

ArchSafe

ARS Spezifikation 4.0 ARS Signaturformate VERSION 1.0

Dokumententitel: ARS Signaturformate
Dateiname: 2007-02-12_Std_ARS_4_0_V10.doc
Version: 1.0
Anzahl Seiten: 24
Status: Freigegeben

erstellt am:	01.09.2006	von:	Dr. W. Zimmer
geprüft am:	26.09.2006	von:	T. Schäfer
Geändert am:	26.09.2006	von:	T. Schäfer
Freigegeben am:	12.02.2007	von:	T. Schäfer

Standort: PTB
Verteiler:

Inhalt

0	Versionshistorie	4
0.1	Dokumentverantwortlicher	4
0.2	Verteilerliste.....	4
1	Zielsetzung des Dokumentes	5
2	Einführung	8
3	Digitale Signaturen.....	9
3.1	Cryptographic Message Syntax (CMS) – PKCS#7	9
3.1.1	<i>Signaturerstellung.....</i>	<i>10</i>
3.1.1.1	Digest-Algorithmen.....	10
3.1.1.2	Signaturalgorithmen	10
3.1.1.3	Schlüsselinformationen	11
3.1.2	<i>Signaturprüfung</i>	<i>11</i>
3.1.2.1	Digest-Algorithmen.....	11
3.1.2.2	Signaturalgorithmen	11
3.1.2.3	Schlüsselinformationen	12
3.2	XML Signatur	13
3.2.1	<i>Signaturerstellung.....</i>	<i>14</i>
3.2.1.1	Digest-Algorithmen.....	14
3.2.1.2	Signaturalgorithmen	14
3.2.1.3	Kanonisierungsalgorithmen	14
3.2.1.4	Transformationsalgorithmen	15
3.2.1.5	Schlüsselinformationen	15
3.2.2	<i>Signaturprüfung</i>	<i>16</i>
3.2.2.1	Digest-Algorithmen.....	16
3.2.2.2	Signaturalgorithmen	16
3.2.2.3	Kanonisierungsalgorithmen	16
3.2.2.4	Transformationsalgorithmen	16
3.2.2.5	Schlüsselinformationen	17
4	Elektronische Zeitstempel.....	18

4.1 Archivzeitstempel	18
4.1.1 <i>Zeitstempelanfrage</i>	19
4.1.1.1 Hash-Algorithmen	19
4.1.1.2 Signaturalgorithmen	19
4.1.1.3 Transportprotokoll	20
4.2 Gesetzeskonforme Signaturerneuerung	20
4.2.1 <i>Bildung des Archivzeitstempels</i>	20
4.2.1.1 Syntax des Archivzeitstempels	21
4.2.1.2 Bildung des Archivzeitstempels	21
4.2.1.3 Verifikation des Archivzeitstempels	22
4.2.1.4 Bereitstellung und Aufruf der Verifikation des Archivzeitstempels	22
5 Referenzen	23

0 Versionshistorie

Version	Editor	Datum	Kommentar
0.1	Dr. W. Zimmer	18.08.2006	Entwurf
0.2	Dr. W. Zimmer	22.08.2006	Entwurf
0.3	Dr. W. Zimmer, T. Gondrom	01.09.2006	Entwurf
0.4	Dr. W. Zimmer	06.09.2006	Entwurf
0.5	T. Schäfer	26.09.2006	Korrektur
1.0	T. Schäfer	12.02.2007	Freigabe

0.1 Dokumentverantwortlicher

Rolle	Name / OE	Bemerkung
Dokumentverantwortlicher	Tobias Schäfer	

0.2 Verteilerliste

Rolle	Name / OE	Bemerkung
Projektleiter PTB	Hr. Tobias Schäfer	
CC DS	Hr. Jobst Biester	
CC VBPO	Fr. Jutta Lautenschlager	
Extern	Hr. Dr. Wolf Zimmer	

1 Zielsetzung des Dokumentes

Dieses Dokument ist eine Spezifikation zur Unterstützung des ArchiSafe Konzepts für die rechtssichere elektronische Langzeitspeicherung von elektronischem Schriftgut. Die Beziehungen zwischen dem ArchiSafe Konzept (**ArchiSafe Recordkeeping Strategy**), den Spezifikationen, die dieses Konzept unterstützen und den ArchiSafe Empfehlungen für die Umsetzung zeigt die folgende Abbildung.

Rechtssichere Schriftgutverwaltung Anforderungen Schlussfolgerungen aus dem DOMEA Organisationskonzept Einführung in ARS	
ARS Spezifikation 1.0: Funktionale Anforderungen	ARS DOMEA Empfehlungen 1: Funktionale Anforderungen
ARS Spezifikation 2.0: ARS XML Datenschema	ARS DOMEA Empfehlungen 2: XML Datenschema
ARS Spezifikation 3.0: ARS Langzeitdokumentenformate	ARS DOMEA Empfehlung 3: Langzeitdokumentenformate
ARS Spezifikation 4.0: ARS Signaturformate	ARS DOMEA Empfehlung 4: Elektronische Signaturen
ARS Spezifikation 5.0: ARS Schnittstellen	ARS DOMEA Empfehlung 5: Import & Export
ARS: ArchiSafe Recordkeeping Strategy	

Abb. 1: ArchiSafe Spezifikationen

Im Einzelnen beschreiben die Spezifikationen und Empfehlungen die folgenden Inhalte:

Einführung in ARS (ArchiSafe Recordkeeping Strategy): Dieses Dokument erläutert das ArchiSafe Konzept aus verwaltungsrechtlicher Sicht und die sich hieraus ergebenden grundsätzlichen Anforderungen und Ziele von ArchiSafe. Die detaillierten funktionalen und technischen Anforderungen und Definitionen werden in fünf Spezifikationen beschrieben.

