Standardisierte Key- und Infoboxen der österreichischen Bürgerkarte		Konvention **1.2.1** Empfehlung
Kurzbeschreibung	Das vorliegende Dokument spezifiziert die jedenfalls verwendbaren Key- bzw. Infoboxen der österreichischen Bürgerkarte.	
Autoren:	Arno Hollosi Gregor Karlinger Thomas Rössler Martin Centner et al.	Projektteam/Arbeitsgruppe AG Bürgerkarte
Datum:	1.3.2005	

Inhaltsverzeichnis

1. Allgemeines

1.1. Namenskonventionen

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

Folgende Namenraum-Präfixe werden in dieser Spezifikation zur Kennzeichnung der Namenräume von XML-Elementen verwendet:

Präfix	Namenraum	Erläuterung

sl	http://www.buergerkarte.at/namespaces/securitylayer/1.2#	Elemente der Applikationsschnittstelle Security-Layer
pr	http://reference.e-government.gv.at/namespace/persondata/20020228#	Elemente aus [PersonData]

2. Keyboxen

Dieser Abschnitt spezifiziert jene Keyboxen, welche die *Bürgerkarten-Umgebung* über die Applikationsschnittstelle *Security-Layer* zur Verfügung stellen MUSS. Neben diesen obligaten Keyboxen DARF eine *Bürgerkarten-Umgebung* beliebige weitere Keyboxen für Signatur und/oder Verschlüsselung zur Verfügung stellen.

2.1. Keybox für elektronische Signaturen

Die *Bürgerkarten-Umgebung* MUSS eine Keybox mit dem Namen `SecureSignatureKeypair` zur Verfügung stellen.

Diese Keybox MUSS zur Erstellung von Signaturen und DARF zur Durchführung von Entschlüsselungen geeignet sein. Eine *Applikation* MUSS die tatsächlichen Eignungen von der *Bürgerkarten-Umgebung* mit Hilfe des Befehls *Abschnitt 8.1, „Abfrage der Umgebungseigenschaften“ in Die österreichische Bürgerkarte - Applikationsschnittstelle Security-Layer* ermitteln können.

Bietet eine *Bürgerkarten-Umgebung* eine sichere Signatur nach [SigG] bzw. eine nach [E-GovG] damit befristet gleichgestellte Verwaltungssignatur an, so MUSS diese besonders qualifizierte Signatur über die Keybox `SecureSignatureKeypair` zur Verfügung gestellt werden.

2.2. Keybox für elektronische Signatur und Verschlüsselung

Die *Bürgerkarten-Umgebung* MUSS eine Keybox mit dem Namen `CertifiedKeypair` zur Verfügung stellen.

Diese Keybox MUSS sowohl zur Erstellung von Signaturen als auch zur Durchführung von Entschlüsselungen geeignet sein.

3. Infoboxen

Dieser Abschnitt spezifiziert jene Infoboxen, die von der *Bürgerkarten-Umgebung* verpflichtend zu implementieren sind. Es sind dies Infoboxen zur Speicherung von Zertifikaten, der Personenbindung sowie von Vollmachten des Bürgers.

3.1. Infobox für Zertifikate

Diese Infobox enthält Zertifikate, die mit den Signaturschlüsseln des Bürgers zusammenhängen. Jedenfalls enthalten sein müssen (entsprechende Initialisierung der *Bürgerkarte* vorausgesetzt) die Zertifikate zu den beiden auf der *Bürgerkarte* standardmässig vorhandenen Signaturschlüsseln.

Die zu verwendenen Schlüsselbegriffe für den Abruf dieser beiden Zertifikate aus der Infobox entsprechen den Keybox-Bezeichnern aus Abschnitt 2, „Keyboxen“ (`SecureSignatureKeypair` bzw. `CertifiedKeypair`).

Darüber hinaus können in dieser Infobox weitere Zertifikate (wie etwa Zertifikate zu weiteren Signaturschlüsseln oder Zertifikate des Zertifizierungspfades zu einem Signaturschlüssel) abgelegt werden.

3.1.1. Bezeichner der Infobox

Diese Infobox trägt den Bezeichner `Certificates`. Dieser Bezeichner wird von der *Applikation* zur Selektion der Infobox bei Lese- und Update-Zugriffen verwendet.

