

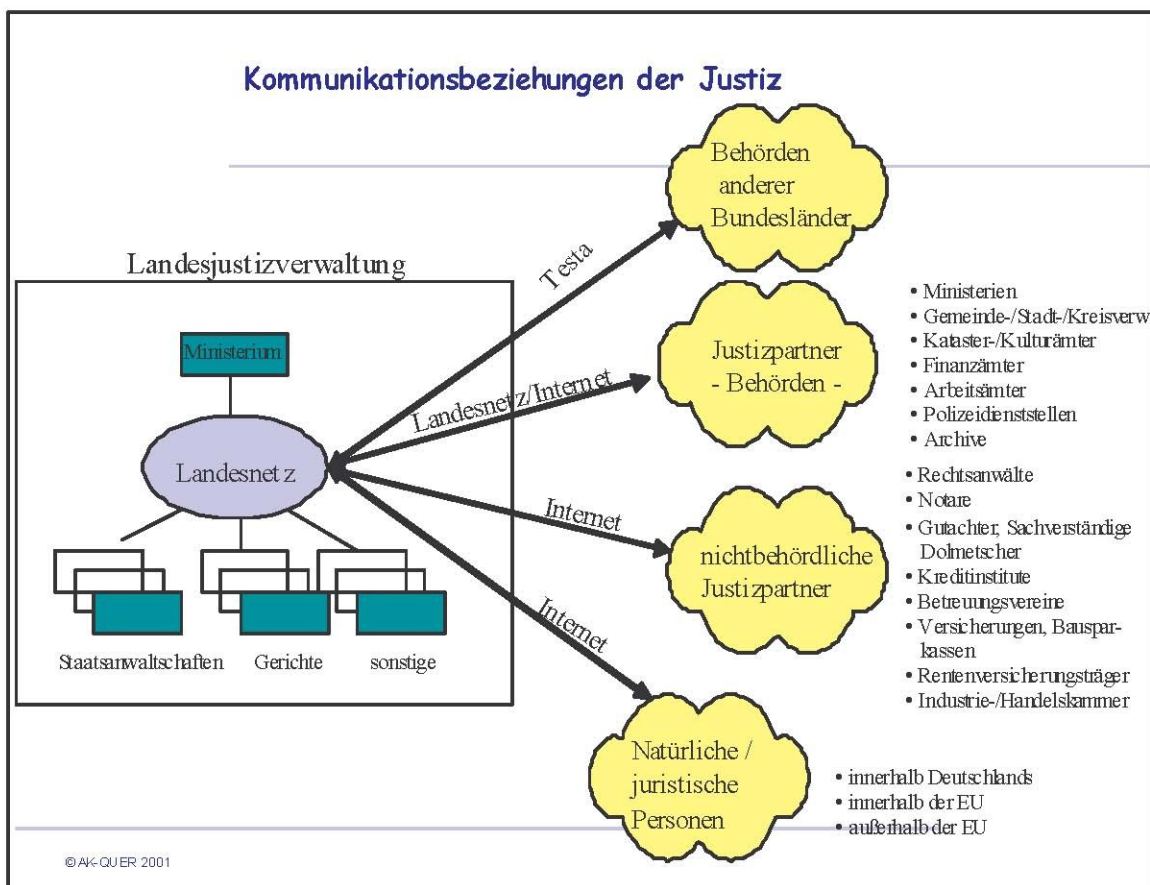
## Technische Rahmenvorgaben für den elektronischen Rechtsverkehr

Stand: ... November 2009

Ziel der Standardisierungsvorgaben der Justiz ist es, unter Beachtung des pragmatisch Leistbaren, eine verlässliche und wirtschaftliche Grundlage für Verfahrensentwicklungen zur elektronischen Kommunikation zu bieten.

Aufgrund der technischen Entwicklung und nach Schaffung der gesetzlichen Grundlagen, z.B. durch das Justizkommunikationsgesetz kann der Schriftverkehr der Justiz nicht mehr nur in Papierform, sondern auch -wirtschaftlich -elektronisch abgewickelt werden.

Dies gilt für viele der beispielhaft dargestellten Kommunikationsbeziehungen:



Die Standards (z.B. für interoperable Produkte zur elektronischen Signatur, Standards für sichere Übertragungen) werden in einem ständigen Prozess in den zuständigen Gremien fortentwickelt.

Endgültige Festlegungen wird es am Markt in absehbarer Zeit nicht geben. Die hier getroffenen Festschreibungen werden daher durch die BLK einheitlich fortgeschrieben und den Dienststellen zugänglich gemacht werden.

Auftragnehmer der Justiz sollen im Rahmen des ERV – mit Auftragserteilung durch eine Justizverwaltung – schriftlich zur Nutzung bzw. Einhaltung der hier aufgeführten Basisverfahren bzw. Standards<sup>1</sup> verpflichtet werden.

Der elektronische Rechtsverkehr wird vorrangig unter dem Gesichtspunkt von Außenwirkungen (z.B. andere Behörden, Notare, Steuerberater, Anwälte, Bürger) -also der Schnittstellen -betrachtet. Die vorgeschlagenen einheitlichen Technologien beziehen sich hierauf. Wenn es im Einzelfall wirtschaftlicher sein sollte, an der Schnittstelle zu konvertieren und innerhalb eines EDV-Verfahrens der Justiz andere Technologien einzusetzen bzw. eine bereits eingesetzte Technologie beizubehalten, ist dies unbenommen. Da die Vernetzung und der Austausch von Daten immer mehr zunehmen werden und zukünftig Bereiche einbeziehen können, die zurzeit noch gar nicht absehbar sind, sollten bei neuen EDV-Verfahren auch intern grundsätzlich die vorgeschlagenen Technologien eingesetzt werden, um für jetzt noch nicht absehbare Anforderungen ohne tiefgreifende Änderung der bestehenden EDV-Verfahren gerüstet zu sein.

Eine wesentliche Rationalisierungschance des elektronischen Rechtsverkehrs liegt in der möglichen Datenübernahme aus den Schriftsätzen der Parteien in das gerichtliche Schreibwerk sowie in der vereinfachten Auswertung und Aufbereitung strukturierter Eingaben. Das Datenaustauschformat XJustiz legt die Schnittstelle zum Austausch strukturierter Daten für alle Kommunikationspartner der Justiz verlässlich und verbindlich fest.

