VERTRAUENSWÜRDIGE IDENTITÄTEN FÜR DIE CLOUD

Dr. Detlef Hühnlein, Johannes Schmölz

ecsec GmbH, Sudetenstraße 16,
D-96247 Michelau
{detlef.huehnlein | johannes.schmoelz}@ecsec.de

Zusammenfassung

Dem Markt für das so genannte »Cloud Computing« werden große Wachstumspotenziale vorausgesagt [Ber+10]. Zunehmend werden auch sensible Geschäftsprozesse in die Cloud verlagert, wodurch der grundsätzliche Bedarf an starken und flexibel nutzbaren Authentisierungsmechanismen steigt. Während in vielen Cloud- und Web-Applikationen noch immer Benutzername und Passwort zur Authentisierung genutzt werden und selbst bei international führenden Cloud Computing Anbietern erhebliche Schwachstellen in den implementierten Authentisierungsverfahren entdeckt wurden [SHJ+11], stehen den deutschen Anwendern mit dem neuen Personalausweis (nPA), der elektronischen Gesundheitskarte (eGK) und vergleichbaren Chipkarten der eCard-Strategie oftmals bereits sichere Hardwaretoken zur Verfügung, die für die starke Authentisierung in der Cloud genutzt werden könnten.

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 geplante SkIDentity-Lösungsarchitektur und beleuchtet insbesondere die Chipkarten-spezifischen Aspekte.

1 Einleitung

Im Zuge der Industrialisierung von IT-Services und der Entwicklung 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 Web-Anwendungen bislang noch fast immer mit Benutzername/Passwort. Außerdem wurde in [SHJ+11] gezeigt, dass selbst die Authentisierungssysteme der international führenden Cloud Plattform Anbieter noch erhebliche Schwachstellen enthalten.

Auf der anderen Seite existiert mit der Ausgabe des nPA [nPA-Portal] endlich auch in Deutschland, ähnlich wie in einigen anderen Mitgliedsstaaten der Europäischen Union [HuHo09], eine sichere Infrastruktur für elektronische Ausweise und Identitäten (eID), die auf dem umfassend neu geregelten Personalausweisgesetz beruht. In ähnlicher Form können auch andere Chipkarten, wie z. B. die eGK, für die starke Authentisierung und den Chipkarten-basierten Identitätsnachweis genutzt werden (vgl. [EHP+10] und [HSW11]).

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: Abschnitt 2 liefert zunächst einen groben Überblick über die SkIDentity-Lösungsarchitektur und beleuchtet dann ausgewählte Chipkarten-spezifische Aspekte in dieser innovativen Sicherheitsinfrastruktur. Abschnitt 3 fasst schließlich die wesentlichen Aspekte des Beitrags zusammen und liefert einen Ausblick auf zukünftige Entwicklungen.

2 Die SkIDentity-Lösungsarchitektur

2.1 Überblick

Um die verschiedenen elektronischen Ausweise leicht in Cloud Computing Infrastrukturen einsetzen zu können, soll im SkIDentity-Projekt die in Abbildung 1 dargestellte Systemarchitektur umgesetzt und in einigen breitenwirksamen Pilotanwendungen erprobt werden.

