

## Positionspapier

### Empfehlungen der ITK-Wirtschaft zur Einführung des Elektronischen Personalausweises

August 2009  
Seite 1

#### Einleitung

Die Einführung und Nutzung möglichst geprüfter, elektronischer Identitäten ist eine wesentliche Voraussetzung, um zukünftig Transaktionen im Internet sicherer und damit vertrauenswürdiger zu gestalten. Der elektronische Personalausweis wird ab 1. November 2010 an die Bundesbürger ausgegeben. Mit seiner optional frei zu schaltenden eID-Funktion steht in Deutschland erstmalig eine flächendeckende, einheitliche elektronische Identitätsfunktion auf Basis eines behördlichen Ausweisdokuments zur Verfügung.

BITKOM hat die Aktivitäten im Vorfeld der Einführung des Elektronischen Personalausweises seit Ende 2006 intensiv durch die Arbeit seiner Gremien (insb. des Fachausschusses „Elektronische Identitäten“) begleitet. Zu erwähnen seien hier die Workshops, die BITKOM in den Jahren 2007 und 2008 mit großer Beteiligung seitens Anwenderbranchen und ITK-Sektor durchgeführt hat. Auch für 2009 ist ein weiterer Workshop in Vorbereitung.

Die Einführung des Elektronischen Personalausweises steht in Deutschland in weniger als 15 Monaten bevor. Um den Einsatz der vorgesehenen eID-Funktion des Elektronischen Personalausweises zu testen und wichtige Erkenntnisse für die spätere Einführung und den Betrieb zu sammeln, sind die nun anstehenden Anwendungstests von besonderer Bedeutung. Der Fachausschuss „Elektronische Identitäten“ beabsichtigt, mit diesem Positionspapier Empfehlungen bereitzustellen und kritische Faktoren zu benennen, die für den Erfolg des Personalausweises als Träger einer elektronischen Identitätsfunktion von entscheidender Bedeutung sein werden. Zielgruppe für diese Publikation sind sowohl die verantwortlichen Ministerien und Behörden als auch die Branchen, die den elektronischen Personalausweis zukünftig in ihren Geschäftsprozessen einsetzen werden.

Im Rahmen der Diskussion der kritischen Erfolgsfaktoren haben sich die Schwerpunktthemen Ergonomie, Interoperabilität, Supportprozesse und Zertifikatsdienstleistungen herausgebildet. Diese sollen in den nachfolgenden Ausführungen im Besonderen beleuchtet werden.

Als weiteres Strukturierungsmodell hat sich in den vorhergehenden Workshops und Dokumentationen des BITKOM die Einteilung der Anforderungen nach bestimmten Kriterien bewährt. Diese werden nachfolgend – so anwendbar – zur Strukturierung der Empfehlungen verwendet. Im Einzelnen sind das: Geschäftsmodell - FIN, Technische Lösung. TEC, Gesetze, Bestimmungen und Standards - IUS, Organisation und Prozesse - ORG, Ergonomie und Benutzung - USE, Politik und Gesellschaft - POL.

Bundesverband  
Informationswirtschaft,  
Telekommunikation und  
neue Medien e.V.

Albrechtstraße 10 A  
10117 Berlin-Mitte  
Tel. +49. 30. 27576-0  
Fax +49. 30. 27576-400  
bitkom@bitkom.org  
www.bitkom.org

#### Ansprechpartner

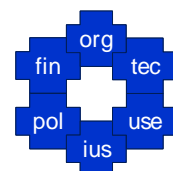
Lutz Neugebauer  
Bereichsleiter Sicherheit  
Tel. +49. 30. 27576-242  
Fax +49. 30. 27576-409  
l.neugebauer@bitkom.org

#### Präsident

Prof. Dr. Dr. h. c. mult.  
August-Wilhelm Scheer

#### Hauptgeschäftsführer

Dr. Bernhard Rohleder



## **Positionspapier**

Einführung des Elektronischen Personalausweis

Seite 2

### **1 Ergonomie des Elektronischen Personalausweises in der Benutzung mit dem Bürgerclient**

***Die Benutzerführung muss so einfach, schnell, sicher und komfortabel wie möglich sein!***

- Entscheidende Punkte für eine breite Akzeptanz des Personalausweises liegen in einer einfachen, verständlichen und multilingualen Benutzerführung. Hierbei sind auch körperliche Einschränkungen zu berücksichtigen.
- Die Benutzerführung sollte auf "Bekanntes" zurückgreifen und an bestehenden grafischen Oberflächen orientieren.
- Authentisierung mit dem Elektronischen Personalausweis ist ohne Vorkenntnisse durchzuführen und im Aufwand (Zeit, Eingaben) mit anderen Authentisierungstechniken mindestens vergleichbar.

