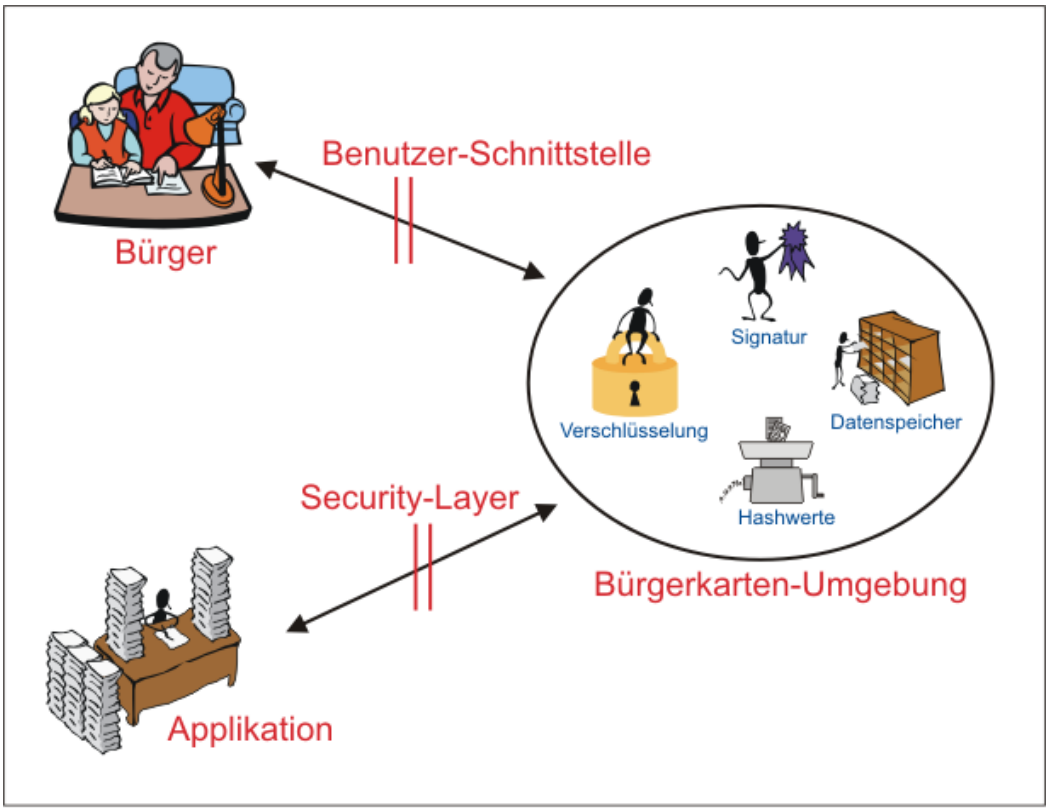
Einführung in die österreichische Bürgerkarte		Konvention 1.2.0 Empfehlung
Kurzbeschreibung	Das vorliegende Dokument gibt eine Einführung in die österreichische Bürgerkarte.	
Autoren:	Arno Hollosi Gregor Karlinger Thomas Rössler Martin Centner et al.	Projektteam/Arbeitsgruppe AG Bürgerkarte
Datum:	14.5.2004	

Inhaltsverzeichnis

1. Modell

Vorbemerkung: Zur besseren Lesbarkeit wurde in diesem Dokument auf geschlechtsneutrale Formulierungen verzichtet. Die verwendeten Formulierungen richten sich jedoch ausdrücklich an beide Geschlechter.

Die *Bürgerkarte* ist ein Modell, dass eine Reihe von unterschiedlichen Funktionen für die sichere Abwicklung von E-Government und E-Commerce zur Verfügung stellt. Im Wesentlichen können mit der *Bürgerkarte* elektronische Signaturen über elektronische Dokumente angefertigt und überprüft, elektronische Dokumente ver- und entschlüsselt, Hashwerte über elektronische Dokumente berechnet und überprüft, sowie Daten in einen Datenspeicher geschrieben sowie von diesem gelesen werden.



Das Modell der Bürgerkarte

Das Bild zeigt die bei einer Verwendung der *Bürgerkarte* Beteiligten. Es sind dies die *Bürgerkarten-Umgebung*, welche die oben erwähnten Funktionen kapselt, der *Bürger*, der diese Funktionen verwendet, sowie die *Applikation*, welche die *Bürgerkarten-Umgebung* so ansteuert, dass der *Bürger* die Funktionen bequem verwenden kann.

