

# Authentisierungsverfahren für eGovernment-Dienste in Europa

(Extended Abstract<sup>1</sup>)

Detlef Hühnlein<sup>1</sup> · Detlef Houdeau<sup>2</sup>

<sup>1</sup>secunet Security Networks AG  
detlef.huehnlein@secunet.com

<sup>2</sup>Infineon Technologies AG  
detlef.houdeau@infineon.com

## Zusammenfassung

Bei der Umsetzung der verschiedenen eGovernment-Programme in Europa spielen die Verfahren zur Authentisierung und Identifizierung der Bürger eine zentrale Rolle zu. Da es hierfür keine verbindliche EU-weite Regulierung gibt, ist es nicht verwunderlich, dass für die einzelnen eGovernment-Dienste in den verschiedenen Mitgliedsstaaten bisweilen sehr unterschiedliche Verfahren ausgewählt, entwickelt und eingesetzt werden. Der vorliegende Beitrag beleuchtet detailliert die verschiedenen „Dimensionen“ der heute bekannten Authentisierungs- und Identifizierungsverfahren und liefert einen kompakten Überblick über die im eGovernment-Umfeld eingesetzten und geplanten Verfahren in Europa.

## 1 Einleitung

Die Verwaltungsmodernisierung durch elektronische Medien (eGovernment) ist ein erklärtes politisches Ziel auf dem Weg zur Umsetzung der i2010-Strategie<sup>2</sup> der Europäischen Union. Hierbei spielt die Authentisierung und Identifizierung der Bürger bei den angebotenen elektronischen Diensten eine besonders wichtige Rolle. Ausgehend von den nationalen Vorarbeiten zu diesem Thema (siehe z.B. [BSI05]) gewinnt die Europäische Perspektive (vgl. [CEN15264]) zunehmend an Bedeutung. Deshalb liefert der vorliegende Beitrag einen detaillierten Überblick zu den bereits umgesetzten eID-Programmen in den EU-Mitgliedsstaaten (siehe auch [ENISA09a]) und skizziert weitere, bereits öffentlich angekündigte Projekte sowie die flankierend laufenden Aktivitäten zur internationalen Standardisierung (z.B. [CEN15480]) und zur Interoperabilität (z.B. STORK<sup>3</sup>).

---

<sup>1</sup> Das vollständige Papier und eine aktuelle Übersicht über die in Europa eingesetzten Authentisierungsverfahren und eID-Karten findet sich unter <http://www.eID-Lab.de/map> .

<sup>2</sup> Siehe [http://ec.europa.eu/information\\_society/eeurope/i2010/strategy/index\\_en.htm](http://ec.europa.eu/information_society/eeurope/i2010/strategy/index_en.htm) .

<sup>3</sup> Siehe <http://www.eid-stork.eu/> .

Nach diversen Studien von KPMG, E&Y und McKinsey dienen eGovernment-Dienste zur Verringerung der Korruption, Erhöhung der Transparenz, Verbesserung der Serviceleistung und Reduzierung der Verwaltungskosten.

## 2 Authentisierungs- und Identifikationsverfahren

### 2.1 Überblick

Bevor näher auf die verschiedenen „Dimensionen“ der Authentisierung und Identifizierung eingegangen wird, sollen diese beiden zentralen Begriffe näher bestimmt werden.

[Hühn08] definiert die *Authentisierung* als das Aufstellen einer Behauptung über eine partielle Identität, die wiederum als eine bestimmte Untermenge von Attributen einer Entität definiert ist. *Identifizierung* bezeichnet hingegen den Vorgang unter Verwendung von behaupteten oder beobachteten Attributen zu bestimmen, um welche Entität es sich tatsächlich handelt.

Somit könnte ein Bürger nach entsprechender Authentisierung einen personalisierten eGovernment-Dienst unter Verwendung eines Pseudonyms nutzen und nur bei Bedarf eine Identifizierung durchführen, um seine tatsächliche Identität preiszugeben.

Bei den derzeit bekannten Verfahren zur Authentisierung und Identifizierung können folgende „Dimensionen“ unterschieden werden:

- Faktoren
- Protokolle
- Ausweisformate
- Vertrauensmodelle
- Umgang mit Identifikatoren

Auf diese Unterschiede soll in den Abschnitten 2.2 – 2.6 näher eingegangen werden. Darüber hinaus können weitere Unterschiede (z.B. bei der Mandatsverwaltung) existieren.