Spezifikationen: Diese fünf Dokumente spezifizieren die funktionalen und technischen Anforderungen, die den ARS Standard unterstützen. Nutzer und Anwender des ARS Konzeptes

sind gehalten, die obligatorischen Anforderungen des vorgeschlagenen Standards einzuhalten und den optionalen Empfehlungen weitestgehend zu folgen.

Die fünf Spezifikationen im Einzelnen sind:

- **Spezifikation 1:** Funktionale Anforderungen an eine dauerhafte und rechtssichere elektronische Ablage. Dieses Dokument beschreibt die allgemeinen und grundsätzlichen Anforderungen und Funktionen, die ein elektronisches, ARS konformes Ablagesystem erfüllen muss, um elektronisches Schriftgut rechtssicher und dauerhaft elektronisch aufbewahren zu können.
- **Spezifikation 2:** ARS Metadaten und ARS XML-Schema. Dieses Dokument spezifiziert und beschreibt die für eine rechtssichere und dauerhafte elektronische Ablage von elektronischem Schriftgut erforderlichen Metadaten (2a) und eine technische Definition des ARS Langzeitspeicherformats (2b).
- **Spezifikation 3:** Dieses Dokument spezifiziert die aus Sicht von ARS geeigneten Dokumentformate, die für eine rechtssichere, dauerhafte elektronische Ablage von ARS konformen Systemen jedenfalls unterstützt werden müssen.
- **Spezifikation 4:** Dieses Dokument spezifiziert die von ARS konformen Systemen unterstützten elektronischen Signaturformate.
- **Spezifikation 5:** Dieses Dokument beschreibt die Schnittstellen von ARS konformen Langzeitspeichersystemen.

Empfehlungen: Die ARS Empfehlungen liefern Hintergrundinformationen, erläuterndes Material und Beispiele zur Unterstützung der Standards und zugehörigen Spezifikationen abgeleitet aus dem Fachkonzept und den praktischen Erfahrungen aus der Umsetzungsrealisierung in der Physikalisch-Technischen Bundesanstalt.

Beziehung zwischen den Spezifikationen: Die Zusammenhänge zwischen den einzelnen Spezifikationen verdeutlicht die folgende Abbildung.

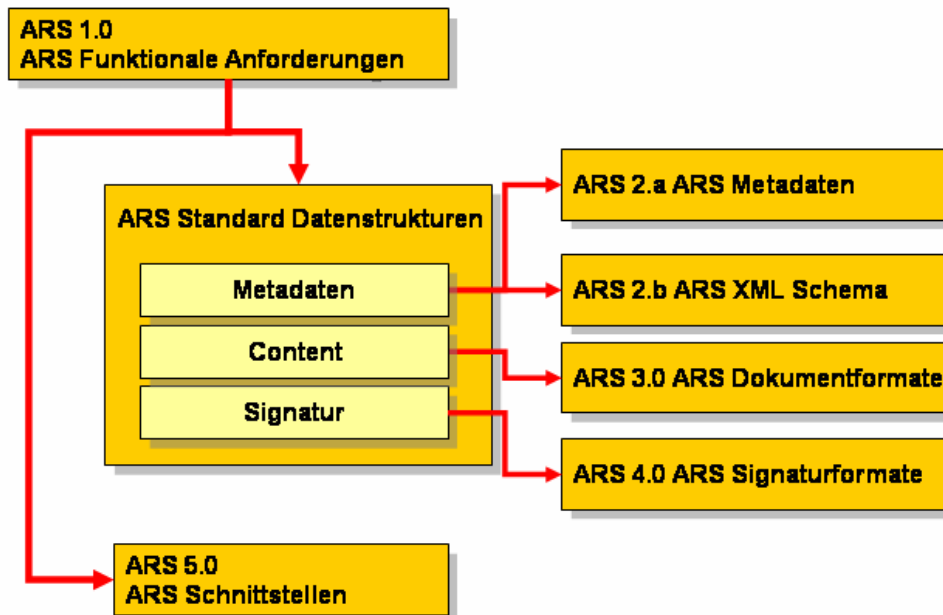


Abb. 2: Beziehungen zwischen den ArchiSafe Spezifikationen

Die Spezifikation 1 (Funktionale Anforderungen) definiert die allgemeinen Anforderungen an einen elektronischen Datenspeicher zur rechtssicheren und dauerhaften Ablage von elektronischem Schriftgut. Insbesondere muss das System in der Lage sein, die abgelegten Dokumente und Daten im Bedarfsfall in einem standardisierten Format zu exportieren.

Die allgemeinen und obligatorischen Merkmale dieses Standarddatenformats (Syntax und Semantik des gesamten Archivpakets und der Metadaten zur Beschreibung des Dokumentkontextes) definiert die Spezifikation 2 (ARS Standard Datenstrukturen), die Spezifikationsdetails der unterstützten Signaturformate beschreibt die Spezifikation 4 (ARS Signaturformate). Die Spezifikation 3 (ARS Langzeitdokumentformate) definiert Dokumentformate die für eine dauerhafte Speicherung von Daten und Informationen in Übereinstimmung mit anerkannten Verwaltungsstandards (DOMEA, SAGA) geeignet sind.

Die Spezifikation 5 (ARS Schnittstellen) schließlich beschreibt die funktionalen Schnittstellen und Mechanismen für den Datenaustausch.

2 Einführung

Für eine dauerhafte und rechtssichere Aufbewahrung von elektronisch gespeichertem Schriftgut muss sichergestellt sein, dass die Vollständigkeit, Integrität, Authentizität und Verkehrsfähigkeit des elektronischen Schriftguts mindestens für die Dauer gesetzlich vorgeschriebener Aufbewahrungsfristen durch geeignete Maßnahmen gewährleistet werden kann. Hinsichtlich der Sicherung der Integrität und Authentizität elektronischen Schriftguts setzt das ArchiSafe Konzept vor allem auf den Einsatz kryptographischer Maßnahmen, insbesondere qualifizierter elektronischer Signaturen und elektronischer Zeitstempel.