#### **TEC – Technische Lösung**

- Kleinere Animationen zur Benutzerführung sind vorzusehen, welche einzelne Anwendungsfälle interaktiv lernbar wiedergeben. Auch hier ist das Thema multilingual und Barrierefreiheit zu berücksichtigen.
- Die Nutzung von Kartenlesern muss problemlos möglich sein (Toleranz gegenüber Auflageposition des Elektronischen Personalausweises, er muss nicht ständig festgehalten werden).
- Informationen und Abfragen der eCard-API sind klar strukturiert und aus Sicht der Nutzer vertrauenerweckend.
- Eine Unterstützung mobiler Endgeräte und Handhelds muss unter ergonomischen Gesichtspunkten vorgesehen werden.

#### **IUS – Gesetze, Bestimmungen und Standards**

- Mehrfacheingaben, die nur auf numerischen Eingaben beruhen sind zu vermeiden.
- Der Verifikationsprozess gegenüber Diensteanbietern muss <10sec sein und durch "Warte-Symbole" unterstützt werden.
- Dem Nutzer sind durch die Benutzerführung bei allen Schritten der Authentisierung seine Rechte und Pflichten bekannt und in der Anwendung möglichst sichtbar.
- Der Sicherheitsgewinn ist für den Nutzer transparent.

#### **ORG – Organisation und Prozesse**

- Die Benutzerführung bei Webanwendungen ist selbsterklärend.
- Eine klare Benutzerführung ist besonders im Fehlerfall notwendig.

## Positionspapier

Einführung des Elektronischen Personalausweis

Seite 3

### USE – Ergonomie und Benutzung

- Bei Übergabe in der Meldestelle werden dem Nutzer bereits alle wesentlichen Informationen zur Nutzung des Elektronischen Personalausweises vermittelt (Vorteile der Nutzung, Vorgehensweise bei notwendigen Installationen und beim Einsatz, Angebot von Hilfe).

### POL – Politik und Gesellschaft

- Für den Problemfall sind schnelle, gute und kostenlose/preisgünstige Unterstützungsangebote möglichst über verschiedene Kommunikationskanäle für die Nutzer vorzusehen.
- Diensteanbieter müssen in den Lernprozess der Nutzer eingebunden werden (Gewinnung von Anwendungen, die die Einführung aktiv unterstützen und einen guten Nutzersupport bieten).

## 2 Interoperabilitäts-Anforderungen an den Elektronischen Personalausweis

**„Das reibungslose Zusammenwirken der Komponenten des Elektronischen Personalausweises mit bestehenden Systemen, Prozessen, Standards ist ein entscheidender Erfolgsfaktor und vermindert das Projektrisiko für Anwendungsunternehmen.“**

### FIN – Geschäftsmodell

- Die Interoperabilität zwischen eCard-API und bestehenden Systemen der Unternehmen muss gewährleistet sein!

*Die Interoperabilität zwischen eCard-API mit anderen bereits existierenden Standards und unternehmenskritischen Systemkomponenten muss gewährleistet sein, um eine positive Entscheidungsbereitschaft beim Top Management für den Einsatz des Elektronischen Personalausweises herbeizuführen. Eine Adaption des Elektronischen Personalausweises in bestehende Geschäftsmodelle bedeutet, dass bereits getätigte Investitionen in die Infrastruktur berücksichtigt werden müssen (Investitionsschutz). Insbesondere im Hinblick auf die momentane wirtschaftliche Lage sind hohe Integrationskosten zu vermeiden, die durch fehlende Interoperabilität entstehen können.*

### TEC – Technische Lösung

- Internationale Standards abgleichen!