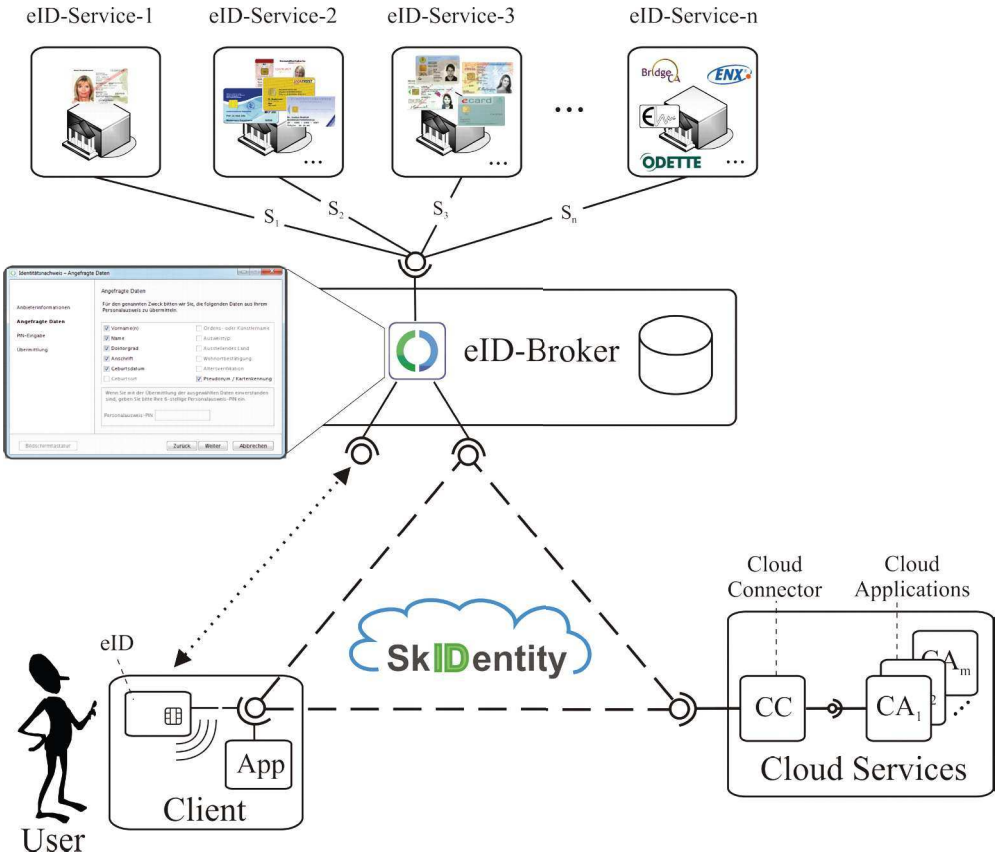

Abb. 1: SkIDentity-Systemarchitektur im Überblick

Ähnlich wie bei anderen Systemen für das föderierte Identitätsmanagement [HRZ10] verfügt der Benutzer über ein Client-System (siehe Abschnitt 3.1), das eng mit dem Browser des Benutzers verbunden ist und mit dem er auf die angebotenen Cloud Services (siehe Abschnitt 3.2) zugreifen kann. 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.

2.2 Client

Damit die unterschiedlichen elektronischen Ausweiskarten, wie z. B. nPA, eGK, Signatur- und Bankkarten, Bürgerkarten aus dem Europäischen Ausland etc., im SkIDentity-Projekt über einheitliche Schnittstellen genutzt werden können, müssen die eingesetzten Clients die benötigten Funktionen des eCard-API-Frameworks [BSI-TR-03112] unterstützen.

Neben der »AusweisApp« des Bundes [AusweisApp] soll hier insbesondere auch die quelloffene »Open eCard App« [OpeneCard] zum Einsatz kommen, da diese nicht nur den *CardInfo*-Mechanismus aus [HuBa07] bzw. [CEN15480-3] unterstützt, sondern auch die mobile Nutzung des neuen Personalausweises mit NFC-fähigen Mobiltelefonen ermöglichen wird [HHH12].