Der Zweck dieser Spezifikation ist, Profile und Protokolle elektronischer Signaturen und elektronischer Zeitstempel zu beschreiben, die von einem ArchiSafe konformen elektronischen Archivsystem jedenfalls unterstützt werden müssen.

Diese Spezifikation gilt im Zusammenhang mit folgenden weiteren Spezifikationen:

- ARS 1.0 : ARS Funktionale Anforderungen
- ARS 2.0 : ARS XML Datenpakete und Metadatenschema
- ARS 3.0 : ARS Langzeitdokumentenformate,
- ARS 5.0 : ARS Schnittstellen

3 Digitale Signaturen

Die Gewährleistung der Authentizität und Integrität von Daten und die zuverlässige Identifizierung ihres Urhebers sind zentrale Anforderungen des elektronischen Rechts- und Geschäftsverkehrs und können nach heutigem Stand der Wissenschaft und der aktuellen Rechtslage mit dem Einsatz elektronischer Signaturen sichergestellt werden. Die Verwendung qualifizierter elektronischer Signaturen und qualifizierter elektronischer Signaturen mit Anbieterakkreditierung ermöglicht nicht nur die Erfüllung der Anforderungen der elektronischen Form (§ 126 Abs. 3 BGB, § 3a VwVfG, § 87a AO, § 36s SGBI), sondern begründet auch einen hohen Beweiswert für die in dieser Form vorliegenden elektronischen Dokumente. Diese Rechtsfolge knüpft an die im Signaturgesetz vorgesehenen technischen und organisatorischen Sicherheitsmaßnahmen der Zertifizierungsdiensteanbieter an, die qualifizierte Zertifikate ausstellen.

3.1 Cryptographic Message Syntax (CMS) – PKCS#7

Ein ArchiSafe konformes elektronisches Archivsystem *muss* für die rechts- und revisionssichere, dauerhafte Speicherung elektronisch signierter Dokumente mindestens den von der Internet Engineering Task Force (IETF) veröffentlichten Cryptographic Message Syntax Standard (CMS/PKCS#7) unterstützen.

Erläuterung:

Die als RFC 3852 – Cryptographic Message Syntax (CMS) im Juli 2004 durch die Internet Engineering Task Force (IETF) veröffentlichte Spezifikation bezeichnet und beschreibt eine Syntax, nach der Daten durch kryptographische Maßnahmen wie digitale Signaturen oder Verschlüsselung geschützt, respektive Signaturdaten über das Internet ausgetauscht werden können. Sie basiert auf dem ursprünglich durch die RSA Laboratories veröffentlichten PKCS#7 (Public Key Cryptography Standard) Dokument in der Version 1.5, das eine allgemeine Syntax für Daten, wie digitale Umschläge oder Unterschriften darstellt, die chiffriert oder unterschrieben sein können. Der PKCS#7v1.5 Standard ist Grundlage des S/MIME Protokolls und der in PDF Dokumenten eingebetteten elektronischen Signaturen sowie der Authentizitätssicherung von ausführbaren Softwaredateien.

Die Syntax ist rekursiv, so dass Daten und Umschläge verschachtelt oder bereits chiffrierte Daten unterschrieben werden können. Die Syntax ermöglicht zudem, dass weitere Attribute wie z. B. Zeitstempel mit den Daten oder dem Nachrichteninhalt authentifiziert werden können. PKCS#7 ist zu PEM kompatibel, so dass unterschriebene und chiffrierte Nachrichten ohne kryptographische Operationen in PEM-Nachrichten und umgekehrt konvertiert werden können. PKCS#7 unterstützt eine Vielzahl von Architekturen für die Schlüsselverwaltung auf der Basis von Zertifikaten.

3.1.1 Signaturerstellung

Dieser Abschnitt spezifiziert ein Profil von [CMS], das von einer ArchiSafe konformen Umgebung bei der Erstellung von Signaturen unterstützt werden *muss*.

3.1.1.1 Digest-Algorithmen

Zur Berechnung des Message Digest nach [CMS], *muss* eine ArchiSafe konforme Umgebung die von der Bundesnetzagentur zum Zeitpunkt der Archivierung als sicher eingestuft Algorithmen und Parameter verwenden [BNetzA-ALG]. Danach gelten die Algorithmen SHA-1 [CMS-ALG] bis Ende 2009, RIPEMD-160 [ISO/IEC 10118-3] bis Ende 2010 und die Algorithmen SHA-224, SHA-256, SHA-384 und SHA-512 bis Ende 2011 als für die Anwendung bei digitalen Signaturen geeignet. Um die Zukunftssicherheit der Umgebung zu gewährleisten empfiehlt es sich insbesondere die Algorithmen SHA-256, SHA-384 und SHA-512 zu unterstützen.

3.1.1.2 Signaturalgorithmen

Zur Berechnung des Signaturwerts nach [CMS], *muss* eine ArchiSafe konforme Umgebung die zum Zeitpunkt der Archivierung von der Bundesnetzagentur [BNetzA-ALG] als geeignet eingestufte Signaturalgorithmen und Parameter unterstützen. Zum Zeitpunkt der Veröffentlichung dieser Spezifikation sind dies:

- für RSA-Schlüssel den Algorithmus nach [CMS-ALG], Abschnitt 3.2, mit einer Schlüssellänge von wenigstens 1024 Bit (empfohlen 2048 Bit)
- für DSA-Schlüssel den Algorithmus nach [CMS-ALG], Abschnitt 3.1, mit einer Schlüssellänge von wenigstens 1024 Bit (empfohlen 2048 Bit)
- und für EC-DSA-Schlüssel den Algorithmus nach [ECDSA-CMS], Abschnitt 2.1.1.

