

SAGA-5.0-Empfehlungen für die staatlichen Behörden des Freistaates Sachsen

1 Einleitung

Für die in SAGA 5.0 enthaltenen Spezifikationen gelten für den jeweiligen Status der Spezifikation bestimmte Regeln:

»Beobachtet«

Wenn es neben den beobachteten Spezifikationen keine konkurrierenden, empfohlenen oder verbindlichen Spezifikationen gibt, SOLLTEN beobachtete Spezifikationen in Software-Systemen eingesetzt werden. Nur in begründeten Ausnahmen KÖNNEN beobachtete Spezifikationen empfohlenen Alternativen vorgezogen werden.

»Empfohlen«

Konkurrierende Spezifikationen KÖNNEN nebeneinander empfohlen sein, wenn sich ihre Anwendungsschwerpunkte deutlich unterscheiden. In solchen Fällen SOLLTE die für die jeweilige Anwendung am besten geeignete Spezifikation angewendet werden.

Von den empfohlenen Spezifikationen KANN in begründeten Ausnahmen abgewichen werden. Zu einer empfohlenen Spezifikation gibt es keine verbindliche Alternative, da eine Empfehlung neben einer verbindlich einzusetzenden Spezifikation nicht sinnvoll ist.

»Verbindlich«

Konkurrierende Spezifikationen KÖNNEN nebeneinander verbindlich sein, wenn sich die Anwendungsschwerpunkte deutlich unterscheiden. In solchen Fällen MUSS die für die jeweilige Anwendung am besten geeignete Spezifikation verwendet werden.

Spezifikationen dieser Klassifikation sind im eigentlichen Sinne des Wortes verbindlich, MÜSSEN also bei der Einführung eines neuen Software-Systems jeder Alternative vorgezogen werden. Abweichungen gefährden die Ziele von SAGA in hohem Maße und sind deshalb nicht zugelassen.

Bei der funktionalen Änderung oder Erweiterung eines Software-Systems KÖNNEN als »Bestandsgeschützt« klassifizierte Spezifikationen weiterhin genutzt werden. Es MUSS jedoch geprüft werden, ob die Migration zur verbindlichen Spezifikation vorteilhaft ist.

»Bestandsgeschützt«

Bei der funktionalen Änderung oder Erweiterung eines Software-Systems stehen diese Spezifikationen unter Bestandsschutz und KÖNNEN auch weiterhin eingesetzt werden. Es SOLLTE geprüft werden, ob eine Migration zu den in SAGA als »Beobachtet« oder »Empfohlen« klassifizierten Spezifikationen Vorteile gegenüber dem Festhalten an als »Bestandsgeschützt« klassifizierten Spezifikationen bringt. Gibt es eine als »Verbindlich« klassifizierte Alternative, MUSS diese Überprüfung durchgeführt werden. Für neue Software-Systeme SOLLTEN bestandsgeschützte Spezifikationen NICHT mehr zum Einsatz kommen.

Für den Freistaat Sachsen werden die in der Anlage definierten Spezifikationen empfohlen, die sich an SAGA 5.0 orientieren.

2 Empfehlungen für die staatlichen Behörden des Freistaates Sachsen

In der folgenden Übersicht sind jeweils die in SAGA 5.0 der Bundesverwaltung definierten Standards tabellarisch aufgeführt sowie (gelb gekennzeichnet) die daraus abgeleiteten Empfehlungen für die staatlichen Einrichtungen des Freistaates Sachsen enthalten. Soweit keine Empfehlungen für Sachsen explizit angegeben sind, wird den Empfehlungen von SAGA 5.0 gefolgt.