Außerdem erwähnt das Bild zwei Schnittstellen, deren detaillierte Beschreibung die Hauptaufgabe der vorliegenden Spezifikationen ist: Die *Benutzer-Schnittstelle* regelt die Kommunikation zwischen dem *Bürger* und der *Bürgerkarten-Umgebung*, während die Schnittstelle *Security-Layer* die Interaktion zwischen der *Applikation* und der *Bürgerkarten-Umgebung* festschreibt.

Das nachfolgende Glossar beschreibt die Schnittstellen und Beteiligten im Detail.

Glossar

Glossar

Applikation

Jenes Programm, das Anfragen an die *Bürgerkarten-Umgebung* über den *Security-Layer* richtet und die entsprechenden Antworten entgegennimmt und auswertet.

Benutzer-Schnittstelle

Jene Schnittstelle, über die der *Bürger* mit der *Bürgerkarten-Umgebung* kommuniziert. Über diese Schnittstelle wird einerseits die Benutzerinteraktion abgewickelt, die gegebenenfalls zur Abwicklung eines Befehls des *Security-Layers* notwendig ist (z.B. die Anzeige eines zu signierenden Dokuments beim Befehl zur Erzeugung einer XML-Signatur); andererseits kann der *Bürger* über diese Schnittstelle seine *Bürgerkarten-Umgebung* nach seinen persönlichen Bedürfnissen konfigurieren (z.B. kann er Einstellungen zum Zugriffsschutz auf seine Infoboxen verändern). Die Vorgaben an die *Benutzer-Schnittstelle* sind in Minimale Umsetzung des Security-Layers geregelt.

Bürger

Jene Person, die die Funktionen der *Bürgerkarten-Umgebung* für die sichere Abwicklung von E-Government oder E-Commerce verwenden möchte. Die Ansteuerung der *Bürgerkarten-Umgebung* erfolgt in der Regel nicht durch den *Bürger* selbst, sondern durch die *Applikation*, welche die E-Government oder E-Commerce Anwendung repräsentiert.

Bürgerkarte

Laut [E-GovG], §10 ZI 10 ist die *Bürgerkarte* „die unabhängig von der Umsetzung auf unterschiedlichen technischen Komponenten gebildete logische Einheit, die eine elektronische Signatur mit einer Personenbindung (§ 4 Abs. 2) und den zugehörigen Sicherheitsdaten und -funktionen sowie mit allenfalls vorhandenen Vollmachtsdaten verbindet“. Im Sinne der in den Spezifikationen zur österreichischen Bürgerkarte gebrauchten Terminologie ist die *Bürgerkarten-Umgebung* die Implementierung der logischen Einheit *Bürgerkarte*.

Bürgerkarten-Umgebung

Jenes Programm bzw. jener Dienst, der die Funktionalität der *Bürgerkarte* zur Verfügung stellt. Grundsätzlich vorstellbar ist die Ausführung als Programm, das lokal am Rechner des *Bürgers* läuft (*lokale Bürgerkarten-Umgebung*), oder als serverbasierter Dienst, der über das Internet angesprochen wird (*serverbasierte Bürgerkarten-Umgebung*). Die Interaktion mit diesem Programm bzw. Dienst wird über zwei Schnittstellen abgewickelt: Über die *Benutzer-Schnittstelle* sowie über den *Security-Layer*.

Hash-Eingangsdaten

Jene Daten, die für die Berechnung des Hash-Wertes für eine `dsig:Reference` verwendet werden. Sind für die `dsig:Reference` Transformationen angegeben, entsprechen diese Daten dem Ergebnis der letzten Transformation. Sind keine Transformationen spezifiziert, gleichen die Hash-Eingangsdaten den *Referenz-Eingangsdaten*.

Impliziter Transformationsparameter

Siehe Abschnitt 2.2.2.2, „Implizite Transformationsparameter“ in Die österreichische Bürgerkarte - Applikationsschnittstelle Security-Layer

Referenz-Eingangsdaten

Jene Daten, die sich aus der Auflösung der im Attribut `URI` der `dsig:Reference` angegebenen URI ergeben. Sind für die `dsig:Reference` Transformationen angegeben, werden diese Daten als Eingangsdaten zur Berechnung der ersten Transformation verwendet. Sind keine Transformationen spezifiziert, gleichen die Referenz-Eingangsdaten den *Hash-Eingangsdaten*.