Versionsnummern von Dateiformaten (z.B. Word V 2003) können zusätzlich zu den nachfolgend festgelegten Dokumentenformaten bekannt gemacht werden, um die tatsächliche Bearbeitbarkeit eines Eingangs durch das Gericht (vgl. z.B. § 130a ZPO)

sicherstellen und um anderen Beteiligten am elektronischen Rechtsverkehr einen verlässlichen Rahmen für ihre Teilnahme aufzeigen zu können.

Es wird ein Mindestzeitraum vorgesehen, seit dem eine zugelassene Version verfügbar sein sollte, um sowohl eine gewisse Verbreitungschance bei den am elektronischen Rechtsverkehr Beteiligten wahren als auch mögliche Probleme und die Stabilität der Version aufgrund von Erfahrungen einschätzen zu können.

---

<sup>1</sup> Auf verbindlich vorzugebende Standards wird im Folgenden durch entsprechende Formulierungen im Text hingewiesen. Tabellarisch werden sie auch in der Inhaltsübersicht aufgeführt.

Übersicht:

	<b>Verbindliche Standards</b>	<b>Seite</b>
<b>I. Organisatorischer Rahmen</b>	SAGA	<b>5</b>
1. Übergreifende Standards		5
2. Risiko-und Bedrohungsanalyse:		5
3. Verfügbarkeit		6
4. Virenschutz		6
5. Firewalls		6
6. Signaturzertifikatsprüfung bei Eingang		6
7. Dokumentation des Zugangszeitpunktes, Zeitstempel		6
<b>II. Medien und Anlagengröße</b>		<b>8</b>
1. Anlagengröße bei E-Mails	max. 5 MB	8
2. CD-ROM		8
3. DVD	(Einsatz nicht empfohlen)	8
<b>III. Dokumentenformate</b>		<b>9</b>
1. Erfordernis einheitlicher Dokumentenformate		9
2. Kriterien der Formatvorgaben		9
3. Formate zum Austausch codierter Daten	ASCII, UNICODE, RTF, PDF/A, XML, Word	10
4. Formate zum Austausch nicht-codierter Daten	PDF/A, TIFF	13
5. Langfristige Speicherung, Archivierung	PDF/A	14
<b>IV. Übergabe strukturierter Daten, (Xjustiz)</b>	XJustiz	<b>17</b>
1. Zielgruppen		17
2. Aufbau von XJustiz		17
3. Anpassungen und Erweiterungen von XJustiz		18
4. Informationen zu XJustiz		19
<b>V. Authentisierung und Verschlüsselung</b>		<b>19</b>
1. Basisverfahren	Common-PKI-Profilierung von X.501, X.509 V3, PKCS#7, PKCS#11	19
2. Elektronische Signaturen nach SigG und Attribute		21
3. Gesetzeskonformität von Signaturanwendungskomponenten		23
4. Fortgeschrittene elektronische Signatur		24
5. Verschlüsselung		24
<b>VI. Übertragungswege</b>		<b>25</b>
1. E-Mail	SMTP	25
2. Nutzung von Webservern/Portalen		26
a) Zugang über Browser	SSL, S-HTTP	26
b) Zugang über Applikationen	OSCI V 1.2	26
<b>VII. Elektronische Akte</b>	(Abstimmung mit XDOMEA	<b>27</b>

## I. Organisatorischer Rahmen

### 1. Übergreifende Standards

SAGA<sup>2</sup> ist ein Standard des Bundes und beschreibt empfohlene technische Rahmenbedingungen für die Entwicklung, Kommunikation und Interaktion von IT-Systemen der Bundesbehörden. Für Prozesse und Systeme, die E-Government-Dienstleistungen des Bundes erbringen, ist die Konformität mit SAGA verbindlich. Für Systeme, die keine direkten Schnittstellen zum E-Government haben, wird eine Migration empfohlen, wenn die Kosten-Nutzen-Betrachtung positiv ausfällt. Standards werden in drei Klassen eingeordnet: "obligatorisch", "empfohlen" und "unter Beobachtung". Standards sind "obligatorisch", wenn sie sich bewährt haben und die bevorzugte Lösung darstellen -sie sind verbindlich. Als "empfohlen" gelten Standards, wenn sie sich bewährt haben, aber entweder nicht zwingend erforderlich sind bzw. nicht die bevorzugte Lösung darstellen. Standards stehen "unter Beobachtung", wenn sie der gewünschten Entwicklungsrichtung folgen, aber noch nicht ausgereift sind oder sich noch nicht bewährt haben.

Es wird empfohlen, in ERV-Projekten den SAGA-Standard zugrunde zu legen und entsprechende Konformitätszusicherungen einzuholen.

### 2. Risiko-und Bedrohungsanalyse

Inwieweit die Komponenten des Kommunikationssystems für den angestrebten Verwendungszweck als sicher anzusehen sind bzw. – z.B. über Verschlüsselung – zusätzlich zu sichern sind, ist durch eine Risiko-und Bedrohungsanalyse, die auch mögliche dezentrale Client-Standorte und mögliche zentrale Posteingangsstellen berücksichtigt, festzustellen.

Dabei ist zu klären, an welcher Stelle einzelne Verarbeitungsschritte erfolgen (wenn z.B. die Verschlüsselung von Mailanhängen nicht auf dem Client, sondern auf dem Mailserver durchgeführt würde, müsste ggf. zwischen Client und Mailserver eine sichere Verbindung bestehen).

---

<sup>2</sup> „Standards und Architekturen für E-Government-Anwendungen (SAGA)“ – Empfehlungen des Bundes für den IT-Einsatz in öffentlichen Verwaltungen.

Zur aktuellen Version siehe unter: [http://www.cio.bund.de/cln\\_103/DE/Standards/SAGA/saga\\_node.html](http://www.cio.bund.de/cln_103/DE/Standards/SAGA/saga_node.html)

### **3. Verfügbarkeit**

In einer Analyse ist verfahrensspezifisch und in Abhängigkeit von den Landesystemkonzepten festzulegen, welche Verfügbarkeit der einzelnen Komponenten der EDV-Systeme erforderlich ist.