### 2.2 Faktoren

Bei der Authentisierung kann man grob danach unterscheiden, welche der generell möglichen Faktoren *Wissen*, *Besitz* und *Sein* genutzt werden. Beispielsweise werden in Portugal [PT] ID-Karten (Besitz) ausgegeben, die mit PIN (Wissen) und/oder Fingerabdruck (Sein) aktiviert werden können.

Bzgl. der Identifizierung ist erwähnenswert, dass durch den Einsatz biometrischer Verfahren eine besonders starke Personenbindung erreicht werden kann.

### 2.3 Protokolle

Bei den Authentisierungsprotokollen (siehe [BoMa03]) kann grundsätzlich danach unterschieden werden, ob sich der Bürger und der eGovernment-Dienst ein Geheimnis teilen (*symmetrisch*) oder ein *asymmetrisches* Verfahren zum Einsatz kommt.

Im ersten Fall kann weiterhin danach unterschieden werden, ob das Geheimnis (z.B. ein Passwort) im Zuge der Authentisierung *selbst* oder nur ein *statisch* (z.B. Hashwert des Pass-

worts) oder *dynamisch* (z.B. unter Verwendung eines Zeitstempels, einer Sequenznummer oder einer vom Kommunikationspartner gewählten Zufallszahl) daraus abgeleiteter Wert übertragen wird.

In ähnlicher Weise existieren dynamische Authentisierungsverfahren auf Basis von asymmetrischen kryptographischen Algorithmen (z. B. *Challenge-Response-Verfahren*) und so genannte *Zero-Knowledge-Verfahren*, bei denen ein Angreifer aus der Kenntnis bisheriger Protokollabläufe bewiesenermaßen keinen Nutzen ziehen kann.

Generelle Authentisierungsverfahren unter Verwendung symmetrischer Verschlüsselungsverfahren, digitaler Signaturen, Hashfunktionen bzw. Zero-Knowledge-Verfahren sind in [ISO9798] (Teil 2-5) standardisiert. Authentisierungsprotokolle für Chipkarten sind beispielsweise in [CEN14890] und [ISO24727-3] (Annex A) standardisiert.

## 2.4 Ausweisformate

Weitere Unterschiede können hinsichtlich der Formate für die digitalen Ausweise (engl. Credentials) existieren. Hier kann man (vgl. [WS-Trust], KeyType in Section 9.2) grob zwischen

- digitalen Ausweisen mit *symmetrischen Schlüsseln* („Symmetric Key Credentials“, z.B. [WS-S-Kerb, WS-S-UN, WS-S-XCBF]),
- digitalen Ausweisen mit *asymmetrischen Schlüsseln* („Asymmetric Key Credential“, z.B. Public-Key-Zertifikate [X.509, ISO7816-8, WS-S-X.509] und u.U.<sup>4</sup> SAML-Assertions [SAML])
- digitale Ausweise *ohne Schlüssel* („Bearer Tokens“) (z.B. Attribut-Zertifikate [RFC3281] und SAML-Assertions [SAML]) und
- sonstigen digitalen Ausweisen (z.B. Rights Expression Language Lizenzen [ISO21000-5] oder Zero-Knowledge-Techniken [Bran00, BCL04]) unterscheiden.

Neben den heute mehr oder weniger gebräuchlichen Standardformaten für Zertifikate [X.509, ISO7816-8] und XML-basierte Assertions [SAML] scheinen im eGovernment-Kontext insbesondere die Verfahren aus [Bran00, BCL04] erwähnenswert, da hier mittels Zero-Knowledge-Techniken gezielt Aussagen über einzelne Identitätsattribute bewiesen werden können und deshalb besonders datenschutzfreundliche (vgl. [ENISA09b]) digitale Ausweise ermöglicht werden. Solche Datenschutzaspekte sind insbesondere dann bedeutsam, wenn der digitale Ausweis einen eindeutigen Identifikator des Bürgers enthalten soll (vgl. Abschnitt 2.6).

## 2.5 Vertrauensmodelle

Den Authentisierungssystemen können unterschiedliche Vertrauensmodelle zu Grunde liegen, wobei in Abhängigkeit der eingesetzten Authentisierungsprotokolle (vgl. Abschnitt 2.3) und Ausweisformate (vgl. Abschnitt 2.4) der Bürger entweder *direkt* beim eGovernment-Dienst registriert ist (z. B. bei Benutzername / Passwort – basierten Systemen) oder einen *Ausweis*

---

<sup>4</sup> Eine SAML-Assertion ist genau dann ein digitaler Ausweis mit asymmetrischen Schlüsseln wenn die „holder of key“ subject confirmation method genutzt wird. Andernfalls ist es z.B. ein

besitzt, der vom eGovernment-Dienst akzeptiert wird. Beim Einsatz von Zertifikaten [X.509, ISO7816-8] sind hier insbesondere *hierarchische* Strukturen üblich<sup>5</sup>, während SAML-Assertions [SAML] zumeist in Verbindung mit *föderierten* Systemen (vgl. [Posc08]) eingesetzt werden.