Security-Layer

Jene Schnittstelle, über die die *Applikation* mit der *Bürgerkarten-Umgebung* kommuniziert. Das genaue Protokoll, das über diese Schnittstelle gesprochen werden kann, wird in Applikationsschnittstelle Security-Layer spezifiziert. Die möglichen Bindungen dieses Protokolls an Transportschichten wie HTTP oder TCP wird in Transportprotokolle Security-Layer geregelt.

Signaturmanifest

Siehe Abschnitt 2.2.2.2, „Implizite Transformationsparameter“ in Die österreichische Bürgerkarte - Applikationsschnittstelle Security-Layer .

2. Befehle

Dieser Abschnitt gibt einen Überblick über die Funktionen, welche die *Bürgerkarten-Umgebung* zur Verfügung stellt. Die Funktionen lassen sich im Wesentlichen in vier große Bereiche unterteilen:

1. Erstellen und Prüfen von elektronischen Signaturen;
2. Verschlüsselung und Entschlüsselung von elektronischen Dokumenten;
3. Berechnung und Überprüfung von Hashwerten über elektronische Dokumente;
4. Lesen und Schreiben von Daten aus einem bzw. in einen Datenspeicher.

2.1. Signatur

Der *Bürger* kann mit Hilfe der *Bürgerkarten-Umgebung* sowohl elektronische Dokumente signieren, als auch bestehende Signaturen über elektronische Dokumente prüfen.

Ein sehr wesentliches Merkmal der *Bürgerkarten-Umgebung* ist in beiden Fällen die Möglichkeit, dass der *Bürger* sich die gegenständlichen elektronischen Dokumente anzeigen lassen kann: Bei der Erstellung einer elektronischen Signatur kann er zuvor genau kontrollieren, welche Daten er tatsächlich unterschreibt. Bei der Überprüfung einer bestehenden Signatur kann der *Bürger* exakt feststellen, welche Daten durch die überprüfte Signatur gesichert sind.

Bietet eine *Bürgerkarten-Umgebung* eine sichere Signatur nach [SigG] bzw. eine nach [E-GovG] damit befristet gleichgestellte Verwaltungssignatur an, so kapselt sie damit auch sämtliche gesetzliche Verantwortlichkeiten dieser beiden qualifizierten Arten einer elektronischen Signatur. So befinden sich beispielsweise die für eine Erstellung einer sichere elektronische Signatur gesetzlich vorgeschriebene, zertifizierungspflichtige Signaturerstellungseinheit bzw. die dafür ebenfalls gesetzlich normierte, bescheinigungspflichtige Anzeigeeinheit innerhalb der *Bürgerkarten-Umgebung*. Dies hat für Entwickler von Applikationen den großen Vorteil, dass sie sich beim Design einer *Applikation* nicht um solche gesetzliche Vorgaben kümmern müssen.

2.2. Verschlüsselung

Der *Bürger* kann mit Hilfe der *Bürgerkarten-Umgebung* sowohl eigene elektronische Dokumente für beliebige Empfänger verschlüsseln, als auch bestehende, verschlüsselte Dokumente mit Hilfe eines der in der *Bürgerkarten-Umgebung* vorrätigen Entschlüsselungs-Schlüssels entschlüsseln.

2.3. Hashwerte

Der *Bürger* kann mit Hilfe der *Bürgerkarten-Umgebung* sowohl einen Hashwert für ein elektronisches Dokument berechnen, als auch einen bestehenden Hashwert über ein elektronisches Dokument prüfen.

2.4. Datenspeicher

Die *Bürgerkarten-Umgebung* stellt dem *Bürger* einen Datenspeicher zum Lesen und Schreiben beliebiger Daten zur Verfügung, die für E-Government oder E-Commerce Verfahren benötigt werden.

In den vorliegenden Spezifikationen ist der Datenspeicher in logische Einheiten gegliedert, die als Infoboxen bezeichnet werden. Im Datenspeicher können Infoboxen neu angelegt, gelesen, verändert und gelöscht werden.