### **4. Virenschutz**

Serversysteme (Dateiserver, Mailserver, Applikations- und Datenbankserver) sowie die Clients sind mit Virenschutzsoftware, die regelmäßig aktualisiert wird, auszustatten. Virenschutzprogramme sind so zu konfigurieren, dass Dokumente nicht verändert werden und dadurch z.B. die Signatur zerstört wird.

### **5. Firewalls**

Der Übergang zu öffentlichen Netzen ist nach dem Stand der Technik mit Firewall-Systemen auszustatten. Dabei sind die Firewall-Systeme so einzurichten, dass nicht erwünschte Mailanhänge bzw. Dateien (z.B. Java-Scripts, ActiveX-Programme, ausführbare Dateien (.exe) automatisch gesperrt werden.

### **6. Signaturzertifikatsprüfung bei Eingang**

Um Probleme mit der wiederholten Prüfung und der – längerfristigen – Ablage und Prüfung einer elektronischen Signatur zu umgehen, ist an einer festzulegenden Stelle (z.B. beim Übergang in ein sicheres Landesnetz oder in der Eingangsstelle des Gerichts) die Signaturzertifikatsprüfung durchzuführen und das Ergebnis festzuhalten. Der entschlüsselte, aber noch signierte Originaleingang ist zur Beweissicherung bis Verfahrensabschluss ebenfalls abzuspeichern.

### **7. Dokumentation des Zugangszeitpunktes, Zeitstempel**

Alle modernen EDV-Systeme verfügen in allen Komponenten (Client-PC's, Server, Netzkomponenten) standardmäßig über eingebaute Uhren. Beim Versand und dem Empfang elektronischer Dokumente per Mail bzw. bei der Nutzung von online angebotenen Formularen können diese verwendet werden, um den Zeitpunkt eines Zu- bzw. Abgangs zu dokumentieren.

Alle gängigen Betriebssysteme speichern zusammen mit dem Dateinamen auch den Zeitpunkt der Erstellung der Datei, der letzten Änderung und des letzten Zugriffs.

Die Uhren von Servern werden normalerweise zentral gewartet. Die Verlässlichkeit die-

ser Uhren ist damit höher als die der Clients, wenn diese nicht automatisch und vom Benutzer unbeeinflusst – z.B. beim login – mit der Server-Uhrzeit abgeglichen und eine spätere Änderung der Uhrzeit durch den Benutzer nicht technisch ausgeschlossen wird.

Es sind im Regelfall die Zeitangaben von Eingangs-Servern heranzuziehen und organisatorisch / technisch sicherzustellen, dass diese Uhren regelmäßig geprüft und gestellt werden und dass Manipulationen vorgebeugt ist. In die Eingangsbestätigung ist dieser Zeitstempel mit aufzunehmen.

In besonders begründeten Fällen kann geprüft werden, ob auf qualifizierte Zeitstempeldienste zurückgegriffen werden muss.

## II. Medien und Anlagengröße

Die Übermittlung von Dokumenten und Dateien im elektronischen Rechtsverkehr erfolgt grundsätzlich über Datenleitungen.

### 1. Anlagengröße bei E-Mails

Aufgrund der Beschränkung der Größe von E-Mail-Anlagen bei den verschiedenen Providern soll eine **Anlagengröße von 5 MB** eingehalten werden.

Für umfangreichere Anlagen sind, wenn eine Übermittlung per Upload auf einen Server nicht in Betracht kommt, CD-ROMs zu übersenden.

### 2. CD-ROM

Die CD R Standards für CD Recordable Medien sind im sog. "Orange Book"<sup>3</sup> festgelegt. Ergänzende Festlegungen finden sich im sogenannten Joliet-Standard<sup>4</sup>, der die Festlegungen für das Dateisystem auf einer CD nach ISO 9660 für UNICODE erweitert. Die heute verfügbaren Medien und Geräte halten diese Standards ein, so dass es bei "handelsüblichen Geräten" zu keinen Problemen kommt.

Weitergehende Vorgaben für CD-ROMs im Rahmen des elektronischen Rechtsverkehrs sind nicht erforderlich.

### 3. DVD

Die Übersendung von DVD bedarf der bilateralen Festlegung im Einzelfall.

Für DVD gibt es verschiedene Standards: DVD-RAM, DVD-R und DVD-RW DVD+R, DVD+RW.<sup>5</sup> Derzeit kann noch keine allgemein gültige Empfehlung gegeben werden, welcher DVD-Standard eingesetzt werden sollte.

<sup>3</sup> Das „Orange Book“ ist eines von mehreren „Bunten Büchern“ (vgl. „[http://www.cdrompage.com/basics/book\\_standard.php](http://www.cdrompage.com/basics/book_standard.php)“) in denen insbesondere die Firmen Sony und Philipps Standards für verschiedene Aspekte der CD spezifiziert haben (vgl. weiterführend auch zum „Orange-Forum“: „<http://www.orangeforum.or.jp/e/index.html>“).

<sup>4</sup> Zu „Joliet“ vgl. „[http://whatis.techtarget.com/definition/0,,sid9\\_gci212402\\_00.html](http://whatis.techtarget.com/definition/0,,sid9_gci212402_00.html)“ (Überblick) sowie weiterführend „<http://bmrc.berkeley.edu/people/chaffee/jolspec.html>“.

<sup>5</sup> Außerdem können Wiedergabeprobleme bei der Kombination bestimmter Hersteller von DVDs mit bestimmten DVD-Brennern auftreten.

### III. Dokumentenformate

#### 1. Erfordernis einheitlicher Dokumentenformate

Eine Festlegung über die im Rahmen des elektronischen Rechtsverkehrs zulässigen Dateiformate ist zwingend erforderlich, um sicherstellen zu können, dass

- elektronisch eingehende Schriftstücke vom Gericht gelesen werden können,
- vom Gericht erstellte oder an Beteiligte weitergeleitete elektronische Dokumente von den Empfängern gelesen werden können,
- die - signierten - Dateien gespeichert und automationsgestützt in ein Format überführt werden können, das für die Aufnahme in eine elektronische Akte oder zur Archivierung innerhalb der Verwahrungs- und Aufbewahrungsfristen nach Abschluss des Verfahrens geeignet ist.