## 2.6 Umgang mit Identifikatoren

Für die Personalisierung der eGovernment-Dienste der Bürger sind Identifikatoren notwendig, durch die der Bürger in einem bestimmten Kontext eindeutig bezeichnet wird. Hierbei kann es sich um ein Pseudonym<sup>6</sup> handeln oder im Rahmen einer tatsächlichen Identifizierung der reale Name des Bürgers verwendet werden. Die wesentlichen Unterschiede ergeben sich nun daraus, wo dieser Identifikator gebildet und gespeichert wird. Während der zukünftige deutsche Personalausweis (vgl. [EACv2]) selbst Dienst- oder Sektor-spezifische Pseudonyme erzeugt, wird dies bei der Österreichischen Bürgerkarte (vgl. [AT]) von einem zentralen Dienst erledigt. Auf der anderen Seite existieren in Finnland [FI], Estland [EE] und Schweden [SE] Sektor-übergreifende Identifikatoren<sup>7</sup>, die in den Zertifikaten enthalten sind. In ähnlicher Weise wird auch in Italien [IT] ein Sektor-übergreifendes Pseudonym<sup>8</sup> als Common Name in den Zertifikaten genutzt, wodurch eine Profilbildung grundsätzlich möglich wäre. In Belgien [BE] ist die als Identifikator fungierende „National Registry Number“ nicht in den Zertifikaten enthalten, sondern lediglich auf der Karte gespeichert und die Nutzung derselben wird durch die „Privacy Commission“ streng überwacht.

## 3 EU-Landkarte

Bei der Betrachtung der aktuellen Situation in den verschiedenen EU-Mitgliedsstaaten kann zum Einen die Frage dienen, welches grundlegende Modell den behördlichen Online-Diensten zu Grunde liegt (vgl. Abschnitt 3.2) und ob eID Karten (Besitz) ausgegeben oder geplant sind (vgl. Abschnitt 3.1).

### 3.1 Status der eID Karten Programme

#### 3.1.1 EU Mitgliedsstaaten mit bereits ausgegebenen eID Karten

Von 27 EU-Mitgliedstaaten haben bereits 8 Staaten elektronische Identitätsausweise bis Ende 2008 eingeführt [Houd06]. Namentlich sind dies Spanien (2006 [ES]), Portugal (2007, Project PEGASUS [PT]), Italien (2006, Carta d'identità Elettronica, CIE, Carta Nazionale dei Servizi, CNS [IT]), Belgien (2005, BELPIC [BE]), Österreich (2004, Bürgerkarte (e-card) [AT]), Finnland (2002, FINEID [FI]), Schweden (2005 [SE]) und Estland (2004 [EE]). Als weiterer Staat mit einem laufenden eID-Karten Programm im osteuropäischen Raum, das derzeit nicht Mitglied der EU ist, kann Serbien genannt werden [Stan08]. Drei Grund-Modelle für nationa-

---

<sup>5</sup> Wie in [BHS08] gezeigt, ist es auch in föderierten Systemarchitekturen möglich, [X.509]-basierte Zertifikate einzusetzen.

<sup>6</sup> Hierbei können Dienst- oder Sektor-spezifische und Sektor-übergreifende Pseudonyme unterschieden werden.

<sup>7</sup> Während der „Personal Identity Code“ in Estland und die „Personal Identity Number“ in Schweden auch auf der Karte aufgedruckt sind, ist dies bei der finnischen FINUID („FINEID based unique electronic identifier“) nicht der Fall.

<sup>8</sup> Dieses Pseudonym ist der Hashwert der auf der Karte gespeicherten „Dati\_Personali“-Datei.

le eID-Programme mit Online-Dienste-Funktion haben sich bisher etabliert. Alle Staaten haben die elektronische Authentisierung für Internet-Dienste über die Zwei-Faktoren-Authentisierung (Besitz und Wissen) möglich gemacht.