3.1.2. Typ der Infobox

Diese Infobox hat den Typ *Assoziatives Array*. Für die damit verbundenen möglichen Lese- und Update-Zugriffe siehe *Abschnitt 7, „Zugriff auf Infoboxen“ in Die österreichische Bürgerkarte - Applikationsschnittstelle Security-Layer* .

3.1.3. Boxspezifische Parameter

3.1.3.1. Lese-Parameter

Für diese Infobox sind keine boxspezifischen Lese-Parameter festgelegt.

3.1.3.2. Update-Parameter

Für diese Infobox sind keine boxspezifischen Update-Parameter festgelegt.

3.2. Infobox für die Personenbindung

Diese Infobox enthält die Personenbindung des Bürgers. Dies ist jener von der Stammzahlenregisterbehörde elektronisch signierte Datensatz, der die Stammzahl des Bürgers an die Zertifikate der Signaturschlüssel des Bürgers bindet.

> **Anmerkung**
>
> Für die Spezifikation der Personenbindung siehe [PersBin].

3.2.1. Bezeichner der Infobox

Diese Infobox trägt den Bezeichner `IdentityLink`. Dieser Bezeichner wird von der *Applikation* zur Selektion der Infobox bei Lese- und Update-Zugriffen verwendet.

3.2.2. Typ der Infobox

Diese Infobox hat den Typ *Binärdatei*. Für die damit verbundenen möglichen Lese- und Update-Zugriffe siehe *Abschnitt 7, „Zugriff auf Infoboxen“ in Die österreichische Bürgerkarte - Applikationsschnittstelle Security-Layer* .

3.2.3. Boxspezifische Parameter

3.2.3.1. Lese-Parameter

Nach den Bestimmungen des § 14 [E-GovG] darf ein Auftraggeber des privaten Bereichs zur Identifikation des Bürgers ein aus der Stammzahl abgeleitetes wirtschaftsbereichspezifische Personenkennzeichen (wbPK) verwenden. Entsprechend den Bestimmungen des § 12 (1) lit. 4 [E-GovG] darf jedoch die Berechnung dieses abgeleiteten Kennzeichens nicht durch den Auftraggeber des privaten Bereichs selbst vorgenommen werden.

Die *Bürgerkarten-Umgebung* stellt daher diese Berechnung implizit über einen parametrisierten Lesezugriff auf die Infobox der Personenbindung zur Verfügung: Wird die zur Ableitung des wbPK notwendige Bereichskennung als boxspezifischer Parameter in der Anfrage zum Auslesen der Personenbindung übergeben, liefert die *Bürgerkarten-Umgebung* eine modifizierte Personenbindung zurück: Die ursprünglich darin kodierte Stammzahl wird ersetzt durch das aus der Bereichskennung und der Stammzahl abgeleitete wbPK. Wird kein boxspezifischer Parmeter angegeben, liefert die *Bürgerkarten-Umgebung* die originale Personenbindung zurück.

Die Bereichskennung wird gegebenenfalls wie folgt als boxspezifischer Lese-Parameter angegeben: Im Container für boxspezifische Lese-Parameter (`sl:BoxSpecificParameters`) wird ein einziges Element `sl:IdentityLinkDomainIdentifier` übergeben. Dieses Element enthält als URI die Bereichskennung für die Bildung des aus der Stammzahl abgeleiteten wbPK. Für die genaue Spezifikation der Bereichskennung siehe [Stammzahl], Abschnitt "Ermittlung des Wirtschafts-bPK". Die formale Definition des Elements `sl:IdentityLinkDomainIdentifier` befindet sich im XML-Schema zur Applikationsschnittstelle Security-Layer.

Die Modifikation der Personenbindung ist gegebenenfalls wie folgt durch die *Bürgerkarten-Umgebung* vorzunehmen: Anstatt der Stammzahl wird in die Personendaten der Personenbindung (vergleiche [PersBin], Abschnitt 2.2.1.1) das aus Stammzahl und Bereichskennung abgeleitete wbPK eingesezt: Das Element `pr:Type` erhält als neuen Wert den Inhalt des übergebenen boxspezifischen Leseparameters `sl:IdentityLinkDomainIdentifier`, das Element `pr:Value` erhält als neuen Wert das nach [Stammzahl], Abschnitt "Ermittlung des Wirtschafts-bPK" gebildete wbPK in base64-kodierter Form.