2.1 IT-Sicherheitskonzeption

Managementsysteme für Informationssicherheit			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • BSI-Standard 100-1 ≥ 1.5 • BSI-Standard 100-1 1.5 			<ul style="list-style-type: none"> • BSI-Standard 100-1 1.0

IT-Grundschutz-Vorgehensweise			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • BSI-Standard 100-2 ≥ 2.0 • BSI-Standard 100-2 2.0 			<ul style="list-style-type: none"> • BSI-Standard 100-2 1.0

Risikoanalyse			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • BSI-Standard 100-3 ≥ 2.5 • BSI-Standard 100-3 2.5 			<ul style="list-style-type: none"> • BSI-Standard 100-3 2.0

Notfallmanagement			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • BSI-Standard 100-4 ≥ 1.0 • BSI-Standard 100-4 1.0 			

Umsetzung der Sicherheitskonzeption			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • BSI, IT-Grundschutz-Kataloge in der jeweils aktuellen Version 			<ul style="list-style-type: none"> • BSI, E-Government-Handbuch, Modul »Authentisierung im E-Government« • KoopA ADV, Handlungsleitfaden 1.1

2.2 Prozessmodelle

Technologien zur Prozessmodellierung			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • UML 2.x • Flussdiagramme • BPMN 1.1/1.2 • EPK 	<ul style="list-style-type: none"> • BPMN 2.0 	<ul style="list-style-type: none"> • UML ≤1.5

Austauschformate für Prozessmodelle			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • XMI 2.x 	<ul style="list-style-type: none"> • XPDL 2.1 • EPML 1.2 	<ul style="list-style-type: none"> • XMI 1.x

2.3 Datenmodelle

Technologien zur Datenmodellierung			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • ERD • UML 2.x 		<ul style="list-style-type: none"> • UML ≤1.5

Austauschformate für Datenmodelle			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
<ul style="list-style-type: none"> • XSD 1.0 	<ul style="list-style-type: none"> • Relax NG • XMI 2.x 		<ul style="list-style-type: none"> • XMI 1.x • DTD

Beschreibungssprachen für Metadaten			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • RDF 		

Vokabulare für Metadaten			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • DCES 		

2.4 Applikationsarchitektur

Applikationsarchitektur für große Projekte			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • Java EE 7 • CLI 		<ul style="list-style-type: none"> • Java EE 5 • J2EE 1.4 • J2EE 1.3

Hinweis: SAGA 5.0 der Bundesverwaltung empfiehlt abweichend zu Sachsen Java EE 6

Applikationsarchitektur für kleine und mittlere Projekte			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • Java SE 8 • PHP 5.x • C++ • Python 	<ul style="list-style-type: none"> • Ruby • CLI 	<ul style="list-style-type: none"> • J2SE 5.0 • J2SE 1.4 • J2SE 1.3 • PHP 4.x • Perl

Hinweis: SAGA 5.0 der Bundesverwaltung empfiehlt abweichend zu Sachsen Java SE 6

Dienstorientierte Architekturen			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • WS-I Basic Profile 1.1 / 1.2 • WSDL 1.1 • WS-BPEL 2.0 	<ul style="list-style-type: none"> • WS-I Basic Profile 2.0 • WSDL 2.0 • SCA 1.0 	

2.5 Client

Client-Anwendungen			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • Java SE 8 • JNLP 6.x 		<ul style="list-style-type: none"> • J2SE 5.0 • JNLP 1.5

Hinweis: SAGA 5.0 der Bundesverwaltung empfiehlt abweichend zu Sachsen Java SE 6

Informationszugriff mit mobilen Endgeräten			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
		<ul style="list-style-type: none"> • Java ME 8.x 	

Hinweis: SAGA 5.0 der Bundesverwaltung empfiehlt abweichend zu Sachsen Java ME / MIDP 2.0

Technologien zur Authentisierung			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • WS-Trust 1.3 • WS-Federation 1.1 • SAML ≥1.0 • XACML 2.0 	<ul style="list-style-type: none"> • Kerberos 5 • Open-ID 2.0 • Open-ID 2.0 • ID-SIS 1.0 	<ul style="list-style-type: none"> • ID-FF 1.2 • ID-WSF 1.1 • BSI, E-Government-Handbuch, Modul »Authentisierung im E-Government«