- Elektronische Ausweise für ausschließlich regulierte Behörden Online-Dienste, für den Bürger (G2C); Beispiel: Portugal.
- Elektronische Ausweise für ausschließlich regulierte Behörden Online-Dienste, für den Bürger, erweitert um elektronische Ticket-Funktion (G2C + eTicketing); Beispiel: Italien, zweite Generation.
- Kombination des elektronischen Ausweises für Behörden Online-Dienste, für den Bürger, mit Travel- und/oder eBanking-Funktion; Beispiele: Schweden, Belgien, Estland und Finnland.

Bemerkenswert ist, dass Italien zwei eID-Programme jeweils parallel umgesetzt haben, um Einzelfunktionen getrennt anzubieten. Während in Italien die nationale eID Karte (CIE) ausschließlich zur Identifikation (ohne MRZ) genutzt werden kann, ist die zweite Karte (CNS) Träger der Online-Dienste, die in der Ausbaustufe mit der elektronischen Ticket-Funktion für die Staatsbahn erweitert werden soll.

Nur in Estland besteht bisher eine Ausweispflicht in Verbindung mit der Signatur-Funktion. In allen anderen Staaten kann die Signatur-Funktion auf Wunsch des Bürgers deaktiviert werden bzw. bleiben.

### 3.1.2 EU Mitgliedsstaaten mit eGovernment ohne eID Karten

In einigen EU Mitgliedsstaaten werden regulierte behördliche Online-Dienste angeboten, die auf der Ein-Faktor-Authentisierung basieren (Wissen). Diese sind beispielsweise England mit GATEWAY für die Steuerzahlung [UK], die Niederlande mit LIMOSA, Dänemark mit My Page [DK] für eine Vielzahl von eGovernment Dienste auf Bundes-, Regionen-, und Städteebene und Deutschland für die elektronische Steuererklärung (ELSTER). Es wird erwartet, dass weitere Staaten diesem Modell folgen werden, um eGovernment-Dienste zu ermöglichen.

### 3.1.3 EU Mitgliedsstaaten mit angekündigten eID

Bis zum Ende 2008 haben vier weitere EU Mitgliedsstaaten eID-Programme aufgesetzt und offiziell angekündigt: Frankreich (2009, Programme de Protection de l'Identité, PPI [FR]), Deutschland (2010, elektronischer Personalausweis, ePA [DE]), Polen (2010, Polish Identity-card, PLID [PL]) und England (2011; kein Pflichtdokument [UK]). England plant bislang keine Online-Dienste Funktion anzubieten. Dagegen wird über eine Erweiterung der Funktion hin zu einer Bankenkarte nachgedacht (vgl. [EMV-CAP]). Dies wird im Zusammenhang mit einem Anreizmodell in Erwägung gezogen, da seit 1951 in England keine Ausweispflicht besteht [Godd51].

## 3.2 Grundlegendes Modell der elektronischen Dienste

Auf Basis der bisher entwickelten elektronischen Dienste können – in Abhängigkeit davon, ob geschlossene oder offene Systeme in vollständig staatlicher oder teilweise privatisierter Hand angeboten werden – drei Modelle unterschieden werden:

- *Regulierte elektronische Dienste, geschlossener Behördenkreis (eGovernment, geschlossene Anwendung)*

Als Beispiel kann hierfür Portugal [Rodr07] herangezogen werden, bei denen fünf dedizierte Dienste und Behörden zum Einsatz kommen. Eine Erweiterung auf Bundes-, Kommunen bzw. Städte-Ebene ist zunächst nicht vorgesehen. Die Dienste werden hauptsächlich in Bürgerbüros, sogenannten Kiosken, angeboten.

- *Regulierte elektronische Dienste, offener Behördenkreis (eGovernment, offene Anwendung)*

Exemplarisch kann hier Frankreich [Amin08] genannt werden. Alle eID/Online-Dienste werden künftig von diversen Behörden auf Bundes-, Landes-, Kommunen- und Städte-Ebene frei anbietbar. Der Zeitpunkt der Einführung und die Art der Dienste sind z.B. jeweils von den Stadtverwaltungen frei wählbar. Für industrielle Anbieter sollen diese Dienste-Plattformen zunächst nicht zugelassen werden.

- *Regulierte elektronische Dienste, offener Behördenkreis und elektronische Dienste, offener Industriekreis (eGovernment + eBusiness, offene Anwendung)*

Das "Modell Deutschland" weist ein offenes eID/Online-Dienste Angebot auf, das von Behörden auf allen Ebenen, von Industrie (insbes. IP- und Online-Handel), Banken und Versicherungen von Beginn an frei nutzbar werden soll.

