Detlef Hühnlein, Manuel Bach

Die Standards des eCard-API-Frameworks

Eine deutsche Richtlinie im Konzert internationaler Normen

Die eCard-Strategie der Bundesregierung zielt auf die breite Verwendbarkeit der im Rahmen der verschiedenen Kartenprojekte der Bundesverwaltung ausgegebenen und genutzten Chipkarten ab. Eine besondere Rolle bei der Realisierung dieses Zieles spielt das eCard-API-Framework, durch das ein einfacher und einheitlicher Zugriff auf die Funktionen dieser unterschiedlichen Chipkarten ermöglicht wird. Um die nationale und internationale Akzeptanz dieses Rahmenwerkes nachhaltig sicherzustellen, wurde bei der Spezifikation des eCard-API-Frameworks auf international anerkannte Standards zurückgegriffen. Der Beitrag gibt einen kompakten Überblick über das eCard-API-Framework und die wesentlichen damit zusammenhängenden Standards.

1 Einleitung

Durch die eCard-Strategie der Bundesregierung [eCard-PM, Kowa07] werden die Kartenprojeke der Bundesverwaltung – die elektronische Gesundheitskarte (eGK), der elektronische Personalausweis, das JobCard-Verfahren (elektronischer Einkommensnachweis, ELENA) und die elektronische Steuererklärung (ELSTER) – eng aufeinander abgestimmt. Gleiche Standards und die breite Verwendbarkeit der Chipkarten für den elektronischen Geschäftsverkehr sollen Effizienzgewinne und Kosteneinsparungen zum Nutzen von Bürgerinnen und Bürgern, Wirtschaft und Verwaltung gewährleisten. Eine zentrale Rolle bei der Umsetzung der eCard-Strategie spielt das eCard-API-Framework [BSI-TR03112], durch das ein einfacher und einheitlicher Zugriff auf die Funktionen der unterschiedlichen Chipkarten, die in den Kartenprojekten der Bundesverwaltung ausgegeben oder genutzt werden, ermöglicht wird.

Um die nationale und internationale Akzeptanz des eCard-API-Frameworks nachhaltig sicher zu stellen, wurde bei der Spezifikation wo immer dies möglich war auf international anerkannte Standards zurück gegriffen. Umgekehrt wurden die innovativen Elemente und die für den Erfolg der eCard-Strategie wesentlichen Aspekte des eCard-API-Frameworks (z.B. die Nutzung von Webservice-Schnittstellen und CardInfo Files (vgl. [HuBa07a]) der internationalen Standardisierung zugeführt.

Die folgenden Abschnitte geben einen kompakten Überblick über das eCard-API-Framework und beleuchten insbesondere die wichtigsten damit zusammenhängenden Standards. Nach der Darstellung der gesamten Architektur in Abschnitt 2 wird in den folgenden Abschnitten 3 bis 6 näher auf die einzelnen Schichten des eCard-API-Frameworks und die wesentlichen darin unterstützten Standards eingegangen. In Abschnitt 7 werden schließlich die wichtigsten Aspekte des Beitrages kurz zusammengefasst.

2 Architektur des eCard-Frameworks

Das Ziel des eCard-API-Frameworks ist das Bereitstellen einer einfachen und homogenen Schnittstelle, um in den verschiedenen Anwendungen eine einheitliche Nutzung der unterschiedlichen Chipkarten (eCards) zu ermöglichen. Damit hierbei auch verschiedenste Anwendungsszenarien (vgl. [HuBa07b], Abschnitt 2.4) leicht unterstützt werden können, wurde – wie in Abbildung 1 ersichtlich – eine aus mehreren Schichten bestehende Architektur gewählt:

- Application Layer
- Identity Layer
- Service Access Layer
- Terminal Layer

Hierbei sind die jeweiligen Schnittstellen als Webservices gemäß [WSDL] spezifiziert. Die Funktionalität der einzelnen