3.1.1.3 Schlüsselinformationen

In einer CMS-Signatur können Informationen zum Auffinden des Prüfschlüssels in Form einer Sammlung von X509-Zertifikaten im Feld `certificates` (vgl. [CMS], Abschnitt 5.1) angegeben werden. Eine ArchiSafe konforme Umgebung *muss* in diese Sammlung mindestens das Signaturzertifikat aufnehmen. Zur Erhaltung des Beweiswertes signierter Dokumente auf der Grundlage der Authentizität der elektronischen Unterschrift wird *empfohlen*, die gesamte Kette an Zertifikaten, die zur Prüfung der Signatur benötigt wird (Signaturzertifikat bis zu einer vertrauenswürdigen Wurzelinstanz), ebenfalls in diese Sammlung aufzunehmen.

3.1.2 Signaturprüfung

Dieser Abschnitt spezifiziert ein Profil von [CMS], das von einer ArchiSafe konformen Umgebung im Kontext einer Signaturprüfung jedenfalls unterstützt werden *muss*.

3.1.2.1 Digest-Algorithmen

Eine ArchiSafe konforme Umgebung *muss* mindestens einen der in Abschnitt 3.1.1.1 dieses Dokuments genannten Algorithmen zur Berechnung des Message Digest im Rahmen der Signaturprüfung nach [CMS] unterstützen (insbesondere SHA-1, RIPEMD-160).

3.1.2.2 Signaturalgorithmen

Die nachfolgende Tabelle spezifiziert die Anforderungsniveaus an eine ArchiSafe konforme Umgebung betreffend die Unterstützung von Signaturalgorithmen im Rahmen der Signaturprüfung nach [CMS].

Bezeichnung	OID	Normative Referenz	Anforderung
RSA	{ iso(1) member-body(2) us (840) rsadsi(113549) pkcs (1) pkcs-1(1) 5 }	[CMS-ALG]	Erforderlich
DSA	{ iso(1) member-body(2) us (840) x9-57 (10040) x9cm (4) 3 }	[CMS-ALG]	Erforderlich
ECDSA	{ iso(1) member-body(2) us (840) ansi-x9-62(10045) signatures(4)1 }	[ECDSA-CMS]	Erforderlich



3.1.2.3 Schlüsselinformationen

In einer CMS-Signatur können Informationen zum Auffinden des Prüfschlüssels in Form einer Sammlung von X509-Zertifikaten im Feld „certificates“ (vgl. [CMS], Abschnitt 5.1) angegeben sein. Eine ArchiSafe konforme Umgebung *sollte* diese Informationen zum Auffinden des Prüfschlüssels sowie zur Bildung der Zertifikatskette hin zu einer vertrauenswürdigen Wurzel verwenden.

In einer CMS-Signatur können Widerrufsinformationen in Form einer Sammlung von X509-Widerrufslisten im Feld crls (vgl. [CMS], Abschnitt 5.1) angegeben sein. Ergänzend oder anstelle der Widerrufslisten (CRL's) können wie in [RFC3126] beschrieben hier auch OCSP-Responses gespeichert werden.

Eine ArchiSafe konforme Umgebung sollte diese Möglichkeiten nutzen und diese Informationen zur Feststellung des Status eines Zertifikats im Rahmen der Validierung einer Zertifikatskette verwenden und sollte sich organisatorisch oder systemtechnisch von der Authentizität der verwendeten Daten überzeugen.

3.2 XML Signatur

Ein ArchiSafe konformes elektronisches Archivsystem *kann* für die rechts- und revidierungssichere, dauerhafte Speicherung elektronisch signierter Dokumente den von der Internet Engineering Task Force (IETF) veröffentlichten XML Signatur Standard [XMLDSIG] unterstützen.

Erläuterung

Die XML Signatur Spezifikation (auch XMLDSig) definiert eine XML Syntax für digitale Signaturen. In ihrer Funktion ähnelt sie dem PKCS#7 Standard, ist aber leichter zu erweitern und auf das Signieren von XML Dokumenten spezialisiert. Sie findet Einsatz in vielen weiterführenden Web-Standards wie etwa SOAP, SAML oder dem deutschen OSCl.

Mit XML Signaturen können Daten jeden Typs signiert werden. Dabei kann die XML-Signatur Bestandteil des XML Datenpakets sein (enveloped signature), die Daten können aber auch in die XML-Signatur selbst eingebettet sein (enveloping signature) oder mit einer URL adressiert werden (detached signature).

Eine XML Signatur ist immer mindestens einer Ressource zugeordnet, das heißt ein XML Baum oder beliebige Binärdaten auf die ein XML-Link verweist. Beim XML Baum muss sichergestellt sein, dass es zu keinen Mehrdeutigkeiten kommt. Um dies erreichen zu können, ist eine so genannte Kanonisierung des Inhalts erforderlich. Dabei werden nach Maßgabe des Standards alle Elemente in der Reihenfolge ihres Auftretens aneinander gereiht und alle Attribute alphabetisch geordnet, so dass sich ein längerer UTF-8 String ergibt. Aus diesem wird dann der eigentliche Hashwert für die Signatur gebildet.

Da die Signatur eine binäre Zeichenfolge ist, lässt sie sich nicht direkt in ein XML Dokument einbetten. Man codiert die binären Werte im Base64-Format [RFC 1521], um so aus ihnen ASCII lesbare Zeichen zu gewinnen.

Im Rahmen der Struktur eines XML Dokuments lassen sich Subelemente explizit vom Signieren ausschließen, so auch die Signatur selbst. Umgekehrt lassen sich beliebig viele Referenzen auflisten, die als Gesamtheit zu signieren sind.

3.2.1 Signaturerstellung

Dieser Abschnitt spezifiziert ein Profil von [XMLDSIG], das von einer ArchiSafe konformen Umgebung im Kontext der Erzeugung einer XML Signatur verwendet werden *soll*.

3.2.1.1 Digest-Algorithmen

Zur Berechnung der Message Digests für eine XML-Signatur *muss* jedenfalls einen der in Abschnitt 3.1.1.1 dieses Dokuments genannten und von der Bundesnetzagentur zum Zeitpunkt der Archivierung als sicher eingestuftem Algorithmen und Parameter (zumindest also SHA-1 oder RIPEMD-160) verwendet werden.