Jedenfalls in der *Bürgerkarten-Umgebung* sind eine Reihe von standardisierten Infoboxen. So können beispielsweise die zu den in der *Bürgerkarten-Umgebung* vorrätigen Signatur- bzw. Verschlüsselungsschlüsseln zugehörigen Zertifikate ausgelesen werden. Ebenfalls über Infoboxen kann auf die im E-GovG normierten Datensätze Personenbindung und Vollmachten zugegriffen werden.

Die vorliegenden Spezifikationen machen bewusst keine Angaben zum physikalischen Ort, an dem die Daten des Datenspeichers. Vorstellbar sind mehrere Möglichkeiten, wobei diese Möglichkeiten durchaus miteinander zu einem gemeinsamen logischen Datenspiecher kombiniert werden können, z.B.:

- Speicher auf einer sicheren Signaturerstellungseinheit (Smart-Card, USB-Token, ...), wenn von der *Bürgerkarten-Umgebung* die erstellung einer sicheren Signatur angeboten wird;
- Speicher auf der Festplatte des *Bürgers*, wenn es sich bei der *Bürgerkarten-Umgebung* um ein lokal am Computer des *Bürgers* laufendes Programm handelt;

- Über das Internet ansprechbarer Speicher in der Hoheit des Diensteanbieters, wenn es sich bei der *Bürgerkarten-Umgebung* um einen serverbasierenden Dienst handelt.

Da es sich bei den im Datenspeicher abgelegten Infoboxen durchaus auch um sensible Informationen handeln kann, legen die vorliegenden Spezifikationen entsprechende Anforderungen an die Aufbewahrung sowie an den Zugriffsschutz fest.

3. Spezifikationen

Dieser Abschnitt gibt einen Überblick über die einzelen Spezifikationsdokumente zur österreichischen Bürgerkarte. Alle diese Dokumente haben normativen Charakter.

3.1. Einführung

Das vorliegende Dokument.

3.2. Applikationsschnittstelle Security-Layer

Dieses Dokument beschreibt die Schnittstelle *Security-Layer*, über die eine *Applikation* die in der *Bürgerkarten-Umgebung* verfügbaren Funktionen ansteuern kann. Die Schnittstelle normiert eine Reihe von Befehlen; jeder Befehl gehorcht einem einfachen Anfrage/Antwort Schema, d.h. die *Applikation* stellt eine Anfrage an die *Bürgerkarten-Umgebung*, und die *Bürgerkarten-Umgebung* antwortet nach der Abarbeitung des Befehls (und gegebenenfalls Interaktion mit dem *Bürger*über die *Benutzer-Schnittstelle*) mit der entsprechenden Antwort an die *Applikation*. [Applikationsschnittstelle Security-Layer]

3.3. Standardisierte Key- und Infoboxen

Dieses Dokument normiert die Bezeichner für die jedenfalls vorhandenen Keyboxen und Infoboxen.

Eine Keybox bezeichnet einen in der *Bürgerkarten-Umgebung* vorrätigen Schlüssel, der für die Erstellung von elektronischen Signaturen und/oder die Entschlüsselung von elektronischen Daten zur Verfügung steht. Über den Keybox-Bezeichner wird in den entsprechenden Befehlen des *Security-Layer* festgelegt, welcher Schlüssel für die Signaturerstellung bzw. Entschlüsselung verwendet werden soll.

Eine Infobox bezeichnet eine in der *Bürgerkarten-Umgebung* abgelegte Datensammlung, auf die mit Befehlen des *Security-Layer* lesend und verändernd zugegriffen werden kann. Über den Infobox-Bezeichner wird in diesen Befehlen festgelegt, welche Datensammlung angelegt, gelesen, verändert oder gelöscht werden soll. [Standardisierte Key- und Infoboxen]

3.4. Minimale Umsetzung des Security-Layers

Dieses Dokument legt fest, welche Befehle des *Security-Layers* von einer *Bürgerkarten-Umgebung* jedenfalls implementiert sein müssen. Weiters enthält es Profile der von den Befehlen zur Signaturerstellung, Signaturprüfung, Verschlüsselung und Entschlüsselung verwendeten Signaturformaten, Regelungen zur Anzeigekomponente der *Bürgerkarten-Umgebung*, sowie Anforderungen an die Auflösung von in den einzelnen Befehlen vorkommenden URLs. [Minimale Umsetzung des Security-Layers]