*Um die Technologieabhängigkeiten zu vermeiden, muss der Elektronische Personalausweis und die erforderliche Infrastruktur für die eID-Funktion (z.B. Bürgerclientsoftware) einen hohen Grad an Interoperabilität mit anderen internationalen Standards gewährleisten (wie z. B. SAML, WS\* etc.) Die Interoperabilität der verwendeten Soft- und Hardwarekomponenten mit den globalen/europäischen Standards für zukunftssicheren Betrieb insbesondere in Europa (STORK Projekt) ist sicherzustellen.*

## Positionspapier

Einführung des Elektronischen Personalausweis

Seite 4

- eID unter dem Gesichtspunkt „offener Standard“ muss internationale Aspekte berücksichtigen und die möglichen Konsequenzen auf die Zusammenarbeit mit der EU noch näher untersucht werden.
- Interoperabilität mit Standardbetriebssystemkomponenten, Wartungs- und Support-Prozessen müssen definiert sein.
- Es müssen technische Ersatzlösungen bei Sperrung (Verlust, Missbrauch) des Personalausweises angeboten werden!

*Die Bereitstellung von hochsicheren, temporären "Ersatzdiensten" im Falle eines Verlustes des elektronischen Personalausweises muss vorgesehen werden – Dazu gehört eine Interoperabilität zwischen Security Token Services und eID-Diensten mit Revisionssicherheit.*

- Eine Beschreibung der eCard-API und wie Unternehmen diese in ihre Anwendungen integrieren können, muss offen zugänglich sein!

### IUS – Gesetze, Bestimmungen und Standards

- Lizenzfallen müssen vermieden werden!

*Das Lizenzierungsmodell der eingesetzten Softwarekomponenten und die damit verbundenen Nutzungsrechte / Regelungen zum Geistigen Eigentum (z. B. ISO 24727, eCard Middleware) muss transparent und eindeutig für die Unternehmen geregelt sein, um Lizenzfallen und die damit verbundenen unternehmerischen Risiken zu vermeiden.*

### ORG – Organisation und Prozesse

- Eine einfache Integration in bestehende Entwicklungs- und Anwendungsumgebungen muss sichergestellt werden!

*Dazu gehört insbesondere die Interoperabilität mit Bestandsanwendungen. Auch sollten die spezifischen Anforderungen bestimmter Branchen weiterhin berücksichtigt werden. Beispielsweise die Integration der eCard-Middleware in bestehende Prozesse der Bankensysteme.*

### USE – Ergonomie und Benutzung

- Eine einfache und einheitliche Benutzerführung sollte auch über verschiedene Systeme hinweg realisiert sein!

*Eine konsistente und benutzerfreundliche Anwenderführung über alle Betriebssysteme hinweg muss sichergestellt sein. Die Umstellung bzw. Ergänzung der bisherig genutzten Authentisierungssysteme (Username und Passwort) muss für jeden Nutzer einfach nachvollziehbar sein. Für die Anwender muss die einfache Nutzung mit ihren vorhandenen PCs gegeben sein – d.h. die Unterstützung mit den meistverbreiteten Betriebssysteme und Anwendungen muss gewährleistet sein.*

## Positionspapier

Einführung des Elektronischen Personalausweis

Seite 5

### POL – Politik und Gesellschaft

- Kommunikation zum Thema Interoperabilität mit Unternehmen verstärkt aufbauen!

*Dazu gehört die Aufklärung über die Standards, die beim elektronischen Personalausweis verwendet werden. Hier muss aufgezeigt werden, wie der Elektronische Personalausweis in heterogenen Umgebungen genutzt werden kann. Weiterhin sollte erläutert werden, wie die verschiedenen Komponenten/Standards zusammenarbeiten und welche höhere Sicherheit ergibt sich daraus ergibt.*

### 3 Support-Prozesse für die Anwendung des elektronischen Personalausweises

**„Support-Prozesse müssen schlank, kostengünstig und mit der vorhandenen Infrastruktur kompatibel sein!“**

### FIN – Geschäftsmodell

- Es müssen wirtschaftliche Anreize für Nutzer und private Projektpartner geschaffen werden!