Die Fallunterscheidung in geschlossene bzw. offene Anbieterkreise gestattet auch eine Indikation der staatlichen Politik, hinsichtlich hoheitlichen, semi-hoheitlichen bzw. privatwirtschaftlichen Aufgaben im Umfeld von elektronischen Diensten um eGovernment. Als wichtiges Element in der Anwendung kann z.B. das Bürgerportal eingestuft werden. In einigen Staaten wird dieses Portal durch eine Behörde gestellt und betrieben. Dazu zählen Portugal, Spanien, Estland, Norwegen, England und Italien. In anderen Staaten wie in Deutschland soll dieses Portal durch die Industrie gestellt und betrieben werden [Reis09].

Ein weiteres Element stellt das Trustcenter dar, das für die Anwendung von elektronischer bzw. digitaler Signatur (z.B. für eBilling) benötigt wird. Bis auf Estland ist diese Funktion in den bisherigen eID-Kartenprogrammen vom Bürger frei wählbar. Auch hier kommen mehrere Optionen zur Anwendung:

- a) Behörden bieten diese Lösung (z.B. Portugal, Estland und Spanien)
- b) Sicherheitsindustrie bietet diese Lösung (z.B. A-Trust in Österreich; in Planung in Deutschland).
- c) Bundesbehörde und Sicherheitsindustrie bieten gemeinsam eine nationale Trustcenter-Lösung (z.B. in den Niederlanden; gemeinsame Tochter der Bundespolizei zusammen mit SAGEM-IDENTIFICATION, vormals SDU).

Die nationalen Entscheidungen über derartige Leistungen aus Behörden heraus oder als Industrie-Angebot können unter anderen aus den Aspekten a) Finanzierung für Anschaffung und den laufenden Betrieb, b) Kontrolle und Überwachung von Abläufen insbesondere unter Berücksichtigung von genutzten digitalisierten Personendaten c) nationaler Datenschutz und Gesetzeslage.

## 4 Ausblick

In 8 von 27 EU Staaten wird bereits eine 2-Faktor-Authentisierung für eGovernment Services eingesetzt. In den nächsten 18 Monaten planen weitere EU-Staaten mit der Ausgabe. Diese sind u.a. England (2011), Frankreich (2009), Deutschland (2010), Polen (2011) und Tschechien (2010). Betrachtet man alle genannten EU-Staaten, mit laufenden Programmen zuzüglich der Staaten mit Programm-Ankündigungen werden kumuliert 80% der EU-Einwohner abgedeckt. In nahezu allen Staaten besteht die gesetzliche Ausweis-Pflicht.

Es ist zu erwarten, das im Zuge der Interoperabilitätsbestrebungen der EU Kommission (siehe z.B. die EU-Förder-Projekt GUIDE, TERREGOV und LSP e-ID/STORK und die EU Organisation wie IDABC) eine Angleichung der Technologien, der Protokolle und der Sicherheitsarchitekturen zu erwarten ist, insbesondere in den Ländern die bereits Chipkarten-basierende eGovernment-Dienste anbieten oder kurz vor der Ausgabe stehen.

### Literatur









- [Amin08] Jean Luc Aminot: *The French Secure Documents Agency and the French e-ID Card Project*; Vortrag auf "World eID" '08, 18.09.2008, Sophia Antipolis, Frankreich
- [BCL04] Endre Bangerter, Jan Camenisch und Anna Lysyanskaya: *A Cryptographic Framework for the Controlled Release of Certified Data*, Security Protocols Workshop 2004, SS. 20-42, <http://www.zurich.ibm.com/~jca/papers/bacaly04.pdf>
- [BHS08] Bud P. Bruegger, Detlef Hühnlein und Jörg Schwenk: *TLS-Federation - A secure and Relying-Party-friendly approach for Federated Identity Management*, in A. Brömme & al. (Hrsg.), Tagungsband „BIOSIG 2008: Biometrics and Electronic Signatures“, GI-Edition Lecture Notes in Informatics (LNI) 137, 2008, SS. 93-104, <http://www.ecsec.de/pub/TLS-Federation.pdf>
- [Bial08] K. Bialoszewski: *Polski Biometryczny Dowod Osobisty*; Vortrag auf Sicherheitskonferenz "Polskie Karty i Systemy", 07.03.2008, Warschau, Polen
- [BKMN08] J. Bender, D. Kügler, M. Margraf und I. Naumann: *Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis*, Datenschutz und Datensicherheit (DuD), Seiten 173–177, 2008
- [BMI08] BMI: *Einführung des elektronischen Personalausweises in Deutschland, Grobkonzept - Version 2.0*, [http://netzpolitik.org/wp-upload/bmi\\_epa-grobkonzept-2-0\\_2008-07-02.pdf](http://netzpolitik.org/wp-upload/bmi_epa-grobkonzept-2-0_2008-07-02.pdf)
- [BoMa03] Colin Boyd und Anish Mathuria: *Protocols for authentication and key establishment*, Springer Verlag, 2003
- [Bran00] Stefan Brands: *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*, MIT Press, 2000, [http://www.credentica.com/the\\_mit\\_pressbook.html](http://www.credentica.com/the_mit_pressbook.html)

