eGovernment-Symposium 2010

ifib
Institut für Informationsmanagement Bremen GmbH

Authentisierung und Autorisierung im E-Government

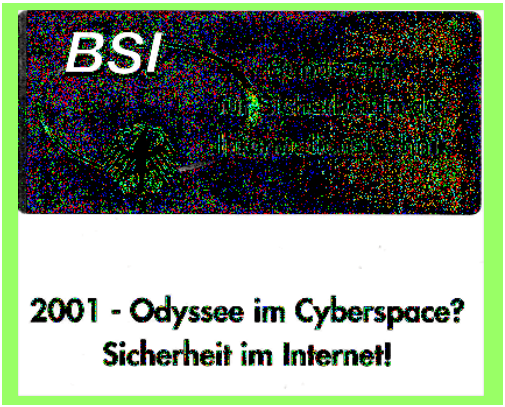
Zeit für einen Paradigmenwechsel

Prof. Dr. Herbert Kubicek
Institut für Informationsmanagement Bremen (ifib)/
Universität Bremen

eGovernment-Symposium 2010

ifib
Institut für Informationsmanagement Bremen GmbH

Übersicht:



Herbert Kubicek:
Die digitale Signatur **zwischen** Bürger und Verwaltung – Erleichterung oder Erschwernis?
7. Deutscher IT-Sicherheitskongreß des BSI, S. 11-22

In vielen Sprachen ist der Begriff „Odyssee“ zu einem Synonym für lange Irrfahrten geworden. Aber wer „irrt“ in diesem Fall ?

Ende des 24 Gesangs: „An zwei aufeinander folgenden Abenden erzählt Odysseus den Phaiaken und ihrem König Alkinoos seine Geschichte. Anschließend beschenken sie ihn reich und bringen ihn heim nach Ithaka

eGovernment-Symposium 2010 **1. Aus Erfahrungen mit elektron. Signaturen lernen**

Die digitale Signatur **zwischen** Bürger und Verwaltung – Erleichterung oder Erschwernis?

Aufwändiger Beschaffungsprozess
- Registrierung,
- teures Jahres-Abo
- Erwerb und Installation Kartenleser
- Erwerb und Installation Client-Software

+

komplizierte Nutzung
(Starten des Clients, mehrere zusätzl. Dialogschritte)

-> **für ungewissen Nutzen** (was kann man damit machen, was sonst nicht geht ?)

-> **in nicht nachvollziehbarer und daher nicht unbedingt vertrauensbildender Art und Weise**

ifib
Institut für Informationsmanagement Bremen GmbH

Die digitale Signatur **zwischen** Bürger und Verwaltung – Erleichterung oder Erschwernis?

Löst man die Probleme der digitalen Signatur durch Verkürzung der Registrierungs- und/oder der Dialogschritte beim Signieren?

ODER

Ist es wie beim Starten des Auto-Motors, dass man nicht die Kurbel sicherer und einfacher machen muss, sondern....

eGovernment-Symposium 2010 **1. Aus Erfahrungen mit elektron. Signaturen lernen**

ifib
Institut für Informationsmanagement Bremen GmbH

Die digitale Signatur **zwischen** Bürger und Verwaltung – Erleichterung oder Erschwernis?

Bisher hatte ich aber keine Anhaltspunkte, wie das **alternative Paradigma*** aussehen könnte.

Durch ein vergleichendes Forschungsprojekt habe ich nun Anhaltspunkte gefunden: Der Schlüssel liegt in einer **Verlagerung der Schwerpunkte** der Maßnahmen für mehr Sicherheit im E-Government von der **Authentisierung** zur **Autorisierung**.

*) Das Wort Paradigma ... bedeutet „Beispiel“, „Vorbild“, „Muster“ oder „Abgrenzung“, „Vorurteil“; in allgemeinerer Form auch „Weltsicht“ oder „Weltanschauung“.

2. Das herrschende eID-Paradigma

Viele Bürgerinnen und Bürger informieren sich im Internet, **verzichten** aber aufgrund von Sicherheitsbedenken auf Online-Transaktionen.