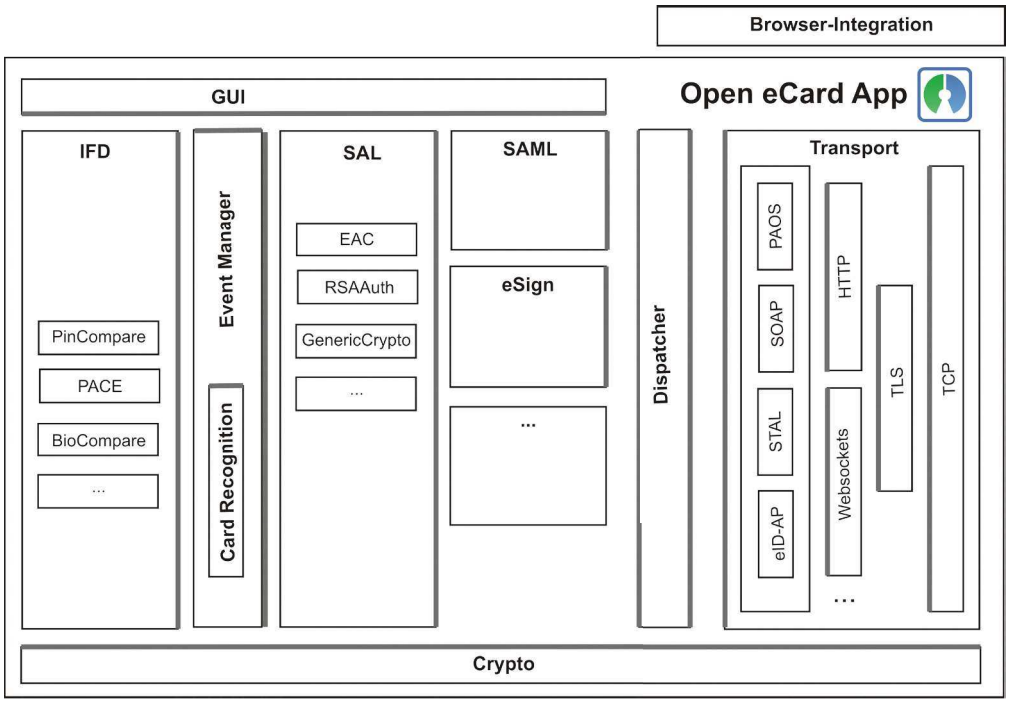

Abb. 2:
Die »Open eCard App«

Wie in Abbildung 2 dargestellt und in [OpeneCard] näher erläutert, umfasst die »Open eCard App« die folgenden Module:

- *Interface Device (IFD)*
  Diese Komponente implementiert die IFD-Schnittstelle gemäß Teil 6 von [BSI-TR-03112] bzw. [ISO24727-4], sowie verschiedene Protokolle zur Benutzerauthentisierung, wie z. B. das PACE-Protokoll gemäß [BSI-TR3110].
- *Event Manager*
  Der Event Manager überwacht die im IFD-Layer auftretenden Ereignisse (z.B. hinzugefügte oder entfernte Kartenterminals oder Chipkarten) und führt die Erkennung des Chip-kartentyps auf Basis eines Erkennungsbaumes durch, der vom *CardInfo*-

Repository der ecsec GmbH (siehe http://repository.cardinfo.eu/) mit dem in [Wich11] entwickelten Algorithmus aus einer Menge von *CardInfo*-Dateien erzeugt wird.