3.2.1.2 Signaturalgorithmen

Zur Berechnung des Signaturwerts nach [XMLDSIG], *muss* eine ArchiSafe konforme Umgebung die zum Zeitpunkt der Archivierung von der Bundesnetzagentur [BNetzA-ALG] als geeignet eingestuftem Signaturalgorithmen und Parameter unterstützen. Zum Zeitpunkt der Veröffentlichung dieser Spezifikation sind dies:

- für RSA-Schlüssel der Algorithmus nach [XMLDSIG], Abschnitt 6.4.2, mit einer Schlüssellänge von wenigstens 1024 Bit (empfohlen 2048 Bit),
- für DSA-Schlüssel der Algorithmus nach [XMLDSIG], Abschnitt 6.4.1, mit einer Schlüssellänge von wenigstens 1024 Bit (empfohlen 2048 Bit),
- und für EC-DSA-Schlüssel der Algorithmus nach [ECDSA-XML], Abschnitt 3

3.2.1.3 Kanonisierungsalgorithmen

Die nachfolgende Tabelle spezifiziert die Anforderungsniveaus an eine ArchiSafe konforme Umgebung betreffend die Unterstützung von Kanonisierungsalgorithmen im Kontext der Erzeugung von XML Signaturen.

Bezeichnung	URI	Referenz	Anforderung
C14N	http://www.w3.org/TR/2001/REC-xml-c14n-20010315	[XMLDSIG]	Erforderlich
EC14N	http://www.w3.org/2001/10/xml-exc-c14n	[EC14N]	Erforderlich

3.2.1.4 Transformationsalgorithmen

Die nachfolgende Tabelle spezifiziert die Anforderungsniveaus an eine ArchiSafe konforme Umgebung betreffend die Unterstützung von Transformationsalgorithmen im Kontext der Erzeugung von XML Signaturen

Bezeichnung	URI	Referenz	Anforderung
C14N	http://www.w3.org/TR/2001/REC-xml-c14n-20010315	[XMLDSIG]	Erforderlich
EC14N	http://www.w3.org/2001/10/xml-exc-c14n	[EC14N]	Erforderlich
Base64 Decoder	http://www.w3.org/2000/09/xmlsig#base64	[XMLDSIG]	Erforderlich
XPath Filter 1	http://www.w3.org/TR/1999/REC-xpath-19991116	[XMLDSIG]	Erforderlich
XPath Filter 2	http://www.w3.org/2002/06/xmlsig-filter2	[XPF2]	Erforderlich
Enveloped Signature	http://www.w3.org/2000/09/xmlsig#envelopedsignature	[XMLDSIG]	Erforderlich
XSLT	http://www.w3.org/TR/1999/REC-xslt-19991116	[XMLDSIG]	Erforderlich
Binary Mode Decryption	http://www.w3.org/2002/07/decrypt#Binary	[XMLDTF]	Erforderlich

3.2.1.5 Schlüsselinformationen

In einer XML-Signatur können Informationen zum Auffinden des Prüfschlüssels im XML-Element `dsig:KeyInfo` (vgl. [XMLDSIG]) angegeben werden. Eine ArchiSafe konforme Umgebung *muss* in dieses XML-Element jedenfalls das Signaturzertifikat aufnehmen. Darüber hinaus wird *empfohlen*, die gesamte Kette an Zertifikaten, die zur Prüfung der Signatur benötigt wird (Signaturzertifikat bis zu einer vertrauenswürdigen Wurzelinstanz), ebenfalls in dieses XML-Element aufzunehmen.

Es wird empfohlen, gemäß [XMLDSIG], unter dem `dsig:KeyInfo` Element in einer Liste von X509Data Elementen die zur Prüfung der Signatur benötigten Zertifikate und öffentlichen Schlüssel abzulegen.

3.2.2 Signaturprüfung

Dieser Abschnitt spezifiziert ein Profil von [XMLDSIG], das von einer ArchiSafe konformen Umgebung im Kontext der Verifikation einer XML Signatur zumindest beherrscht werden *sollte*.

3.2.2.1 Digest-Algorithmen

Eine ArchiSafe konforme Umgebung *muss* jedenfalls einen der in Abschnitt 3.1.1.1 dieses Dokuments aufgeführten Algorithmen zur Berechnung des Message Digest im Rahmen einer Signaturprüfung nach [XMLDSIG] unterstützen (SHA-1, RIPEMD-160).

3.2.2.2 Signaturalgorithmen

Die nachfolgende Tabelle spezifiziert die Anforderungslevels an eine ArchiSafe konforme Umgebung betreffend die Unterstützung von Signaturalgorithmen im Rahmen einer Signaturprüfung nach [XMLDSIG]

Bezeichnung	URI	Normative Referenz	Erforderlich
RSA-SHA1	http://www.w3.org/2000/09/xmldsig#dsasha1	[XMLDSIG]	Ja
DSA-SHA1	http://www.w3.org/2000/09/xmldsig#rsasha1	[CMS-ALG]	Ja
ECDSASHA1	http://www.w3.org/2001/04/xmldsigmore#ecdsa-sha1	[ECDSA-XML]	Ja

3.2.2.3 Kanonisierungsalgorithmen

Für die Tabelle der Anforderungslevels an eine ArchiSafe konforme Umgebung betreffend die Unterstützung von Kanonisierungsalgorithmen im Rahmen einer Signaturprüfung nach [XMLDSIG] siehe Abschnitt 3.2.1.3.

3.2.2.4 Transformationsalgorithmen

Für die Tabelle der Anforderungslevels an eine ArchiSafe konforme Umgebung betreffend die Unterstützung von Transformationsalgorithmen im Rahmen einer Signaturprüfung nach [XMLDSIG] siehe Abschnitt 3.2.1.4.