#### 2. Kriterien der Formatvorgaben

Folgende Kriterien wurden bei den Format-Vorgaben herangezogen:

- **Herstellerunabhängigkeit und Verfügbarkeit**

Vorgeschriebene Dateiformate sollten sowohl allgemein verfügbar sein, als auch Festlegungen auf einen bestimmten Hersteller nach Möglichkeit vermeiden.

- **Offengelegte Formate**

Die Beschreibung der Dateiformate soll offen verfügbar – optimaler Weise national und international standardisiert - sein.

- **Transparenz aller übermittelten Informationen**

Es sollten Dateiformate vermieden werden, die die Gefahr in sich bergen, dass die Parteien im elektronischen Rechtsverkehr Informationen übermitteln, die sie nicht übermitteln wollten, d.h. die Dateiinhalte sollen im Klartext lesbar sein.

- **Verringerung des Risikos von Computerviren (keine aktiven Elemente)**

Aktive Elemente in Dateien (sich selbst aktualisierende Felder, Autoexec-Makros pp.) sind im elektronischen Rechtsverkehr in vielerlei Hinsicht problematisch und sollten ausgeschlossen werden. Zum einen können hier Beteiligten unterschiedliche Inhalte angezeigt werden, zum anderen kann nicht davon ausgegangen werden, dass alle Beteiligten über aktuelle Virens Scanner bzw. virenfreie Systeme verfügen, die derartig ausführbaren Code auf bekannte Schädwirkungen prüfen können.<sup>6</sup>

---

<sup>6</sup> Ein Schaden kann aber schon darin gesehen werden, dass ggf. über den fristwährenden Eingang einer Erklärung gestritten wird, die von einem Virusscanner entfernt wurde. Dateiformate, die keine aktiven Elemente kennen, tragen daher zur Eindeutigkeit der Kommunikation bei.

### 3. Formate zum Austausch codierter Daten<sup>7</sup>

Für den Austausch codierter Daten sind die Formate

- ASCII, Standard,
- UNICODE, Standard,
- RTF,
- PDF/A,
- XML und
- mit den unten genannten Einschränkungen Word .doc,

zu verwenden. Es sollen nur Versionen verbindlich zugelassen werden, die seit mindestens einem Jahr verfügbar sind.

Aktive Komponenten (z.B. Makros, EXE-Dateien) sind grundsätzlich nicht zulässig.

#### **Erläuterung zu den Formaten:**

##### **Word** (bis einschließlich Office 2003)

Nachdem noch vor einigen Jahren eine Vielzahl von Editoren mit jeweils eigenen Dateiformaten innerhalb und außerhalb der Justiz im Einsatz waren<sup>8</sup>, hat sich inzwischen MS-Word sowohl in der reinen Bürokommunikation als auch als Textsystem in Fachverfahren weitgehend durchgesetzt (zu Open-Source-Produkten s.u.). Dabei kommen unterschiedliche Versionen der Software zum Einsatz, die in der Standardeinstellung auch versionsspezifische Dateiformate generieren.<sup>9</sup> Ältere Softwareversionen können dabei häufig neuere Dateiformate nicht direkt bearbeiten.<sup>10</sup>

Das Dateiformat von MS-Word war bisher proprietär. Dateien, die in einem Format vor Word 2007 gespeichert wurden, können im Klartext von einem Nur-Text-Editor nicht angezeigt werden. Dateibesreibungen wurden von Microsoft nicht offengelegt. Wiederholt war aufgefallen, dass mit Word-Dateien verborgen System-Informationen oder sogar eine Bearbeitungshistorie übermittelt wurden, von deren Übermittlung der Absender keine Kenntnis hatte. (Durch solche verborgenen Inhalte sind in Einzelfällen Informationen übermittelt worden, die in den vorhergehenden Versionen eigentlich herauskorrigiert waren, was nicht nur unter Datenschutzgesichtspunkten inakzeptabel ist, sondern die Akzeptanz der elektronischen Kommunikation untergraben kann. Die Signierung eines solchen Dokumentes auf Dateiebene würde auch alle verborgenen Inhalte betreffen, was dieses Format für rechtsbindende Schriftstücke unbrauchbar werden lässt.<sup>11</sup>

Obwohl verschiedene Word-Formate wegen ihrer Verbreitung auch von einigen anderen Programmen erkannt und zum Teil auch erzeugt werden können, kann von einer plattformübergreifenden Verfügbarkeit nicht gesprochen werden. Archivverwaltungen, die sich grundsätzlich der Übernahme digitaler Daten öffnen, haben Word-Formate daher bisher als nicht archivierungsfähig bezeichnet.

<sup>7</sup> Als „codiert“ werden hier Daten bezeichnet, bei denen die Informationen zeichenorientiert übermittelt werden im Gegensatz zu „nicht-codierten“ Daten, die auf der Übermittlung von Pixelinformationen beruhen. Texte, die über einen Editor erfasst und in Dateien gespeichert werden, sind typische Beispiele codierter Daten, während Bilder und eingescannte Texte (ohne OCR-Nachbehandlung!) nicht-codierte Informationen enthalten.

<sup>8</sup> Zu denken ist an die vielfältigen Editoren aus der mittleren Datentechnik (z.B. HIT), an die unterschiedlichen PC-Systeme (neben den IBM-kompatiblen auch Atari, Apple) und an die verschiedenen SW-Alternativen unter DOS / Windows (z.B. Textverarbeitungen wie WordPerfekt, aber auch StarWriter oder Wordstar und integrierte Programme z.B. „F&A“ oder „Framework“).

<sup>9</sup> Eine Ausnahme machen Word 6.0 und Word 7.0 (=Word aus MS-Office '95), die letzte 16-bit- und die erste 32-bit-Version des Textprogramms; hier sind die Dateiformate kompatibel. In neueren Versionen kann ein früheres Dateiformat als Standardformat für das Speichern vorgegeben werden, bzw. ältere können importiert werden.

<sup>10</sup> Im Einzelfall hat Microsoft Patches bereitgestellt, die Vorgängerversionen von Word befähigen, auch das Dateiformat eines Nachfolgeproduktes öffnen und bearbeiten zu können (z.B. Word-2000-Dateien durch Word-97; Word-2007 durch Word-2003). Diese Option besteht aber nicht durchgängig.

