wie europäische Dienstleistungsrichtlinien Kfz, 115, die unterwegs sind und dann perfekte Synchronisationspunkte bieten würden in unterschiedlichen Pilotphasen und auch in der Konzipierung dieser Projekte gewissermaßen, um eine Einführung vom ePA nahtlos in diese Projektidee einzuführen. Ich habe bis jetzt nichts über diese Felder gehört und wie diese Synchronisation auf der technischen Ebene und auf der inhaltlichen Ebene mit den Deutschland-Online Projekten stattfinden.

Dr. Helmbrecht:
Wer von Ihnen möchte darauf antworten? Herr Schallbruch, bitte.

Herr Schallbruch, BMI:
Herr Popesku-Zeletin, die Projekte, bei denen der Personalausweis eine Rolle spielen könnte, haben sich mit dem Personalausweis auch schon auseinandergesetzt. Das ist insbesondere das Projekt Kraftfahrzeugzulassung, wo der Ausweis ein Teil des angedachten neuen Prozesses der Kraftfahrzeugzulassung ist. Die Kollegen aus Hamburg, die das machen, kennen unser Projekt zum Personalausweis genau und berücksichtigen das auch. Auch die Blaupause, die das Projekt für die Umsetzung der EU Dienstleistungsrichtlinie erstellt und die im September fertig sein wird, wird für Prozesse, bei denen es um die Authentisierung von Dienstleistungserbringern geht, den elektronischen Personalausweis berücksichtigen. Die anderen Projekte haben mehr infrastrukturellen Charakter und haben nicht unbedingt Bürgerkontakt wie die Deutschland-Online Infrastruktur. Und das Projekt 115 sehe ich jetzt auch nicht als Anwendungsfall für den elektronischen Personalausweis – da lerne ich aber gerne dazu.

Dr. Helmbrecht:
Vielen Dank, Herr Schallbruch. Herr Eberspächer...

Prof. Eberspächer:
Gibt es irgendwelche Äußerungen zu der europäischen Harmonisierung? Wir haben ja das letzte Mal mehr darüber gehört. Es gibt andere Länder die schon weiter sind. Und wie sieht das mit der technischen Harmonisierung aus?

Dr. Helmbrecht:
Es gibt dazu ein Stichwort, das „Large Scale Pilot Projekt“. Vielleicht könnte Herr Kowalski erläutern wie das in die EU eingebettet ist und was der Inhalt des Projektes ist.

Herr Kowalski:
Ich möchte kurz etwas zum eID-LSP sagen. Anschließend würde ich gern an Herrn Houdeau von Infineon weitergeben, der sich bestens mit den europäischen Aktivitäten auskennt. Also, eID-LSP ist ein Projekt, bei dem sich das BMI und das BSI gleichermaßen engagieren, um mit insgesamt 13 Mitgliedstaaten eID-Lösungen in Europa zu standardisieren. Natürlich gibt es in Europa verschiedene Lösungsansätze. Die Projekte, die derzeit umgesetzt sind, arbeiten vor allen Dingen mit kontaktbehafteten Karten. Wir haben ja eine kontaktlose Karte und damit eine neue Technologie mit ganz anderen Möglichkeiten. Wir haben auch einen Ansatz, den wir Middleware-Ansatz nennen, d.h. die Kompatibilität zu eID-Lösungen in anderen Ländern wollen wir dadurch erreichen, dass zum Beispiel ein spanischer Ausweisinhaber hier in Deutschland auf einen deutschen Client zugreifen kann, wo die Middleware die

Umsetzung der spanischen Karte auf unsere eID-Lösung gewährleistet und umgekehrt, dass diese Möglichkeit allein auch passiert.
Dann gibt es noch das Proxy-Modell. Diese verschiedenen Modelle, um Interoperabilität in Europa zu erreichen, sollen in diesem großen, von der EU finanzierten Projekt im Zeitraum bis 2011 untersucht werden. Und natürlich haben wir das Interesse, unsere deutschen Vorstellungen und die Lösungen der deutschen Industrie dort einzubringen. Ich denke, auch die Chancen stehen dort eigentlich gar nicht schlecht. Was wir aber nicht erreichen werden, ist, dass in Europa in allen Ländern die gleiche technische Lösung eingesetzt wird. Aber das heißt nicht, dass die dahinter liegenden Dienstleistungen das nicht beherrschen könnten. Deswegen kommt es eben nicht nur auf das Ausweisdokument an, auf das sich die anderen Länder im Wesentlichen konzentrieren, sondern auch auf die Infrastrukturkomponenten wie Lesegeräte, Middleware Komponenten, Zertifikatsdienste usw. Vielleicht sollte ich noch Herrn Houdeau die Möglichkeit geben, konkreter auf einzelne Länder einzugehen.

Herr Houdeau, Infineon:
Vielleicht sage ich noch etwas zu meiner Person. Zunächst einmal bin ich der Leiter des Fachausschusses *Chipkarte und Ausweissysteme* bei BITKOM. Ich bin natürlich auch noch hauptberuflich tätig bei der Firma Infineon, einem Halbleiterhersteller, börsennotiert. Zum Thema EU kann man sagen, derzeit sind acht Länder bekannt, die Lösungen haben, zum Teil aus den Jahren 99, 2000, 2001, d.h. weit vor einer europäischen Standardisierung definiert worden und deren Einführungen zurückführen bis 2002, wenn man Finnland als erstes Land berücksichtigt. Estonia 2003, das mittlerweile über 80% der Bevölkerung mit diesen Bürgerkartenfunktionen ausgestattet hat. Das sind alles so genannte proprietäre Lösungen. Das Wort fiel vorhin ja schon einmal. Proprietär heißt, sie sind nicht in der Technik untereinander kompatibel. Die Karten können im Ausland nicht einwandfrei für die gleichen Dienste benutzt werden. Das ist bisher der Status. Wir haben allerdings seit 2004, 2005 einen EU-weiten Standard in Vorbereitung, einen CEN- Standard, der nicht weltweit gilt sondern nur in Europa. Deutschland hat auch das deutsche Profil für den deutschen Personalausweis genau 1:1 in diesen Standard eingebracht. Die Franzosen werden das wahrscheinlich in den nächsten Wochen ebenfalls tun. Wir haben klare Indikatoren, dass viele Länder achten, wie reif dieser Standard ist, beispielsweise Polen gehört dazu, um dann zum geeigneten Zeitpunkt letztendlich genau auf diese standardisierte und auch harmonisierte Lösung aufzuspringen. Das heißt, Deutschland wäre eines der ersten Länder, die dann genau diesen Standard erfüllen würden wie Frankreich. Auch Länder wie die Niederlande und Polen könnten diesem relativ zeitnah folgen. Auch dort werden Terminpläne mit 2009/10 für die Einführung von flächendeckenden Personalausweisen mit Bürgerkarten-Funktionen, die genau diese Online Authentisierung abbilden sollen. So gesehen stehen wir sozusagen an einem Wendepunkt von proprietären Lösungen aus der Historie zu künftigen interoperablen EU-weit harmonisierten und standardisierten Lösungen.
Das zweite, was dann folgen würde, wäre die Frage der Dienste, weil wenn die Technik standardisiert ist, wäre der nächste Schritt, auch die Dienste zu standardisieren. Herr Kowalski hat vorhin kurz das Thema LSP, Large Scale Pilot EU, angedeutet. Ich muss auch als Student in der Lage sein, wenn ich zum Beispiel ein Gastsemester in Italien haben will als Deutscher, dass der Prozess in Italien für die Anmeldung harmonisiert ist gegenüber dem, was ich an der TU in München machen müsste. Dass auch solche grenzüberschreitenden Dienste, es kann auch zweiter Wohnsitz oder Fahrzeuganmeldung in einem zweiten Lande sein, letztendlich diesem Applikationsstandard von der Technik her folgen. Das wäre der nächste logische Schritt auf der europäischen Standardisierungslinie. Ich glaube, damit ist die Frage erschöpfend beantwortet.

Dr. Helmbrecht:
Vielen Dank. Ich darf nun Herrn Grönewald aufrufen:

Herr Dr. Grönewald, Debold & Lux GmbH:
Ich habe heute Abend viel gelernt über Technik, über Standards und über Applikationen, aber das Wort Akzeptanzmanagement habe ich nicht so richtig aufgenommen. Eine Folie zeigte einmal etwas zu diesem Thema. Wer ist eigentlich dafür bei uns im Lande zuständig, dass eine entsprechende Publikation gemacht wird, PR gemacht wird für die Einführung des ePA? Ich erinnere mich, in Österreich hatte das eCard-Projekt ein zusätzliches Budget in Höhe von 10 oder 20% des System-Volumens für PR in Fernsehen, Medien und ähnlichem. Die intensive PR-Begleitung bildet eine wesentliche Grundlage für die Akzeptanz und damit den Erfolg des ePA. Wer ist zuständig?

Prof. Thielmann:
Vielen Dank für das Statement. Das spricht mir voll aus dem Herzen. Ich habe einige Zeit auch die elektronische Gesundheitskarte begleitet in meiner Funktion bei Fraunhofer. Da hatten wir das gleiche Problem. Ich denke, das ist ein wichtiger Punkt, der sehr frühzeitig angesprochen werden muss, denn wenn man diese Akzeptanz und die Kommunikation dazu nicht frühzeitig im Auge hat, dann werden alle guten Lösungen nicht akzeptiert. Ich darf Herrn Osthaus dazu bitten, der uns dazu vorher auch ein Statement abgeliefert hat, einiges dazu zu sagen.

Dr. Osthaus, eBay GmbH:
Ich bin, um das gleich klarzustellen, wohl nicht der Zuständige für die Vermarktung, aber es ist genau ein Punkt, den ich auch gerne in die Diskussion heute einbringen wollte. Denn ich glaube, wir sind jetzt an einem Punkt, wo die Diskussion über den elektronischen Personalausweis die Öffentlichkeit erreicht. Öffentlichkeit heißt im Augenblick insbesondere die Politik, und wir sehen jetzt bereits das Entstehen verschiedener Widerstände, die am Ende den Erfolg dieses Projektes wesentlich verzögern, im schlechteren Fall sogar vielleicht auch verhindern können. Es sind zwei Punkte, die ich im Augenblick im Besonderen wahrnehme, zwei Bedenken, die wir sehr frühzeitig adressieren müssen.
Das Erste ist ein tatsächlich juristisch fundiertes Bedenken bei der Frage: Darf ein staatliches Ausweisdokument zwangsweise mit einer der Privatwirtschaft nutzenden Funktion ausgestattet werden, nämlich der Authentisierungsfunktion? Da gibt es bereits viele kritische Aussagen, auch aus Ressorts der Bundesregierung, aber insbesondere auch von Parlamentariern der Opposition, die das sehr kritisch sehen. Die sagen, es gibt ein verfassungsrechtliches Übermaßverbot. Der Staat darf eben kein Verwaltungshandeln ausüben, das tatsächlich nicht für die Bürger zwingend notwendig ist. Und zwingend notwendig ist natürlich eine Authentisierungsfunktion auf den ersten Blick nicht. Auf den zweiten Blick vielleicht schon, wenn man darüber nachdenkt, dass es durchaus eine Aufgabe des Staates sein kann, Infrastruktur für einen erfolgreichen Wirtschaftsbetrieb bereitzustellen. Und in Zeiten, in denen ein immer größerer Teil des Wirtschaftslebens auf elektronischem Wege abgewickelt wird, gehört das vielleicht zu den unverzichtbaren Infrastrukturen. Nur muss das eben auch vermittelt werden, und das muss in allererster Linie mal der Politik vermittelt werden, weil sich hier im Augenblick diese Bedenken entwickeln. Sie scheinen mir jedoch sehr juristisch-theoretisch auf den ersten Blick. Für die Argumentation ist es ganz wichtig, eine Größe zu definieren und das ist die Frage: Wie groß ist tatsächlich der Mehraufwand für den einzelnen Bürger? Das macht natürlich einen Unterschied, ob ich ihnen 20 Euro oder nur 3 Euro mehr abverlange für den Personalausweis. Ich glaube, das weiß noch keiner so ganz genau. Aber je früher wir es wissen, desto eher können wir fundiert in diese Diskussion hineingehen. Das ist der eine Punkt.