3.2.2.5 Schlüsselinformationen

In einer XML-Signatur können Informationen zum Auffinden des Prüfschlüssels im XML-Element `dsig:KeyInfo` (vgl. [XMLDSIG], Abschnitt 4.4) angegeben sein. Die nachfolgende Tabelle spezifiziert die Anforderungslevels an eine ArchiSafe konforme Umgebung betreffend die Unterstützung von XML-Elementen, die darin vorkommen können. Alle nicht explizit in der Tabelle erwähnten XML-Elemente *dürfen* von der ArchiSafe Umgebung ausgewertet werden.

Kindelement	Anforderung	Anmerkung
<code>dsig:RSAKeyValue</code>	EMPFOHLEN	-
<code>dsig:DSAKeyValue</code>	EMPFOHLEN	-
<code>Dsm:ECDSAKeyValue</code>	EMPFOHLEN	-
<code>dsig:X509IssuerSerial</code>	EMPFOHLEN	Dieses Element bezeichnet auf eindeutige Weise ein Zertifikat.
<code>dsig:X509Certificate</code>	ERFORDERLICH	-
<code>dsig:X509CRL</code>	ERFORDERLICH	Eine mit diesem Element kodierte Widerrufsliste muss zwar von einer ArchiSafe konformen Umgebung verstanden, aber nicht verwendet werden.
<code>dsig:RetrievalMethod</code> mit Verweis auf <code>dsig:X509Data</code>	ERFORDERLICH	Für die XML-Kindelemente des <code>dsig:X509Data</code> , auf das verwiesen wird, gelten wiederum die Anforderungslevels dieser Tabelle.

Für die dauerhafte Überprüfbarkeit elektronischer Signaturen wird empfohlen, gemäß [XMLDSIG], unter dem `dsig:KeyInfo` Element in einer Liste von `X509Data` Elementen die zur Prüfung der Signatur benötigten Zertifikate, CRL's oder OCSP-Responses und Schlüsselinformationen abzulegen.

4 Elektronische Zeitstempel

Mit Hilfe qualifizierter elektronischer Signaturen und qualifizierter elektronischer Signaturen mit Anbieterakkreditierung kann nach dem Signaturgesetz die Integrität und Authentizität elektronischer Dokumente nachgewiesen werden, wenn die zugrunde liegenden kryptographischen Algorithmen und deren Parameter sicherheitsgeeignet sind. Umgekehrt wird der Beweiswert elektronischer Dokumente beeinträchtigt, wenn diese Algorithmen im Laufe der Zeit ihre Sicherheitseignung verlieren. Der Anwender elektronischer Archivsysteme ist daher gehalten, geeignete Maßnahmen zu ergreifen, mit denen der Beweiswert elektronischer Signaturen und elektronisch signierter Dokumente über im Voraus unbestimmte Zeit erhalten werden kann.

ArchiSafe setzt für den Nachweis, dass elektronische Dokumente zu einem bestimmten Zeitpunkt dem elektronischen Archiv übergeben wurden und für den Erhalt der Beweiskraft elektronisch signierter Dokumente durch die gesetzeskonforme Signaturneuerung gemäß § 17 Signaturverordnung, auf den Einsatz elektronischer Zeitstempel nach dem ArchiSig-Konzept [ArchiSig].

4.1 Archivzeitstempel

Ein ArchiSafe konformes elektronisches Archivsystem *muss* die Verifikation, dass zu einem bestimmten Zeitpunkt elektronische Dokumente dem elektronischen Archivsystem zur Ablage vorgelegt wurden durch die Bildung elektronischer Archivzeitstempel gemäß dem ArchiSig-Konzept und konform dem z. Z. in Verabschiedung befindlichen Standard ERS der IETF Arbeitsgruppe LTANS unterstützen. Als Zeitstempelformat und –protokoll muss hierzu der IETF RFC3161 [TSP 2001] unterstützt werden.

Erläuterung

Bei dem als RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol [TSP 2001] veröffentlichten Dokument handelt es sich um die Spezifikation eines Trusted-Third-Party-Protokolls, das zum Nachweis der Existenz eines elektronischen Dokuments zu einem gewissen Zeitpunkt dient. Das European Telecommunication Standards Institute (ETSI) hat auf der Grundlage des RFC 3161 seinerseits einen elektronischen Zeitstempel

spezifiziert, der jedoch eine Vielzahl der im RFC 3161 möglichen Optionen einschränkt [ETSI-TS].

Darauf aufbauend hat die IETF Arbeitsgruppe Long-Term Archive and Notary Services (LTANS) einen Spezifikationsvorschlag für einen Archivzeitstempel unterbreitet [LTANS:ERS]. Danach ist ein Archivzeitstempel ein Datenkonstrukt aus einem Zeitstempel (gemäß RFC 3161) und einer Sammlung (Liste) von Hashwerten, das es erlaubt, die Existenz eines Datenobjektes oder einer Gruppe von Datenobjekten zu einem bestimmten Zeitpunkt zu verifizieren. Die Sammlung (Liste) der Hashwerte kann durch Reduktion eines geordneten Merkle-Hashbaumes [MER 1980] erzeugt werden.

4.1.1 Zeitstempelanfrage

Dieser Abschnitt spezifiziert ein Profil von [TSP 2001], das von einer ArchiSafe konformen Umgebung bei einer Zeitstempelanfrage unterstützt werden *muss*.

4.1.1.1 Hash-Algorithmen

Zur Berechnung des Hashwertes für eine Zeitstempelanfrage nach [TSP 2001], *muss* eine ArchiSafe konforme Umgebung die von der Bundesnetzagentur zum Zeitpunkt der Archivierung als sicher eingestuft Algorithmen verwenden [BNetzA-ALG]. Danach gelten der Algorithmen SHA-1 [CMS-ALG] bis Ende 2009, RIPEMD-160 [ISO/IEC 10118-3] bis Ende 2010 und die Algorithmen SHA-224, SHA-256, SHA-384, SHA-512 bis Ende 2011 als für die Anwendung bei digitalen Signaturen geeignet.

