SkIDentity – Vertrauenswürdige Identitäten für die Cloud

Detlef Hühnlein[1] · Gerrit Hornung[2] · Heiko Roßnagel[3] ·
Johannes Schmölz[1] · Tobias Wich[1] · Jan Zibuschka[3]

[1]ecsec GmbH, Sudetenstraße 16, D-96247 Michelau
vorname.nachname@ecsec.de

[2]Universität Passau, Innstr. 39 , D-94032 Passau
gerrit.hornung@uni-passau.de

[3]Fraunhofer Institut für Arbeitswirtschaft und Organisation,
Nobelstr. 12, D-70569 Stuttgart
vorname.nachname@iao.fraunhofer.de

Zusammenfassung

Durch die zunehmende Verlagerung von Geschäftsprozessen in die Cloud steigt der Bedarf an starken und flexibel nutzbaren Authentisierungsmechanismen. Vor diesem Hintergrund wird im SkIDentity-Projekt (siehe http://www.skidentity.de), das zu den Gewinnern des „Trusted Cloud“ Technologiewettbewerbs des Bundesministerium für Wirtschaft und Technologie zählt, eine umfassende Vertrauensinfrastruktur für die sichere, wirtschaftlich sinnvolle und rechtlich zulässige Nutzung elektronischer Ausweise in Cloud-Anwendungen entwickelt. Der vorliegende Beitrag liefert einen Überblick über die wesentlichen in diesem Projekt adressierten Probleme und skizziert die geplante SkIDentity-Lösungsarchitektur.

1 Einleitung

Vor dem Hintergrund der wirtschaftlichen Vorzüge der Industrialisierung von IT-Services und dem großen wirtschaftlichen Potenzial des Internet der Dienste [Ber+10] bilden sich zunehmend neue und verbesserte Angebote für Cloud-basierte Dienste [ShKa09]. Während eine zuverlässige Identitätsverwaltung als essentielle Voraussetzung für das vertrauenswürdige Cloud Computing gilt und das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Einsatz starker Authentifizierungsverfahren auch für Cloud-Nutzer empfiehlt [BSI-MSACC], erfolgt die Benutzerauthentifizierung für Cloud-Dienste und Anwendungen bislang noch fast immer mit Benutzername/Passwort.

Auf der anderen Seite existiert mit der Ausgabe des neuen Personalausweises (nPA) [nPA-Portal] endlich auch in Deutschland, ähnlich wie in einigen anderen Mitgliedsstaaten der Europäischen Union, eine sichere Infrastruktur für elektronische Ausweise und Identitäten (eID)

P. Schartner J. Taeger (Hrsg.) D·A·CH Security 2011, pp. *xx*

(siehe [HuHo09]), die auf dem umfassend neu geregelten Personalausweisgesetz beruht (näher [RoHo09]).

Vor diesem Hintergrund zielt das SkIDentity-Projekt darauf ab, eine tragfähige Brücke zwischen den sicheren elektronischen Ausweisen und den heute existierenden bzw. sich entwickelnden Cloud-Computing-Infrastrukturen zu schlagen, um vertrauenswürdige Identitäten für die Cloud bereit zu stellen, so dass komplette Prozess- und Wertschöpfungsketten sicher gestaltet werden können.

Die Verbindung der beiden Bereiche eröffnet erhebliche Chancen für innovative Produkte: Das deutsche Marktvolumen im Bereich Identifikation, Authentifizierung inklusive Biometrie und RFID wird sich von 920 Mio. € im Jahr 2008 auf 1.720 Mio. € im Jahr 2015 fast verdoppeln [VDI09]. Noch vielversprechender sind aber die Perspektiven im Bereich des Cloud Computings: Dort soll sich das deutsche Marktvolumen im Bereich von Public Clouds von derzeit 702 Mio. € bis zum Jahr 2025 auf 21,99 Mrd. € erhöhen und somit mehr als verdreißigfachen [Ber+10]. Somit adressiert das SkIDentity-Projekt strategisch äußerst attraktive Märkte.