2.6 Präsentation

Barrierefreie Darstellung			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • BITV 			

Zeichensätze und -kodierungen			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • Unicode ≥2.1 • UTF-8 • Umsetzung des IT-Planungsratsbeschlusses: <u>Verbindliche Nutzung des Zeichensatzes »Lateinische Zeichen in UNICODE«</u> 			<ul style="list-style-type: none"> • ISO 8859-1 • ISO 8859-15 • UTF-16

Technologien zur Informationsaufbereitung			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • MIME 1.0 	<ul style="list-style-type: none"> • XHTML 1.0 • HTML 4.01 • CSS2 • XSL 1.1 • XSLT 1.0 / 2.0 • XQuery 		<ul style="list-style-type: none"> • HTML 3.2 • XSL 1.0

Spezifikationen für aktive Inhalte			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • ECMAScript, 3rd Ed. 		<ul style="list-style-type: none"> • ECMAScript, 5th Ed.

Formulare			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
		<ul style="list-style-type: none"> • XForms 1.1 	<ul style="list-style-type: none"> • XForms 1.0

Austauschformate für Daten			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • XML 1.0 	<ul style="list-style-type: none"> • EML 5.0 	

Formate für Textdokumente zum Informationsaustausch			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • PDF ≥1.4 	<ul style="list-style-type: none"> • Text 		<ul style="list-style-type: none"> • PDF 1.3

Formate für Textdokumente zur Weiterbearbeitung			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • Text • OOXML (MS Word 2010) • ODF Text (OpenOffice 4.1.x / LibreOffice 4.2.x) 	<ul style="list-style-type: none"> • ODF 1.1 • OOXML Transitional • OOXML Strict • DocBook 4.5 	<ul style="list-style-type: none"> • ODF 1.0 • MS Office File Formats • XML 1.0

Formate für Tabellen zum Informationsaustausch			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • PDF ≥1.4 • CSV • HTML 4.01 • XHTML 1.0 		<ul style="list-style-type: none"> • PDF 1.3

Formate für Tabellen zur Weiterbearbeitung			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • CSV • OOXML (MS Excel 2010) • ODF Spreadsheet (OpenOffice 4.1.x / LibreOffice 4.2.x) 	<ul style="list-style-type: none"> • ODF 1.1 • OOXML Transitional • OOXML Strict 	<ul style="list-style-type: none"> • ODF 1.0 • MS Office File Formats • XML 1.0

Formate für Präsentationen zum Informationsaustausch			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • PDF ≥1.4 • HTML 4.01 • XHTML 1.0 	<ul style="list-style-type: none"> • SMIL 3.0 	<ul style="list-style-type: none"> • PDF 1.3 • SMIL 2.0

Formate für Präsentationen zur Weiterbearbeitung			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • OOXML (MS Powerpoint 2010) • ODF Presentation (OpenOffice 4.1.x / LibreOffice 4.2.x) 	<ul style="list-style-type: none"> • ODF 1.1 • OOXML Transitional • OOXML Strict 	<ul style="list-style-type: none"> • ODF 1.0 • MS Office File Formats • XML 1.0

Gesicherter Dokumentenaustausch			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • Common PKI 2.0 • XadES ≥1.3.2 • XML Encryption • XML Signature 		<ul style="list-style-type: none"> • Common PKI 1.1 • ISIS-MTT 1.0 • MTT v2 • XadES 1.2

Austauschformate für Bilder			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • JPEG • PNG 1.2 • GeoTIFF 1.8.2 • GIF v89a • TIFF 6.0 	<ul style="list-style-type: none"> • SVG 1.1 • JPEG 2000 	<ul style="list-style-type: none"> • ECW

Animation			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • GIF v89a 	<ul style="list-style-type: none"> • SVG 1.1 	

Austauschformate für Audiodateien			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • Ogg • MP4 	<ul style="list-style-type: none"> • RealMedia • ASF 1.2 	<ul style="list-style-type: none"> • MP3