Sicherheitsbedenken betreffen insbesondere die Angst vor

- Phishing / Identity Theft,
- sowie im E-Commerce vor mangelhafter Lieferung / Reklamationen etc.

Vor Identitätsdiebstahl soll eine **elektronische Identität** und eine **stärkere Authentisierung** schützen.

Im E-Government können bisher viele Dienstleistungen nicht komplett online angeboten werden, weil eine sichere Authentisierung fehlt.

2. Das herrschende eID-Paradigma

Authentisierung ist der **Nachweis** der Identität einer Person
(Autorisierung ist die Prüfung einer Berechtigung dieser Person)

Authentisierungsverfahren im E-Government und E-Commerce:

- Benutzername und Password
- Benutzername, Password und TAN (OTP)

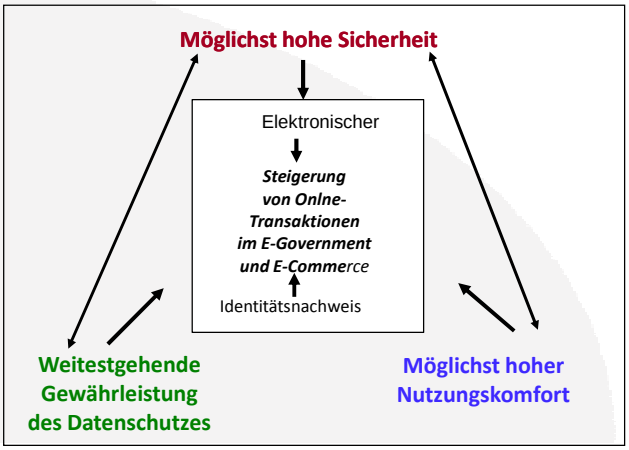
- ID-Attribute und Zertifikat
  insbes. Name, Vorname, Geb.Datum, PKZ aus Melderegister
  - Software-Zertifikat
  - Chip
    - ohne PIN Schutz
    - ***mit PIN Schutz*** ← **Stärkste (= sicherste) Authentisierung**

Starke Authentisierung beruht auf Besitz und Wissen

Herbert Kubicek: Zeit für einen Paradigmenwechsel

eID in Europa: Manchester Ministerial Conference 2005:

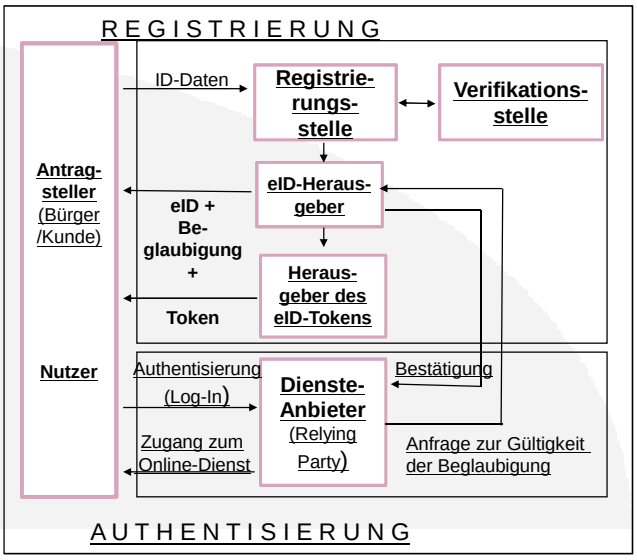
„By 2010 European citizens and businesses shall be able to benefit from **secure** means of electronic identification that maximise **user convenience** while respecting **data protection** regulations. Such means shall be made available under the **responsibility of the Member States** but recognised across the EU.“



eID in Europa

- EU Kommission fördert einen Large Scale Pilot zur Interoperabilität der unterschiedlichen nationalen eIDs, an dem mehr als 11 Mitgliedstaaten teilnehmen -> https://www.eid-stork.eu
- Föderativer Ansatz – Network of Trust: Wechselseitige Anerkennung:

4 Authentication Assurance Level



2. Das herrschende eID-Paradigma

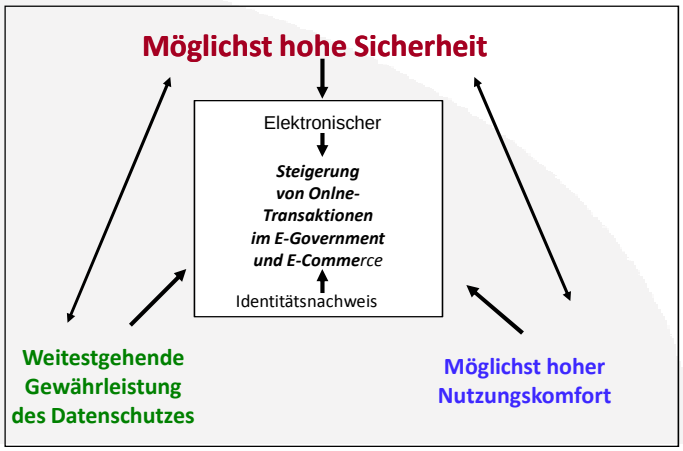
Je höher der Authentication Assurance Level

-> desto größer die Sicherheit von Transaktionen und Nutzern im Internet

-> desto größer ihr Vertrauen in diese Sicherheit

-> desto größer die Nutzerzahl und Nutzungsintensität bei E-Government und E-Commerce

Die optimistische These



Herbert Kubicek: Zeit für einen Paradigmenwechsel

3. Ein vergleichendes Forschungsprojekt

Neben der technischen Sicherheitsdiskussion

gibt es - zumindest in einigen Ländern – eine kontroverse öffentliche Diskussion über Folgen für die staatliche Überwachung und den Datenschutz

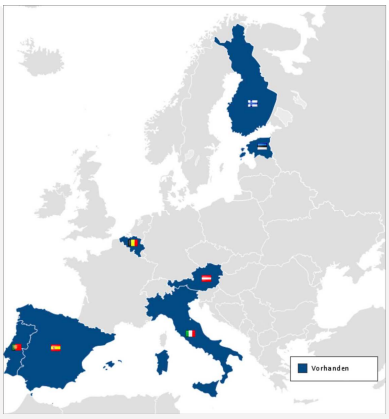
und darüber, wie die Identitäten in den sozialen Netzwerken gewählt werden und wie sie wirken,

bis hin zur philosophischen Fragen, was überhaupt eine Identität ist

12

Herbert Kubicek: Zeit für einen Paradigmenwechsel

3. Ein vergleichendes Forschungsprojekt



Länder mit eID-Karten 2007

Einige Länder haben schon früher eine nationale eID eingeführt:

- Finnland 1999
- Estland 2002
- Schweden 2003
- Dänemark 2003
- Belgien 2004
- Österreich 2004
- Spanien 2006.

Daher können die dortigen Erfahrungen untersucht und Schlussfolgerungen für den neuen deutschen Personalsausweis gezogen werden, der seit dem 1. 11. 2010 ausgegeben wird.

3. Ein vergleichendes Forschungsprojekt

Systemic Change of the Identification of Citizens by Government

Electronic Identity Management as a Complex Technical Innovation and its Organisational, Legal and Cultural Matching in Selected European Countries