Der Rest des Beitrags ist folgendermaßen gegliedert: In Abschnitt 2 wird näher auf die im SkIDentity-Projekt adressierten Problemstellungen eingegangen. Abschnitt 3 skizziert die SkIDentity-Lösungsarchitektur, mittels der die aufgeworfenen Probleme gelöst werden sollen. Abschnitt 4 enthält schließlich einen Ausblick auf zukünftige Entwicklungen.

2 Problemstellung

Bei der Bereitstellung sicherer Identitäten für die Cloud sind eine Reihe von technischen, organisatorischen, rechtlichen und wirtschaftlichen Problemen zu lösen:

- **Fehlende Integration von eID- und Cloud-Infrastrukturen:** Die Infrastrukturen für elektronische Ausweise und Cloud-basierte Dienste sind bislang nicht in zufriedenstellender Weise auf einander abgestimmt – geschweige denn integriert. Beispielsweise sind die im eID- und Cloud-Umfeld eingesetzten Authentifizierungsprotokolle komplett unterschiedlich und können nicht ohne Weiteres in sicherer Art und Weise kombiniert und integriert werden.
- **eID-Services werden bislang nur für den nPA angeboten:** Bisher werden eID-Services in Deutschland nur für den nPA angeboten. Während für die elektronische Gesundheitskarte und den elektronischen Heilberufsausweis [EHP+10] sowie zur Akzeptanz internationaler Ausweise [STORK] zumindest entsprechende Konzepte und Prototypen existieren, steht die Integration anderer Public-Key Infrastrukturen (PKI) [EsKo08] in eine umfassende „eID-Services-Cloud“ noch gänzlich aus.
- **eID-Services für den nPA sind nicht „handelbar“ und somit für KMU ungeeignet:** Besonders problematisch ist die Tatsache, dass eID-Services für den nPA im Regelfall nicht in einem „Internet der Dienste“ handelbar sind, da jeder Diensteanbieter ein eigenes Berechtigungszertifikat benötigt und die Übermittlung der Daten an Dritte aus Datenschutzerwägungen explizit ausgeschlossen ist (siehe [PAuswG] und [RHS08]).
- **Ungeklärte Sicherheitsfragen für elektronische Identitäten in der Cloud:** In [SHJ+10] wurde gezeigt, dass das Identitätsmanagement für die Sicherheit von Cloud-Computing

eine entscheidende Rolle spielt: Die sichere Integration von eID- und Cloud-Services ist jedoch ein noch nicht befriedigend gelöstes Problem.

- **Ungeklärte Rechtsfragen elektronischer Identitäten in der Cloud:** Derzeit bestehen im Bereich des Einsatzes von eID-Service-Brokern (also im Dreipersonenverhältnis) rechtliche Unsicherheiten über die Zulässigkeit einzelner Systemumsetzungen, weil die Diskussion sich bisher auf die Datenschutzfragen im Zweipersonenverhältnis [RHS08] [RoHo09] und haftungsrechtliche Probleme [Borg10] [RoHo09] konzentriert hat. In Bezug auf das Cloud-Computing kommen Fragen des Beweisrechts und der Compliance im Unternehmen hinzu, die bislang erst andiskutiert worden sind.
- **Fehlende bzw. unklare Geschäftsmodelle für Identitätsdienste in der Cloud:** eID-Services für den nPA sind für KMUs und kommunale Behörden oft aufgrund wirtschaftlicher Faktoren nicht oder nur sehr eingeschränkt nutzbar. Abhilfe könnte hier von eID-Brokern geschaffen werden, die als Informationsintermediäre agieren und die eID-Services in gebündelter und aufbereiteter Form bereitstellen [ZFR+07].
- **Fehlende Standards für elektronische Identitäten in der Cloud:** Obwohl das Cloud Computing seit geraumer Zeit zu den wichtigen IT-Trends zählt, steckt die diesbezüglich Standardisierung noch „in den Kinderschuhen“. Ein aktueller, aber leider nicht ganz vollständiger Überblick über die Cloud-spezifischen Aktivitäten der verschiedenen Standardisierungsgremien findet sich in [KhJa10].