Austauschformate für Audio-Streaming			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • HTTP 1.1 • RTSP • Ogg • MP4 	<ul style="list-style-type: none"> • RealMedia • ASF 1.2 	<ul style="list-style-type: none"> • HTTP 1.0

Austauschformate für Videodateien			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • Ogg • MP4 	<ul style="list-style-type: none"> • ASF 1.2 	<ul style="list-style-type: none"> • QTFF • RealMedia

Austauschformate für Video-Streaming			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • HTTP 1.1 • MP4 • Ogg • RTSP 	<ul style="list-style-type: none"> • ASF 1.2 	<ul style="list-style-type: none"> • HTTP 1.0 • QTFF • RealMedia

3D-Daten			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
		<ul style="list-style-type: none"> • X3D Ed. 2 • U3D, 4th Ed. 	

Austauschformate für Geoinformationen			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
<ul style="list-style-type: none"> • GML 3.2.x 	<ul style="list-style-type: none"> • CityGML 1.0.0 • GeoTIFF 1.8.2 • KML 2.2.0 		<ul style="list-style-type: none"> • GML 3.1.1, GML 3.0 • GML 2.1.2, GML 2.0

Datenkompression			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • ZIP 4.5 • Gnu ZIP 4.3 / TAR 		<ul style="list-style-type: none"> • ZIP 2.0

Technologien für die Präsentation auf mobilen Endgeräten			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
<ul style="list-style-type: none"> • SMS 		<ul style="list-style-type: none"> • XHTML Basic 1.1 • WAP 2.0 	<ul style="list-style-type: none"> • XHTML Basic 1.0 • WAP 1.x • WML 1.x

2.7 Kommunikation

Kommunikation zwischen Applikationen innerhalb der Verwaltung			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
<ul style="list-style-type: none"> • WS-Security 1.1 	<ul style="list-style-type: none"> • SOAP 1.1 • MTOM • JMS 1.1 • HTTP 1.1 • Java Portlet Specification ≥1.0 • WSRP ≥1.0 	<ul style="list-style-type: none"> • SOAP 1.2 	<ul style="list-style-type: none"> • WS-Security 1.0 • SwA • JCA 1.5 • CORBA • JAV2I 1.0 • HTTP 1.0

Kommunikation mit verwaltungsexternen Applikationen			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
<ul style="list-style-type: none"> • WS-Security 1.1 	<ul style="list-style-type: none"> • SOAP 1.1 • MTOM • HTTP 1.1 	<ul style="list-style-type: none"> • SOAP 1.2 	<ul style="list-style-type: none"> • WS-Security 1.0 • SwA • CORBA • HTTP 1.0

Netzwerkprotokolle			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
<ul style="list-style-type: none"> • IPv4/IPv6 • DNS 			

E-Mail-Kommunikation			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
<ul style="list-style-type: none"> • MIME 1.0 • SMTP 	<ul style="list-style-type: none"> • Common PKI 2.0 • IMAP4rev1 • POP3 • DKIM 	<ul style="list-style-type: none"> • Sender ID • SPF 1.0 	<ul style="list-style-type: none"> • Common PKI 1.1 • ISIS-MTT 1.0 • MTTv2

IP-Telefonie			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • H.323 • SIP 2.0 		

Anwendungsprotokolle			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • FTP • HTTP 1.1 • OSCI-Transport 1.2 • SSH-2 • TLS 1.1 / 1.2 • WebDAV • Handlungsempfehlungen der AG IS 	<ul style="list-style-type: none"> • OSCI-Transport 2.0 • SPMLv2 • XMPP • FTAM 	<ul style="list-style-type: none"> • HTTP 1.0 • SPML 1.0

Hinweise: Mit Beschluss des AK ITEG Nr. 6/2014 wurden die Handlungsempfehlungen der AG IS »Abschaltung veralteter Verschlüsselungsalgorithmen und Härtung der HTTPS-Konfiguration« bestätigt. Hierin wurde die Abschaltung der optionalen Datenkompression (SSL/TLS Compression) bei TLS 1.1 / 1.2 beschlossen. Darüber hinaus wurde mit Beschluss des AK ITEG Nr. 7/2014 die Abschaltung des als unsicher eingestuft Verschlüsselungsalgorithmus SSLv3 – von SAGA 5.0 der Bundesverwaltung als »Bestandsgeschützt« deklariert – auf allen Internetseiten und -diensten der Landesverwaltung beschlossen.