- *Service Access Layer (SAL)*
  Dieses Modul implementiert den Service Access Layer wie in Teil 4 von [BSI-TR-03112] und [ISO24727-3] beschrieben. Ein wichtiger Aspekt dieser Komponente ist, dass sie einen Erweiterungsmechanismus zur Verfügung stellt, der es in Zukunft möglich macht, neue Authentisierungsprotokolle hinzuzufügen, ohne andere Teile der Open eCard App ändern zu müssen.
- *Crypto*
  Das Crypto-Modul vereinheitlicht den Zugriff auf kryptografische Funktionen. Durch die Verwendung der Java Cryptography Architecture [JCA] kann zudem die konkrete Implementierung der Cryptographic Service Provider leicht gewechselt werden.
- *Grahpical User Interface (GUI)*
  Die GUI ist durch eine allgemeine Schnittstelle eingebunden und somit einfach austauschbar. Dies macht es möglich, Plattformspezifische GUI-Implementierungen bereitzustellen, während die anderen Module der Open eCard App nicht verändert werden müssen.
- *Security Assertion Markup Language (SAML)*
  Diese Komponente liefert Support für das SAML Enhanced Client and Proxy (ECP) Profile [SAML-ECP], das es möglich macht, einen *AuthnRequest* via PAOS-Binding [PAOS-v2.0] zu empfangen und die eID-basierte Authentisierung mit einem passenden Identity Provider zu starten. Verglichen mit dem Web Browser Single Sign-On (SSO) Profile, das in [BSI-TR-03130] verwendet wird, führt die Unterstützung des ECP-Profils zu einem weniger komplexen Protokollablauf, der insbesondere auch einfacher abzusichern ist.
- *Electronic Signatures (eSign)*
  Diese Komponente macht es möglich, mit der in [BSI-TR-03112] definierten und auf [OASIS-DSS] basierenden Schnittstelle, fortgeschrittene elektronische Signaturen gemäß [ETSI-101733], [ETSI-101903] und [ETSI-102778] zu erzeugen.
- *Dispatcher*
  Der Dispatcher liefert einen zentralen Einstiegspunkt zur Vermittlung eingehender und ausgehender Nachrichten. Durch diese Zentralisierung sorgt der Dispatcher für eine Minimierung des Java-Codes und einer Reduktion der Komplexität der Open eCard App.
- *Transport*
  Die Transportkomponente kapselt die verschiedenen Bindings (z. B. [PAOS-v2.0], [SOAP-v1.1]) und Transportprotokolle, wie z. B. http und Websockets.
- *Browser Integration*
  Damit die Open eCard App bei Aufruf einer entsprechend vorbereiteten Webseite automatisch starten kann, wird ein mit dem Browser verbundener Mechanismus benötigt, der die Applikation startet und entsprechende Verbindungs-Parameter übermittelt (siehe Teil 7 von [BSI-TR-03112]). Darüber hinaus sollen hier zukünftig auch die von den weit verbreiteten Browsern implementierten Standard-Schnittstellen, wie z. B. [PKCS#11], unterstützt werden.

2.3 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 eine bewusst einfach gehaltene Schnittstelle in beliebige Cloud- und Webapplikationen integriert werden. Wie in [HHR+11] näher erläutert, enthält diese Schnittstelle eine einzige Funktion: Mit der *Authenticate*-Funktion kann ähnlich wie in [STORK-API] eine Authentisierung entsprechender Güte (*Policy*) und eine Folge von Identitätsattributen (Attribute) angefordert werden.

2.4 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[1], elektronische Gesundheitskarte, Heilberufsausweis, Bank- und Signaturkarten und andere Europäische Bürgerkarten) über einfache und einheitliche Schnittstellen zur sicheren Authentisierung in Cloud-basierten Anwendungen genutzt werden.

Hierbei soll der eID-Broker längerfristig zwei unterschiedliche Betriebsmodi unterstützen:

- *Dispatcher Mode*
  In diesem vergleichsweise einfachen Betriebsmodus fungiert der eID-Broker nur als Vermittler (Dispatcher) und bestimmt einen geeigneten eID-Service, der sodann die Authentisierung des Benutzers durchführt und eine entsprechende Assertion erzeugt, die vom Cloud Service konsumiert werden kann.
- *Claims Transformer Mode*
  In diesem technisch anspruchsvolleren Betriebsmodus führt der eID-Broker bei Bedarf verschiedene Authentisierungsergebnisse und Attribute von mehreren eID-Services zusammen und transformiert die jeweiligen Attribute und Assertions in ein für den Cloud Service geeignetes Format. Bei den vom eID-Broker in diesem Betriebsmodus ausgestellten Credentials können wiederum die folgenden beiden Ausprägungen unterschieden werden:
  - *Session Credential*
    Hierbei kann es sich beispielsweise um eine SAML- [SAML] oder OpenID-Assertion [OpenID]) handeln, die nur eine kurze Lebensdauer hat und dem Cloud Service mehr oder weniger direkt präsentiert wird.
  - *Attributbasiertes Credential*
    In diesem Fall ist das vom eID-Broker ausgestellte Attribut-basiertes Credential (vgl. [Idemix], [U-Prove], [BBC08] und [KLN+11]) über einen vergleichsweise langen Zeitraum gültig und kann vom Benutzer zukünftig selbstbestimmt für die Authentisierung oder für den datensparsamen Nachweis der im Credential enthaltenen Identitätsattribute bei den angeschlossenen Cloud Services verwendet werden.