- [BSI05] BSI: *Authentisierung im E-Government - Mechanismen und Anwendungsfelder der Authentisierung*, 2005, [www.bsi.bund.de/fachthem/egov/download/4\\_Authen.pdf](http://www.bsi.bund.de/fachthem/egov/download/4_Authen.pdf)
- [CEN14890] Comité Européen de Normalisation (CEN): *Application Interface for smart cards used as Secure Signature Creation Devices - Part 1-2*, Preliminary European Norm, 2008
- [CEN15264] CEN: *Architecture for a European interoperable eID system within a smart card infrastructure*, CWA 15264-1, April 2005, [ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eAuth/cwa15264-01-2005-Apr.pdf](http://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eAuth/cwa15264-01-2005-Apr.pdf)
- [CEN15480] CEN: *Identification card systems - European Citizen Card - Part 1-4*, Technical Specifications
- [CWP04] D. De Cock, K. Wouters, B. Preneel: *Introduction to the Belgian EID Card: BELPIC*, EuroPKI 2004, LNCS 3039, Springer, SS. 1-13, 2004
- [EACv1] BSI: *Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)*, Technical Guideline TR-03110, Version 1.11, 2008, [http://www.bsi.bund.de/fachthem/epass/TR-03110\\_v111.pdf](http://www.bsi.bund.de/fachthem/epass/TR-03110_v111.pdf)
- [EACv2] BSI: *Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC) and Password Authenticated Connection Establishment (PACE)*, Technical Guideline TR-03110, Release Candidate Reloaded, 2008
- [EMV] EMVCo Llc.: *EMV Integrated Circuit Card Specifications for Payment Systems*, Version 4.2, 2008, <http://www.emvco.com>
- [EMV-CAP] MasterCard: *SecureCode™ 3-D Secure Chip Authentication Program - Functional Architecture*, June 2003
- [ENISA09a] ENISA: *Report on the state of pan-European eIDM initiatives*, ENISA Report, Januar 2009, [http://www.enisa.europa.eu/doc/pdf/deliverables/enisa\\_eID\\_management.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_eID_management.pdf)
- [ENISA09b] ENISA: *Privacy Features of European eID Card Specifications*, ENISA Position Paper, Februar 2009, [http://www.enisa.europa.eu/doc/pdf/deliverables/enisa\\_privacy\\_features\\_eID.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_features_eID.pdf)
- [Gaze07] Gazzetta Ufficiale, 9-11-2007, *Serie generale* n. 261
- [Godd51] Lord Goddard, 20th June 1951, *Entscheidung des Justizministers*
- [Hill08] M. Hillier: *The National Identity Scheme – an update*; Vortrag auf “Security Document World”, 22.04.2008, London, Großbritannien