3.5. Transportprotokolle Security-Layer

Die Schnittstelle *Security-Layer* kann über unterschiedliche Transportprotokolle angesprochen werden. Dieses Dokument beschreibt die Bindung des *Security-Layers* an die Transportprotokolle TCP, TLS, HTTP und HTTPS. [Transportprotokolle Security-Layer]

3.6. Anforderungen an die Benutzer-Schnittstelle

Für die Abarbeitung einer Reihe von Befehlen des *Security-Layers* ist eine Kommunikation der *Bürgerkarten-Umgebung* mit dem *Bürger*über die *Benutzer-Schnittstelle* notwendig, beispielsweise im Falle der Signaturerstellung die Anzeige der zu signierenden Daten sowie das Auslösen der Siganturfunktion durch den *Bürger*. Dieses Dokument legt die Anforderungen an diese *Benutzer-Schnittstelle* für die einzelnen Befehle fest. [Anforderungen an die Benutzer-Schnittstelle]

3.7. Zugriffsschutz

Die Ausführung bzw. das Resultat der meisten Befehle des *Security-Layers* ist schützenswert. Das bedeutet, dass nicht jede beliebige *Applikation* jeden Befehl des *Security-Layers* ausführen, bzw. auf das Resultat der Befehlsausführung zugreifen darf. Dieses Dokument spezifiziert eine jedenfalls von einer *Bürgerkarten-Umgebung* einzuhaltenden Zugriffsschutz. Dazu wird zunächst eine Klassifizierung der Authentifizierung der zugreifenden *Applikation* vorgenommen. Ausgehend von dieser Klassifizierung werden Regeln definiert, die festlegen, ob eine *Applikation* letztendlich einen Befehl ausführen darf oder nicht. [Zugriffschutz]

3.8. Standard-Anzeigeformat

Wesentlich für die Akzeptanz der *Bürgerkarte* ist es, dass alle am Markt verfügbaren *Bürgerkarten-Umgebung* zumindest ein gemeinsames Dokumenten-Format in ihrer Anzeigekomponente (die beispielsweise zur Anzeige der zu signierenden Daten bei der Signaturerstellung verwendet wird) verarbeiten können. Dieses Format sollte entsprechende Möglichkeiten zum Layout sowie zur Einbindung von Bildern haben, dabei aber trotzdem prinzipiell als Anzeigeformat für sichere Signaturen geeignet sein. Dieses Dokument spezifiziert ein solches Dokumenten-Format basierend auf XHTML und CSS2. [Standard-Anzeigeformat]

3.9. Fehlercodes Security-Layer

Kann ein Befehl aus irgendeinem Grund von der *Bürgerkarten-Umgebung* nicht abgearbeitet werden, antwortet sie der *Applikation* anstatt mit der zur Anfrage zugehörigen Antwort mit einer eigens spezifizierten Fehler-Antwort. Dieses Dokument spezifiziert die in dieser Fehler-Antwort mitgelieferten Fehlercodes. [Fehlercodes Security-Layer]

3.10. Errata

Dieses Dokument listet die bekannten Errata in den Spezifikationen zur österreichischen Bürgerkarte ab der Version 1.1.0. Mit dem Erscheinen eines der Spezifikationsdokumente mit einer höheren Versionsnummer werden die bis zu diesem Erscheinungsdatum gelisteten Errata in die aktualisierte Spezifikation eingearbeitet, sämtliche Errata bleiben jedoch in diesem Dokument weiter gelistet. Sobald ein Erratum in dieses Dokument eingetragen wurde, gilt er - falls anwendbar - im Sinne der im Eintrag angeführten Korrektur als behoben. [Errata]

4. Erläuterungen

Dieser Abschnitt gibt einen Überblick über die weiteren Dokumente zur österreichischen Bürgerkarte. Diese Dokumente enthalten Erläuterungen haben lediglich informativen Charakter.

4.1. Tutorium

Dieses Dokument enthält ein Tutorium für Entwickler von *Applikation*en. Es finden sich darin Beispiele für alle Befehle des *Security-Layers*, als auch mehrstufige Abläufe für gängige Anwendungsfälle der *Bürgerkarte*. [Tutorium]

Referenzen

[CMS] BHously, R.: *RFC 3369: Cryptographic Message Syntax (CMS)* , IETF Request For Comment, August 2002

[CMS-AES] chaad, J.: *RFC 3565: Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)* . IETF Request For Comment, Juli 2003.