<sup>11</sup> Vgl. c't magazin für computertechnik, Heft 3 / 2002 S.172, Dokumente durchleuchtet: Was Office-Dateien verraten können.

Aktive Elemente (Makros) können integriert werden und wurden wiederholt Gegenstand von Missbrauch.

Das Dateiformat von Word, „\*.doc“, zeigte hinsichtlich der dargestellten Beurteilungskriterien schwerwiegende Mängel. Insbesondere wegen mangelnder Transparenz und Sicherheit bestehen Bedenken gegen seinen Einsatz im Rahmen des elektronischen Rechtsverkehrs. Soweit das Format wegen seiner weiten Verbreitung und Akzeptanz in der Öffentlichkeit gleichwohl zugelassen werden soll, ist die - ab Word2000 verfügbare – Einstellung, nur zertifizierte Makros zu erlauben, einzuschalten (Dann erfolgt bei nicht-zertifizierten Makros ein Warnhinweis.).

**Word** (neuere Entwicklung / ab Office 2007)

Microsoft hat seine Office-Formate – und darunter insbesondere auch das Word-Format – mit der Version von MS-Office 2007 auf eine interne XML-Codierung umgestellt (Endung: .docx). Dieses offengelegte Format, „Office-Open-XML“ (OOXML), wurde Anfang April 2008 auch von der ISO als Standard 29500 anerkannt, nachdem sich bereits das deutsche DIN<sup>12</sup> sowie die europastämmige ECMA International<sup>13</sup> für eine Anerkennung von OOXML als ISO-Standard ausgesprochen hatten.<sup>14</sup>

#### **Exkurs: ODF**

Anders stellt sich die Situation bezüglich des Textformates „Open Document Format“, ODF, der Open-Source-Software OpenOffice dar. ODF wurde bereits 2006 international als Standard anerkannt (ISO/IEC-26300) und wegen seiner Herstellerunabhängigkeit in einigen Staaten zum einzig zulässigen Textformat für die Speicherung staatlicher Dokumente erklärt<sup>15</sup>. Aus technischer Sicht betrachtet, wäre das ebenfalls XML-basierte ODF daher durchaus geeignet und neben Words „doc“ ebenfalls zuzulassen. Da jedoch das verbreitete MS-Office ODF erst ab der Version Office 2007 in Verbindung mit dem Servicepack 2 lesen kann, kann die Verarbeitbarkeit von ODF noch nicht bei allen am ERV Teilnehmenden vorausgesetzt werden. Da umgekehrt jedoch OpenOffice Wordformate sowohl zu erzeugen als auch darzustellen vermag, schließt eine Beschränkung auf das Wordformat derzeit niemanden vom elektronischen Rechtsverkehr aus. Im elektronischen Rechtsverkehr geht es – im Unterschied zur „C2G“- oder „B2G“-Kommunikation vieler E-Government-Szenarien<sup>16</sup> - nicht nur um die zweiseitige Kommunikation einer Partei mit dem Gericht, sondern jede Verfahrensbeteiligte muss alle Beiträge aller anderen Beteiligten zur Kenntnis erhalten und deren Dokumente daher zumindest darstellen können.

Von einer Zulassung des ODF-Formates im elektronischen Rechtsverkehr wird daher derzeit noch unter dem pragmatischen Gesichtspunkt des Vorrangs niedrighschwelliger Teilnahmevoraussetzungen abgesehen.<sup>17</sup>

#### **Rich-Text-Format (RTF)**

Auch das RTF-Format ist grundsätzlich ein proprietäres Format von Microsoft, lehnt sich allerdings stark an das international normierte ODA/ODIF<sup>18</sup> an. Alle Einträge einschließlich der Formatierungsanweisun-

<sup>12</sup> DIN: Deutsches Institut für Normung

<sup>13</sup> ECMA International: ursprünglich: „European Computer Manufacturers Association“; ECMA-Standard 376

<sup>14</sup> Die Kritik an OOXML verweist zum einen darauf, dass mit ODF (ISO/IEC-26300) bereits seit 2006 ein anerkannter ISO-Standard verfügbar und kein Bedarf nach einem weiteren Standard für die gleiche Aufgabenstellung erkennbar sei. Vielmehr würde mit der parallelen Anerkennung eines weiteren Standards der Zweck einer Standardisierung konterkariert, die Interoperabilität der darauf aufsetzenden Anwendungen durch Nutzung einheitlicher Standards zu verbessern. Zum anderen sei die Dokumentation mit rund 6.500 Seiten für einen Standard unbrauchbar, weil ein Standard auch kleineren Unternehmungen einen Markteinstieg ermöglichen müsse.

<sup>15</sup> Vgl. Übersicht in Wikipedia: [http://de.wikipedia.org/wiki/OpenDocument#Einsatz\\_des\\_OpenDocument-Formats\\_bei\\_C3.B6ffentlichen\\_Stellen](http://de.wikipedia.org/wiki/OpenDocument#Einsatz_des_OpenDocument-Formats_bei_C3.B6ffentlichen_Stellen)

<sup>16</sup> Kommunikation von Bürgern („Citizen“) bzw. Unternehmen („Business“) mit staatlichen Stellen („Government“)

<sup>17</sup> Die Einbeziehung von ODF wird zu überprüfen sein, wenn von einer hinreichenden Verbreitung ODF-fähiger Textverarbeitungen, insbesondere von OpenOffice selbst sowie von Microsofts Office-2007 SP2 oder höher, ausgegangen werden kann.

<sup>18</sup> „Open Document Architecture“ / „Open Document Interchange Format“

gen werden in Klartext aufgelöst und können im Klartext von einem ASCII<sup>19</sup>-Editor angezeigt werden. Das RTF-Format gibt das Layout z.B. von Word-Dateien wieder, kennt jedoch keine Makros.<sup>20</sup>

Das RTF-Format kann von allen Word-Versionen und von vielen anderen Textverarbeitungsprogrammen verarbeitet werden.

Nicht-textuelle Darstellungen sind integrierbar, allerdings nimmt die Dateigröße dadurch überproportional zu.