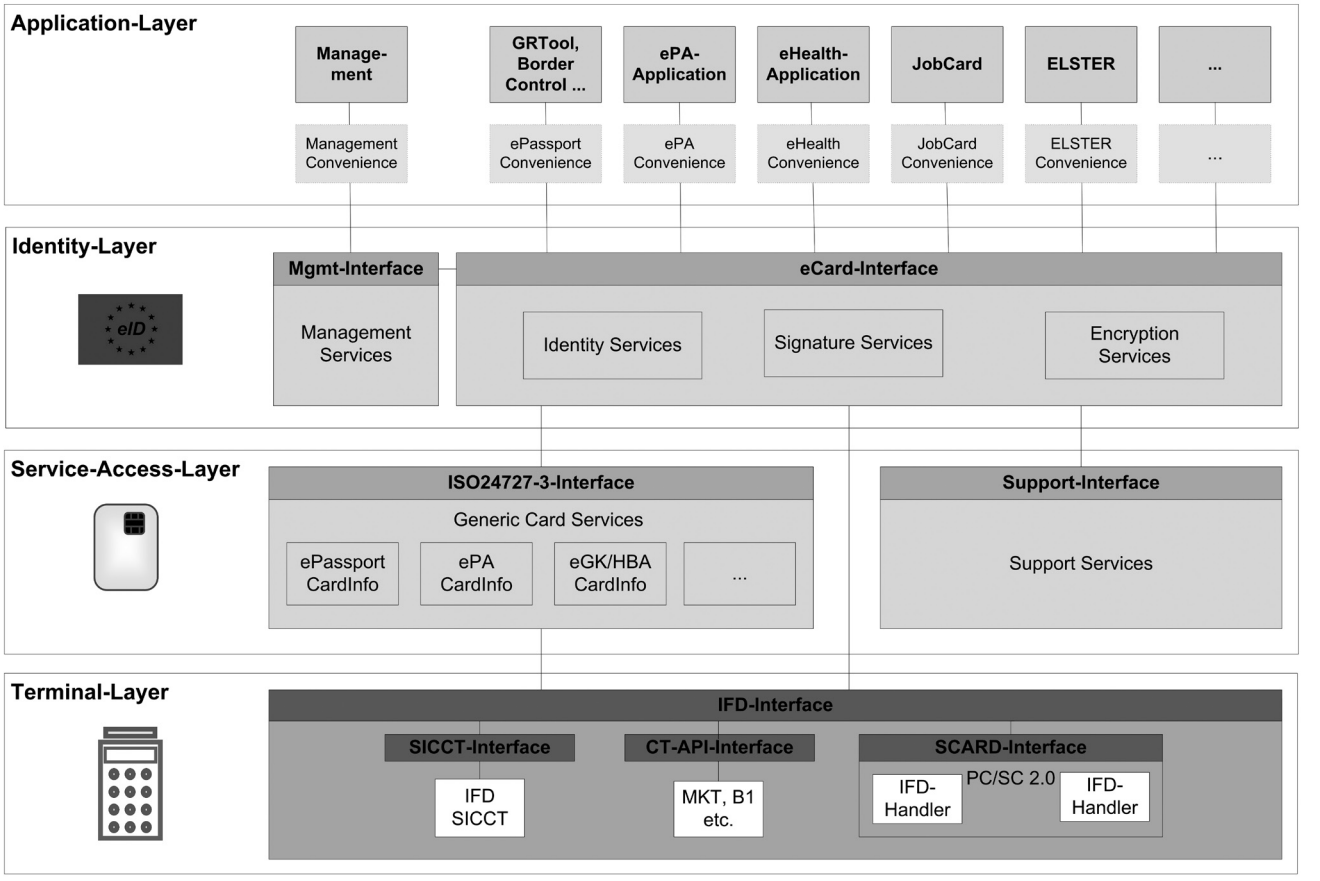
Dr. Detlef Hühnlein

ist seit mehr als zehn Jahren bei der secunet Security Networks AG – u.a. im Bereich Chipkartentechnologie – tätig.
E-Mail: detlef.huehnlein@secunet.com

Manuel Bach

Manuel Bach ist seit 2005 im Referat Industriekooperation für das BSI tätig und u.a. mit der Entwicklung des eCard-API-Frameworks betraut.
E-Mail: manuel.bach@bsi.bund.de

Abbildung 1: Die Architektur des eCard-API-Frameworks



Schichten wird in den folgenden Abschnitten kurz erläutert. Eine ausführlichere Darstellung findet sich in der Spezifikation des eCard-API-Frameworks [BSI-TR03112].