3 Die SkIDentity Lösungsarchitektur

Um die aufgezeigten Probleme zu lösen, soll im SkIDentity-Projekt die in Abbildung 1 dargestellte Systemarchitektur umgesetzt und in breitenwirksamen Pilotanwendungen erprobt werden. Ähnlich wie bei anderen Systemen für das föderierte Identitätsmanagement (vgl. [HRZ10]) verfügt der Benutzer über ein Client-System (siehe Abschnitt 3.1) mit dem er auf die angebotenen Cloud Services (siehe Abschnitt 3.2) zugreifen möchte. Für das Identitätsmanagement ist in der SkIDentity-Lösungsarchitektur aber statt einem klassischen „Identity Provider“ ein eID-Broker (siehe Abschnitt 3.3) vorgesehen, der als Informationsintermediär agiert und die unterschiedlichen eID-Services (siehe Abschnitt 3.4) in gebündelter und aufbereiteter Form bereitstellt.

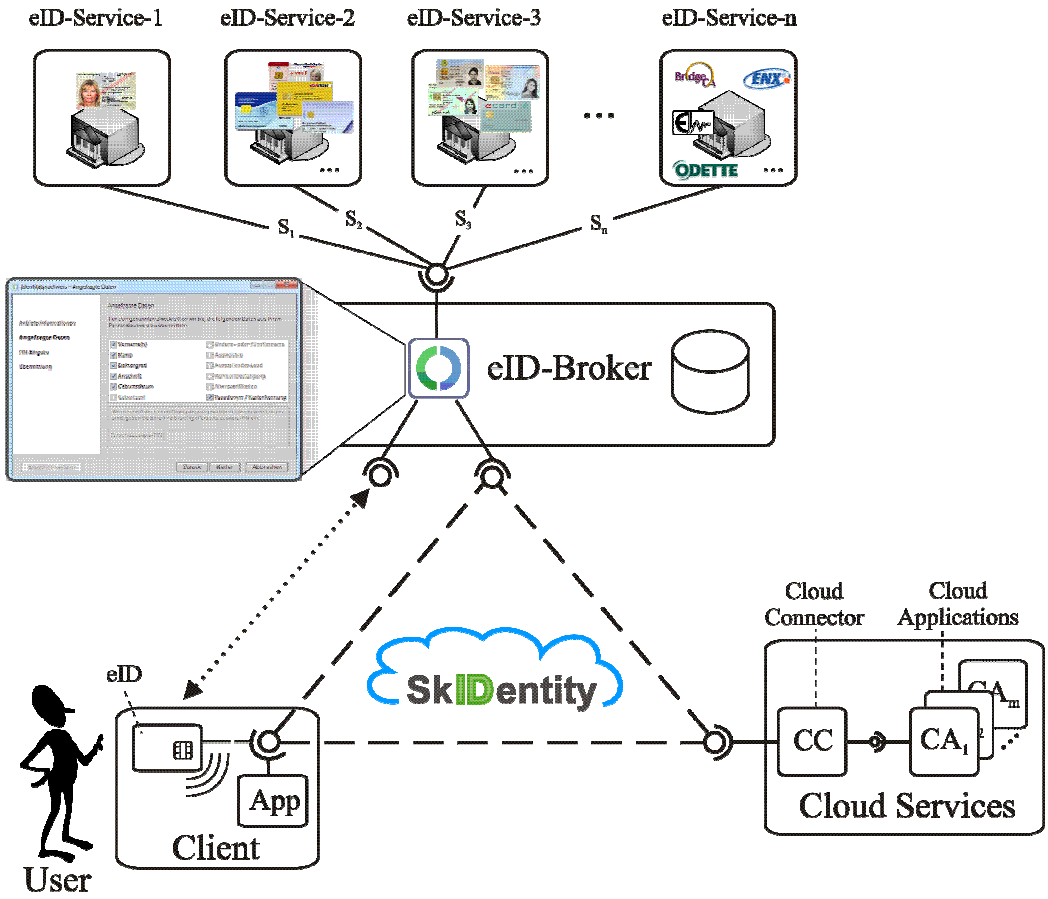

Abb. 1: SkIDentity-Systemarchitektur im Überblick

3.1 Client

Die Client-Komponente in der SkIDentity-Systemarchitektur soll auf Basis der „AusweisApp“ des Bundes [AusweisApp] realisiert werden, so dass die eID-Services für den nPA gemäß [BSI-TR-03130] genutzt und über den CardInfo-Mechanismus aus [HuBa07] bzw. [BSI-TR-03112] leicht weitere Chipkarten integriert werden können.