Der zweite Punkt betrifft noch einmal diese Frage der biometrischen Daten, und ich bin der Letzte, der sich anmaßen möchte, eine Entscheidung darüber zu treffen, ob wir biometrische Daten auf einem Personalausweis brauchen oder nicht. Ich glaube einfach mal, wenn unsere Ansprechpartner sagen, dass es eine sehr sinnvolle Sache ist, wenn man sie draufhat. Was wir aber auch erleben, sind hierzu Bedenken in Gesprächen mit der Zivilbevölkerung, wie es immer heißt, mit der Gesellschaft. Ich sehe, dass Bedenken bestehen, dass nicht nachvollzogen wird, dass solche biometrischen Daten eben nur tatsächlich für die hoheitlichen Funktionen – wie immer wieder klar betont wird – gebraucht werden und sicher geschützt werden können gegen den Zugriff durch andere. Und alle fragen uns dann, ob denn eBay den Fingerabdruck haben will. Nein, wollen wir natürlich nicht. Aber das eben so klar und verständlich zu machen, ist eine ganz große Aufgabe.
Ich kann eine ganz kleine Antwort auf die sehr berechtigte Frage geben, die gerade zur Vermarktung gestellt wurde. Wir von eBay leiten ja auch diese bereits angesprochene Arbeitsgruppe 4 zu Sicherheit und Vertrauen in IT und Internet im Rahmen des IT-Gipfelprozesses. Tatsächlich wird in Vorbereitung jetzt des dritten IT- Gipfels, der im November dieses Jahres in Darmstadt stattfinden wird, genau das Ziel sein, die Anwendungsfelder und Vorteile einer elektronischen Identifizierung zu vermitteln. Da kann man im Zusammenwirken von Staat, Wirtschaft und gesellschaftlichen Gruppen, zum Beispiel in der Initiative „Deutschland sicher im Netz“ viel erreichen. Ob wir dann nachher wirklich die Fernsehspots haben, die jeden im letzten Winkel dieses Landes erreichen, bezweifle ich, aber vielleicht müssen wir, wie gesagt, erst einmal die Multiplikatoren in diesem Lande erreichen und das ist eben im Augenblick die Politik.

Dr. Helmbrecht:
Vielen Dank. Herr Staatssekretär Dr. Beus.

Dr. Beus:
Natürlich haben wir ein Kommunikationskonzept für dieses Projekt. Ich will nur eins sagen – wir können nicht akzeptieren, dass gesagt wird, erstens: die Politik soll es durchsetzen und zweitens: wir, die Wirtschaft haben hinterher den Profit. Bei dieser Aufgabenteilung sollten wir uns heute Abend hier nicht aufhalten, sondern entweder schaffen wir es gemeinsam und da brauchen wir Sie alle – darum sind wir heute Abend hier, um es deutlich zu sagen – oder wir schaffen es eben nicht gemeinsam. Deshalb ist es wichtig, dass auch alle potenziellen Nutzer sich dazu öffentlich artikulieren. Das ist der entscheidende Punkt.
Zur Frage: Darf der Staat das? Da würde ich zunächst einmal sagen: Auch heute nutzt die Wirtschaft den Personalausweis, und niemand ist auf die Idee gekommen zu fragen: Darf denn die Bank, wenn sich jemand authentifizieren soll, verlangen, dass er den Personalausweis vorlegt, der zunächst einmal als staatliches Dokument erstellt worden ist? Ja! Das ist heute gängige Praxis und wird auch so bleiben, wenn man einen neuen technischen Standard einführt. Allerdings werden wir die Möglichkeit vorsehen, dass jemand, der den elektronischen Identitätsnachweis absolut nicht will, optieren kann, dass diese Funktion auf seinem Personalausweis nicht aktiviert wird. Insofern wird niemand gezwungen, einen Ausweis mit sich herumzutragen, mit dem er das machen kann. Wenn er den abholt, kann er sagen, dass er das nicht möchte und dann wird das ausgeschaltet. Insofern wird diesen Bedenken Rechnung getragen. Ich möchte noch einmal wiederholen: Ich glaube, wir müssen alle diese Vorteile deutlich machen. Wir werden sicher unseren Anteil leisten, völlig klar. Das ist Aufgabe der Verwaltung und der Politik, aber es ist genauso Aufgabe der potentiellen Nutzer, dahinter zu stehen und zu sagen, wir wollen das und wir brauchen das. Weil das natürlich auch eine Überzeugungskraft anderer Art hat, wenn wir das gemeinsam tun, als wenn das nur von einer Seite getan wird. Es ist ja richtig, dass es auch den Funktionsteil gibt – der sicher kritisch diskutiert werden wird –, der die Sicherheit des Ausweises durch die

biometrischen Daten bei den Kontrollfunktionen vorsieht. Den brauchen wir auch. Aber den werden wir besser durchsetzen, wenn auch deutlich wird, dass es einen anderen Funktionsteil gibt, wo der tägliche Nutzen des Bürgers auf der Hand liegt. Deshalb haben wir das auch mit BITKOM zusammen besprochen, welche Schritte man gehen kann. Die werden nach der Sommerpause beginnen, und wir werden das dann intensiv betreiben und Sie auch immer wieder einladen, uns da zu unterstützen.

Prof. Thielmann:
Vielen Dank, Herr Dr. Beus. Aber wäre das nicht heute Abend eines der Ergebnisse, die wir festhalten sollten, dass wir eine gemeinsame Kommunikationsinitiative starten? Ich frage Sie im Arbeitskreis. Das wären die wichtigen Akteure, und da sehe ich nicht nur BITKOM. Ich bin selbst BITKOM Mitglied. BITKOM hat eine Interessensseite, nämlich auf der Anbieterseite. Aber dass wir da auch die anderen Seiten mit einbeziehen und sagen, wir bilden eine Initiative – das müssen wir heute Abend nicht zu Ende diskutieren, die gemeinsam mit Ihnen, mit dem Innenministerium, diese Kommunikationsthematik und die Akzeptanzthematik weiter angeht. Wer wäre bereit, dabei mitzumachen, einfach spontan? Diese sollten sich nachher am besten bei Herrn Schallbruch melden. Da war noch eine Wortmeldung.

Herr Köhler, Microsoft:
Mein Name ist Tom Köhler von Microsoft Deutschland. Ich bin verantwortlich für die Sicherheitsstrategie bei uns im Haus im deutschen Raum. Meine Anmerkung war dazu, dass wir nicht nur über ein Kommunikationskonzept nachdenken müssen, sondern auch über ein pädagogisches Konzept, d.h. wie bringen wir das Thema in die Schulen? Ich denke, es ist ein Riesenpotenzial gerade die Verwendung eines neuen Mediums in die Schulen zu bringen, weil wir generell das Problem der Sicherheitsvermittlung im schulischen Bereich haben. Es würde mich natürlich interessieren, was man da andenkt. Meine Frage wäre: Gibt es Überlegungen, die Altersgrenze, die Anwendung des elektronischen Personalausweises, zu beschränken, ab 12, an 16, ab 18? Vielen Dank.

Herr Helmbrecht:
Vielen Dank für die Frage. Vielleicht ad hoc: Wir haben ergänzend mit dem „Verein Deutschland sicher im Netz“ eine Kommunikationsplattform, die das Thema auch vom Bund in die Länder in die Kommunen bringen kann. Wenn es z.B. um die Schulen geht, ist es sicherlich eine Schwierigkeit, da wir die Länderhoheit berücksichtigen müssen, insofern können wir das sicherlich konstruktiv aufnehmen.
Zur Frage der Altersbeschränktheit haben wir eine Wortmeldung von Herr Reisen:

Herr Reisen, BMI:
Ich wollte auch nur kurz auf die Frage antworten. Wir sehen vor, dass der elektronische Identitätsnachweis erst mit 16 Jahren möglich ist. Bei der Ausgabe des Personalausweises wird bei unter 16-jährigen die eID-Funktion deaktiviert sein. Das machen wir im Wesentlichen am Sorgerecht fest, weil die Funktionalitäten, die mit der elektronischen Funktion im Internet einhergehen, für Kinder gewisse Haftungsfragen nach sich ziehen. Das müssen wir im Gesetz berücksichtigen. Wir wollen aber auch die Möglichkeit schaffen, dass Kinder, wenn Sie das 16. Lebensjahr vollendet haben, zum Amt gehen und sich unmittelbar die Funktion freischalten lassen können. Wir haben aber aus den besagten Gründen keine Möglichkeit gesehen, diese Tätigkeit mit diesen Funktionen vorher zu realisieren.

Herr Helmbrecht:
Vielen Dank, Herr Reisen. Wir haben nun zwei Wortmeldungen, zunächst Herr Prof. Hackel bitte:

Prof. Hackel, Braunschweig:
Mein Name ist Siegfried Hackel von der Physikalisch-Technischen Bundesanstalt in Braunschweig. Ich unterstütze die Aktivitäten im Bereich des ePA. Gleichzeitig würde es begrüßen, wenn die Funktionalität der qualifizierten elektronischen Signatur (qeS) seitens der Bundesregierung stärker unterstützt würde. So sind wir jetzt hier in Deutschland in der Lage, eine komplette Prozesskette für elektronisch signierte Dokumente abzubilden.
Die Vorteile eine breit ausgerollten qeS liegen klar auf der Hand: Jeder Bürger kann sich nicht nur sicher Authentifizieren, was ja auch ohne die qeS möglich ist, sondern auch rechtlich verbindlich Dokumente signieren. Dies wird durch die Tatsache unterstützt, dass der Lebenszyklus eines elektronisch signierten Dokumentes mittlerweile lückenlos unproblematisch abgebildet werden kann.
So gibt es seit der CeBIT eine nach EAL 4+ zertifizierte Schnittstelle zur Anbindung von Applikationen an nahezu beliebige Chipkartenlesern und ebenso nahezu beliebige Chipkarten, und zwar konform nach dem Signaturgesetz. Dies ist unter dem Schlagwort eCard-API Framework zusammengefasst. Somit lassen sich problemlos elektronisch signierte Dokumente erzeugen.
Werden die Dokumente in dem nach ISO standardisierten Format PDF/A angefertigt und signiert, so hat man in Verbindung mit der Datenablage nach dem ArchiSafe-Prinzip eine rechtssichere Methode der Langzeitspeicherung dieser Dokumente. Für in PDF signierte Dokumente gibt es seit etwa zwei Jahren einen nach EAL 4+ zertifizierten Viewer, der genau das anzeigt, was unterzeichnet wurde.
Weiterhin wäre es wünschenswert, wenn der Bürger nicht nur Bescheinigungen online beantragen kann, sondern auch online rechtsverbindlich zugesandt bekommen kann, beispielsweise die Kfz-Zulassung oder das polizeiliche Führungszeugnis. Diese könnten als PDF/A-Dokument, welches mit der qeS rechtsgültig signiert wurde, online an den Antragsteller gesandt werden.
Hier haben wir gegenüber anderen einen erheblichen zeitlichen Vorteil, den ich auf zwei bis drei Jahre schätze. Diesen Vorsprung sollten wir nutzen. Vielen Dank.