## PDF

Das „**Portable Document Format**“ (PDF) der Firma Adobe war ursprünglich ein gleichfalls proprietäres Format, das allerdings mit einem von Adobe kostenfrei verbreiteten Anzeigeprogramm, dem Acrobat-Reader, dargestellt und ausgedruckt werden konnte. Außerdem sind eine Vielzahl von Tools frei verfügbar, die aus anderen Dateien ein PDF-Format erzeugen. Insbesondere sogenannte „PDF-Drucker“ ermöglichen quasi als Systemfunktion eine einfache Bereitstellung einer Konvertierungsoption für beliebige Anwendungsprogramme. Das Format ist im Internet sehr weit verbreitet. Der „Acrobat-Reader, ein vergleichsweise „schlankes“ Programm, kann kostenlos weitergegeben werden und wird daher vielfach zum Download mit angeboten. Das PDF-Format garantiert eine layoutgetreue Wiedergabe von Dateien auf unterschiedlichen Plattformen. Es steht als alternatives Fremdformat insbesondere auch in verbreiteten DTP-Programmen<sup>21</sup> zur Verfügung.

Auch mit eingebetteten Grafikelementen bleiben PDF-Dateien vergleichsweise klein. Aktive Inhalte sind möglich, gleichwohl sind Probleme mit Computerviren nicht bekannt geworden. Die Entwicklung ist zu beobachten.

Inzwischen wurde eine spezielle Variante, PDF/A, bei der ISO normiert (ISO 19005-1:2005).<sup>22</sup> Dabei existieren zwei Varianten. PDF/A-1a ermöglicht neben der visuellen Reproduzierbarkeit auch den Erhalt UNICODE-basierten Texts und inhaltlicher Strukturierung, während PDF/A-1b sich auf den Erhalt der visuellen Reproduzierbarkeit beschränkt. Office-Dokumente sollen im ERV grundsätzlich im Format PDF/A-1a gespeichert werden, um neben allen in UNICODE darstellbaren Zeichen auch möglichst viel Funktionalität, wie z.B. Strukturinformationen, zu erhalten. Wird jedoch ein Schriftstück eingescannt, so kann nur die Variante PDF/A-1b – mit oder ohne OCR-Text im Hintergrund – erzeugt werden. Auch dabei wird das Bild des transformierten Dokuments stets layoutgetreu angezeigt. Die OCR-Informationen im Hintergrund können jedoch Erkennungsfehler enthalten und es werden Strukturinformationen zu dem Text fehlen. Das Dateiformat PDF/A wurde speziell für die Langzeitarchivierung konzipiert und erscheint gegenwärtig für den elektronischen Rechtsverkehr vorzugswürdig.<sup>23</sup>

## Textformat (ASCII und UNICODE)

Der „**American Standard Code of Information Interchange**“ enthält die mit 7 Bit darstellbaren Zeichen - einschließlich Steuerzeichen wie der Zeilenschaltung -, wobei diese Bit-Kodierung auch in 8-Bit-Zeichensätzen beibehalten wird, jedoch um nationale Sonderzeichen ergänzt werden kann. Der ASCII-Zeichensatz ist auf praktisch allen Computersystemen zur Zeichendarstellung implementiert. Eine Beschränkung auf den ASCII-Zeichensatz eignet sich daher besonders für plattformübergreifenden

<sup>19</sup> „**American Standard Code of Information Interchange**“

<sup>20</sup> Dynamische Informationen in Word (z.B. Nummerierungs- und Gliederungsfunktionen) werden in statische umgewandelt. Zur grundsätzlichen Eignung vgl. das Grundschutzhandbuch des BSI unter Abschnitt M 4.44, online aufrufbar unter: „<http://www.bsi.de/gshb/deutsch/m/m4044.htm>“. Allerdings können unter bestimmten Bedingungen auch Makros angesprochen werden, jedoch wird das Schadensrisiko geringer eingeschätzt. Vgl. dazu ergänzend ebenfalls beim BSI: <http://www.bsi.de/av/texte/rtf-makro.htm>. Ergänzend siehe auch: „<http://www.aboutit.de/view.php?ziel=/01/21/07.html>“

<sup>21</sup> DTP: Desk Top Publishing

<sup>22</sup> Detaillierte Informationen zur Normierung von PDF/A unter <http://www2.din.de/> zum DIN/ISO Normentwurf ISO/DIS 19005-1, Ausgabe:2004-12, Dokumentenmanagement - Elektronisches Dokumentendateiformat für Langzeitarchivierung - Teil 1: Verwendung von PDF 1.4 (PDF/A)

<sup>23</sup> PDF/A kann von Adobe Acrobat ab der Version 8.0 und auch über weitere Tools erzeugt werden.

Datenaustausch. Dateien, die auf Formatierungen und Layout-Angaben verzichten, können auf allen Plattformen von einfachen ASCII-Editoren ausgegeben werden.

Textauszeichnungen kennt das ASCII-Format ebenso wenig wie die Integration nicht-textualer Elemente.

Als Nachfolger des ASCII-Formats setzt sich derzeit das UNICODE-Format durch, das – aufgrund einer Darstellung mit 16 Bit – einen erheblich größeren Zeichenumfang besitzt, aber ebenso wie ASCII keinerlei Formatierungen ermöglicht. UNICODE stellt auch für Justizverfahren eine zukunftsweisende Alternative zu ASCII dar, da hiermit ohne Bindung an einen speziellen (Windows-) Zeichensatz länderübergreifende Sonderzeichen dargestellt werden können. So können Textelemente über verschiedene Plattformen hinweg uneingeschränkt weiterverwendet werden. Dies zu gewährleisten, war die Grundidee bei der Entwicklung von UNICODE. Hieraus resultiert der Einsatz dieses Codes bei XML.

Auch zur Speicherung in Datenbanken bietet sich UNICODE an. Strukturierte Daten sollen deshalb generell im UNICODE-Zeichensatz ausgetauscht werden.

## **XML**

Die „**Extensible Markup Language**“, heute bereits ein „Markt-Standard“, ist im Gegensatz zum bekannten HTML eine echte Teilmenge von SGML, einem internationalen Standard. XML ist wesentlich einfacher zu handhaben als SGML und eher eine Metasprache mit einer Definitionsoption für eigene Elemente, die in einer „**Document Type Definition**“ (DTD) oder in einer XML Schema Datei beschrieben werden. Die Dateiinhalte sind als ASCII-Zeichen oder im UniCode<sup>24</sup> vollständig darstellbar. Der Inhalt (Text) einer XML-Datei wird typischer Weise mit spezifischen Tags strukturiert und vollständig von Formatierungsanweisungen getrennt. Die Formatierung des Dokuments wird in unterschiedlicher Form (z.B. als „cascading style sheet“ [.css] oder als „extensible stylesheet language“ [.xsl]) in besonderen Dateien niedergelegt.