3.2 Cloud Services

Sofern die verschiedenen Cloud Services nicht bereits mit standardisierten Schnittstellen für das föderierte Identitätsmanagement ausgestattet sind, kann die Integration in die SkIDentity-Architektur über einen so genannten Cloud Connector erfolgen.

Dieser Cloud Connector wird über eine Konfigurationsdatei parametrisiert und kann über die bewusst einfach gehaltene IConnector-Schnittstelle in beliebige Cloud- und Webapplikationen integriert werden. Wie in Abbildung 2 ersichtlich, umfasst diese Schnittstelle eine einzige Funktion: Mit dieser *Authenticate*-Funktion kann eine Authentisierung entsprechender Güte (*Policy*) und eine Folge von Identitätsattributen (*Attribute*) angefordert werden.

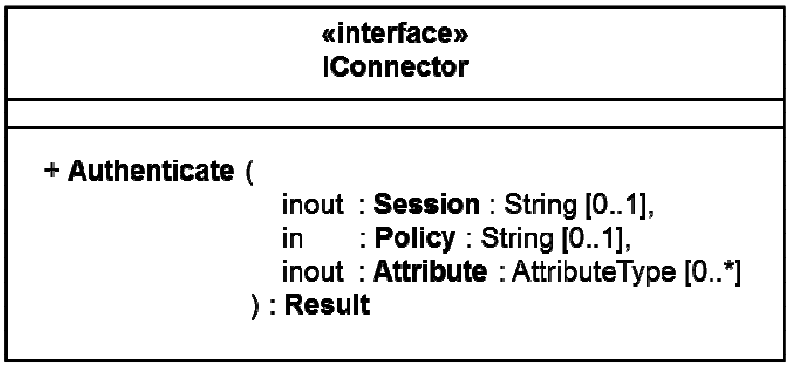

Abb. 2: IConnector-Interface des SkIDentity Cloud Connectors

3.3 eID-Broker

Der eID-Broker fungiert als Informationsintermediär und stellt die unterschiedlichen eID-Services in gebündelter und aufbereiteter Form bereit. Hierdurch können die unterschiedlichen eID-Services (siehe Abschnitt 3.4) und Ausweistoken (nPA, elektronische Gesundheitskarte, Heilberufsausweis, Bank- und Signaturkarten und andere Europäische Bürgerkarten) über einfache und einheitliche Schnittstellen zur sicheren Authentisierung in Cloud-basierten Anwendungen genutzt werden.

Für die Umsetzung dieser Lösung sind insbesondere beim nPA die strengen Vorgaben des Personalausweisrechts zu beachten. Aus Datenschutz- und Transparenzgründen bindet dieses die Verwendung der nPA-Daten an den Einsatz eines Berechtigungszertifikats, das kostenpflichtig beantragt werden muss und dessen Verwendung einen eID-Server gem. BSI-TR 03130 erfordert. Das Berechtigungszertifikat wird dem Ausweisinhaber vor der Eingabe seiner PIN angezeigt, um ihm die Identität der verantwortlichen Stelle und den Zweck der Datenverarbeitung deutlich zu machen, bevor er seine Einwilligung erteilt. Dieses Ziel des Gesetzgebers würde nicht erreicht, wenn Adresshändler Berechtigungszertifikate erhalten und die Daten im Anschluss beliebig weiterverwenden könnten. Deshalb schließt § 21 Abs. 2 Satz 1 Nr. 2 PAuswG die Erteilung eines Zertifikats aus, wenn der Zweck in der geschäftsmäßigen Übermittlung der Daten bestehen soll oder Anhaltspunkte für die geschäftsmäßige oder unberechtigte Übermittlung der Daten vorliegen (näher [HoMö11]).