Dr. Helmbrecht:
Vielen Dank für diese Ergänzung. Heute sieht es ja so aus, dass, wenn ich ein polizeiliches Führungszeugnis bei einer Bewerbung im öffentlichen Dienst brauche, dieses ausdrucke. Ich glaube, wenn man dies zu Ende denkt, müssen wir die gesamten Prozessketten überall durchgängig machen, um so etwas auch zu nutzen.
Herr Reisen, bitte:

Herr Reisen:
Das Konzept des Rückkanals, also der Bescheidzustellung, wird gerade durch den Dokumentensafe bei den Bürgerportalen realisiert. Man muss wirklich das integrale Konzept von Bürgerportalen und Personalausweis an der Stelle sehen. Das ist ein Konzept, das genau den medienbruchfreien Prozess insgesamt beschreibt und darin liegt der Mehrwert: die Authentisierung gegenüber den Diensteanbietern zu ermöglichen und bei Bescheidverfahren über die Verfahren des Bürgerportals auch den Bürgern und Bürgerinnen die Möglichkeit zu geben, die Dokumente, die sie erhalten, für sich authentisch, integritätsgesichert zu speichern, auf Dauer im Zugriff zu haben und wieder verwerten zu können. Dadurch wird aus beiden Projekten ein Ganzes.

Dr. Helmbrecht:
Vielen Dank für diese Botschaft. Jetzt hatten wir hier vorn eine Meldung von Herrn Binninger.

Herr Binninger, CDU/CSU Bundestagsfraktion:
Ich war Berichterstatter für den ePass, den wir seit dem 1. November eingeführt haben und bin jetzt Berichterstatter in unserer Fraktion für das Thema ePersonalausweis. Aus der Sicht eines Politikers sehe ich eine große Gefahr für dieses Projekt. Dass wir die Diskussion darüber zu sehr unter uns führen. Hier die Experten und die eigentlich Überzeugten, aber die öffentliche Diskussion bestimmen die, die es politisch ablehnen, der Chaos Computerclub und andere IT Experten oder solche, die sich dafür halten. Die haben die Deutungshoheit in den Medien. Zumindest immer ein Stück weit, und es ist ungeheuer schwierig, dann etwas wieder zu Recht zu rücken.
Ich will es an einem Beispiel deutlich machen. Wir hatten eine Sachverständigenanhörung zum Thema - und das wird beim ePersonalausweis wieder kommen – „Kann man denn das, was auf dem Chip gespeichert ist, quasi im Vorbeigehen, wie auch immer, mit einem HiTech-Scanner über die RFID Schnittstelle ohne direkte Verbindung auslesen?“ Da gab es irgendeinen Experten, der gesagt hatte, es sei ihm gelungen. Damit sei dieser Chip, anders als vom BSI, BMI und von uns als Regierungsfraktion behauptet, doch nicht so sicher wie man tun würde. Wir haben dann, weil wir uns relativ sicher waren, dass das nicht stimmt, in der Sachverständigenanhörung immer wieder nachgehakt. Und am Ende kam folgendes heraus: Um die Daten aus dem Chip auszulesen, muss man vorher schon im Besitz der Daten sein, die man auslesen will. Dann funktioniert es. Wozu man es dann noch macht, ist natürlich schleierhaft und eher irrelevant. Wenn man aber nicht im Besitz dieser Daten ist, darf sich der Chip 12 Tage (!) - das ist der Verschlüsselungsalgorithmus hochgerechnet - nicht vom Fleck bewegen und max. 20 cm vom unberechtigten Lesegerät entfernt sein. Dann gelingt es vielleicht.
Trotz dieses völlig unwahrscheinlichen Szenarios hat sich dieses Beispiel hartnäckig gehalten und als der BKA Präsident gesagt hat, dass er seinen Pass in eine Schutzhülle steckt, wie man nun mal ein Dokument in eine Schutzhülle steckt, ging es wochenlang durch die Medien, dass auch der BKA Präsident diesem Dokument nicht trauen würde und deshalb eine alubeschichtete Schutzhülle hätte, um das Auslesen zu verhindern. Diese Aussage war falsch und wurde so gar nicht gesagt, wie anhand des Protokolls belegt werden konnte.
Entschuldigung, dass ich etwas ausgeholt habe mit dieser Geschichte, aber es macht deutlich, und das war vorher der Wunsch der Kommunikationsstrategie, das Projekt ist beim BMI und beim BSI in sehr guten Händen. Und natürlich hilft es, wenn Sie zusammenarbeiten. Aber ich glaube, es hilft uns noch mehr, wenn jeder von Ihnen in seinem Bereich gegenüber seinen Kunden, gegenüber den Medien, die er kennt, mit den Zugängen, die Sie haben, dieses Projekt befördert, erklärt und auf technischen Unfug wirklich auch schnell reagiert. Wir werden nicht beim Zusatznutzen des ePersonalausweis noch eine große politische Diskussion bekommen, auch nicht mit unserem Koalitionspartner. Wir werden die Diskussion beim ePersonalausweis an einer Stelle wahrscheinlich noch haben; das ist das Thema ‚Brauchen wir biometrische Merkmale auf dem Chip?’
Deshalb hätte ich jetzt dazu eine Frage an einen der technischen Experten; ich bin keiner. Der Datenschutzbeauftragte könnte sich vorstellen zwei Chips auf diese kleine Karte zu installieren, einen mit den Zusatzfunktionen und einen Chip mit den biometrischen Daten, weil es nur dann sicher wäre. Brauchen wir das oder wäre das einfach nur ein bisschen Symbolik, um irgendetwas Rechnung zu tragen?
Die zweite Diskussion, die wir bekommen werden: Brauchen wir die biometrischen Merkmale, weniger vom Gesicht, daran stört sich keiner, aber von den Fingerabdrücken. Jetzt

sind wir schon sehr weit entgegengekommen und haben gesagt, dass wir die Fingerabdrücke nach dem Produktionsprozess löschen, anstatt sie wie alle anderen Daten des Passes, bei der Passbehörde zu speichern. Das biometrische Bild wird gespeichert, der Fingerabdruck wird gelöscht. Trotzdem werden wir diese Diskussion erneut bekommen. An der Stelle würde ich mir erhoffen, dass Sie als Experten deutlich machen: wer Angst hat, dass von diesem Chip die verschlüsselten Fingerabdrücke ausgelesen und missbräuchlich verwandt werden könnten, der müsste eigentlich jeden Tag mit Handschuhen herumlaufen, weil der Fingerabdruck ein flüchtiges biometrisches Merkmal ist, den wir etwa 500mal am Tag irgendwo hinterlassen, am Glas, am Türgriff, an Ihrem Schreibtisch. Das heißt, wenn jemand Ihre Fingerabdrücke will, gibt es 100mal leichtere Methoden als sich diesen ePA zu besorgen und dann mühsam rückwärts zu entschlüsseln. Trotzdem werden wir diese Diskussion zu führen haben. Die können wir aber allein, weil uns immer natürlich politisches Interesse unterstellt wird, nicht gewinnen. An der Stelle brauchen wir auch Sie, nicht erst im Zusammenspiel, sondern jeder von Ihnen auch wieder in seinem Bereich. Sie haben das Know how. Sie haben die Akzeptanz und auch die fachliche Expertise, deutlich zu machen, dass hier Sorgen unbegründet sind, der Nutzen sehr groß ist und wir in Deutschland mit diesem Dokument wahrscheinlich dann auch den ‚State of the Art' für alle Dokumente der Zukunft bestimmen werden. Wenn wir die Ersten sind. Noch können wir es sein. Beim Pass waren wir es zusammen mit ein paar anderen. Beim ePA mit Zusatzfunktionen wären wir definitiv die Ersten. Wir werden dann mit führend bei dieser Technik sein, und diese Chance sollten wir nicht vertun. Ich bitte um Nachsicht, dass ich etwas länger geredet habe, es ist die Schwäche von Politikern. Ich hoffe, es war trotzdem einigermaßen hilfreich für die Diskussion. Herzlichen Dank.

Dr. Helmbrecht:
Vielen Dank. Sie sprechen mir als BSI-Vertreter da aus der Seele. Vielleicht noch eine Bemerkung dazu: Ich glaube, die größte Schwierigkeit ist, dass man einmal auf der rationalen Ebene argumentiert, dann emotional mit Journalisten oder dem Chaos Computer Club, die dann tolle Sendungen oder irgendwelche apokalyptischen abstrusen Szenarien darstellen, . Aber Sie haben hier Herrn Kowalski vom BSI, Herrn Houdeau von Infineon und Herrn Bartels von NXP, die das fachlich 100%ig beantworten können. Wer möchte beginnen? Herr Kowalski:

Herr Kowalski, BSI:
Zunächst einmal hat mir sehr gefallen, was Sie gesagt haben. Beim ePass haben wir auch Neuland betreten. Wir haben uns früh gegen die Bedenkenträger engagiert. Damit hatten wir die Gelegenheit, die internationalen Standards wesentlich mitzugestalten. Die Fragen und Aufgaben ‚Wie sicher ist ein ePass, wie sehen die Sicherheitsverfahren aus?' konnten wir auf dem Niveau der deutschen Sicherheitsüberlegungen festlegen. Diese Chance hätten wir nicht gehabt, wenn wir erst in fünf Jahren damit angefangen hätten. Dasselbe gilt eigentlich für den ePA auch, auch für die europäische Standardisierung von eIDs. Zum Thema ‚Bringen zwei Chips in einem ePA mehr Sicherheit?' Ich könnte Ihnen das jetzt technisch erklären, will es Ihnen aber ersparen. Ich kann aber sagen, dass der Bundesdatenschutzbeauftragte und seine Experten in die Überlegungen einbezogen sind. Sie nehmen ständig an unseren Arbeitsgruppen teil. Ich bin sicher, dass sie auch davon überzeugt sind, dass zwei Chips nicht notwendig sind. Falls die Bedenken weiter bestehen, sind wir gern bereit, eine Sonderveranstaltung für die Datenschutzbeauftragten zu machen, um das noch einmal eingehend zu erklären.

Herr Houdeau, Infineon:
Vielleicht machen wir das etwas bildhaft. Stellen Sie sich vor, Sie haben ein Miethaus mit zwei Mietern, Müller und Meier. Beide haben dasselbe Dach, bzw. den denselben Chip. Beide

haben zwei Zutrittsverfahren, der eine für seine Wohnung, der andere für die andere Wohnung und beide Schlüssel sind untereinander nicht austauschbar. Sie müssen sich die hoheitliche Funktion auf dem Chip vorstellen mit einem Zutrittsmechanismus, ein Schlüssel für die Travel Funktion und den zweiten, für die Authentisierungsfunktion. Das wäre die Voraussage: wenn Sie einen Chip haben mit zwei Zugangsmechanismen, ist das nichts weiter als zwei getrennte Wohnungen mit getrennten Schlüsseln unter demselben Dach. Das könnten Sie natürlich auch in zwei Häusern bauen nebeneinander und sagen, dass es tatsächlich physikalisch zwei Eingänge, zwei Dächer und zwei Türen. Sie können aber auch sagen, das Ganze ist ein Miethaus mit zwei Wohnungen – bildhaft gesprochen. Es ist der gleiche Mechanismus. Sie haben die gleiche Sicherheit.