Wegen seiner großen Flexibilität sowohl im Austausch strukturierter Daten als auch bei der Darstellung komplexer Texte und seiner Stabilität bei dem Wechsel von Systemplattformen, kommt XML derzeit in immer weiteren Bereichen zum Einsatz. Die Justiz hat mit ihrem „Grunddatensatz“ XJustiz und den ausdifferenzierten Fachdatensätzen eine einheitliche Plattform für den Datenaustausch zwischen den Fachverfahren und mit Externen geschaffen. Die Koordinierung mit parallelen Bestrebungen in anderen Ressorts der öffentlichen Verwaltung erfolgt über die OSCI-Leitstelle und in der XÖV-Abstimminstanz.

XML wurde als Format auch mit dem Ziel festgelegt, die Langlebigkeit der erstellten Dokumente, unabhängig von dem – inzwischen üblichen – raschen Formatwechsel in gängigen Textverarbeitungssystemen zu gewährleisten. Dies ist nach Ansicht der AG-IT-Standards in der Justiz dann der Fall, wenn die XML-Spezifikationen des W3C eingehalten werden und auf (firmen-) spezifische Erweiterungen verzichtet wird. Die Standardisierungen bzw. Standardisierungsbestrebungen bei den Dateiformaten von Officeanwendungen auf der Basis von XML (s.o.) gehen in diese Richtung.

Offen ist hingegen derzeit noch die Nutzung der Möglichkeiten von XML zur internen Strukturierung von Schriftsätzen (z.B. durch Auszeichnungen des Rubrums, von Anträgen, Beweismitteln, Normen), wodurch deren Auswertung insbesondere in sehr umfangreichen Verfahren unterstützt werden könnte.

## **4. Formate zum Austausch nicht-codierter Daten**

Zum Austausch nicht-codierter Daten soll entweder das TIFF-Format<sup>25</sup> in der Version 6.0, CCITT/TSS Gruppe 4, verwendet werden oder eine Umwandlung in eine PDF/A Datei erfolgen.

<sup>24</sup> UniCode ist der (16bit) Nachfolger des ASCII-Zeichensatzes, mit dem auch länderspezifische Alphabete und Sonderzeichen wie z.B. mathematische Symbole dargestellt werden können (entspricht ISO 10646).

<sup>25</sup> TIFF ("Tag Image File Format")

Nach der Abstimmung mit der Arbeitsgruppe „Elektronische Systeme in Justiz und Verwaltung“ der Archivreferentenkonferenz des Bundes und der Länder werden beide Formate bei eventuellen Abgaben an die Archive akzeptiert, Konvertierungen würden erspart.

Die Version 6.0 des TIFF-Formats wurde bereits 1992 verabschiedet und ist allgemein verbreitet. Mit der „Fax-Group 4“ wird ein Komprimierungsverfahren vorgegeben, das zu sehr kompakten Dateien führt.

PDF/A Dateien eignen sich besonders für die zusätzliche inhaltliche Erschließung eingescannter Dokumente. Da der über eine Texterkennung erfasste Inhalt als Index mit in der PDF/A-Datei abgelegt wird, sind selbst auf diese Weise erzeugte elektronische Dokumente im Volltext durchsuchbar.

## **5. Elektronische Akten, langfristige Speicherung und Archivierung**

### **5.1 Dokumente**

Sofern elektronische Akten gebildet werden, können sich daraus weitere Anforderungen an die Dateiformate der aufzunehmenden elektronischen Dokumente ergeben.

Längerfristig werden auch papierene Dokumente durch Einscannen in eine elektronische Akte mit aufzunehmen sein. Hierfür kommen nur Dateiformate in Betracht, die eine layoutgetreue, fehlerfreie Wiedergabe gewährleisten<sup>26</sup>.

Unabhängig von den für die Aktenbildung eingesetzten Systemen und ihren gegebenenfalls spezifischen Anforderungen sollen die eingesetzten Dateiformate für eine langfristige Speicherung und Bearbeitbarkeit<sup>27</sup> geeignet sein, um zusätzliche Konvertierungen zu vermeiden.

Die Anforderungen können am besten durch PDF/A erfüllt werden, so dass dieses Format grundsätzlich für die Bildung elektronischer Akten und zur langfristigen Speicherung empfohlen wird.

### **5.2 Signaturen**

Im Blick auf die Zielsetzung, langfristig elektronische Dokumente verlässlich wiedergeben zu können, sind drei Formen elektronischer Signaturen zu betrachten, die sich in der Art ihrer Verbindung mit dem signierten Dokument unterscheiden:

- „enveloping“ – die elektronische Signatur bildet einen „Umschlag“ um die signierte Datei. Typischerweise erhält dabei die Datei eine neue Dateiendung, z.B. „.p7s“. Diese Datei lässt sich dann später nur mit einer entsprechenden Anzeigekomponente öffnen, die die Signaturdaten interpretiert und das ursprünglich signierte Dokument aus diesem „Umschlag“ heraus zur Anzeige bringt. Die damit gegebene zusätzliche Abhängigkeit der Darstellung des

<sup>26</sup> Die Anforderung kann generell nur von Bildformaten erfüllt werden, da eine OCR-Konvertierung keine Fehlerfreiheit gewährleisten kann. Eine Sonderstellung nimmt hierbei lediglich das Format PDF/A 1b ein, da hierbei das Bild (Image) einer Textseite mit den Daten aus ihrer OCR-Erkennung hinterlegt werden kann (s.o.).

<sup>27</sup> Der Begriff der Bearbeitbarkeit ist hier weit auszulegen, d.h. sie beginnt bereits bei der Speicherung, Übertragung und Anzeige von Daten. Ein Überarbeiten der Texte ist selbstverständlich nicht gemeint. Hingegen können Maßnahmen einer üblichen Aktenbearbeitung, wie dem Anbringen von Annotationen, auch nach längerer Zeit und nach Abschluss des Verfahrens - bspw. im Falle einer Beziehung der Akte - noch erforderlich sein.