3 Application Layer

Im Application Layer befinden sich die verschiedenen Anwendungen, die das eCard-API-Framework für den Zugriff auf die eCards und damit verbundene Funktionen nutzen wollen. In dieser Schicht können auch weitere anwendungsspezifische „Convenience-Schnittstellen" existieren, in denen wiederkehrende Aufruffolgen in applikationsnahen Aufrufen gekapselt werden. Diese Schnittstellen sind jedoch derzeit nicht Gegenstand von [BSI-TR03112].

4 Identity Layer

Der Identity Layer enthält das *Management Interface* und das *eCard Interface* und realisiert Funktionen zur Verwaltung und Nutzung elektronischer Identitäten, die für den Aufbau gesicherter Netzwerkverbindungen und für den Schutz von Dokumenten mittels Signatur und Verschlüsselung genutzt werden.

4.1 Management Interface

Im *Management-Interface* (siehe [BSI-TR03112], Teil 3) werden wesentliche Management-Funktionen abgebildet. Hierzu gehört beispielsweise die Verwaltung

- von Zugriffskontrolllisten für Funktionen des Frameworks,
- von (vertrauenswürdigen) Zertifikaten (ggf. unter Verwendung von Trust-Service Status Lists gemäß [ETSI-102231]),
- der über CardInfo-Files (vgl. [HuBa07a] unterstützten Chipkartentypen,
- der vom eCard-API-Framework genutzten Zeitstempel-, Verzeichnis-, Management- und Updatedienste und
- der Standardparameter, durch die das generelle Verhalten des eCard-API-Frameworks bestimmt wird.

4.2 eCard Interface

Das *eCard Interface* (siehe [BSI-TR03112], Teil 2) enthält [DSS-Core, DSS-AdES, DSS-SigG]-konforme Funktionen zur Erstellung und Prüfung von Signaturen und Zeitstempeln in verschiedenen Formaten, wie z.B. [RFC3852, ETSI-101733, XML-DSig, ETSI-101903, PDF(v1.4), RFC3161, DSS-Core, RFC4998] sowie Funktionen zur vertrauenswürdigen Darstellung von zu signierenden Dokumenten und Prüfergebnissen. Für eine Signaturgesetz-konforme und revisionssichere Dokumentation der einzelnen Schritte bei einer Signaturprüfung können ausführliche Prüfberichte angefordert werden, wie sie derzeit in der DSS-X-Arbeitsgruppe von OASIS standardisiert werden (vgl. [DSS-VR]).

In diesem Zusammenhang wird derzeit auch über ein weiteres Profil der [DSS-Core]-Schnittstelle für Zwecke der langfristig beweiskräftigen Archivierung von signierten Dokumenten diskutiert.

Außerdem existieren an [DSS-EP] angelehnte Funktionen zur Verschlüsselung und Entschlüsselung von Dokumenten gemäß [RFC3852, XML-Enc] sowie darü-

ber hinaus die generische Funktion `GetCertificate` zum Download von Zertifikaten (z.B. gemäß des in Teil 2 von [ISIS-MTT] spezifizierten „Simple Enrollment Protocol").

Da diese Funktion mit beliebigen Protokollen genutzt werden kann, ist es zukünftig möglich, weitere anbieter- oder kartenspezifische Protokolle für das Nachladen von qualifizierten Zertifikaten zu ergänzen. In ähnlicher Form können auch spezifische Protokolle für den Bezug von CV-Zertifikaten für Authentisierungsterminals gemäß [BSI-TR-03110] oder sonstige in [NKB08] geforderten PKI-Funktionen ergänzt werden.

5 Service Access Layer

Der Service Access Layer enthält das *Support-Interface* und das *ISO24727-3-Interface*, über das auf beliebige Chipkarten und andere „Smart Devices" mittels generischer Funktionen zugegriffen werden kann.

5.1 ISO24727-3 Interface

Das *ISO24727-3 Interface* (siehe [BSI-TR03112], Teil 4) ist eine Webservice-basierte Umsetzung des gleichnamigen Standards [ISO24727-3]. Diese Schnittstelle enthält Funktionen, um

- (kryptographisch geschützte) Verbindungen zu Chipkarten herzustellen,
- Chipkartenapplikationen zu verwalten,
- Daten zu lesen oder zu schreiben,
- kryptographische Operationen auszuführen sowie
- das entsprechende Schlüsselmaterial (in Form von so genannten „Differential-Identities") und
- entsprechende Zugriffsrechte zu verwalten.