Juli 2007 – April 2010

Gefördert durch VolkswagenStiftung Wir stiften Wissen

in Kooperation mit

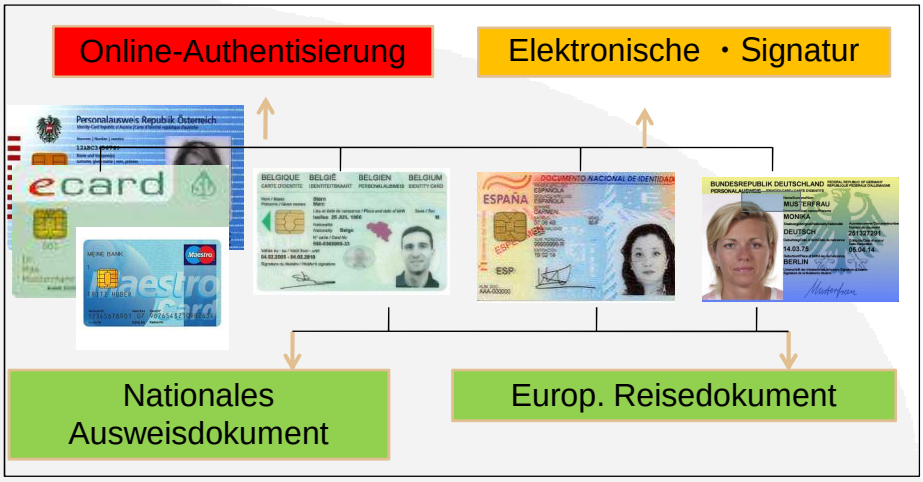
smit IBBT

Studies on Media, Information and Telecommunication at the Vrije Universiteit Brussel, part of IBBT, the Interdisciplinary Institute for Broadband Technology.

ITA INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG ÖAW

Institut Européen d'Administration Publique
European Institute of Public Administration

Funktionale und technische Unterschiede



Unterschiede zwischen den nationalen eID-Systemen		AUT	BEL	GER	ESP
carrier card	national ID-card	Nein	X	X	X
card character	obligatory / age	Geburt	> 12	>16	>14
card function	authentication (online)	Opt in	Opt in	Opt in	X
	authentication (visual)	(X)	X	X	X
	e-signature	X	Opt out	Opt in	X
eID attribute	national register number	–	X	–	X
	visual data: o address o owners photograph	Dep. On card	– X	X X	X X
	contact/contactless chip	contact	contact	RFID	contact
	PIN-protected data	X	X	X	X
	Biometric face Digital fingerprints	– –	– –	X Opt in	X X

3. Ein vergleichendes Forschungsprojekt

Online-Authentisierung

Elektronische Signatur

Estland | Finnland | Schweden | Dänemark

Digital Signatur

NEM ID

Nationales Ausweis-dokument

Europäisches Reisedokument

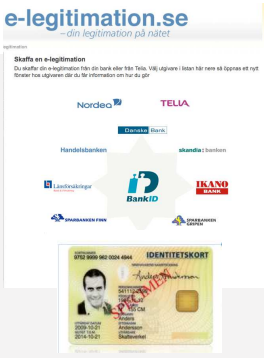
Estland

eID + eSig wird in Lizenz von einem Konsortium aus Banken und Telekom-Unternehmen auf dem PA implementiert

Finnland

Nachdem die eID auf dem PA nicht nachgefragt wurde, wurde das PIN/TAN Verfahren der Banken über ein gemeinsames Portal auch für E-Government akzeptiert.

Schweden



eID in Lizenz von Banken heraus-gegeben, als SW-Zertifikat (99%) oder auf Bankkarte (1%)

Dänemark

Digital Signatur

NEM ID

Kein PA, Digitale Signatur für E-Gov (OCES) als SW- Zertifikat, seit 2010 mit eID der Banken NET ID fusioniert zur NEM ID, von Banken in Lizenz heraus-gegeben, immer noch SW-Zertifikat

3. Ein vergleichendes Forschungsprojekt

Die Systeme weisen ein hohes Maß an **Pfadabhängigkeit** in organisatorischer Hinsicht auf.

Das heißt sie sind tief in den nationalen Institutionen und Traditionen verwurzelt

JORDI PLAY

Las comisarías de Barcelona que expiden el nuevo DNI disponen de un sistema digital para tomar las huellas