Herr Bartels, NXP Semiconductors:
Ich stimme dem völlig zu, was Herr Houdeau gerade sagte. Vielleicht kann man noch eins darauf setzen, indem man sagt: Es ist sicherlich auch ein Vorteil, wenn man ein integriertes Sicherheitskonzept hat, das eben beide Anwendungen, die voneinander getrennt sind, umfasst und auf die Art und Weise dann die Sicherheit insgesamt sicherstellt.

Herr Kowalski:
Ich gebe Ihnen völlig Recht. Die Schwierigkeit ist, und das erlebe ich im BSI auch, wie man diese fachliche Argumentation in die Breite bringt. Um die Frage der Vorredner noch einmal aufzunehmen: Was wir brauchen, ist ein Kommunikationskonzept, wie man aus der Fachlichkeit diese Thematik dem Bürger darstellt und erklärt. Dabei darf man nicht vergessen und das ist nicht böse gemeint, dass überspitzt formuliert nicht alle das gleiche intellektuelle Niveau haben. Dessen muss man sich einfach bei der Kommunikation bewusst sein.

Herr Wendling, SCM Microsystems:
Vielen Dank. Ich wollte versuchen, den Kreis zu schießen, was wir hier gehört haben von Herrn Staatssekretär Beus und auch soeben. Lassen Sie mich eine Frage an Sie stellen, wir sind hier doch ein ganz elitärer Kreis. Wer von Ihnen hat einen Personalausweis? Jeder? Einer nicht? Ich will jetzt nicht in die Persönlichkeitsstrukturen eindringen, aber wollen wir uns darauf festlegen, dass 90% einen Personalausweis haben? An die 90% Verbliebenen: wie viele von Ihnen haben diesen Personalausweis in den letzten zwölf Monaten wissentlich genutzt? Einige. Beim Einchecken im Flugzeug, im Hotel? Sehr gut.

Prof. Thielmann:
Und wenn Sie im Kaufhaus etwas einkaufen wollen über 500 Euro mit EC-Karte, müssen Sie einen Personalausweis vorlegen.

Herr Wendling:
Ich persönlich kann als Vorschlag einbringen, dass wir vielleicht unter Federführung des Münchner Kreises ein Gremium bilden sollen, dass über die Finanzierung der Einführung diskutieren soll - hier geht es ausschließlich um Marketingmaßnahmen – natürlich unter Beteiligung der Bundesregierung. Beide haben einen Vorteil davon, die hoheitlichen wie die privatwirtschaftlichen Anwendungen. Also müssen die Kosten auch beide irgendwie tragen. Ich weis aktuell nicht was der neue Personalausweis den Bürger kosten wird und was Staat, Bürger und Privatwirtschaft durch die Verwendung einsparen können. Man müsste das einfach einmal erarbeiten. Es geht nur nicht, dass man sagt, okay, Privatwirtschaft, seht ihr mal zu, dass ihr das zum Laufen kriegt. Mein Vorschlag ist, einen Arbeitskreis, eine Gruppe, eine Formation zu gründen, die das Grundwerk dafür legt, damit hier ordentliches Marketing betrieben werden kann, ansonsten gibt es ein Rohrkrepierer.

Prof. Thielmann:
Vielen Dank. Ob der Münchner Kreis die richtige Plattform dafür ist, sollten wir im Moment noch offen lassen. Aber ich denke, die Diskussionen dazu und dass wir so etwas brauchen, ist sicher wichtig, und das sollten wir auch so festhalten.

Herr Chiachiarella, Versicherungswirtschaft:
Es wurden heute viele Befürchtungen und Bedenken hinsichtlich des Erfolges eines Personalausweises als „Bürgerkarte" geäußert. Sicherlich gibt es immer Bedenken bei neuen Verfahren und Technologien, aber auf der anderen Seite auch viele Chancen und ich sehe – trotz Berücksichtigung aller Vorbehalte – lieber die Chancen, die letztendlich für den Fortschritt so wichtig sind. Lassen Sie mich direkt einige konkrete zukunftorientierte Szenarien – natürlich aus der Versicherungswirtschaft – aufzeigen:
Drei Beiträge des heutigen Abends meiner Vorredner befassten sich bereits mit dem Thema Kfz-Zulassung. Wie Sie sicherlich wissen gibt es seit 1. März diesen Jahres keine papiergebundene Doppelkarte mehr, sondern eine elektronische Versicherungsbestätigung, die so genannte eVB. Die Kunden benötigen nur noch eine Nummer, die Sie der Zulassungsstelle mitteilen. Die Versicherungsbestätigung wird bereits vorab vollelektronisch von der Versicherungswirtschaft zur Zulassungsstelle übertragen. Das ist der erste bereits realisierte Schritt. Der zweite logische Schritt müsste zukünftig der sein, dass der Kunde über den elektronischen Personalausweis gesichert online Versicherungsschutz beantragen und bekommen kann. Wenn der Kunde wie im Projekt der Bundesregierung „Kfz-Online 2010" geplant auch die Zulassung selbst vollelektronisch mit der Behörde abwickeln könnte, hätten wir hier eine Massenanwendung für den ePA.
Ich bringe Ihnen noch ein zweites mögliches Beispiel aus dem Bereich der Versicherungsleistungen. Nach einen Unfall oder sonstigem Schadenereignis geht es darum, den Kunden möglichst umgehend zu helfen. Rechtlich abgesicherte Schadenmeldungen könnten mithilfe eindeutiger digitaler Identitäten viel unbürokratischer, sicherer und vor allen Dingen schneller erfolgen. Wenn wir die Anwendungen und rechtlichen Rahmenbedingungen dafür haben, kann der berechtigte Anspruchssteller noch schneller über die Schadenersatzleistung verfügen. Ich danke Herrn Büger insbesondere für eine Aussage in seinem Vortrag; wir müssen natürlich die bestehenden Formvorschriften so anpassen, dass der ePA für die Geschäftsprozesse rechtssicher genutzt werden kann. Und zum Schluss noch ein Hinweis aus unserer Branche: Für viele elektronische Kommunikationsprozesse benötigt der Kunde keinen Kartenleser oder entsprechendes Endgerät, weil wir unsere Kunden zu Hause beraten und das technische Equipment heute schon bereits – wo möglich – im Einsatz haben und zum Kunden mitbringen. Das war ein kleines Statement aus der Anwendungswelt, wie wir uns vorstellen und wünschen, den neuen ePA verwenden und einsetzten zu können. Wir sind gern bereit, dass BMI bei der Entwicklung und Fortführung des ePA weiterhin zu unterstützen.

Dr. Helmbrecht:
Ja, danke. Jetzt bitte Herr Dr. Baumgart.

Dr. Baumgart, secunet Security Networks:
Ich bin Rainer Baumgart von der secunet. Ich wollte nur eine Anmerkung machen. Es ist schon mehrfach das Thema Lesegeräte angesprochen worden. Wir sind eigentlich für Hochsicherheitssysteme in Deutschland zuständig, haben aber auch erhebliche Erfahrungen, wie einige andere hier auch im Raum, aus dem Umfeld Signaturen, Signaturgesetz. Ich will jetzt nicht sagen, dass das deutsche Signaturgesetz, was sicherlich ganz früh entstanden ist und wir da auch in Deutschland zumindest europaweit eine Vorreiterrolle hatten, aus vielerlei Gründen nicht zum Erfolg geführt hat. Aber ein Grund sind sicherlich auch nicht vorhandene

oder zu aufwändige Lesegeräte, die aufgrund von entsprechenden Vorschriften verlangt worden sind. Ob das immer sinnvoll war, möchte ich durchaus dahingestellt lassen. Wir dürfen auch beim elektronischen Personalausweis nicht vergessen, dass wir die PIN und dann noch z.B. den Besitz des Ausweises als ein Sicherheitsmerkmal haben. Wir sollten nicht alles auf die PIN zurückverfolgen, denn die PIN ist nur ein Sicherheitsmerkmal, aber es darf nicht das alleinige sein. So haben wir eine ganze Menge zusätzlicher Kryptographien und Verfahren, wie Authentisierungen und Kryptographie sowie weitere Mechanismen. Wenn wir dann am Ende Lesegeräte fordern, die der Anwender oder auch ein Sponsor eventuell nicht ohne weiteres beschaffen wird, weil er entsprechende aufwändige Infrastrukturen benötigt, wird die Sache nicht unbedingt zu einem Erfolg. Man kann aber noch nachbessern. Denn man ist heute sicherlich in der Lage, auch Softwaretechnologien auf den Rechnersystemen einzusetzen, die eine weitestgehende Verbesserung der PIN-Eingabe mit Schutz gegen Trojaner ermöglichen, Herr Helmbrecht, Sie hatten es angesprochen, auch damit wirksam schützen können. Ich bitte, nicht Rechtsvorschriften zu erlassen oder Rahmenbedingungen zu wählen, die dazu führen, dass wir keine Leser im Feld haben und wir Lesegeräte niemals in der breiten Masse so vorfinden werden.

Dr. Helmbrecht:
Möchte dazu jemand etwas sagen? Dann will ich das für den Moment einmal tun und vielleicht jetzt Wasser in den Wein gießen, weil, wie Sie wissen, ich hier das Bundesamt für Sicherheit und Informationstechnik vertrete – ich bin jetzt im Moment nicht Moderator, sondern trete als BSI Präsident auf. Als beratende, technische Fachbehörde werden wir in dem Umfeld durchaus schwierige Diskussionen haben. Ich mache das einmal am Beispiel des Themas Phishing deutlich. Wenn wir über Phishing und Trojaner reden, dann wissen wir, dass wir heute unsichere Rechnerplattformen haben und dass es möglich ist, mit krimineller Energien PIN und TAN abzugreifen. Wir diskutieren darüber, wie man zum Beispiel sichere Token oder andere technische Maßnahmen nutzt. Wenn ich vorhin das Beispiel noch einmal kurz erläutere, was Herr Zeino-Mahmalat erzählt und vorgeführt hat, ist, dass Sie einen einfachen USB Leser haben und die PIN dann an der PC- Tastatur eingeben. Damit haben Sie natürlich ein Sicherheitsrisiko, dass Sie die Eingabe mit einem Trojaner abfangen können. Daraus folgt die Frage, wie man mit skalierbarer Sicherheit umgeht, d.h. wir haben heute Verfahren, wo Sie über Passwort und User ID reden. Wir haben dann einfache USB Leser. Es gibt USB Leser mit Fingerabdruck, den wollen wir beim ePA nicht privatwirtschafltich nutzen, wir haben Klasse 3 Leser. Es gibt Leser, die teilweise in die Hardware integriert sind. Insofern ist es sicherlich schwierig, zu argumentieren und zu sagen: Wie gehen wir mit Sicherheitsrisiken um, wenn wir einen billigen einfachen Leser im Feld haben, der dann ggf. Risiken hat? Jetzt kann man sicherlich sagen, wenn Sie das in der Versicherungswirtschaft, bei eBay machen, dann können Sie das versichern. Dann haben Sie ein Restrisiko. Aber wie gehen wir damit um, wenn der Staat ein Bürgerportal anbietet, wo der Staat in der Verantwortung ist. Wenn dann die Frage in der Öffentlichkeit nach der Sicherheit gestellt wird, dann erwartet der Bürger 100% Sicherheit. Und dann geht jemand vom Chaos Computer Club hin und nimmt dann nicht den Fingerabdruck, den er mit Silikon fälscht, sondern zeigt, dass der schöne einfache USB ePA-Leser gehackt werden kann. Und wie gehen wir dann damit um? Ich will Ihnen nur verdeutlichen, dass dies eine Frage ist, die wir gerade in diesen Tagen in unserem Hause diskutieren und die sicherlich nicht einfach ist. Auf der einen Seite sind wir für das Thema IT Sicherheit als Bundesbehörde verantwortlich und auf der anderen Seite sehen wir natürlich auch, dass wir die Geschäftsmodelle in der Privatwirtschaft voranbringen müssen.