[CMS-Alg] Hously, R.: *RFC 3370: Cryptographic Message Syntax (CMS) Algorithms* . IETF Request For Comment, August 2002.

[CMS-RSAES-OAEP] Hously, R.: *RFC 3560: Use of the RSAES-OAEP Key Transport Algorithm in the Cryptographic Message Syntax (CMS)* . IETF Request For Comment, Juli 2003.

[CSS 2] Bert Bos, Håkon Wium Lie, Chris Lilley und Ian Jacobs: *Cascading Style Sheets, level 2* . W3C Recommendation, Mai 1998.

[EC14N] Boyer, John, Eastlake, Donald und Reagle, Joseph: *Exclusive XML Canonicalization. W3C Recommendation, Juli 2002* .

[ECDSA-CMS] Blake-Wilson, S., Brown, D., Lampert, D.: *RFC 3278: Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)* . IETF Request For Comment, April 2002.

[ECDSA-XML] Blake-Wilson, S., Karlinger, G. und Wang, Y.: *ECDSA with XML-Signature Syntax* . Internet-Draft, Jänner 2004.

[E-GovG] *BGBl. I Nr. 10/2004.*

[ESS-S/MIME] Hoffman, P.: *RFC 2634: Enhanced Security Services for S/MIME* , IETF Request For Comment, Juni 1999

[ETSICMS] European Telecommunications Standards Institute: *ETSI TS 101733: Electronic Signature Formats, v1.5.1* , Technical Specification, Dezember 2003

[ETSIQCert] European Telecommunications Standards Institute: *ETSI TS 101 862: Qualified certificate profile, v1.2.1* , Technical Specification, Juni 2001

[ETSIXML] European Telecommunications Standards Institute: *ETSI TS 101903: XML Advanced Electronic Signatures (XAdES), v1.2.2* , Technical Specification, April 2004

[GIF] *Graphics Interchange Format, Version 89a* . CompuServe Incorporated, Juli 1990.

[HTML4] Dave Ragget, Arnaud Le Hors und Ian Jacobs: *HTML 4.01 Specification* . W3C Recommendation, Dezember 1999.

[HTTP1.1] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leech und T. Berners-Lee: *Hypertext Transfer Protocol -- HTTP/1.1*. IETF Request For Comment, Juni 1999.

[HTTPS] E. Rescorla *HTTP over TLS*. IETF Request For Comment, Mai 2000

[ISO-8859-1] *ISO/IEC 8859-1*:1998: Information technology -- 8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No. 1.

[ISO-8859-10] *ISO/IEC 8859-10*:1998: Information technology -- 8-bit single-byte coded graphic character sets -- Part 10: Latin alphabet No. 6.

[ISO-8859-15] *ISO/IEC 8859-15*:1999: Information technology -- 8-bit single-byte coded graphic character sets -- Part 15: Latin alphabet No. 9.

[ISO-8859-2] *ISO/IEC 8859-2*:1999: Information technology -- 8-bit single-byte coded graphic character sets -- Part 2: Latin alphabet No. 2.

[ISO-8859-3] *ISO/IEC 8859-3*:1999: Information technology -- 8-bit single-byte coded graphic character sets -- Part 3: Latin alphabet No. 3.

[ISO-8859-9] *ISO/IEC 8859-9*:1999: Information technology -- 8-bit single-byte coded graphic character sets -- Part 9: Latin alphabet No. 5.

[JPEG] Eric Hamilton: *JPEG File Interchange Format, Version 1.02* . C-Cube Microsystems, September 1992.

[KEYWORDS] Bradner, S.: *RFC 2119: Key words for use in RFCs to Indicate Requirement Levels* , IETF Request For Comment, März 1997

[MIME] Freed, N. und Borenstein, N.: *RFC 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types* , IETF Request For Comment, November 1996

[PersBin] Hollosi, Arno und Karlinger, Gregor: *XML-Definition der Personenbindung* . Konvention zum E-Government Austria erarbeitet von der Stabsstelle IKT-Strategie des Bundes, Technik und Standards. Öffentlicher Entwurf, Version 1.2.2, 14. Februar 2005.