Neben dem „Generic Card Interface" aus [ISO24727-2] und den dafür vorgesehenen, [ISO7816-15]-basierten Mechanismen unterstützt das eCard-API-Framework auch die zusätzlichen Kommandos der „European Citizen Card" gemäß [CEN15480-2] und – über den CardInfo-Ansatz aus [HuBa07a] – auch Chipkarten, auf denen keine selbstbeschreibenden Informationen abgelegt sind. Hierdurch können sowohl elektronische Gesundheitskarten als auch beliebige Signaturkarten unterstützt werden. Da alle Funktionen, die „Differential-Identities" nutzen oder verwalten, über protokollspezifische Object Identifier parametrisiert sind, ist es möglich, über die existierende Schnittstelle auch alle zukünftigen „Chipkartenprotokolle" oder beliebige andere „Smart Devices" (z.B. Trusted Platform Modules, Internet Smart Cards, Secure Memory Cards oder Mobiltelefone) zu unterstützen.

5.2 Support Interface

Das *Support Interface* (siehe [BSI-TR03112], Teil 5) enthält eine Reihe von unterstützenden Funktionen – beispielsweise zur Validierung von XML-Dokumenten oder der Codierung und Decodierung von Daten gemäß [RFC1952, RFC3548].

6 Terminal Layer

Der Terminal Layer enthält das *IFD-Interface* (siehe [BSI-TR03112], Teil 6), das inzwischen in [ISO24727-4] eingebracht wurde. Diese Schnittstelle, die in etwa das „kleinste gemeinsame Vielfache" der [PC/SC]- und der (für das deutsche Gesundheitswesen wichtigen) [SICCT]-Spezifikation ist, übernimmt die Generalisierung von konkreten Lesertypen und verschiedenen Schnittstellen sowie die technische Kommunikation mit der Chipkarte. Somit ist es für die darüber liegenden Schichten weder von Bedeutung, ob die eCard via [PC/SC], einem [SICCT]-Leser oder einem herstellerspezifischen Interface angesprochen wird, noch, ob sie kontaktbehaftet oder kontaktlos ist.

7 Fazit und Ausblick

Das eCard-API-Framework umfasst eine Reihe von inzwischen harmonisch aufeinander abgestimmten internationalen Standards [ISO24727, DSS-Core] zur Authentisierung und elektronischen Signatur und bildet das technische Fundament für eine erfolgreiche Realisierung der eCard-Strategie der Bundesregierung. Insbesondere soll das eCard-API-Framework für jeweils rund 80 Millionen elektronische Gesundheitskarten und elektronische Personalausweise eingesetzt werden. Daneben unterstützt das eCard-API-Framework aber auch viele andere deutsche Chipkartenprojekte mit großer Wirkbreite (z.B. im Umfeld von Bank- und Signaturkarten, elektronischen Aufenthaltskarten, elektronischen Visa-Dokumenten, des elektronischen Reisepasses oder des Dienstausweises des Bundesinnenministeriums) sowie andere international bedeutsame elektronische Identifikationskarten – z.B. im Umfeld der „European Citizen Card".

Da hiermit ein entsprechend attraktiver Markt verbunden ist, ist es nicht verwunderlich, dass bereits eine Vielzahl deutscher Unternehmen die zeitnahe Umsetzung des eCard-API-Frameworks angekündigt haben (vgl. [T7-PM]). Da inzwischen auch ein erstes Zertifizierungsverfahren gestartet wurde [BSI-PM] und die Spezifikation des eCard-API-Frameworks die Grundlage sowohl für die Middleware- als auch die Gateway-Lösung im von der Europäischen Union geförderten „Large Scale Pilot" Projekt „Secure IdentiTy AcrOss BoRders AcKnowledged (STORK)" bilden soll, ist zu erwarten, dass in nicht allzu ferner Zukunft nachweislich sichere, deutsche Implementierungen des eCard-API-Framworks auch im internationalen Markt eine rege Nachfrage erfahren werden.