*Als wesentlicher Erfolgsfaktor ist die Geschwindigkeit zu sehen, mit der eine "kritische Masse" an Benutzern der eID-Funktion mobilisiert werden kann. Für die Bürger wird die – möglichst kostenlose - Bereitstellung eines "Bürgerclient-Paket" einschließlich Leser ein wesentlicher Motivationsfaktor sein.*

*Auch müssen Anreize für Endgerätehersteller geschaffen werden, um Leser und SW in Neugeräte zu integrieren. Für die Akzeptanz insbesondere bei nicht-technisch versierten Nutzern haben vorinstallierte und vorkonfigurierte Systeme erhebliche Vorteile.*

- Der Handel muss in die Vermarktung/Verbreitung eines Bürgerclient-Paketes einbezogen werden!

*Bei dem Kauf von neuen Endgeräten sollte die Option zum zusätzlichen Erwerb eines Bürgerclientpakets immer vorhanden sein. Bestenfalls beraten die Verkäufer des Einzelhandels die jeweiligen Kunden in dieser Richtung.*

- Gezielte Anschubinvestitionen unterstützen die schnelle Verbreitung von Diensten!

*Mit der finanziellen und organisatorischen Unterstützung der Anwendertests ist die Bundesregierung auf dem richtigen Weg. Um die Henne-Ei-Problematik und die hierbei vorliegenden Geschäftsrisiken für zukünftige Diensteanbieter zu minimieren, sollte der Staat hier den Weg weiter gehen und finanzielle Unterstützung für weitere Dienste vorsehen.*

- Effiziente Prozesse und transparente Gebührenstrukturen für Anwenderbranchen schaffen!

*Die Preisgestaltung aller oben genannten Komponenten ist zu verproben bzw. abzustimmen und ggf. zielgruppengerecht zu staffeln, ohne dabei die*

## Positionspapier

Einführung des Elektronischen Personalausweis

Seite 6

*Markttransparenz zu gefährden. Die notwendige Einbeziehung verschiedener Institutionen (BVA, Zertifikatsdienstleister, etc.) darf nicht dazu führen, dass jeweils eigene Gebühren für Leistungen erhoben werden, die als kumulierte Kosten die Anwendung des Elektronischen Personalausweises unattraktiv machen.*

- Minimierung der Mehrkosten beim gleichzeitigen Angebot unterschiedlicher Authentisierungsmethoden ermöglichen!

*Da die Anwendungsanbieter für Einführung und Unterstützung des Elektronischen Personalausweises zunächst einen „dualen Betrieb“ (d.h. mit Rückfallebene ohne eID-Funktion) vorsehen müssen, sollten dringend Maßnahmen überlegt werden, die die Mehrbelastungen der Unternehmen hieraus minimieren.*

- Der elektronische Personalausweis muss übergreifende Angebote mehrerer Dienstleister unterstützen können!

*Zukünftig werden auch die Angebote vernetzter Dienstleister durch den elektronischen Personalausweis unterstützt werden müssen. Hierzu sind entsprechende Konzepte, insbesondere im Management der Berechtigungszertifikate, zu überlegen.*

### TEC – Technische Lösung

- Technische Lösungen müssen das gleichzeitige Angebot unterschiedlicher Authentisierungsmethoden ermöglichen!

*Für den elektronischen Personalausweis sind technische Lösungen bereitzustellen, die im Parallelbetrieb zu bestehenden Authentisierungsmechanismen funktionieren und die Integration in bestehende Lösungen erleichtern.*

- Die Strategie zur Ausgabe von Kartenlesern muss mit anderen Großprojekten abgeglichen werden!

*Hierfür muss ein Abgleich mit anderen Kartenherausgebern, Herstellern (Gesundheitskarte, Signaturkarten, Kreditwirtschaft etc.) und den zuständigen Verbänden vorgenommen werden, um die Kompatibilität sicher zu stellen.*

- eID-Funktion "Identitätsnachweis" muss sicher ("nachweisbar") mit einer Internet-Session bzw. Transaktion verbunden werden!
- Proprietäre Lösungsansätze müssen in jedem Fall vermieden werden!