- [Houd06] D. Houdeau, M. v. Foerster, K. Wolfenstetter: *Biometrics in ID Documents, Security and Privacy, Technology and Practice*; Vortrag auf Omnicard `09, Seite 202, ff
- [Hühn08] D. Hühnlein: *Identitätsmanagement - Eine visualisierte Begriffsbestimmung, Datenschutz und Datensicherheit (DuD)*, 3/2008, SS. 163-165, [http://www.ecsec.de/pub/2008\\_DuD\\_Glossar.pdf](http://www.ecsec.de/pub/2008_DuD_Glossar.pdf)
- [ICAO] ICAO: *Machine Readable Documents, Doc 9303, Machine Readable Travel Documents*, <http://mrttd.icao.int/>
- [ISO7816] ISO/IEC 7816: *Identification cards - Integrated circuit cards - Part 1-15*, International Standard
- [ISO9798] ISO/IEC 9798: *Information Technology - Security Techniques - Entity Authentication - Part 1-6*, International Standard
- [ISO14443] ISO/IEC 14443: *Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1-4*, International Standard
- [ISO21000-5] ISO/IEC 21000: *Information technology - Multimedia framework (MPEG-21) - Part 5: Rights Expression Language*, International Standard, 2004
- [ISO24727-3] ISO/IEC 24727-3: *Identification cards - Integrated circuit cards programming interfaces - Part 3: Application programming interface*, International Standard, 2008
- [LHP02] H. Leitold, A. Hollosi, R. Posch: *Security Architecture of the Austrian Citizen Card Concept*, ACSAC 2002, SS. 391-402, 2002
- [Mart07] T. Martens: *Estonia-The Country with Identification Infrastructure*; Vortrag im Rahmen des "Electronic Passport Forum", 21st June, 2007, Istanbul, Türkei
- [Posc08] R. Posch: *A Federated Identity Management Architecture for Cross-Border Services in Europe*, in A. Brömme & al. (Hrsg.), Tagungsband „BIOSIG 2008: Biometrics and Electronic Signatures“, GI-Edition Lecture Notes in Informatics (LNI) 137, 2008, SS. 141-152
- [Reis07] A. Reisen: *The Federal German ID Card: Concepts and Application*; Vortrag auf der "ISSE 2007", Warschau, Polen
- [Reis08] A. Reisen: *Digitale Identität im Scheckkartenformat – Datenschutzvorkehrungen für den elektronischen Personalausweis*. *Datenschutz und Datensicherheit (DuD)*, SS. 164–167, 2008
- [Reis09] A. Reisen: *Der Anwendungstest für den elektronischen Personalausweis*, OMNICARD 2009, SS. 160

- [RFC3281] S. Farrel and R. Housley. An Internet Attribute Certificate Profile for Authorization. Request For Comments - RFC 3281, <http://www.ietf.org/rfc/rfc3281.txt>, April 2002.
- [Rodr07] G. Rodrigues: *The Portuguese Citizen Card Experience*; Vortrag auf "Security Document World", 22nd May, 2007, London, Großbritannien
- [Rouc08] EUROSMAART, subgroup eID, Besprechung 03.07.2008; Interview mit Bruno Rouchouze/Gemalto, in Brüssel, Belgien
- [SAML] Scott Cantor, John Kemp, Rob Philpott und Eve Maler: *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS Standard, 15.03.2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>, 2005
- [WS-S-Kerb] Anthony Nadalin, Chris Kaler, Ronald Monzillo, and Phillip Hallam-Baker: *Web Services Security Kerberos Token Profile 1.1*, OASIS Standard, 01.02.2006. <http://www.oasis-open.org/committees/download.php/16788/wss-v1.1-spec-os-KerberosTokenProfile.pdf>, 2006
- [WS-S-UN] Anthony Nadalin, Chris Kaler, Ronald Monzillo and Phillip Hallam-Baker: *Web Services Security UsernameToken Profile 1.1*, OASIS Standard, 01.02.2006. <http://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf>, 2006
- [WS-S-XCBF] Phillip H. Griffin and Monica J. Martin: *Web Services Security XCBF Token Profile*, OASIS Working Draft 1.0, 25.11.2002. <http://xml.coverpages.org/WSS-XCBF-Token.pdf>, 2002.
- [WS-S-X.509] Anthony Nadalin, Chris Kaler, Ronald Monzillo and Phillip Hallam-Baker: *Web Services Security X.509 Certificate Token Profile 1.1*, OASIS Standard, 01.02.2006. <http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf>, 2006.
- [WS-Trust] Anthony Nadalin, Marc Goodner, Martin Gudgin, Abbie Barbir, and Hans Granqvist. *WS-Trust 1.3*. OASIS Standard, 19.03.2007. <http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf>, 2007.
- [X.509] ITU-T: *ITU-T Recommendation X.509 - ISO-IEC 9594-8:2005. Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*, 2005