Herr Zeino-Mahmalat:
Da Sie mein Beispiel genannt haben, kann ich vielleicht kurz darauf eingehen. Die Frage haben wir uns auch gestellt. Wie viel Sicherheit brauchen wir denn eigentlich? Wie viel Sicherheit haben wir heute? Also, heute haben wir im Prinzip gar keine, weil ja der Kunde, der Mensch, der vor dem Bildschirm sitzt, irgendeinen Namen eingeben kann, und ich bekomme Daten übermittelt von einer Person, die vielleicht überhaupt nicht existiert. Es sei denn, ich lasse mir die Unterschrift zuschicken, und dann geht das im Prinzip nicht online. Was ist jetzt der Schaden, der eintreten könnte? Jemand, der den Personalausweis stiehlt, muss erst einmal in den Besitz dieses materiellen Gegenstandes kommen und es dann noch schaffen, die PIN zu hacken. In unserem Beispiel könnte er jetzt für diese Person ein eTicket kaufen. Also, nicht einmal für sich selbst, sondern zum Beispiel für seinen Nachbarn. Das heißt, der Angreifer schreibt auf seine Chipkarte ein eTicket, was für seinen Nachbarn gilt. Also, kann er selbst gar nicht fahren. Da fällt er sofort in der nächsten Kontrolle auf. Jetzt kommt der Betroffene und meldet sich bei uns, da werden wirklich 20 oder 50 Euro vom Konto abgebucht, weil offenbar jemand eine Lastschrift eingegeben hat für ein eTicket, und sagt, dass er das nicht getan hat. Wir blockieren das eTicket, geben ihm die 50 Euro zurück und entschuldigen uns. Die Frage ist, wo ist wirklich Angriffspotenzial? Und wenn dann wirklich jemand einen Angriff gemacht hat: was für ein Schaden hat er eigentlich angerichtet? Ich habe mich eigentlich gewundert, dass es viel weniger Diskussionen gibt rund um den Versandhandel. Da ist das Angriffspotenzial noch viel höher. Da bestelle ich auf den Namen meines Nachbarn bei Neckermann.de einen DVD-Player. Ich weiß ganz genau, wann der Postbote kommt, stehe vor dem Haus und nehme das Paket an. Dann ist der DVD-Player weg. Das würde mit dem ePA so nicht mehr gehen. Ich müsste erst von meinem Nachbarn den Personalausweis stehlen und dann noch seine PIN hacken. Man muss sich einmal bewusst machen, dass wir damit ein höheres Sicherheitsniveau haben werden, als wir heute haben. Wir haben keine absolute Sicherheit. Es wird nie eine absolute Sicherheit geben. Man muss nur das Niveau regulieren.

Dr. Helmbrecht:
Sie verkennen einen wesentlichen Aspekt. Ich will zwei Aspekte erläutern. Das eine ist, was aus dem politischen Umfeld gesagt wird. Das ist das, was in der Presse stehen wird. Das zweite ist, das bitte ich, sich einfach einmal bildlich vorzustellen. Da steht ein BSI Mitarbeiter in einer Anhörung einer Bundestagesausschusssitzung - das kann ich sein, das kann ein Mitarbeiter des BSI sein – und wird gefragt, ob der elektronische Reisepass sicher ist. Der elektronische Reisepass ist auf dem Stand der Technik sicher, dazu stehe ich. Da bin ich mit meinen Spezialisten einer Meinung. Das Argument, das ich bringe, ist plakativ: das Gesichtsbild kann ich besser fotografieren, den Fingerabdruck kann ich einfacher vom Glas nehmen, als umständliche illegal aus dem ePass auslesen zu wollen. Jetzt stellen Sie sich irgendeine Anhörung vor. Da wird ein BSI Mitarbeiter gefragt, ob das Bürgerportal mit dem einfachen Leser sicher ist. Was sagt mein Mitarbeiter oder ich dann, wenn Sie über unsichere Plattformen oder potenzielle Risiken reden? Und in dem Moment vielleicht noch irgendein Pressevertreter vom Chaos Computer Club dabei haben. Den kann man bei Silikonfingern noch überzeugen mit Lebendfingererkennung technologisch weitermachen. Aber dann sagen Sie mir bitte auch heute, welche technologische Lösung Sie für einen einfachen Leser haben, Herr Dr. Baumgart sagte es, eine unsichere Plattform sicher machen. Darum geht es am Ende. Es geht nicht darum, dass ich Ihnen persönlich glaube oder ob man das versichern kann. Oder dass ich Geld zurückerstatten kann. Was ist denn, wenn von einem Bürgerportal ein Finanzamtsbescheid irgendwo in der Presse landet? Darüber reden wir dann, und damit müssen wir umgehen. Und da sind wir wieder bei dem Kommunikationsprozess und bei den Themen skalierbare Sicherheit, und qualifizierte Signatur. Das müssten wir diskutieren.

Prof. Thielmann:
Wir müssen langsam zum Ende kommen.

Herr Walloschke, Fujitsu Siemens Computers:
Ich möchte noch einmal auf die technologischen Themen etwas näher eingehen, die Sie indirekt, vielleicht auch aus dem politischen Umfeld heraus angesprochen haben, also das gefühlte Erfolgserlebnis, wenn ich das mal so sagen darf. Wir wissen, dass über die letzten 30 Jahre ein unglaublicher Technologiefortschritt stattgefunden hat, und wir momentan immer noch eine hohe Innovation erleben. Ich kann mir momentan nicht vorstellen, dass wir ein Versäumnis der letzten 30 Jahre, nämlich die Chiptechnologie zu integrieren, richtig wahrnehmen. Seit 1985 gibt es die kommerzielle Chiptechnologie, also 20 Jahre hätten wir die Chance gehabt, es schon zu tun - das haben wir einfach liegen lassen. Aber die Chiptechnologie hat sich eigentlich im Vergleich zu anderen Technologien gar nicht in gleichem Maße weiter entwickelt. Sie ist mehr oder weniger gar nicht in der gleichen Explosionsartigkeit gewachsen, sie hat nur ein gewisses Nebendasein geführt. Diese Technologie haben viele Betriebssystemanbieter, sprich jene, die es letztlich hätten vor Augen haben können, gar nicht hinreichend wahrgenommen. Heute ist alles Mögliche integriert, nur ausgerechnet diese Technik nicht. Aber es besteht überhaupt kein Grund, warum diese morgen nicht integriert sein soll. Ich verstehe die Diskussion momentan als Übergangs-diskussion, weil uns dies alles bewusst geworden ist. Vor drei, fünf Jahren hätte das niemand ernsthaft als Potenzial erkannt. Deswegen gehe ich davon aus, dass wir uns inzwischen in einer gewissen heißen Diskussionsphase befinden, die uns eben auch gesamtgesellschaftlich Klarheit verschafft. Aber letztendlich werden wir in fünf Jahren diese Diskussion nicht mehr führen, weil dann alle Systeme diese Technologie an Bord haben. Die Frage ist heute in der Fertigung, was so etwas kostet. Die Zahlen, die hier genannt worden sind, sind alle falsch. Ich möchte das einfach an der Stelle sagen: Diese Zahlen sind erst in dem Moment richtig, wenn Sie alle das Endprodukt nicht mehr hinterfragen, die eine derartige Technologie beinhaltet. Damit möchte ich auch noch einmal positiv ein Thema adressieren: wir brauchen natürlich die Treiber, d.h. die Anwendungen. Ohne die wird es garantiert keine Integration geben, ich kann dann niemanden bei uns überzeugen, in der Fertigung eine solche Investition zu tätigen, weil die erste Frage immer den sog. „Forecast“ betrifft. Das bedeutet für uns hier die gleiche Frage: wird es ein Erfolgsprodukt? Deswegen sind wir alle hier direkt voneinander abhängig. Ich glaube, dass es hierzu keinen Dissens gibt, dass es aber erst in dem Moment eine gemeinsame Erfolgsstory geben wird, wenn die „geballte Intelligenz in diesem Raum sich nach draußen ergießt“ - denn hier drinnen nutzt sie uns nur bedingt.

Prof. Thielmann:
Vielen Dank.

Herr Wolfenstetter:
Wir reden hier sehr über das Spannungsfeld Bedienfreundlichkeit, Usability, Komfort einerseits und Sicherheit andererseits. Das ist ein Problem-Klassiker sozusagen. Und hierbei gibt es per se keinen Konsens: Man kann nicht beides zugleich haben. Aber ich habe hier in meiner Hand ein Handy. Und das ist heutzutage eigentlich ein kleiner PC, der potentiell auch Trojaner oder Viren enthält, nichts anderes als bei einem Laptop. Und dennoch ist das Handy eine Success-Story. Wir haben vor vielen Jahren die Sicherheitsmerkmale definiert und spezifiziert - damals in der GSM-Association - haben sogar Kryptoverfahren finden bzw. erfinden müssen. Wir hatten bei allem Tun nicht gewusst, wie es ausgehen würde. Nehmen wir als Beispiel die damaligen Business-Cases: Vor 15 Jahren hieß es noch, dass wir in Deutschland eine Sättigung des Handy-Marktes bei 2 Millionen Teilnehmern bekommen werden. Wir haben jetzt weltweit aber über 3 Milliarden Teilnehmer, die immer noch auf

Basis der damals definierten Sicherheit telefonieren. Sie werden jetzt fragen, was die Sicherheitsziele waren und immer noch sind: Das wichtigste Sicherheitsziel ist: Ich muss dafür sorgen, dass keiner auf Kosten anderer telefonieren kann. Diese Sicherheit muss ich herbeiführen. Es hat bis heute funktioniert, und zwar weltweit, aufgrund eines Standards, den Europäer entwickelt haben. Insofern sollte man diesen Erfolg dann auch kommunizieren. Es gibt natürlich immer etwas zu kritisieren und zu verbessern. Dabei gibt es Leute, die hüpfen sozusagen von Ast zu Ast. Diese Leute finden immer ein Haar in der Suppe, um sich zu profilieren, auch im Fernsehen. Damit müssen wir leben. Was ich damit einfach sagen will, dass wir es jetzt packen und durchsetzen sollten, auch wenn wir Risikoreste in Kauf nehmen müssen.