### IUS – Gesetze, Bestimmungen und Standards

- Haftungsfragen bei der Benutzung des Personalausweises müssen für den Bürger verständlich geklärt und dokumentiert vorliegen!

*Haftungsfragen, die sich insbesondere bei Verlust, Missbrauch und Sperrung des Personalausweises ergeben, sind so gelöst, dass der Sachverhalt für den Bürger einfach verständlich und akzeptabel vorliegt. Das gilt auch für Transaktionen aus dem Ausland.*

## Positionspapier

Einführung des Elektronischen Personalausweis

Seite 7

- Ein Sperrservices muss 24/7 bereitgestellt werden!

*Die jederzeit vollziehbare Sperrung ist für einige Anwendungen (rechtlich) notwendige Voraussetzung dafür, dass der Elektronische Personalausweis als Authentisierungsinstrument genutzt werden kann.*

- Die Einsatzmöglichkeiten des Personalausweises sollten nicht durch zu strenge Gesetze beschränkt werden!

*Es muss ein gesetzlicher Rahmen geschaffen werden, der häufige Nutzung des Elektronischen Personalausweises begünstigt ("pragmatisches Risiko-Management mittels Anscheinsbeweis"). Es sollten daher keine zu hohen Hürden eingezogen werden – z. B. QES für einfachste Transaktionen. Notwendig ist ein Abgleich der rechtlichen Anforderungen mit den aktuellen Regelungen aus dem Versicherungs-, Banken- und Gesundheitsumfeld zur Nutzung von eID Karten.*

### ORG – Organisation und Prozesse

- Anwendungsanbieter benötigen einfache Prozesse zur Integration des Personalausweises in die eigenen Anwendungen!

*Von der Einbindung des eID Servers über den Erhalt von Berechtigungszertifikaten bis zum eigentlichen Betrieb: wünschenswert ist genau eine Anlaufstelle statt drei bis vier.*

- eID-Funktion und QES müssen organisatorisch miteinander verbunden sein!

*Der Prozess ist definiert, wie die Qualifizierte elektronische Signatur mit der eID-Funktion sicher verbunden werden kann. Bei Sperrung des Elektronischen Personalausweises muss auch eine Sperrung der QES erfolgen. Hier sind insbesondere Sperrinformationen an den zuständigen ZDA weiterzuleiten.*

- Das Verfahren, wie die eID-Funktion mit der Transaktion sicher verbunden werden kann, ist geklärt (auch technisch: Transaktionssicherheit, Session-Management).

### USE – Ergonomie und Benutzung

- Eine Telefonnummer für alle Fragen einrichten!

*Der Bürger findet unter einer Telefonnummer / Webseite alle Hilfestellungen zum Elektronischen Personalausweis: PIN vergessen, vorübergehende/vollkommene Sperrung des Elektronischen Personalausweises und optional der QES, Installation des Bürgerclients (Leser und SW), Support Hotline.*

- Parallele Nutzung von eID und QES erproben!

*Die parallele Nutzung von eID-Funktion und qualifizierter elektronischer Signatur sollte im Anwendungstest erprobt werden. Die Spezifikationen hierzu liegen allerdings noch nicht vor, diese sollten zeitnah den Anwendungstestteilnehmern zur Verfügung gestellt werden.*

## Positionspapier

Einführung des Elektronischen Personalausweis

Seite 8

### POL – Politik und Gesellschaft

- Anwendungsfall eGovernment muss ausgebaut werden!

*Erklärungen der Regierung (Bund und Länder) sowie kommunaler Vertretungen, welche Verwaltungsbereiche künftig den Elektronischen Personalausweis (QES bzw. Authentifizierung) nutzen werden, können helfen das Vertrauen zu erhöhen und die kritische Masse schneller zu erreichen.*

- Dem altersbedingten, digitalen Graben in der Bevölkerung entgegenwirken!

*Es sollten spezielle Angebote und Services für die Nutzung durch Senioren vorgesehen werden, um Vorurteilen entgegenzuwirken (Vermarktungskonzept).*

## 4 Zertifikatsdienstleistungen für den elektronischen Personalausweis

**„Die Prozesse zur Bereitstellung von Berechtigungszertifikaten sollen einfach und effizient sein. Die Ausstellung erfolgt kostengünstig und kostendeckend.“**

### FIN – Geschäftsmodell

- Zertifikatsdienstleister müssen möglichst schnell und umfassend in die Prozesse zur Vergabe der Berechtigungszertifikate eingebunden werden!