Geodienste			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • Catalogue Services Specification 2.0.2 • WMS 1.3.0 • WCS ≥1.1 • WFS 2.0 	<ul style="list-style-type: none"> • SFA-2 1.1.0 	<ul style="list-style-type: none"> • SFA-2 1.2.1 • WMTS 1.0.0 	<ul style="list-style-type: none"> • WFS 1.1 • WFS 1.0 • WCS 1.0 • WMS-DE 1.0

2.8 Backend

Zugriff auf Verzeichnisdienste			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • LDAPv3 	<ul style="list-style-type: none"> • DSML v2.0 • UDDI v2.0 	

Zugriff auf Datenbanken und Registrys			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • JDBC 4.0 	<ul style="list-style-type: none"> • JCR 2.0 • CMIS 1.0 • ebXML RS 3.0 / ebXML RIM 3.0 	<ul style="list-style-type: none"> • JDBC 3.0 • JDBC 2.0

Zugriff auf Bestandssysteme			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • WS-Security 1.1 	<ul style="list-style-type: none"> • JCA 1.6 • JMS 1.1 • SOAP 1.1 	<ul style="list-style-type: none"> • SOAP 1.2 	<ul style="list-style-type: none"> • UN/EDIFACT • JCA 1.5 • JAV2I 1.0

2.9 Verschlüsselung

Asymmetrische Verschlüsselungsverfahren			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • RSA • Technische Richtlinie des BSI (Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1) • Handlungsempfehlungen der AG IS 		

Symmetrische Verschlüsselungsverfahren			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • AES 	<ul style="list-style-type: none"> • Technische Richtlinie des BSI (Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1) • Handlungsempfehlungen der AG IS 		<ul style="list-style-type: none"> • IDEA • Triple-DES • Chiasmus

2.10 Elektronische Signatur

Elektronische Signatur			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • Algorithmenkatalog der BNetzA 			

Hashen von Daten			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • SHA-2 			<ul style="list-style-type: none"> • SHA-1 • RIPEMD-160

Asymmetrische Signaturverfahren			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • RSA • DSA 		

Key Management			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
	<ul style="list-style-type: none"> • XKMS 2.0 		

2.11 Smartcards

Kontaktbehaftete Smartcards			
Verbindlich	Empfohlen	Beobachtet	Bestandsgeschützt
<ul style="list-style-type: none"> • Identification Cards – Integrated circuit cards 			

Kontaktlose Smartcards			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
<ul style="list-style-type: none"> • Identification Cards – Contactless integrated circuit cards 			

Lesegeräte und Schnittstellen für Smartcards			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
<ul style="list-style-type: none"> • BSI TR-03112 ≥ 1.1 • BSI TR-03116 ≥ 3.0 	<ul style="list-style-type: none"> • PC/SC 2.x • SICCT 1.20 • Common PKI 2.0 		<ul style="list-style-type: none"> • BSI TR-03112 1.0 • BSI TR-03116 1.0 • SICCT 1.10 • Common PKI 1.1

2.12 Langzeitspeicherung

Langzeitspeicherung			
<i>Verbindlich</i>	<i>Empfohlen</i>	<i>Beobachtet</i>	<i>Bestandsgeschützt</i>
	<ul style="list-style-type: none"> • BSI TR-03125 ≥ 1.1 • PDF/A-1 • JPEG • TIFF 6.0 • XML 1.0 	<ul style="list-style-type: none"> • JPEG 2000 	<ul style="list-style-type: none"> • ArchiSig