3.2.3.2. Update-Parameter

Für diese Infobox sind keine boxspezifischen Update-Parameter festgelegt.

3.3. Infobox für Vollmachten

Diese Infobox enthält Vollmachten des Bürgers. Eine Vollmacht ist die Delegation von Rechten des Vollmachtgebers an den/die Vollmachtnehmer. Vereinfacht dargestellt enthält die Vollmacht durch den Vollmachtgeber signierte Informationen über ihn, den Vollmachtnehmer sowie den Vollmachtszweck.

3.3.1. Bezeichner der Infobox

Diese Infobox trägt den Bezeichner `Mandates`. Dieser Bezeichner wird von der *Applikation* zur Selektion der Infobox bei Lese- und Update-Zugriffen verwendet.

3.3.2. Typ der Infobox

Diese Infobox hat den Typ *Assoziatives Array*. Für die damit verbundenen möglichen Lese- und Update-Zugriffe siehe *Abschnitt 7, „Zugriff auf Infoboxen“ in Die österreichische Bürgerkarte - Applikationsschnittstelle Security-Layer* .

3.3.3. Boxspezifische Parameter

3.3.3.1. Lese-Parameter

Aus den bereits im Abschnitt 3.2.3.1 dargelegten Gründen wird die Berechnung des wirtschaftsbereichspezifischen Personenkennzeichens (wbPK) auch im Rahmen eines Lesezugriffs auf Werte im *Assoziativen Array* `Mandates` (also auf Vollmachten) implizit zur Verfügung gestellt: Wird die zur Ableitung des wbPK notwendige Bereichskennung als boxspezifischer Parameter in der Anfrage zum Lesen von Schlüsseln und Werten bzw. zum Lesen des Werts zu einem Schlüssel (Abschnitt 7.1.2, „Assoziatives Array“ in Die österreichische Bürgerkarte - Applikationsschnittstelle Security-Layer) übergeben, liefert die *Bürgerkarten-Umgebung* die Vollmachten bzw. die Vollmacht in modifizierter Form zurück: Die ursprünglich darin kodierten Stammzahlen von Machthaber und Machtnehmer werden ersetzt durch die jeweils aus der Bereichskennung und der Stammzahl abgeleitete wbPK. Wird kein boxspezifischer Parmeter angegeben, liefert die *Bürgerkarten-Umgebung* die Vollmachten bzw. die Vollmacht unmodifiziert zurück.

Die Bereichskennung wird gegebenenfalls wie folgt als boxspezifischer Lese-Parameter angegeben: Im Container für boxspezifische Lese-Parameter (`sl:BoxSpecificParameters`) wird ein einziges Element `sl:IdentityLinkDomainIdentifier` übergeben. Dieses Element enthält als URI die Bereichskennung für die Bildung des aus der Stammzahl abgeleiteten wbPK. Für die genaue Spezifikation der Bereichskennung siehe [Stammzahl], Abschnitt "Ermittlung des Wirtschafts-bPK". Die formale Definition des Elements `sl:IdentityLinkDomainIdentifier` befindet sich im XML-Schema zur Applikationsschnittstelle Security-Layer.

[TBD]: Genaue Ausführungen über die exakte Modifikation der Vollmacht, Verweis auf das Spezifikationspapier zu den Vollmachten.

3.3.3.2. Update-Parameter

Für diese Infobox sind keine boxspezifischen Update-Parameter festgelegt.

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 .

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* .

A. Historie

Datum	Version	Änderungen
01. 03. 2005	1.2.1	• Erratum Erratum 25 in Die österreichische Bürgerkarte - Errata korrigiert.
14. 05. 2004	1.2.0	• Erläuterungen zu den Keyboxen überarbeitet. • Spezifikation der boxspezifischen Parameter für die standardisierten Infoboxen eingefügt..
31.08.2002	1.1.0	• Diverse editoriale Verbesserungen.