Damit die Interoperabilität der verschiedenen Implementierungen nachhaltig sichergestellt werden kann, sind zukünftig auch entsprechende Konformitätstests unter Berücksichtigung von [ISO24727-5] vorgesehen.

Literatur

[BSI-PM] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Erste Konformitätsprüfung für eCard-Middleware gestartet*, Pressemitteilung vom 16.07.2007, http://www.bsi.de/presse/pressinf/160707_eCard-Middleware.htm, 2007

[BSI-TR-03110] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Advanced Security Mechanism for Machine Readable Travel Documents Extended Access Control (EAC)*, Technical Directive (BSI-TR-03110), Version 2.0 Release Candidate, 2008

[BSI-TR03112] Bundesamt für Sicherheit in der Informationstechnik (BSI): *eCard-API-Framework*, Technische Richtlinie (TR) des BSI Nr. 03112. http://www.bsi.de/literat/tr/tr03112/index.htm, 2008

[CEN15480-2] Comité Européen de normalisation (CEN): *Identification card systems – European Citizen Card – Part 2: Logical data structures and card services*, CEN/TS 15480-2 (Vornorm), 2007

[DSS-AdES] Juan Carlos Cruellas: *Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 1.0*, OASIS Standard, http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-AdES-spec-v1.0-os.pdf, 2007

[DSS-Core] Stefan Drees: *Digital Signature Service Core Protocols, Elements, and Bindings, Version 1.0*, OASIS Standard, http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf, 2007

[DSS-EP] Clemens Orthacker: *Proposal for an Encryption Profile for OASIS DSS*. A-SIT Contribution to DSS-X, 20. September 2007. http://www.oasis-open.org/committees/download.php/25384/oasis-dss_profile-encryption_A-SIT_v0.1.doc , 2007

[DSS-SigG] Andreas Kühne: *German Signature Law Profile of the OASIS Digital Signature Service Version 1.0*, OASIS Standard. http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles_german_signature_law-spec-v1.0-os.pdf, 2007

[DSS-VR] Ingo Henkel, Detlef Hühnlein: *Profile for comprehensive multi-signature verification reports for OASIS Digital Signature Services Version 1.0*, OASIS Working Draft, May 5, 2008, http://www.oasis-open.org/apps/org/ workgroup/dss-x/document.php?document_id=28182, 2008.

[eCard-PM] Bundesregierung: *eCard-Strategie der Bundesregierung*. Pressemitteilung vom 09.03.2005. http://www.bmwi.de/Navigation/Presse/pressemitteilungen,did=60006.html , 2005

[ETSI-101733] ETSI: *Electronic Signatures and Infrastructures (ESI) – Electronic Signature Formats*, ETSI Technical Specification TS 101 733, Version 1.5.1. http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_101733v010501p.pdf, Dezember 2003

[ETSI-101903] ETSI: *Technical Specification XML Advanced Electronic Signatures (XAdES)*, ETSI Technical Specification TS 101 903, Version 1.3.2. http://webapp.etsi.org/action/PU/20060307/ts_101903v010302p.pdf, März 2006

[ETSI-102231] ETSI: *Provision of harmonized Trust-service status information*, ETSI Technical Specification TS 102 231, Version 2.1.1. http://webapp.etsi.org/exchangefolder/ts_102231v020101p.pdf, März 2006

[HuBa07a] Detlef Hühnlein, Manuel Bach: *How to Use ISO/IEC 24727-3 with Arbitrary Smart Cards*, TrustBus 2007, LNCS 4657, Springer, Seiten 280–289, 2007, http://www.ecsec.de/pub/2007_TrustBus.pdf

[HuBa07b] Detlef Hühnlein, Manuel Bach: *From the eCard-API-Framework towards a comprehensive eID-framework for Europe*, ISSE/SECURE 2007, Vieweg, Seiten 276–286, 2007,http://www.ecsec.de/pub/2007_ISSE.pdf

[ISIS-MTT] T7 e.V. und TeleTrusT e.V.: *ISIS-MTT-Spezifikation*, Version 1.1. http://www.isis-mtt.t7-isis.org/uploads/ media/ISIS-MTT_Core_Specification_v1.1_03.pdf, März 2004