Aktivierung (Opt in) und Nutzung bei elektron. Steuererklärung im Vergleich

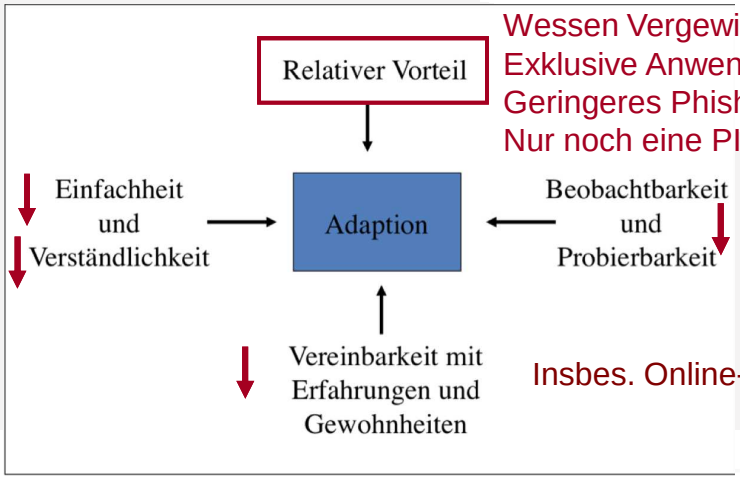
2009	**BE** BelPIC	**ES** DNIe	**AT** Bürger-karte	**DK** OCES	**FI** FINEID	**SE** Bank ID u.a.	**EE** ID-card
Nutzung elektron. Steuer-erklärung (% aller Erklärungen)	56%	21%	25,7%	87%	Keine Angaben	53%	87%
eID Nutzung (% der elektron. Erklärungen)	14,2%	0,2%	1,0%	18,8%	Ge-schätzt 1%	24,4%	ca. 14%
Rangplatz Nutzung 2009	**3**	**7**	**5**	**2**	**5**	**1**	**3**
Rangplatz aktivierte eIDs	1	3	7	5	6	4	2
Stärke des Verfahrens Rang Grad	1 (4)	1 (4)	1 (4)	8 (2)	1 (4)	7 (3)	1 (4)

Anteile unterschiedlicher Authentisierungsverfahren bei der elektronischen Steuererklärung

Authentisierungs-verfahren	Stärke des Ver-fahrens	BE	AT	ES	DK	FI	SE	EE
eID-Card	4	20%*	1%	1%		1%	2%	14%
SW-Zertifikat	3			99%	19%		22,5%	
Papier-basiert OTP/ Code	2-3	80%			81%	99%	37,3%	Ca. 80%
Username +Password	1		99%					
Telefon	2						23,2%	
SMS	2						15,1%	

Herbert Kubicek: Zeit für einen Paradigmenwechsel

Erfolgsfaktoren für die Adaption von Produktinnovationen nach Everett Rogers



Für Wen ? /
Wessen Vergewisserung ?
Exklusive Anwendungen ?
Geringeres Phishing-Risiko ?
Nur noch eine PIN?

Insbes. Online-Banking

Herbert Kubicek: Zeit für einen Paradigmenwechsel

6. Argumente für einen Paradigmenwechsel

Schwerpunkt Authentisierung	Schwerpunkt Autorisierung
eID auf nationalem ID-Dokument – „Ein Ausweis für zwei Welten“	Banken haben in den letzten Jahren die Online-Sicherheit nicht beim Log-In, sondern bei den einzelnen Transaktionen verbessert.
Bestimmender Einfluss nationaler IT-Sicherheitsbehörden – ohne Beachtung der Kosten	Pragmatisch nach Kosten-Nutzen Abwägungen
Zertifikate / Kryptographie	Von der frei wählbaren über die vorgegebene TAN bis zur mTAN und iTAN
Verkennt den Unterschied zwischen den beiden Welten – Kann das Internet nicht so sicher machen wie die Grenzkontrollen	Die statische eID kann die dynamische TAN nicht ersetzen

eGovernment-Symposium 2010

6. Argumente für einen Paradigmenwechsel

ifib

Die größte Nutzung findet die eID, wo sie
- von Banken (mit)herausgegeben wird und
- beim Online-Banking eingesetzt werden kann

Wenn die E-Government-Akteure die Banken nicht von der eID überzeugen können, sollten sie sich von den Sicherheitslösungen der Banken überzeugen lassen

Deutschland kann versuchen, es wie die Esten zu machen. Wenn das nicht zustande kommt, bleibt als Alternative die Strategie der Finnen

Herbert Kubicek: Zeit für einen Paradigmenwechsel

6. Argumente für einen Paradigmenwechsel

In Estland wird die eID aus dem Melderegister entnommen und auf Antrag zusammen mit einer elektronischen Signatur auf den Personalausweis oder ein Mobiltelefon geladen.