4.1.1.2 Signaturalgorithmen

Zur Berechnung der Zeitstempelsignatur nach [TSP 2001], *muss* der Zeitstempeldienstanbieter die zum Zeitpunkt der Archivierung von der Bundesnetzagentur [BNetzA-ALG] als geeignet eingestuft Signaturalgorithmen und Parameter unterstützen. Zum Zeitpunkt der Veröffentlichung dieser Spezifikation sind dies:

- für RSA-Schlüssel den Algorithmus nach [CMS-ALG], Abschnitt 3.2, mit einer Schlüssellänge von wenigstens 1024 Bit (empfohlen 2048 Bit),
- für DSA-Schlüssel den Algorithmus nach [CMS-ALG], Abschnitt 3.1, mit einer Schlüssellänge von wenigstens 1024 Bit (empfohlen 2048 Bit),
- und für EC-DSA-Schlüssel den Algorithmus nach [ECDSA-CMS], Abschnitt 2.1.1.

4.1.1.3 Transportprotokoll

Von den in [TSP 2001] genannten Protokollen *muss* eine ArchiSafe konforme Umgebung mindestens folgendes Protokoll unterstützen:

- Time Stamp Protocol via http (Abschnitt 3.4 in [TSP 2001])

Eine Anfrage via https wird *empfohlen*.

4.2 Gesetzeskonforme Signaturerneuerung

Ein ArchiSafe konformes elektronisches Archivsystem *muss* die Erneuerung der Signaturen elektronisch signierter Dokumente gemäß § 17 Signaturverordnung (SigV) nach dem ArchiSig-Konzept unterstützen.

Erläuterung

Das ArchiSig-Konzept [ArchiSig] sieht vor, bei der Archivierung eines elektronisch signierten Dokuments, spätestens jedoch vor Ablauf der Sicherheitseignung eines verwendeten Algorithmus oder Parameters einen initialen Zeitstempel zu bilden. Zu diesem Zweck wird aus den Hashwerten der archivierten Dokumente ein Hashbaum aufgebaut und ein Zeitstempel eingeholt. Bezieht sich der initiale Archivzeitstempel auf das signierte Dokument mit allen darin enthaltenen Signaturen und sind die kryptographischen Algorithmen und Parameter des Archivzeitstempels noch sicherheitsgeeignet, dann ist dieser Archivzeitstempel beweisgeeignet und die Anforderungen des Signaturgesetzes für die erneute Signatur sind erfüllt.

Die Syntax und das Vorgehen bei der Bildung des Archivzeitstempels sind in [LTANS:ERS] beschrieben.¹

4.2.1 Bildung des Archivzeitstempels

Dieser Abschnitt spezifiziert ein Profil von [LTANS:ERS], das von einer ArchiSafe konformen Umgebung bei der Bildung eines Archivzeitstempels unterstützt werden *muss*.

¹ Eine ausführliche Diskussion der Rechtssicherheit und Beweiskraft dieses Konzeptes findet sich in [ERV].

4.2.1.1 Syntax des Archivzeitstempels

Der Archivzeitstempel ist konform zum ArchiSig-Konzept zu erstellen. Die Syntax muss dem z. Z. in Verabschiedung befindlichen Standard ERS [LTANS:ERS] der WG Long term archiving and notary services (LTANS) entsprechen und zu diesem Standard konform sein.²

4.2.1.2 Bildung des Archivzeitstempels

Der Archivzeitstempel wird über eine definierte Datenmenge gebildet. Dazu werden so genannte Hashbäume aufgebaut mit den Hashwerten der einzelnen zu schützenden Dateien als unterste Blätter (siehe [MER 1980]). Dabei sollten mindestens der ArchiSafe-Container, in diesem referenzierte Dokumente und alle zu diesen Dokumenten gehörenden Signatur- und Beweisdaten ebenfalls von demselben Archivzeitstempel gesichert werden. Weitere Dokumente und deren zusätzlichen Daten können selbstverständlich ebenfalls in die geschützte Menge aufgenommen werden.³

Zum Aufbau des Archivzeitstempels wird nach Erzeugung des Hashbaumes dessen Integrität gesichert indem für den obersten Knoten ein akkreditierter Zeitstempel eingeholt und in der Datenstruktur des Archivzeitstempels gespeichert wird. Beim Einholen dieses Zeitstempels gemäß RFC3161 werden ebenfalls bereits alle zu dessen späterer Prüfung notwendigen Zertifikate bis einschließlich zum obersten Knoten der Kette eingeholt und falls möglich innerhalb des Zeitstempels gespeichert. Vor Eintritt des Verfalls der Sicherheitseignung von Algorithmen oder deren Parametern wird der Archivzeitstempel durch die beschriebenen Verfahren ([LTANS:ERS]) der Signaturerneuerung und der Hashbaumerneuerung erneut gesichert und dadurch ein um diese Daten erweiterter Archivzeitstempel verfügbar.

² Anm.: In der internationalen Literatur wird für Archivzeitstempel auch der Begriff Evidence Record oder kurz ERS (Evidence Record Syntax) verwendet.

³ Typischerweise wird man einen Archivzeitstempel einmal am Tag einholen für alle an diesem Tag eingegangenen Dokumente und deren aggregierte Signatur- und Beweisdaten. Sollten innerhalb des ArchiSafe-Containers die zusätzlichen Daten wie Signaturen und Beweisdaten nur über Links referenziert sein, sollten diese Kopien ebenfalls in dem ArchiSafe konformen System aufbewahrt werden und durch den Archivzeitstempel mit geschützt werden. (Anm.: Die Signaturverordnung spricht im Falle einer Signaturerneuerung in §17 davon, dass „...die Daten ... mit einer neuen qualifizierten elektronischen Signatur zu versehen“ sind. „Diese muss ..., frühere Signaturen einschließen ...“, woraus sich empfiehlt, alle relevanten Daten unter einem gemeinsamen Archivzeitstempel zu sichern.)