Während diese Einschränkung in der Praxis durch eine Beteiligung der Nutzer im Einzelfall lösbar sein sollte, verursacht eine weitere Einschränkung Probleme: Gemäß § 29 Abs. 1 Nr. 2 PAuswV kann ein Berechtigungszertifikat nicht erteilt werden, wenn „der Zweck der Datenerhebung ausschließlich in der Auslesung oder Bereitstellung personenbezogener Daten aus dem Personalausweis für den Ausweisinhaber oder Dritte besteht“. Bei strikter Auslegung könnte diese Bestimmung so verstanden werden, dass jeder Einsatz eines Intermediärs, der – sogar mit informierter und freiwilliger Einwilligung aller Beteiligten im Einzelfall – die Daten ausliest, unzulässig ist. Angesichts der Funktion der Vorschrift, die die informationelle Selbstbestimmung des Ausweisinhabers waren, diesen aber nicht bevormunden soll, wäre eine solche Auslegung zwar sicherlich zu eng. Es besteht aber weithin Unsicherheit in der Praxis darüber, welche Umsetzungsmodelle rechtlich zulässig sind.

Eine Herausforderung des SkIDentity-Projekts besteht deshalb darin, ein zulässiges Modell für den Einsatz des nPA in der Cloud zu entwickeln, das gerade für KMUs und kleinere Behörden praktikabel und finanzierbar ist, ohne das datenschutzrechtlich begrüßenswerte System

des nPA auszuhebeln. Der Einsatz eines Dritten als Auftragsdatenverarbeiter nach § 11 BDSG wäre insoweit möglich, löst aber gerade nicht das Problem, dass der Auftraggeber in diesem Fall ein eigenes Berechtigungszertifikat benötigt und nur das technische Handling an den Dienstleister abgibt. Soll ein eID-Broker aber für mehrere Auftraggeber tätig werden, nähert er sich dem nach geltendem Recht für den nPA unzulässigen Adresshändler an.

Für eine zulässige Umsetzung müssen deshalb mehrere Anforderungen gewahrt werden, für die im Einzelfall technische Lösungen zu entwickeln sind. Um dem datenschutzrechtlichen Grundsatz der Transparenz Rechnung zu tragen, muss dem Ausweisinhaber deutlich werden, wer unter welchen Umständen zu welchen Zwecken seine nPA-Daten verarbeiten möchte, und er muss in diese Verarbeitung einwilligen. Überdies darf die im Gesetz vorgesehene Vorabprüfung im Rahmen der Zertifikatsvergabe (die sich insbesondere auf die Erforderlichkeit der Datenverwendung bezieht) nicht durch den Einsatz eines eID-Brokers unterlaufen werden. Eine denkbare Variante wäre insoweit, durch vertragliche Regelungen hohe Anforderungen an die Tätigkeit des eID-Brokers aufzustellen, die dann im Rahmen der Zertifikatsvergabe an diesen durch die zuständige Behörde berücksichtigt werden könnten. Hierbei könnte sich der eID-Broker beispielsweise zur Erforderlichkeitsprüfung im Verhältnis zu den angeschlossenen Dienstleistern verpflichten, seine Tätigkeit auf bestimmte Dienstleister beschränken oder (so die Umsetzung im Identifikationsservice [Verify-U] der Cybits AG) die Daten aus dem nPA zwar zu Bestätigungszwecken auslesen, jedoch gerade nicht an die Dienstleister weitergeben. Alternativ erscheint denkbar, dem Bürger nach Verwendung des nPA Credentials bereitzustellen, die dann im Verhältnis zum Diensteanbieter zur späteren, eigentlichen Identitätsbestätigung verwendet werden.

3.4 eID-Services

Die eID-Services im SkIDentity-System führen – vermittelt über den eID-Broker und das Client-System – in Verbindung mit dem jeweiligen Ausweistoken die tatsächliche Authentisierung durch. Beispielsweise sollen für die Authentisierung mit dem nPA die existierenden eID-Services (vgl. [eID-Service]) über die entsprechenden Schnittstellen gemäß [BSI-TR-03130] integriert werden. Darüber hinaus sollen im SkIDentity-Projekt weitere Authentisierungsdienste für alternative Ausweistoken (siehe z.B. [EHP+10] und [STORK]) und Zertifikate (siehe z.B. [EsKo08]) angebunden werden. Hierfür soll im SkIDentity-Projekt zunächst aus den verschiedenen existierenden Schnittstellen (siehe z.B. [BSI-TR-03130], [STORK]) eine übergreifende Schnittstelle abgeleitet werden, über die die verschiedenen eID-Services und Authentisierungsdienste integriert werden können.