- Sie wird von einem Konsortium aus Banken und einem Telekom-Unternehmen herausgegeben und
- kann beim Online-Banking eingesetzt werden.

Es gibt
- exklusive Anwendungen, insbes. i-voting
- beobachtbare Anwendungen, z.B. im ÖPNV,
- sicherheitsbedingte Vorteile (höheres Limit bei Überweisungen
- alle Komponenten aus einer Hand
- breit angelegte Kampagnen zur Internetsicherheit mit der eID

7. Forschungsbedarf

Das Wort Paradigma ... bedeutet „Beispiel“, „Vorbild“, „Muster“ oder „Abgrenzung“, ***„Vorurteil“***; in allgemeinerer Form auch „Weltsicht“ oder „***Weltanschauung“.***

Daher müssen die hier vorgetragenen Thesen systematisch und gründlich überprüft werden. Durch
- repräsentative Bestimmung, worauf sich die Sicherheits-bedenken unterschiedlicher Bevölkerungsgruppen beziehen,
- systematische Zuordnung von geeigneten Massnahmen zu diesen Risiken
- subjektive Kosten-Nutzenanalysen für unterschiedliche Massnahmen aus der Sicht unterschiedlicher Nutzergruppen für eID und TAN-Verfahren,
- „objektive“ vergleichende Produkttests für eID und TAN-Verfahren,
- u.a. nach den Rogers-Kriterien

8. Aussichten für die eID in Europa

Für die eID auf dem deutschen Personalausweis wage ich die Prognose in Bezug auf Opt-In, Angebote und Nutzung von 50% / 10% / 20%.

Bei der Suisse ID müsste nach meinen Thesen der USB Stick stärker nachgefragt werden als die Karten-Variante.

Zum **Standard** werden beide im jeweiligen Land **nicht** werden.
Dazu sind die Anforderungen von Anwendungen und verschiedenen Nutzergruppen zu unterschiedlich.
Der ePA und die Suisse ID sind für Erst-Registrierungen mit hohen Sicherheitsanforderungen geeignet, aber nicht für wiederkehrende Transaktionen

8. Aussichten für die eID in Europa

Für die eID auf dem deutschen Personalausweis wage ich die Prognose in Bezug auf Opt-In, Angebote und Nutzung von 50% / 10% / 20%.

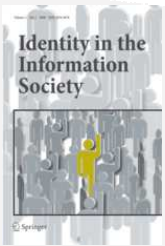
Bei der Suisse ID müsste nach meinen Thesen der USB Stick stärker nachgefragt werden als die Karten-Variante.

Zum Standard werden beide nicht im jeweiligen Land werden.
Dazu sind die Anforderungen von Anwendungen und verschiedenen Nutzergruppen zu unterschiedlich.
Der ePA und die Suisse ID sind für Erstregistrierungen mit hohen Sicherheitsanforderungen geeignet, aber nicht für wiederkehrende Transaktionen.
Daher dürfte national und erst recht international die Vielfalt eher noch größer werden

8. Aussichten für die eID in Europa

Die bestehenden Sicherheitslücken bei Online-Transaktionen im E-Government löst man m. E. nicht, indem man versucht die kartenbezogenen und krytpographiebasierten Verfahren der Authentisierung und Autorisierung noch etwas einfacher zu machen.
Man muss die umständliche Anlasserkurbel durch einfach zu bedienende, fehlerrobuste und gewohnheitskonforme Verfahren ergänzen, wenn der Zündfunke für E-Government überspringen soll.

Zum Nachlesen



Länderfallstudien (in Englisch) sind erschienen
In einer Special Issue des Springer-Online-Journal Identity in the Information Society, Vol. 3 No. 1, Juni 2010

http://www.springer.com/computer/journal/12394

Ausführliche vergleichende Analyse in

Kubicek, Herbert; Noack, Torsten:
Mehr Sicherheit im Internet durch elektronischen Identitätsnachweis?
Der neue Personalausweis im europäischen Vergleich.
Münster: LIT Verlag 2010

Kontakt: kubicek@ifib.de