4.2.1.3 Verifikation des Archivzeitstempels

Die Verifikation des Archivzeitstempels erfolgt gemäß der in [LTANS:ERS] spezifizierten Weise:

Alle Hashbäume, Zeitstempel und deren Verlinkungen innerhalb des Archivzeitstempels werden verifiziert. Zusätzlich wird für jeden Zeitstempel dessen Zertifikatskette bis Wurzel verfolgt und verifiziert. Diese Zertifikate sollten in den Zeitstempeln gemäß RFC3161 im Archivzeitstempel gespeichert werden, können in Ausnahmefällen aber auch zentral im System vorgehalten werden.⁴ Nur wenn alle Prüfungen erfolgreich verifiziert wurden, darf der Archivzeitstempel als gültig angesehen werden.

4.2.1.4 Bereitstellung und Aufruf der Verifikation des Archivzeitstempels

Ein ArchiSafe konformes System muss mindestens eine Schnittstelle anbieten, um den beweissichernden Archivzeitstempel (evidence record) zu einem Dokument zu extrahieren. Es empfiehlt sich, dass diese Schnittstelle über einen einfachen HTTP-Aufruf realisiert wird.

Diese extrahierten Beweisdaten können dann in ihrer transportfähigen Form (spezifiziert in [LTANS:ERS] einem unabhängigen Gutachter oder einer unabhängigen Prüfkomponeute z.B. im Falle eines Rechtsstreites vorgelegt werden. Zur Verifikation ist damit der Zugang zum Gesamtsystem explizit nicht notwendig. Es ist hinreichend die Daten selbst und die Beweisdaten (Archivzeitstempel/evidence record) der prüfenden Instanz vorzulegen.

Zusätzlich sollte ein ArchiSafe konformes System über eine eigene Prüfroutine verfügen.⁵

⁴ Da akkreditierte Zeitstempel verwendet werden, ist eine Überprüfung der OCSP-Responses für die Zertifikatskette der Zeitstempel nicht zwingend erforderlich.

⁵ Damit kann z.B. vor oder bei jeder Abfrage eines Dokumentes der Archivzeitstempel intern auf dem Server verifiziert werden und im Fehlerfall ein entsprechender Hinweis an den Benutzer oder Administrator erfolgen. Hiermit kann sichergestellt werden, dass der Benutzer über möglicher Verfälschungen der Dokumente informiert wird.

5 Referenzen

- ArchiSig** Roßnagel, A., Schmücker, P. (Hrsg.): Beweiskräftige elektronische Archivierung, Economica-Verlag, ISBN 3-87081-427-6
- BNetzA-ALG** Bundesnetzagentur: Geeignete Kryptoalgorithmen. Veröff. Im Bundesanzeiger Nr. 158 – S. 18 562 vom 24. August 2001, unter <http://www.bundesnetzagentur.de>
- CMS** Hously, R.: RFC 3852 – Cryptographic Message Syntax (CMS), Juli 2004, unter <http://www.ietf.org/rfc/rfc3852>
- CMS-ALG** Hously, R.: RFC 3370 – Cryptographic Message Syntax (CMS) Algorithms, August 2002, unter <http://www.ietf.org/rfc/rfc3370>
- EC14N** Boyer, J., Eastlake, D. und Reagle, J.: Exclusive XML Canonicalization. W3C Recommendation, Juli 2002,, unter <http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/>
- ECDSA-CMS** Blake-Wilson, S., Brown, D., Lampert, D.: RFC 3278 – Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS), April 2002, unter <http://www.ietf.org/rfc/rfc3278>
- ECDSA-XML** Blake-Wilson, S., Karlinger, G. und Wang, Y.: ECDSA with XML-Signature Syntax. Internet-Draft, März 2004
<http://tools.ietf.org/id/draft-blake-wilson-xmldsig-ecdsa-09.txt>
- ETSI-TS** ETSI-TS 101 861 V 1.2.1 Time stamping profile, März 2002, unter : <http://www.etsi.org>
- ISO/IEC 10118-3** ISO/IEC 10118-3, Information technology – Security techniques – Hash functions – Part 3: Dedicated hash functions, 1998
- LTANS:ERS** Brandner, R., Gondrom, T., Pordesch, U., Evidence Record Syntax (draft-ietf-ltans-ers-09), Januar 2007, unter

<http://www.ietf.org/internet-drafts/draft-ietf-ltans-ers-09.txt>

- MER 1980** Merkle, R.: Protocols for Public Key Cryptosystems, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA), pages 122-134, April 1980.
- ERV** Fischer-Dieskau, S.: Der elektronische Rechtsverkehr: Das elektronisch signierte Dokument als Mittel zur Beweissicherung, Nomos Verlag, ISBN 3-8329-1819-1
- RFC1521** Borenstein, N., Freed, N.: RFC 1521 - MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies, unter:
<http://www.ietf.org/rfc/rfc1521>
- RFC3126** Pinkas, D., Ross, J., Pope, N.: RFC 3126 – Electronic signature formats for long term electronic signatures, September 2001, unter
<http://www.ietf.org/rfc/rfc3126>
- TSP 2001** Adams, C., Cain, P., Pinkas, D., Zuccherato, R.: RFC 4161 – Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP), August 2001, unter:
<http://www.ietf.org/rfc/rfc3161>
- XMLDSIG** Eastlake, D., Reagle, J., Solo, D.: RFC 3275 – (Extensible Markup Language) XML-Signature Syntax and Processing, März 2002, unter:
<http://www.ietf.org/rfc/rfc3275>
- XMLDTF** Hughes, M., Imamura, T. und Maruyama, H.:
Decryption Transform for XML Signature. W3C Recommendation, Dezember 2002. unter
<http://www.w3.org/TR/2002/REC-xmlenc-decrypt-20021210>
- XPF2** Boyer, J., Hughes, M. und Reagle, J.: XML-Signature XPath Filter 2.0. W3C Candidate Recommendation, Juli 2002, unter
<http://www.w3.org/TR/2002/CR-xmlsig-filter2-20020718/>.