4 Ausblick

Durch die Schaffung von standardisierten und transparenten Sicherheitsfunktionen können zukünftig ganze Prozess- und Wertschöpfungsketten in der Cloud sicher gestaltet werden – von der initialen Registrierung an einem Cloud-Service über die wiederkehrende sichere Authentisierung und Zugangskontrolle bis hin zu modernen Mechanismen zur sicheren Verwaltung des geistigen Eigentums mittels Enterprise Rights Management Systemen. Die hierfür notwendigen eID-Services werden über einen eID-Broker gebündelt, wodurch innovative Geschäfts- und Vertragsmodelle ermöglicht werden, durch die Infrastrukturen wirtschaftlich, rechtssicher und nutzerfreundlich angeboten [ZFR+07] und auf zukünftigen Dienstleistungsmarktplätzen gehandelt werden können.

Die entwickelten Infrastrukturdienste und Anwenderkomponenten werden im Rahmen des SkIDentity-Projektes in breitenwirksamen Pilotprojekten erprobt und zusammen mit den assoziierten Projektpartnern auf eine nachhaltige Nutzung vorbereitet. Hierbei dient die Abwicklung eines komplexen Industrieprojektes in der Cloud als Referenzszenario, das z.B. in der Automobilindustrie auftreten könnte. Hierbei sollen Infrastrukturen und Plattformen, z.B. für den sicheren Geschäftsdatenaustausch aus der Cloud bezogen werden.

Schon in der gegenwärtigen Phase zeigt das Projekt ein außergewöhnliches Potenzial und erhielt eine große Anzahl von Kooperationsanfragen aus Wirtschaft und anderen Forschungsprojekten, die die bisher nur als grober Entwurf vorliegende Sicherheitsinfrastruktur gerne nutzen würden. Anbieter von eID-Services und Cloud-basierten Anwendungen sowie Herausgeber von elektronischen Ausweisen, die an einer Mitwirkung im SkIDentity-Projekt interessiert sind, sind herzlich eingeladen, mit den Autoren dieses Papiers Kontakt aufzunehmen. Weitere Informationen über den Projektverlauf werden über http://www.skidentity.de/ bereitgestellt.

Literatur

[AusweisApp] BMI/BSI: *Informationen zur "AusweisApp"*, http://www.ausweisapp.bund.de

[Ber+10] Berlecon Research & al.: *Das wirtschaftliche Potenzial des Internet der Dienste*, Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi), 2010, http://www.berlecon.de/idd

[Borg10] G. Borges: *Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis. Ein Gutachten für das Bundesministerium des Innern*, abrufbar unter http://www.personalausweisportal.de/cln_102/SharedDocs/Downloads/DE/Studie_Recht_Volltext.html?nn=830468, 2010.

[BSI-MSACC] BSI: *BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter*, Entwurf vom 27.09.2010, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sonsti-ge/Cloud_Computing_Mindestsicherheitsanforderungen.pdf?__blob=publicationFile

[BSI-TR-03112] BSI: *eCard-API-Framework*, Technical Directive (BSI-TR-03112), Version 1.1, Part 1-7, 2009, https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html

[BSI-TR-03130] BSI: *Technische Richtlinie eID-Server*, Technische Richtlinie (BSI-TR-03130), Version 1.4.1, 2010, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_V1_4_pdf.pdf?__blob=publicationFile

[EHP+10] D. Eske, D. Hühnlein, S. Paulus, J. Schmölz, T. Wich, T. Wieland: *OpeneGK – Benutzerfreundliche und sichere Authentisierung für Mehrwert-*

dienste im Gesundheitswesen, in A. Brömme & al. (Hrsg.), Tagungsband „perspeGKtive 2010 – Workshop ‚Innovative und sichere Informationstechnologie für das Gesundheitswesen von morgen'", GI-Edition Lecture Notes in Informatics (LNI) 174, 2010, Seiten 83-103, http://www.ecsec.de/pub/openeGK.pdf

[eID-Service] Kompetenzzentrum neuer Personalausweis: *eID-Service-Anbieter*, 2011, http://www.ccepa.de/eid-service-anbieter