Prof. Thielmann:
Vielen Dank. Herr Büger, Sie wollten…

Dr. Büger:
Ich erlaube mir, auch wenn ich im Vortrag schon ein paar Punkte gesagt habe, hier noch einmal zu den Themen Marketing und Umgang mit dem ePA in der Öffentlichkeit, einige Gedankenanstöße zu geben. Was mir an der Stelle wichtig ist, ist zu erwähnen, dass der ePA nicht aus sich heraus lebt, dass wir nicht mit dem ePA alleine an die Öffentlichkeit gehen können, wir damit sogar manche Ängste bedienen – Sie haben die auch entsprechend erwähnt –, sondern der ePA letztendlich aus den Anwendungen heraus leben muss. Das gilt in ähnlicher Weise wir beim Thema Bankkarten: Niemand fragt, ob eine EC-Karte für sich genommen gut ist. Eine EC-Karte ist kein Produkt. Das Produkt ist das Bezahlen, also die Möglichkeit, bezahlen zu können. Die Karte ist ein Vehikel. Weil ich auch noch Bargeld in der Tasche und damit bezahlen kann, muss ich die Karte nicht nutzen, aber ich kann es. Die Nutzung der Karte ist etwas, was für den Kunden angenehm ist.
Vor diesem Hintergrund ist meine persönliche Empfehlung, dass wir den ePA überall, wo es geht, mit Anwendung verknüpfen – im öffentlichen Bereich natürlich auch mit öffentlichen Anwendungen. Das heißt, dass Sie den ePA über Themen wie ELSTER, ELENA oder Bürgerportale transportieren müssen. Diese Projekte haben Sie genannt, Herr Reisen, und ich begrüße, dass die Projekte auch mit dem ePA verbunden sind. Gern sollte der ePA auch mit Anwendungen aus dem Bereich eJustice verbunden werden. Ich durfte in Hessen an einer eJustice Kommission teilnehmen. Auch da hatten wir eine Nutzergruppe: die Anwälte. Die interessierten sich für Anwendungen. Der ePA war in ihren Augen nur eine Infrastruktur und nur wichtig, weil er der Schlüssel zu bestimmten Anwendungen ist. Ich finde es auch sehr gut, was wir heute über eGovernment in München gehört haben. Wenn ich als Bürger sage, dass ich mit diesem ePA, den ich dann in der Tasche habe, die Möglichkeit habe, bestimmte Dienste wahrzunehmen, der ePA der Schlüssel dafür ist, dann schaffen wir den Wert für den Bürger nicht aus dem ePA heraus, sondern aus diesen Anwendungen.
Wenn man daher die Anwendungen in den Vordergrund stellt, stellt man das Ganze vom Kopf auf die Füße. Wenn man in einer Gesamtstrategie sagt, dass alles damit zusammenwirkt und der ePA der Schlüssel für diese Anwendung ist, dann wird insgesamt ein Schuh daraus und man kann auch den ePA nach außen positionieren.

Prof. Thielmann:
Vielen Dank, Herr Büger. Jetzt darf ich noch einmal die Frage von Herrn Prof. Ziemer von vorhin stellen. Wenn Sie das so herzhaft und energisch kommentieren, wie kommen Sie dann von dem Zustand des wohlwollenden Begleitens in das aktive Handeln? Ich bin immer etwas direkt und fordernd in der Diskussion.

Dr. Büger:
Nein, gar nicht. Um an der Stelle auch das Missverständnis aufzuklären, selbstverständlich kommen wir auch in den Bereich des Handelns. Ich sage auch an der Stelle zu, dass wir natürlich den Personalausweis, wenn das möglich ist rechtlich – Sie wissen als Bank gibt es ganz viele Sachen, die man einfach nicht machen darf -, das auch entsprechend zu tun. Eine Kontoeröffnung mit dem elektronischen Personalausweis darf ich heute nicht durchführen, weil die Geldwäschegesetzabgabenordnung dagegen ist. Ansonsten haben wir im Thema Signaturbündnis selbstverständlich eine Signaturkarte eingesetzt, und damit können Sie Online-Banking machen. In dem Sinne können wir dieselbe Schnittstelle auch für den entsprechenden ePA nutzen. Auch da muss das Bundesfinanzministerium zustimmen, weil wir dort im Übrigen nicht diese Risikoabschätzung machen können. Wir können zum Beispiel nicht im Thema PIN/TAN sagen, dass wir nur eine PIN nehmen, wie das andere ausländische Banken machen. Da muss es zwei unterschiedliche Mechanismen geben. Also, ist das hier eine Diskussion, die wir mit dem Finanzministerium führen müssen, ob zum Beispiel Identifikationsfunktion des Personalausweises ausreicht oder ob notwendig eine qualifizierte Signatur drauf geladen werden müsste. Das wäre wieder eine entsprechende Hürde. Die Diskussion wollen wir gern führen, und wenn ich hier mitnehme, dass wir bei dieser Diskussion unterstützt werden, sage ich selbstverständlich. Und wenn das entsprechend geht und rechtlich möglich ist, dann machen wir das auch.

Prof. Thielmann:
Wen wünschen Sie sich als Partner? Sagen Sie es bitte konkret!

Dr. Büger:
Wir sind bereits mit dem Innenministerium in sehr engem Kontakt, ohne dass ich hier alle Stellen nennen kann. Aber natürlich brauchen wir das Bundesfinanzministerium im Boot. Wir brauchen es übrigens auch bei einer Sache, die wir sofort umsetzen würden: bei elektronischen Bescheinigungen. Meine Kollegen brennen darauf, elektronische Kontoauszüge anzubieten. Wir haben (rechtlich) einen gewissen Durchbruch bei Privatpersonen, aber um elektronische Kontoauszüge auch im Firmenbereich einsetzen zu können, hängen wir noch an bestimmten Sicherungsmechanismen. Hier haben wir im Übrigen einen guten Partner im Wirtschaftsministerium, das in diesem Zusammenhang auch über eine Anpassung im Signaturgesetz nachdenkt. Das sind Dinge, die wir technisch lieber heute als morgen durchsetzen würden, wo wir aber schlicht das Problem haben, dass bestimmte Dinge rechtlich nicht gehen.
Als Partner brauchen wir also das Finanzministerium im Boot, weil es das für uns zuständige Ministerium ist.

Prof. Thielmann:
Vielen Dank noch mal.

Herr Wolter, Lotto Hessen:
Wir haben uns sehr viel über verschiedene Anwendungen des EPA unterhalten, aber ausschließlich über solche im Internet. Es gibt natürlich auch noch andere denkbare Anwendungen für den EPA, die in ganz normalen Geschäften stattfinden. Viele Unternehmen haben das Problem, dass sie eigene Kundenkarten anbieten, aber die Kunden bereits viele Karten haben und keine weitere akzeptieren wollen.
Die Frage ist die, inwieweit kann ein Unternehmen den EPA statt der selbst herausgegebenen Kundenkarten nutzen? Ob das möglich sein kann, ist mir nach der jetzigen Diskussion noch nicht so ganz klar geworden. Es funktioniert natürlich nicht, wenn ich neben dem Personalausweis, den ich auf die Ladentheke lege, auch noch jedes Mal eine PIN eingeben muss, da es

zu anwenderunfreundlich ist. Was für die Kunden zu umständlich ist, wird auch nicht akzeptiert. Das Verfahren geht natürlich nur, wenn ich die wesentlichen Daten auslesen kann, ohne die PIN eingeben zu müssen. Die entscheidende Frage ist, ob das datenschutzrechtlich möglich ist oder nicht?

Dr. Helmbrecht:
Möchte jemand darauf antworten? Keiner. Dann bleibt die Frage unbeantwortet.

Prof. Thielmann:
Ich glaube, wir haben heute Abend sicher noch mehr Fragen aufgeworfen als Antworten gefunden. Hier haben wir noch eine Wortmeldung.

Dr. Mentzinis, BITKOM:
Ich würde gern das Kleeblatt der eCard Strategie von 2005 komplettieren. Wir hatten jetzt ELENA angesprochen, der Personalausweis war heute hier das große Thema, ELSTER, die elektronische Einkommenssteuererklärung und die elektronische Gesundheitskarte sind heute außen vor geblieben. Ich habe dabei vor allen Dingen eine Frage oder Denkanstoß. Von der Konzeption her war es ja so, dass die Gesundheitskarte 2006 flächendeckend ausgerollt sein sollte. Das ist Geschichte. Das ist nicht geschehen. In dem Zuge war auch geplant, dass dann wir zu einem nicht näher definierten Datum eine elektronische Patientenakte bekommen, und die Patientenkarte lässt sich nur bedienen, indem man elektronisch signiert. Kurz und gut, eine weitere qualifizierte elektronische Signatur neben dem elektronischen Personalausweis. Wann der Personalausweis flächendeckend ausgerollt sein wird, kann man noch nicht sicher sagen - lassen Sie es 2015, 2016, spätestens 2019 sein. Bei der Gesundheitskarte ist der Rollout nur sehr schwierig zu prognostizieren, insbesondere wann gerade die freiwilligen Anwendungen flächendeckend von den Kassen angeboten werden. Worauf ich hinaus will, ist, dass wir irgendwann die Situation haben, dass der Bürger in seinem Portemonnaie wahrscheinlich dann zwei Karten hat, mit denen er qualifiziert elektronisch signieren kann und dann auch zwei PINs wieder beherrschen muss. Wie können wir das irgendwie in den Griff bekommen? Ich will gar nicht irgendeine Lösung vorwegnehmen, aber es ist auch nicht so, dass man damit unbedingt Geld einsparen kann, indem man erst einmal sagt, dass die Gesundheitskarte jetzt huckepack genommen wird auf den Personalausweis. Aber wir laufen dann mittelfristig in eine Dualität rein, die doch vielleicht so nicht gewünscht ist, weil wir uns eigentlich immer vorgestellt haben, dass wir nur eine Karte haben wollen.

Dr. Helmbrecht:
Die Lösungen mit den zwei Karten können wir sicherlich als Frage mitnehmen. Das sind im Moment auch zwei unterschiedliche Techniken, kontaktbehaftet vs. kontaktlos. Ich würde das so stehen lassen, weil man eine Lösung heute Abend nicht finden wird, aber als Beitrag ist das sicherlich wertvoll.

Prof. Thielmann:
Es wird bei uns festgehalten auf der Dokumentation.

Dr. Helmbrecht:
Wir hatten sicherlich eine konstruktive und gute Diskussion. Wir haben viele Punkte angesprochen; Stichworte: Kommunikationskonzept, Datenschutz, Sicherheitsniveaus, Finanzierungskonzepte. Wir werden sicherlich im Rahmen der Auswertung des Gesprächsprotokolls prüfen, was noch an Punkten enthalten ist. Ich würde gern zum Abschluss noch einmal Herrn Dr. Beus das Wort erteilen:

Dr. Beus:
Vielen Dank. Ich möchte mich zunächst einmal für die Diskussion bedanken, insbesondere auch für die kritischen Stimmen. Aus denen lernt man ja erfahrungsgemäß am meisten für das weitere Verfahren. Uns war es auf jeden Fall klar und ist vielleicht noch einmal klarer geworden, dass wir über Form und Intensität der Zusammenarbeit weiter nachdenken müssen – auch nachdenken wollen – und dass wir den begonnenen Weg intensiv fortsetzen müssen. Das ist wichtig, auch branchenspezifisch. Wir haben den Dialog mit den Branchen aufgenommen und werden das intensiv fortsetzen. Ich glaube, die Bereitstellung von Anwendungen in dem Augenblick, wo wir die neuen Ausweise ausrollen, ist der entscheidende Punkt. Ich bin da optimistisch, weil jeder Bürger einen Personalausweis haben wird. Bei einem Führerschein ist es schon etwas eingeschränkt, aber einen Personalausweis hat halt jeder, ob er dazu rechtlich verpflichtet ist oder nicht. Und wenn er den hat, wird er überlegen, wofür er ihn anwenden kann. Deshalb sind wir da in einer anderen Ausgangsposition als bei vielen anderen Karten, die es bisher gab und die man haben konnte oder nicht haben konnte. Den Personalausweis hat jeder und deshalb ist er die große Chance, die Anwendung, die wir dann anbieten, auch wirklich durchzusetzen. Wir werden jetzt bis zum Jahresende wahrscheinlich politische Diskussionen haben, insbesondere im Gesetzgebungsverfahren. Darauf müssen wir uns einstellen. Die Diskussion wird kritisch sein und sich wahrscheinlich viel mehr mit den biometrischen Daten befassen als mit dem, was wir heute besprochen haben. Ich glaube, in diesem Stadium ist es wichtig, dass gerade von Ihnen auch immer die andere Seite betont wird, um deutlich zu machen, dass der elektronische Personalausweis eben klar ein Identitätsdokument ist, was Grenzübertritte ermöglicht und eine Passersatzfunktion hat. Aber es hat eben auch den ganz anderen wichtigen Teil – den Identitätsnachweis fürs Internet, der muss bekannt sein, damit das ausbalanciert bleibt und die Diskussion da nicht einseitig wird. In dem Augenblick, wo das Gesetz verabschiedet ist, wird die Diskussion dann auf die Anwendung im Internet gehen. Dann tritt die Biometrie in den Hintergrund und es geht darum, deutlich zu machen, wofür der Bürger den neuen Ausweis wirklich benutzen kann, und dafür zu werben, dass viele den Antrag stellen, den Ausweis schnell zu bekommen, weil sie sehen, was sie damit anfangen können. Diese Zweiteilung steht vor uns, und wir werden in intensivem Kontakt mit Ihnen bleiben, um das so gut, wie wir das können, vorzubereiten. Ich bin bei all dem, was es sicher an Problemen geben wird und die wir auch nicht klein reden sollen, optimistisch, weil ich glaube, dass der elektronische Ausweis ein Projekt ist, was sich von den anderen, die wir bisher hatten, schon wesentlich unterscheidet durch den Ansatz, dass jeder Bürger dieses Stück Plastik in der Tasche haben wird, und das schafft uns Ausgangspositionen, wie wir sie auf jeden Fall besser nicht haben können. Vielen Dank!

Anhang

Statement
Prof. Dr. Siegfried Hackel
Physikalisch-Technische Bundesanstalt, Braunschweig

Ich möchte gern mein Statement vom 2. Berliner Gespräch kurz zusammenfassen und ergänzen:

„Ich unterstütze die Aktivitäten im Bereich des ePA und würde es begrüßen, wenn die Funktionalität der qualifizierten elektronischen Signatur (qeS) seitens der Bundesregierung stärker unterstützt würde. Dies wäre z. B. durch ein Kostenmodell denkbar, wo ein ePA ohne qeS teurer wäre als mit der qeS.

Die Vorteile eine breit ausgerollten qeS liegen klar auf der Hand: Jeder Bürger kann sich nicht nur sicher Authentifizieren (was ja auch ohne die qeS möglich ist), sondern auch rechtlich verbindlich Dokumente signieren. Dies wird durch die Tatsache unterstützt, dass der Lebenszyklus eines elektronisch signierten Dokumentes mittlerweile lückenlos unproblematisch ist.

So gibt es seit der CeBIT eine nach EAL 4+ zertifizierte Schnittstelle zur Anbindung von nahezu beliebigen Chipkartenlesern und ebenso nahezu beliebigen Chipkarten nach dem Signaturgesetz an Applikationen. Dies ist unter dem Schlagwort eCard-API Framework zusammengefasst. Somit lassen sich problemlos elektronisch signierte Dokumente erzeugen.
Werden die Dokumente in dem nach ISO standardisierten Format PDF/A angefertigt und signiert, so hat man in Verbindung mit der Datenablage nach dem ArchiSafe-Prinzip eine rechtssichere Methode der Langzeitarchivierung dieser Dokumente. Für in PDF signierte Dokumente gibt es seit etwa zwei Jahren einen nach EAL 4+ zertifizierten Viewer, der genau das anzeigt, was unterzeichnet wurde. Das Protection Profile nach Common Criteria sowie eine technische Richtlinie für das ArchiSafe-Konzept ist vom BSI überprüft.

Weiterhin wäre es wünschenswert, wenn der Bürger nicht nur Bescheinigungen online beantragen kann, sondern auch online rechtsverbindlich zugesandt bekommen kann (Beispiel: Das polizeiliche Führungszeugnis wird als PDF/A-Dokument, welches mit der qeS rechtsgültig signiert wurde, online an den Antragsteller gesandt).“

S. Hackel

Dir. u. Prof. Dr. Siegfried Hackel
Physikalisch-Technische Bundesanstalt (PTB)
Fachbereich Q.4 Informationstechnologie
Bundesallee 100
D-38116 Braunschweig
Tel.: +49 (531) 592-8400
Fax.: +49 (531) 592-8406
Mailto:siegfried.hackel@ptb.de
http://www.ptb.de
ArchiSafe-URL: http://www.archisafe.de

Statement

Peter Klinger, Fernuniversität Hagen

Die Einführung eines elektronischen Personalausweises (ePA) als Lösung des Problems der digitalen Identität für den Bereich der E – Government - Anwendungen, insbesondere für kommunale E-Government – Transaktionen, ist sehr zu begrüßen. Gerade im kommunalen Bereich mit der Vielzahl an Bürgerkontakten wird E – Government wieder ein Stück vorankommen. Neue Anwendungen werden in den kommunalen Aufgabenfeldern ermöglicht, in denen eine Identitätsprüfung ausreichend ist. Dies trifft insbesondere den Bereich der elektronischen Auskünfte aus bereits gespeicherten Datenbeständen und die Zulassung zu bestimmten Dienstleistungen, deren rechtliche Qualität keinen hohen Stellenwert hat.

Leider wird jedoch die Chance für den großen Durchbruch von E-Government nicht genutzt, indem der ePA für die qualifizierte elektronische Signatur lediglich vorbereitet wird und erst auf besondere Nachfrage des Nutzes aufgebracht wird. Diese Hemmschwelle sollte angesichts der bisherigen Geschichte der qualifizierten elektronischen Signatur in Deutschland vermieden werden. Auch nach Ausgabe des ePA gilt der § 3a der Verwaltungsverfahrensgesetze, die die qualifizierte Signatur im Verwaltungsverfahren immer dann vorschreiben, wenn „Schriftlichkeit“ notwendig ist. Diese vermag auch ein bereichsbezogenes Ordnungsmerkmal durch den ePA nicht zu ersetzen.

Da wegen des rechtlichen Hintergrundes die rechtsverbindliche Unterschriftsleistung nicht durch ein Identitätskennzeichen ersetzt werden kann, kann die Lösung nur lauten: Auf jeden ePA gehört auch eine Signatur.

Gerade das kommunale E-Government wird als Lösungspotential für die Umsetzung der EU Dienstleistungsrichtlinie neuen Schwung gekommen. „"… aus der Ferne und elektronisch…(Artikel 8, Abs. 1 EU DRL) funktioniert nur mit E-Government. Da zu erwarten steht, dass nach der Realisierung der einheitlichen Ansprechpartner für Dienstleistungen rund um das Thema Wirtschaft auch Bürgerdienstleistungen nach dem Prinzipien des One stop Government abgewickelt werden müssen, hat Deutschland die reale Chance im europäischen E-Government – Ranking nach vorne zu rücken. Dies bedingt aber nun auch den ganzen Schritten in die richtige Richtung zu gehen, und nicht nur einen zwar richtigen, aber nicht ausreichenden Teilschritt.

Am Rande sei noch vermerkt, dass der Ausgabezyklus des ePA möglichst kurz gehalten werden muss. Eine flächendeckende Versorgung mit dieser grundlegenden E – Government - Infrastruktur in der Bevölkerung erst im Jahre 2017 ist zu spät. Weiter sollte zur Vermeidung unterschiedlicher Lesesysteme nur eine Zugriffsart (kontaktlos) für alle Funktionen vorgesehen werden.

Peter Klinger
Peter.Karl.Klinger@t-online.de
Fernuniversität Hagen
Rathaus21
www.hagen.de

Statement

Hans-Wolfgang Kunz, Giesecke & Devrient GmbH

Der elektronische Personalausweis als Ausprägung der European Citizen Card

Nachdem der Reisepass den Schritt vom reinen Papierdokument zu einem Ausweis mit komplementären elektronischen Funktionen gemacht hat, war abzusehen, dass auch die europäischen Personalausweise und ID-Karten sich entsprechend weiterentwickeln. Nicht zuletzt, weil diese Dokumente innerhalb der Schengen-Staaten als Reisedokument akzeptiert werden, ist es wünschenswert, die Daten und Anwendungen dieser zukünftigen Dokumente auf einer Smartcard interoperabel und kompatibel zu gestalten.

Aus diesem Grund wurde bzw. wird die europäische Spezifikation CEN prTS 15480 entwickelt, die entsprechende Rahmenbedingungen für eine europäische Bürgerkarte (European Citizen Card, ECC) festlegt.

Das Programm „E-Government 2.0“ der Bundesregierung sieht u.a. bekannterweise die Einführung des elektronischen Personalausweises (ePA) und die Erarbeitung von E-Identity-Konzepten vor. Wie auch andere Europäische Staaten sollen dem Karteninhaber neben der Identifikation in der realen Welt auch sichere IT-Zusatzfunktionen für die virtuelle Welt (Internet) angeboten werden und so neue Prozesse zum Nutzen von Bürgern, Wirtschaft und Verwaltung ermöglicht werden.

Dabei ist insbesondere zu berücksichtigen, dass es neben dem Wirtschaftsraum Europa auch den virtuellen Raum des Internets gibt, der die Grenzen der verschieden Mitgliedsstaaten verschwimmen lässt. Mehr und mehr Bürger der verschiedenen Mitgliedsstaaten werden zu „Europäern“, das heißt sie leben und arbeiten in einem europäischen Nachbarland. Somit ergibt sich die Notwendigkeit einer sicheren europaweit möglichen Authentisierung zu den jeweiligen lokalen E-Government Diensten. Dies ist seitens der EU schon lange gewünscht, jedoch gibt es dafür keinen bindenden europäischen Vorgaben. Die oben erwähnte European Citizen Card ist dafür eine Lösung!

Die unter dem Europäischen Komitee für Normung im Technischen Komitee 224 entwickelte Spezifikation enthält derzeit vier Teile:

- prCEN/TS 15480-1 Physical, electrical and transport protocol characteristics (Hardware)
- prCEN/TS 15480-2 Logical data structures and card services (Software)

- prCEN/TS 15480-3 ECC interoperability using an application interface (Interoperability Framework)
- prCEN/TS 15480-4 Recommendations for ECC issuance, operation and use (Application profiles based on use cases)

Die ersten beiden Teile sind finalisiert und veröffentlicht. Die Teile 3 und 4 befinden sich noch im „working draft“ Stadium.

Das Prinzip der Interoperabilität der European Citizen Card beruht darauf, dass man sich auf einen „Baukasten“ von Mechanismen und Methoden geeinigt hat. Damit kann prinzipiell jedes Land seine spezifischen Applikationen entwickeln. Daraus ergeben sich Anwendungsprofile, die später im Teil 4 der Spezifikation definiert werden. Eine sogenannte Middleware (Interoperability Framework), die im Teil 3 definiert wird, kann jede auf diesem Baukastenprinzip basierte Karte ansprechen und verstehen.

Das Profil der Applikationen des ePA ist als Profil 1 bereits in der Spezifikation der European Citizen Card hinterlegt. Dieses Profil wird im Rahmen des Deutschen Industrieforums (DIF AG 1) in Zusammenarbeit mit dem BSI bearbeitet, um eine Kompatibilität zu dem zukünftigen deutschen Personalausweis zu ermöglichen.