2.5 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-API]) 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-API], [CEN15480-3]) eine übergreifende Schnittstelle abgeleitet werden, über die die verschiedenen eID-Services und Authentisierungsdienste integriert werden können.

3 Zusammenfassung und 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

[1] Bei der Nutzung des nPA sind die rechtlichen Rahmenbedingungen des Personalausweisrechts zu beachten. Weitere Informationen hierzu finden sich in beispielsweise in [HoMö11] und [HHR+11].

Mechanismen zur sicheren Verwaltung des geistigen Eigentums mittels Enterprise Rights Management Systemen. Die hierfür notwendigen eID-Services werden über den eID-Broker gebündelt, wodurch innovative Geschäfts- und Vertragsmodelle ermöglicht werden, durch die diese Identitätsmanagementinfrastrukturen wirtschaftlich, rechtssicher und nutzerfreundlich angeboten 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 sind Anbieter von eID-Services und Cloud-basierten Anwendungen sowie Herausgeber von elektronischen Ausweisen, die an einer Mitwirkung im SkIDentity-Projekt interessiert sind, herzlich eingeladen, mit den Autoren dieses Papiers Kontakt aufzunehmen. Weitere Informationen über das SkIDentity-Projekt werden zu gegebener Zeit über http://www.skidentity.de/ bereitgestellt.

Literatur

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

[BBC08] D. Bauer, D. Blough M., D. Cash: *Minimal information disclosure with efficiently verifiable credentials*, Proceedings of 4th ACM workshop on Digital identity management (DIM '08), New York, 2008, S. 15–24

[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

[BSI-MSACC] BSI: *Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter, Mindestsicherheitsanforderungen in der Informationssicherheit*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile

[BSI-TR3110] BSI: *Advanced Security Mechanism for Machine Readable Travel Documents – Extended Access Control* (EAC), BSI TR-03110, Version 2.05, https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html

[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

[CEN15480-3] CEN/TS 15480-3: *Identification card systems – European Citizen Card – Part 3: European Citizen Card Interoperability using an application interface*, Technical Specification, 2010

[EHP+10] D. Eske, D. Hühnlein, S. Paulus, J. Schmölz, T. Wich, T. Wieland: *OpeneGK – Benutzerfreundliche und sichere Authentisierung für Mehrwertdienste im Gesundheitswesen*, in Tagungsband »perspeGKtive 2010«, GI LNI 174, 2010, Seiten 83–103, http://www.ecsec.de/pub/openeGK.pdf

[eID-Service] Kompetenzzentrum neuer Personalausweis: *eID-Service-Anbieter*, 2012, 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

[ETSI-101733] ETSI: *CMS Advanced Electronic Signatures (CAdES),* ETSI TS 101 733, Version 1.8.1. http://pda.etsi.org/pda/queryform.asp , December 2009

[ETSI-101903] ETSI: *Technical Specification XML Advanced Electronic Signatures (XAdES),* ETSI TS 101 903, Version 1.4.1, http://pda.etsi.org/pda/queryform.asp, June 2009

[ETSI-102778] ETSI: PDF *Advanced Electronic Signature Profiles*, ETSI TS 102 778, part 1–5, http://pda.etsi.org/pda/queryform.asp, 2009

[HHH12] G. Hornung, M. Horsch, D. Hühnlein: *Mobile Authentisierung und Signatur mit dem neuen Personalausweis*, erscheint in DuD 03/2012