[EsKo08] B. Esslinger, H. Koy: *TeleTrust European Bridge CA - Die European Bridge CA als Enabler für sichere E-Mail mit S/MIME zwischen Unternehmen und Behörden*, DuD, 1/2008, SS. 1-5, http://www.teletrust.de/uploads/media/Esslinger-Koy_DuD_TeleTrusT-EBCA.pdf

[HoMö11] G. Hornung, J. Möller: *Passgesetz Personalausweisgesetz. Kommentar*, Verlag C.H.Beck, München 2011

[HRZ10] D. Hühnlein, H. Roßnagel, J. Zibuschka: *Diffusion of Federated Identity Management*, in F. Freiling (Hrsg.), Tagungsband „Sicherheit 2010", GI-Edition Lecture Notes in Informatics (LNI) 170, 2010, SS. 25-37

[HuBa07] D. Hühnlein, M. Bach: *How to use ISO/IEC 24727 with arbitrary smart cards*, in C. Lambrinoudakis, G. Pernul, A.M. Tjoa (Eds.): TrustBus 2007, LNCS 4657, Springer, 2007, SS. 280-289, http://www.ecsec.de/pub/2007_TrustBus.pdf

[HuBa08] D. Hühnlein, M. Bach: *Die Standards des eCard-API-Frameworks - Eine deutsche Richtlinie im Konzert internationaler Normen*, Datenschutz und Datensicherheit (DuD), 06/2008, SS. 379-382, http://www.ecsec.de/pub/2008_DuD_eCard.pdf

[HuHo09] D. Hühnlein, D. Houdeau: *Ein Überblick über Authentisierungs- und Identifizierungsverfahren für eGovernment-Dienste in Europa*, in Horster P. (Hrsg.): Tagungsband „D•A•CH Security", IT-Verlag, 2009

[KhJa10] B. Khasnabish, C. JunSheng: *Cloud SDO Activities Survey and Analysis*, IETF Internet Draft 00, 31.12.2010, http://tools.ietf.org/html/draft-khasnabish-cloud-sdo-survey-00

[nPA-Portal] BMI: *Der neue Personalausweis*, http://www.personalausweisportal.de, 2011

[PAuswG] *Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz – PAuswG)*, Artikel 1 des Gesetzes vom 18. Juni 2009, http://www.bmi.bund.de/cae/servlet/contentblob/607490/publicationFile/34857/eperso.pdf

[RoHo09] A. Roßnagel, G. Hornung: *Ein Ausweis für das Internet. Der neue Personalausweis erhält einen "elektronischen Identitätsnachweis"*, Die Öffentliche Verwaltung 2009, SS. 301-306.

[RHS08] A. Roßnagel, G. Hornung, C. Schnabel: *Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht*, Datenschutz und Datensicherheit 2008, SS. 168-172.

[SHJ+10] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, L. Lo Iacono: *All Your Cloud Are Belong To Us - Security Analysis of the Amazon Cloud*, in Begutachtung

[ShKa09] S. Shankland, J. Kaden: *Gartner: Cloud Computing wird wichtigster IT-Trend 2010*, ZDNet-Beitrag, 21.10.2009, http://www.zdnet.de/news/wirtschaft_unternehmen_business_gartner_cloud_computing_wird_wichtigster_it_trend_2010_story-39001020-41516155-1.htm

[STORK] *STORK (Secure idenTity acrOss boRders linKed), EU-Projekt*, http://www.eid-stork.eu

[VDI09] VDI/VDE: *Marktpotenzial von Sicherheitstechnologien und Sicherheitsdienstleistungen (Studie im Auftrag des BMWi)*, http://www.asw-online.de/downloads/Studie_Sicherheitstechnologien_09.pdf, 2009

[Verify-U] Cybits AG: *Vollelektronische Personenidentifikation [verify-U] nun auch mit neuem Personalausweis möglich*, Pressemitteilung, 9.3.2011

[ZFR+07] J. Zibuschka, L. Fritsch, M. Radmacher, T. Scherner, K. Rannenberg: *Enabling Privacy of Real-Life LBS*, in New Approaches for Security, Privacy and Trust in Complex Environments, SS. 325–336, 2007