Es wird erwartet, dass auch das Profil der französischen ID bald als Profil eingebracht wird. Damit sind Deutschland und Frankreich die Treiber einer interoperablen europäischen ID Lösung. Die Realisierung beider Projekte würde auch einen großen Schritt für die European Citizen Card bedeuten und andere Mitgliedsstaaten ermutigen, den gleichen Weg bezüglich E-Identity zu gehen.

Statement

Dr. Wolf Osthaus, eBay GmbH,

Das Thema „Elektronischer Personalausweis“ hat inzwischen die Fachkreise verlassen und die breite Öffentlichkeit, damit auch die politische Debatte, erreicht. Positionen formen sich, Widerstände entstehen jetzt. Deshalb ist nun auch die Zeit gekommen, neben den zahlreichen offenen Fragen nach Technologien, Marktmodellen und Einführungsszenarien auch die Kommunikation und das Marketing in den Blick zu nehmen, wenn man einen Erfolg des ePA sicherstellen will.

Zwei spezifische Bedenken scheinen mir im Augenblick besonders geeignet, schwierige Diskussionen und mögliche Blockaden entstehen zu lassen.

- Das erste stellt in Frage, ob es berechtigt ist, Bürgern mit einem staatlichen Ausweisdokument ein Instrument für den privaten Wirtschaftsverkehr in Form der geplanten Authentisierungsfunktion „aufzuzwingen“. Es wird argumentiert, das verfassungsrechtliche Übermaßgebot gebiete geradezu, hier nur ein optionales Angebot zu machen, das der Bürger freiwillig wählen kann, aber nicht muss. Die im Regelfall nur seltenen hoheitlichen Nutzungsbedürfnisse reichten nicht aus, um von allen den Mehraufwand für die elektronische Authentisierungsfunktion fordern zu können. Es ist jedoch zu fürchten, dass genau dieser Ansatz einer raschen Verbreitung der Authentisierungsfunktion im Wege stünde. Schon jetzt muss man mit einer Übergangszeit von 10 Jahren zum neuen Ausweistyp rechnen. Ist es dem Bürger aber freigestellt, ob er eine kostenpflichtige Zusatzfunktion wählt, werden viele zunächst von einem auch kleine Zusatzinvestment zurückschrecken, oft aber schon kurze Zeit später bereuen, die Funktion nicht zur Verfügung zu haben. Es ist deshalb jetzt dringend Aufklärung nötig, dass es hier um eine unverzichtbare Funktion des neuen Ausweises geht. Der Staat hat eine Berechtigung, wenn nicht sogar eine Verfplichtung, grundlegende Infrastrukturen für den Wirtschaftsverkehr bereitzustellen. Hierzu gehört in Zeiten, in denen nun einmal ein immer größerer Teil dieses Wirtschaftsverkehrs elektronisch abläuft, muss auch ein bewährtes Instrument um eine entsprechend angepasste Verwendbarkeit ergänzt werden. So wie heute die Sichtfunktion des Personalausweises im privaten Wirtschaftsverkehr selbstverständlich zur Identifizierung zur Verfügung steht, muss dies in einer neuen Ausweisgeneration auch elektronisch für jedermann möglich sein. Adressat der Kommunikation muss zunächst in erster Linie die Politik, die diese Bedenken schürt, aber auch die Bürger müssen über die Vorteile, etwa für ihre eigenen Internetsicherheit, informiert werden, zugleich braucht es zügig Informationen, die klarstellen, dass die Mehrbelastung des Einzelnen in einem – hoffentlich – sehr vertretbaren Rahmen bleibt.
- Die zweite Frage ist mit den vorbezeichneten Ängsten verbunden und betrifft die Frage der Datensicherheit und des Datenschutzes. Insbesondere die Planungen, auch biometrische Daten auf dem Ausweis für hoheitliche Nutzungszwecke zu speichern, führen zu Vorbehalten gegen eine gleichzeitige privatwirtschaftliche Verwendung. Es sollte nun vermieden werden, dass eine aufgeladene Biometrie-Diskussion die Akzeptanz des Ausweises für sonstige Nutzungen gefährdet. Ob die Aufnahme biometrischer Daten tatsächlich notwendig ist, müssen die zuständigen staatlichen Stellen und am Ende die Politik bestimmen. Sofern auf sie nicht im Interesse einer höheren Nutzerakzeptanz verzichtet werden kann, ist es von hoher Bedeutung, den Bürgern die Sicherheit zu vermitteln, dass diese Daten keine Gefährdung ihrer Privatsphäre im privatwirtschaftlichen Einsatz bedeuten, insbesondere also, dass diese Daten absolut zuverlässig gegen den Zugriff unbefugter Dritter geschützt sind, so dass auch beim Auslesen der Identitätsdaten des Ausweises durch Private die iometrischen Daten verborgen bleiben.

Beide aufgezeigten Themen werden schon jetzt zunehmend öffentlich diskutiert. Es ist von hoher Bedeutung, hier frühzeitig steuernd in die Diskussion einzugreifen und Vorbehalte abzubauen, um nicht später vor unüberwindbaren Blockaden zu stehen, die den Gesamterfolg der neuen elektronischen Ausweisgeneration mit ihren vielfältigen, höchst nützlichen Einsatzmöglichkeiten zu gefährden.

Statement

Prof. Dr. Radu Popescu-Zeletin, FhG FOKUS Berlin

Das Fraunhofer FOKUS bietet durch seine Kompetenz in Bereichen der Interoperabilität von Technologien und Produkten in Feldern des eGovernment, eBusiness, Telekommunikation und Mobilität eine hervorragende Plattform für die kooperative Entwicklung und Erprobung innovativer IT-Lösungen. Neben branchenspezifischen und service-orientierten Konzepten nimmt zunehmend auch das Bewusstsein für die Notwendigkeit von einem übergreifenden Identitäts- und Zugangsmanagement bei der Ausgestaltung von IT-Infrastrukturen zu.
Daher hat das Fraunhofer FOKUS sich als Ziel gesetzt, die internen Kompetenzen mit den Erfahrungen und Ergebnissen ihrer Partner zu bündeln.
Das Fraunhofer FOKUS eIdentity-Labor verfolgt daher das Ziel die sichere Kommunikation zwischen Verwaltung, Privatwirtschaft und Bürgern zu fördern und gemeinsam mit Partnern anschauliche Szenarien zu realisieren, die die Einsatzmöglichkeiten in eGovernment, eBusiness, Telekommunikation und Mobilität zu zeigen.

Das Fraunhofer FOKUS eIdentity-Labor versteht sich daher als Plattform um

- die Interoperabilität verschiedener IdM-Ansätze zu evaluieren,
- das Bewusstsein für IdM durch anschauliche Szenarien zu fördern und
- gemeinsame Projekte mit Partnern gezielt durchführen zu können.

Worum geht es?
Alle IT-Systeme mit nicht-öffentlichen bzw. kommerziellen Inhalten benötigen einen funktionierenden Zugriffsschutz, der ohne zuverlässige Identifikation und Authentisierung des Benutzers nicht möglich ist. In der Welt des Internets hat der Nutzer der elektronischen Dienstleistung eine zunehmende Anzahl an unterschiedlichen digitalen Identitäten, die er verwalten muss. Um diesem Wirrwarr an unterschiedlichen Authentifizierungslösungen entgegenzuwirken gibt es Ansätze wie das Single Sign-On, die „Föderation“ oder in den letzten Jahren auch verstärkt Ansätze des nutzerzentrierten Identitätsmanagements. Bei all diesen Ansätzen geht es zunehmend um Themen der Interoperabilität, da hier unterschiedliche, teils monolithische Ansätze und Insellösungen miteinander vernetzt werden müssen.

Was resultiert daraus?
Es besteht die Notwendigkeit zwischen Identitäten Interoperabilität herzustellen. Interoperabilität zwischen den unterschiedlichen Ansätzen und Technologien wird in den letzten Jahren durch die zunehmende Elektronisierung der Prozesse und Dienstleistungen immer wichtiger. Herkömmliche Ansätze wie Single Sign-On und „Föderation“ sind nur bedingt fähig, die derzeitigen Herausforderungen im organisationsübergreifenden Identitätsmanagement bei gleichzeitiger Kontrolle durch Nutzer zu lösen. Der Zwang zu einer Art Identity Metasystem, welches die Insellösungen effektiv und effizient verbindet wird, wächst mit dem steigendem Wunsch des Nutzers Dienstleistungen des eGovernment, eBusiness oder eHealth online sicher und einfach wahrzunehmen.

In allen Bereichen der digitalen Identität stellt sich alsbald die Frage der Interoperabilität:

- technisch – um verschiedene Verfahren und Systeme zu verbinden,
- semantisch – um übermittelte Identitätsattribute korrekt zu verstehen und zu nutzen, und
- organisatorisch – um notwendige Vertrauensverhältnisse herzustellen.

Angebot des Fraunhofer FOKUS eIdentity-Labors:

- Erforschung und Entwicklung von Anwendungen und Verfahren zum interoperablen Management und zum Schutz digitaler Identitäten in kommerziellen und hoheitlichen Prozessen
- Bereitstellung einer prozess- und service-orientierten eIdentity-Infrastruktur
- Integration von eIdentity-Technologien und – Lösungen
- Exemplarische Einbindung digitaler Identitäten in medienbruchfreie Prozesse
- Demonstration ausgewählter Prozesse für die Sicherung digitaler Identitäten über den gesamten Lebenszyklus

Themenschwerpunkte des Fraunhofer FOKUS eIdentity-Labors:

eGovernment/ eBusiness:

- Nutzerzentriertes Identity Management
- elektronische Identitätsdokumente
- Architektur, Interoperabilität, Geschäftsprozesse

Telekommunikation:

- Identitäten in Telekommunikationsszenarien
- Smartcard als Identitätsspeicher
- Anbindung an nutzerzentrische IDM Lösungen

Mobilität:

- Fahrzeugidentitäten
- Sicherheit für die Kommunikation in Fahrzeugnetzen

Kontakt und Ansprechpartner:
Jens Fromm
Tel + 49 (0)30 3463 7167
Jens.Fromm@fokus.fraunhofer.de
www.eIdentitylab.org

Liste der Referenten und Moderatoren

Staatssekretär Hans Bernhard Beus
Bundesministerium des Innern
Referat IT 4
Alt-Moabit 101 d
10559 Berlin
Gundula.Heinen@bmi.bund.de

Dr. Matthias Büger
Vice President
Deutsche Bank AG
60262 Frankfurt
matthias.bueger@db.com

Prof. Dr.-Ing. Jörg Eberspächer
Technische Universität München
Lehrstuhl für Kommunikationsnetze
Arcisstr. 21
80290 München
joerg.eberspaecher@tum.de

Anton Hanfstengl
Stadt München
Kreisverwaltungsreferat
Bürgerbüro-München
Ruppertstr.19
80337 München
anton.hanfstengl@muenchen.de

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

Dr. Jürgen Kaack
Geschäftsführer
FN-Dienste GmbH
Karlstr. 13
88045 Friedrichshafen
kaack@fn-dienste.de

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

Dipl.-Math. Klaus-Dieter Wolfenstetter
Deutsche Telekom AG Laboratories
Innovation Management
Ernst-Reuter-Platz 7
10587 Berlin
k.wolfenstetter@telekom.de

Nils Zeino-Mahmalat
Stabsstellenleiter Kompetenzcenter EFM
Verkehrsverbund Rhein-Ruhr AöR
Augustastr.1
45879 Gelsenkirchen
zeino@vrr.de

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