[ISO24727-2] ISO/IEC 24727-2: *Identification cards – Integrated circuit cards programming interfaces – Part 2: Generic Card Interface*, Final Draft International Standard (2007-10-25), 2007

[ISO24727-3] ISO/IEC 24727-3: *Identification cards – Integrated circuit cards programming interfaces – Part 3: Application programming interface*, Final Committee Draft (2007-09-14), 2007

[ISO24727-4] ISO/IEC 24727-4: *Identification cards – Integrated circuit cards programming interfaces – Part 4: API Administration*, Final Committee Draft (2007-10-31), 2007

[ISO24727-5] ISO/IEC 24727-5: *Identification cards – Integrated circuit cards programming interfaces – Part 5: Testing procedures*, Working Draft, 2006

[ISO7816-15] ISO/IEC 7816-15: *Identification cards – Integrated circuit cards – Part 15: Cryptographic information application*, International Standard, 2004

[Kowa07] Bernd Kowalski: *Die eCard-Strategie der Bundesregierung im Überblick*, in BIOSIG 2007: Biometrics and Electronic Signatures, Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, LNI 108, Seiten 87–96, 2007

[NKB08] E. Neumann, A. Klenk, H.-J. Bierschenk: *Das TeleTrusT PKI-Referenzprojekt*, in IT-Sicherheit, 2008

[PC/SC] PC/SC Workgroup: *PC/SC Workgroup Specifications 2.0*, Part 1-10. http://pcscworkgroup.com, 2005.

[PDF(v1.4)] Adobe Systems Inc.: *PDF Reference – Third Edition – Adobe Portable Document Format Version 1.4*. Addison-Wesley, ISBN 0-201-75839-3. http://partners.adobe.com/public/developer/en/pdf/PDFReference.pdf, November 2001

[RFC1952] P. Deutsch: *GZIP file format specification version 4.3*, Request For Comments – RFC 1952. http://www.ietf.org/rfc/rfc1952.txt, Mai 1996.

[RFC3161] C. Adams, P. Cain, D. Pinkas, R. Zuccherato: *Internet X.509 Public Key Infrastructure – Time-Stamp Protocol (TSP)* Request For Comments – RFC 3161. http://www.ietf.org/rfc/rfc3161.txt, August 2001.

[RFC3548] S. Josefsson: *The Base16, Base32, and Base64 Data Encodings*, Request For Comments – RFC 3548, http://www.ietf.org/rfc/rfc3548.txt, Juli 2003.

[RFC3852] R. Housley: *Cryptographic Message Syntax (CMS)*, Request For Comments – RFC 3852, http://www.ietf.org/rfc/rfc3852.txt, Juli 2004

[RFC4346] T. Dierks, E. Rescorla: *The Transport Layer Security (TLS) Protocol Version 1.1*, Request For Comments – RFC 4346. http://www.ietf.org/rfc/rfc4346.txt, April 2006

[RFC4998] T. Gondrom, R. Brandner, U. Pordesch: *Evidence Record Syntax (ERS)*, Request For Comments – RFC 4998. http://www.ietf.org/rfc/rfc4998.txt, August 2007.

[SICCT] TeleTrusT: *SICCT-Spezifikation*. Version 1.1.0 vom 19.12.2006. http://www.teletrust.de/fileadmin/files/publikationen/Spezifikationen/SICCT_Spezifikation_1.10.pdf, 2006

[T7-PM] Arbeitsgemeinschaft der deutschen Trustcenterbetreiber (T7 e.V.): *Software-Anwendungen bekommen Dolmetscher für die qualifizierte elektronische Signatur*, Pressemitteilung vom 12.12.2007. http://www.where2sign.de/uploads/media/PM-eCARD_API_QES_121207.pdf, 2007

[WSDL] W3C Recommendation: *Web Services Description Language (WSDL)*, Version 1.1, via http://www.w3.org/TR/wsdl

[XML-DSig] D. Eastlake, J. Reagle, D. Solo: *XML-Signature Syntax and Processing*, W3C Recommendation, http://www.w3.org/TR/xmldsig-core/, Februar 2002

[XML-Enc] D. Eastlake, J. Reagle: *XML Encryption Syntax and Processing*. W3C Recommendation. http://www.w3.org/TR/xmlenc-core/, December 2002