*Die Integration der Diensteanbieter in das Zertifizierungssystem des BSI/BVA hat das Ziel, eine umfassende Sicherheit und nachvollziehbare Abläufe zu schaffen. Weiterhin ist ein transparentes und veröffentlichtes Kostenmanagement notwendig.*

- Das Organisationsmodell für die Vergabe von Berechtigungszertifikaten muss zügig definiert und bekannt gemacht werden. Die Ausgabe der Berechtigungszertifikate muss für die akkreditierten Dienstleister mindestens kostendeckend sein!

*Derzeit ist für Zertifizierungsdiensteanbieter nicht transparent, wie und ob ein Geschäftsmodell für die Ausgabe von Berechtigungszertifikaten etabliert werden kann.*

### TEC – Technische Lösung

- Die Laufzeiten für Berechtigungszertifikate sollten je nach Einsatzzweck risikoorientiert und (zumindest in einem Übergangszeitraum) flexibel festgelegt werden.

*Die bislang gesetzlich festgelegte, nur wenige Tage dauernde Gültigkeit eines Berechtigungszertifikats sollte überdacht werden. Für die Altersverifikation am Zigarettensautomaten müssten beispielsweise alle Automaten vernetzt werden, um dies zu ermöglichen. Für weniger risikoreiche Anwendungen sollte daher ein flexiblerer Ansatz gewählt werden, der wesentlich längere Laufzeiten zulässt.*

## Positionspapier

Einführung des Elektronischen Personalausweis

Seite 9

*Für QES-Kartenleser) wäre ein regelmäßiges Zertifikatsupdate nicht praktikabel. Hier würde sich sogar eine Bauartzulassung anbieten.*

### ORG – Organisation und Prozesse

- Entscheidungsprozesse sind für die Unternehmen transparent und nachvollziehbar. Ein möglichst vollständiges Service-Konzept ist vorhanden und verlangt vom Unternehmen nur organisatorische und keine technischen Entscheidungen.

### USE – Ergonomie und Benutzung

- Als Philosophie der Interaktion mit dem Bürger und Unternehmen, die Berechtigungszertifikate benötigen, sollte die Idee einer einzigen Anlaufstelle (Single Point of Contact) dienen.

### POL – Politik und Gesellschaft

- Subventionierte Komfortleser müssen an der Gesamtförderung einen relevanten Anteil haben.

### **"Die Nutzung des Personalausweises zum Signieren muss nicht nur sicher, sondern auch einfach sein!"**

- Die optionale QES soll zukünftig durchgängig bei allen Behörden nutzbar sein!

*Die QES kann bei allen Behörden verwendet werden, Aussagen auf Behördenwebseiten wie: "Die Stadt Utopia weist hiermit darauf hin, das sie noch keinen Zugang gem. VwVfG hat" dürfen von Firmen und Bürgern nicht mehr wahrgenommen werden können.*

- Sperrung von Personalausweis und QES erfolgen automatisch parallel!

Bei einer Sperrung des Elektronischen Personalausweises wird diese für QES-Zertifikate übernommen und bedürfen keiner separaten Sperrung durch den Inhaber. Ggf. muss eine Ermächtigung für ZDA zur Auswertung von Sperrlisten und darauf folgende Sperrung des QES-Zertifikats rechtlich umgesetzt werden, falls technisch keine Lösung möglich ist.

- In den Kommunikationsmaßnahmen muss eine Nutzenargumentation für die "elektronische Unterschrift" erfolgen!

Insbesondere sollten die Vorteile für Bürger betont werden, die QES in Anwendungsszenarien der öffentlichen Verwaltung zu verwenden. Es ist zu prüfen und abzuwägen, ob es nicht eventuell anwenderfreundlicher und auch kostengünstiger wäre, die QES-Zertifikate in den ePA-Auslieferungsstandard mit aufzunehmen, wenn eine ePA-Online-Verwendbarkeit vom Bürger gewählt wird.