EU-Mitgliedsstaat <sup>9</sup>			eID-Programm	Ein-führung	Standards	Weitere Informationen
	[AT]	Österreich	Bürgerkarte (u.a. e-card)	2004	[ISO7816-3/4/8], [X.509], [SAML]	[LHP02], <a href="http://www.buergerkarte.at/de/index.html">http://www.buergerkarte.at/de/index.html</a>
	[BE]	Belgien	BELPIC	2003	[ISO7816-3/4/8], [X.509]	[CWP04], <a href="http://eid.belgium.be/">http://eid.belgium.be/</a> , <a href="http://www.belgif.be/index.php/Authentication/authorization">http://www.belgif.be/index.php/Authentication/authorization</a>
	[DK]	Dänemark	MyPage / OCES	2005	[X.509], [SAML]	<a href="http://e.gov.dk">http://e.gov.dk</a> , <a href="http://www.openoces.org">http://www.openoces.org</a> , <a href="https://www.signatursekretariatet.dk/certifikatpolitikker.html">https://www.signatursekretariatet.dk/certifikatpolitikker.html</a>
	[EE]	Estland		2004	[ISO7816-3/4/8], [X.509]	[Mart07], <a href="http://www.id.ee">http://www.id.ee</a> , <a href="http://www.sk.ee">http://www.sk.ee</a>
	[ES]	Spanien	DNie	2006	[ISO7816-3/4/8/15], [X.509]	<a href="http://www.dnielectronico.es">http://www.dnielectronico.es</a>
	[FI]	Finnland	FINID	2002	[ISO7816-3/4/8/15], [X.509]	<a href="http://www.fineid.fi">http://www.fineid.fi</a> , eID-Spezifikation unter <a href="http://www.fineid.fi/vrk/fineid/home.nsf/Pages/F831E50A2E0E0F36C2256FFF003A373B">http://www.fineid.fi/vrk/fineid/home.nsf/Pages/F831E50A2E0E0F36C2256FFF003A373B</a>
	[FR]	Frankreich	PPI	vorr. 2009	vorr. [ISO7816-3/4/8/15], [ISO14443-3], [CEN15480], [EACv1], [X.509]	[Amin08], eID-Spezifikation unter <a href="http://www.gixel.fr/Portal_Upload/Files/Carteapuce/IASECCv10.pdf">http://www.gixel.fr/Portal_Upload/Files/Carteapuce/IASECCv10.pdf</a>
	[DE]	Deutschland	ePA	vorr. 2010	vorr. [ISO14443-3], [ISO7816-4/8], , [CEN15480], [EACv2], [ICAO], (optional [X.509] für Signatur)	[Reis07], [Reis08], [BKMN08], [BMI08], [EACv2], <a href="http://www.bmi.bund.de/cln_028/nn_1082274/Internet/Content/Themen/PaesseUndAusweise/Listentexte/elPersonalausweis.html">http://www.bmi.bund.de/cln_028/nn_1082274/Internet/Content/Themen/PaesseUndAusweise/Listentexte/elPersonalausweis.html</a>

<sup>9</sup> Die Tabelle stützt sich neben vielfältigen persönlichen Interviews insbesondere auch auf die von der EU (IDABC) im Jahr 2007 durchgeführten Umfrage „eID Interoperability for PEGS“, siehe <http://ec.europa.eu/idabc/en/document/6484/5644> .

EU-Mitgliedsstaat <sup>9</sup>			eID-Programm	Ein-führung	Standards	Weitere Informationen
	[IT]	Italien	CIE/CNS	2006	[ISO7816-3/4/8], [X.509]	<a href="http://www.handelskammer.bz.it/de-DE/nationale-servicekarte-cns-business-key-digitale-unterschrift-90de.html">http://www.handelskammer.bz.it/de-DE/nationale-servicekarte-cns-business-key-digitale-unterschrift-90de.html</a> , [Gaze07], eID-Spezifikation en unter <a href="http://www.confsl.org/images/files/workshops/workshop_sc-egov-floss.zip">http://www.confsl.org/images/files/workshops/workshop_sc-egov-floss.zip</a>
	[PL]	Polen	PLID	vorr. 2010	vorr. [CEN15480]	[Bial08]
	[PT]	Portugal	PEGASUS	2006	[ISO7816-3/4/8/15], [X.509], [MC-CAP]	[Rodr07], <a href="http://www.cartaodocidadao.pt/">http://www.cartaodocidadao.pt/</a>
	[SE]	Schweden		2005	[ISO7816-3/4/8/15], [X.509]	<a href="http://eid.steria.se/">http://eid.steria.se/</a> , <a href="http://www.bankid.com">http://www.bankid.com</a> , <a href="http://www.skatteverket.se">http://www.skatteverket.se</a> , Steria-eID-Spezifikation unter <a href="http://eid.steria.se/documents/Steria%20CryptoFlex%20Card%20Profile.pdf">http://eid.steria.se/documents/Steria%20CryptoFlex%20Card%20Profile.pdf</a>
	[UK]	Vereinigtes Königreich	NeID	vorr. 2011	vorr. [ISO7816-4/8], [ISO14443-3], [CEN15480], [ICAO], [X.509], [MC-CAP]	<a href="http://www.localegov.gov.uk">http://www.localegov.gov.uk</a> , <a href="http://www.gateway.gov.uk/">http://www.gateway.gov.uk/</a> , <a href="http://www.ips.gov.uk/identity/">http://www.ips.gov.uk/identity/</a> [Hill08]