[PersonData] Naber, Larissa: *PersonData Struktur - XML Spezifikation* . Konvention zum E-Government Austria erarbeitet von der Arbeitsgruppe Kommunikationsarchitekturen. Öffentlicher Entwurf, Version 2.0.0, 14. Oktober 2004.

[PKCS#12] RSA Laboratories: *PKCS#12 v1.0: Personal Information Exchange Syntax* , Juni 1999.

[port-numbers] Internet Assigned Numbers Authority: *Port Numbers*

[QCert] Santesson, S. und Nystrom M.: *RFC 3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile* , IETF Request For Comment, März 2004

[SigG] *BGBl I Nr. 190/1999* idF BGBl I Nr. 152/2001.

[SigV] *BGBl II Nr. 30/2000* idF BGBl II Nr. 527/2004.

[Stammzahl] Hollosi, Arno und Hörbe, Rainer: *Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK)* . Konvention zum E-Government Austria erarbeitet von der Stabsstelle IKT-Strategie des Bundes, Technik und Standards sowie vom Bundesminsterium für Inneres. Öffentlicher Entwurf, Version 1.0, 2. Februar 2004.

[TLS] T. Dierks und C. Allen: *The TLS Protocol Version 1.0* . IETF Request For Comment, Januar 1999.

[Unicode] The Unicode Consortium. *The Unicode Standard, Version 4.0.0* , defined by: The Unicode Standard, Version 4.0 (Boston, MA, Addison-Wesley, 2003. ISBN 0-321-18578-1).

[URI] Berners-Lee, T. , Fielding, R. und Masinter, L.: *RFC 2396: Uniform Resource Identifiers (URI): Generic Syntax* , IETF Request For Comment, August 1998

[VerwEig] Hollosi, Arno: *X.509 Zertifikatserweiterungen für die Verwaltung* . Konvention zum E-Government Austria erarbeitet von der Stabsstelle IKT-Strategie des Bundes, Technik und Standards. Öffentlicher Entwurf, Version 1.0.3, 21. Februar 2005.

[X509] Polk, W., Ford, W., Solo, D.: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* . IETF Request For Comment, April 2002.

[XHTML 1.1] Murray Altheim, Frank Boumphrey, Sam Dooley, Shane McCarron, Sebastian Schnitzenbaumer und Ted Wugofski: *Modularization of XHTML* . W3C Recommendation, April 2001.

[XHTML MOD] Daniel Austin, Subramanian Peruvemba, Shane McCarron, Masayasu Ishikawa: *Modularization of XHTML in XML Schema* . W3C Working Draft, Oktober 2003.

[XML] Bray, Tim, Paoli, Jean, Sperberg-McQueen, C.M. und Maler, Eve: *Extensible Markup Language (XML) 1.0 (Second Edition)* , W3C Recommendation, Oktober 2000.

[XMLDecTF] Hughes, Merlin, Imamura, Takeshi und Maruyama, Hiroshi: *Decryption Transform for XML Signature* . W3C Recommendation, Dezember 2002.

[XMLDSIG] Eastlake, Donald, Reagle, Joseph und Solo, David: *XML-Signature Syntax and Processing* , W3C Recommendation, Februar 2002

[XMLDSIG-URI] Eastlake, Donald: *RFC 4051: Additional XML Security Uniform Resource Identifiers (URIs)* , IETF Request For Comments, April 2005

[XMLEnc] Eastlake, Donald und Reagle, Joseph: *XML Encryption Syntax and Processing* , W3C Recommendation, Dezember 2002

[XML-Schema] Thompson, Henry S., Beech, David, Maloney, Murray und Mendelson, Noah: *XML Schema Part 1: Structures* , W3C Recommendation, Mai 2001

[XMLTYPE] Murata, M., St.Laurent, S., und Kohn, D.: *RFC 3023: XML Media Types* , IETF Request For Comment, Jänner 2001.

[XPath] Clark, James und DeRose, Steven: *XML Path Language* , W3C Recommendation, November 1999

[XPF2] Boyer, John, Hughes, Merlin und Reagle, Joseph: *XML-Signature XPath Filter 2.0* . W3C Candidate Recommendation, Juli 2002.

[XPointer] Grosso, Paul, Maler, Eve, Marsh, Jonathan und Walsh, Norman: *XPointer Framework* . W3C Recommendation, März 2003.

[XSS-FAQ] Cgisecurity.com: *The Cross Site Scripting FAQ* .