[HHR+11] D. Hühnlein, G. Hornung, H. Roßnagel, J. Schmölz, T. Wich, J. Zibuschka: *SkIDentity – Vertrauenswürdige Identitäten für die Cloud*, D-A-CH Security 2011, SS. 296–304

[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

[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

[HSW11] D. Hühnlein, J. Schmölz, T. Wich: *Sicherheitsaspekte beim Chipkarten-basierten Identitätsnachweis*, erscheint in »Daten- und Identitätsschutz«, Springer-Verlag, 2012

[Idemix] J. Camenisch, E. van Herreweghen: *Design and implementation of the ide-mix anonymous credential system*, presented at the ACM conference on Computer and communications security, New York, 2002

[ISO24727-3] ISO/IEC: *Identification Cards – Integrated Circuit Cards Programming Interfaces – Part 3: Application Interface*, ISO/IEC 24727-3, International Standard, 2008

[ISO24727-4] ISO/IEC: *Identification Cards – Integrated Circuit Cards Programming Interfaces – Part 4: Application programming interface (API) administration*, ISO/IEC 24727-4, International Standard, 2008

[JCA] Oracle: *Java™ Cryptography Architecture (JCA) Reference Guide*, http://download.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html

[KLN+11] I. Krontiris, A. Lehmann, G. Neven, C. Paquin, H. Zwingelberg: *Architecture for Attribute-based Credential Technologies*, Deliverable D2.1, Dez. 2011, https://abc4trust.eu/download/ABC4Trust-D2.1-Architecture-V1.pdf

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

[OASIS-DSS] OASIS: *Digital Signature Service Core Protocols, Elements, and Bindings, Version 1.0*, OASIS Standard, via http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf

[OpeneCard] D. Hühnlein, J. Schmölz & al.: *On the design and implementation of the Open eCard App*, Tagungsband »Sicherheit 2012«, GI LNI, 2012

[OpenID] OpenID Foundation: *OpenID Authentication 2.0. Final*, December 5, 2007, http://openid.net/specs/openid-authentication-2_0.html

[PAOS-v2.0] Liberty Alliance Project: *Liberty Reverse HTTP Binding for SOAP Specification*, Version v2.0, via http://www.projectliberty.org/liberty/content/download/909/6303/file/liberty-paos-v2.0.pdf

[PKCS#11] RSA Laboratories: *PKCS #11 Base Functionality v2.30: Cryptoki* – Draft 4, 10 July 2009

[SAML] S. Cantor, J. Kemp, R. Philpott, E. 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

[SAML-ECP] S. Cantor & al.: *SAML V2.0 Enhanced Client or Proxy Profile Version 2.0*, Working Draft 02, 19.02.2011, http://www.oasis-open.org/committees/download.php/41209/sstc-saml-ecp-v2.0-wd02.pdf

[SHJ+11] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, L. Lo Iacono: *All Your Clouds are Belong to us – Security Analysis of Cloud Management Interfaces*, In Proceedings of the ACM Cloud Computing Security Workshop (CCSW), 2011, http://www.nds.rub.de/media/nds/veroeffentlichungen/2011/10/22/AmazonSignatureWrapping.pdf

[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

[SOAP-v1.1] W3C Note: *Simple Object Access Protocol (SOAP)* 1.1, 8 May 2000, via http://www.w3.org/TR/2000/NOTE-SOAP-20000508

[STORK-API] J. Alcalde-Moraño, J. L. Hernández-Ardieta, A. Johnston, D. Martinez, B. Zwattendorfer: STORK Deliverable D5.8.1b – Interface Specification, 08.09.2009, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=960

[U-Prove] Microsoft Inc.: *Microsoft U-Prove Community Technology Preview R2*, https://connect.microsoft.com/site1188

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

[Wich11] T. Wich: *Tools for automated utilisation of Smart-Card Descriptions*, Master Thesis, Hochschule Coburg, 2011