Dokuments von der Auflösung seines „Umschlags“ macht diese Variante für eine langfristige Speicherung ungeeignet.

- „enveloped“ – die signierte Datei sieht selbst in ihrem Dateiformat einen Platz für die Hinterlegung von Signaturdaten vor, d.h. sie bildet ihrerseits einen „Umschlag“ für die Signatur. Diese Variante ist beispielsweise von dem verbreiteten PDF-Format her bekannt.<sup>28</sup> In diesem Falle enthält das Anzeigeprogramm (Adobe's Acrobat) einen Menüpunkt, über den die Signaturprüfung und die Anzeige des Ergebnisses angestoßen werden kann.<sup>29</sup> Die Betrachtung des elektronischen Dokuments selbst erfordert keinen gesonderten Signaturviewer.
- „detached“ – die Signatur wird in einer gesonderten Datei (meist gleichen Namens – bis auf das Suffix) abgelegt, ohne die signierte Datei zu verändern, d.h. ein signiertes Dokument besteht bei dieser Variante immer aus zwei Dateien: dem signierten Dokument vor Anbringung der Signatur und der Signaturdatei, die nur zusammen mit jener ersten Datei geprüft werden kann.

Die beiden zuletzt genannten Varianten der Anbringungen elektronischer Signaturen beeinträchtigen die Darstellung der elektronischen Dokumente selbst dann nicht, wenn die zur Prüfung der Signaturen erforderlichen kryptographischen Algorithmen einmal nicht (mehr) zur Verfügung stehen. Sie sind daher für eine längerfristige Speicherung vorzuziehen.

Für einen Datenspeicher der Justiz sind Konzepte, die ein fortlaufendes Nach- oder Übersignieren elektronischer Dokumente zum Erhalt ihrer Beweiskraft vorsehen jedenfalls dann nicht erforderlich, wenn die Datenintegrität und Authentizität bei Eingang der Dokumente geprüft und das Ergebnis zusammen mit den Dokumenten verwahrt wird, weil die Integrität der Daten in den amtlichen Systemen selbst auf andere Weise hinreichend sichergestellt werden kann.<sup>30</sup>

Angesichts der nach langen Zeiträumen möglichen Darstellungs- und Prüfprobleme soll es deshalb ausreichen, wie im Falle einer Transformation elektronischer Dokumente für eine papierbasierte Aktenführung nach [§ 298 ZPO](#), Integritäts- und Signaturprüfungen lediglich bei der Aufnahme eines extern signierten elektronischen Dokuments in einen justiziellen Datenspeicher vorzunehmen und dieses Prüfergebnis bei dem Dokument mit zu verwahren.

In Fällen gerichtlicher elektronischer Dokumente (§ 130b ZPO) und solcher, in denen vom Gesetz eine „untrennbare Verbindung“ elektronischer Dokumente gefordert wird<sup>31</sup>, worunter bisher überwiegend eine „Klammersignatur“ bzw. ein signierter Container verstanden wird, der die zu verbindenden Dokumente enthält, sollen die Signaturen mit den elektronischen Dokumenten gespeichert werden. Ein kontinuierliches

<sup>28</sup> Die Signatur kann auch in dem PDF/A-Format aufgenommen werden.

<sup>29</sup> In der Standardkonfiguration greift Acrobat dabei lediglich auf die im Betriebssystem hinterlegten Zertifikate zu und führt eine lokale Integritätsprüfung ohne externe Abklärung der gesamten Zertifikatskette durch. Die für Authentizitätsprüfungen erforderlichen Root-Zertifikate können aber gesondert importiert werden.

<sup>30</sup> Die reversionssichere Speicherung von Daten ist eine klassische Aufgabe öffentlich-rechtlicher Rechenzentren. Die dazu erforderlichen Techniken werden laufend fortentwickelt.

<sup>31</sup> Vgl. bspw. §§ 105 (1), 164 (4), 315 (3), 319 (2), 320 (4), 734, 813 (2) ZPO

Nachsignieren dieser Dokumente nach Ablauf der Gültigkeit ihrer Signaturen ist innerhalb des gerichtlichen Datenspeichers jedoch ebenfalls nicht erforderlich. Lediglich im Falle einer späteren Herausgabe der gerichtlichen elektronischen Dokumente aus dem Herrschaftsbereich des Gerichts nach Ablauf der Gültigkeit der an dem Dokument angebrachten Signaturen sollen die Dokumente und ihre Signatur anlassbezogen übersigniert werden, sofern es auf die Sicherung ihrer Authentizität außerhalb des justiziellen Netzes ankommt.

## **IV . Übergabe strukturierter Daten (XJustiz)**

Eine erhebliche Rationalisierungschance des elektronischen Rechtsverkehrs liegt in der möglichen Datenübernahme aus den Schriftsätzen der Parteien in das gerichtliche Schreibwerk sowie in der vereinfachten Auswertung und Aufbereitung strukturierter Eingaben.

Mit XML steht eine international standardisierte Metasprache mit einer Definitionsoption für eigene Elemente, die i.d.R. in einer XML-Schema (XSD) Datei beschrieben werden, zur Verfügung. Die Dateiinhalte sind als ASCII-Zeichen oder im UNICODE<sup>32</sup> vollständig darstellbar. Der Inhalt (Text) erscheint unter XML typischer Weise inhaltlich mit spezifischen Tags strukturiert und kann vollständig von Formatierungsanweisungen getrennt werden.

Zur Übergabe strukturierter Daten ist der XJustiz-Datensatz vorgeschrieben. Unter „XJustiz“ wird die Gesamtheit aller Festlegungen für das einheitliche Datenaustauschformat im ERV verstanden. Neben die umfassende Darstellung aller strukturierten Daten eines Verfahrensbereichs treten zunehmend auch Definitionen von XJustiz-Nachrichten, bei denen die XJustiz-Elemente der in einem spezifischen Verfahrensschritt relevanten Daten selektiert und ggf. mit einer Übermittlungsintention (z.B. Neuaufnahme, Änderung, Löschung pp.) verknüpft werden, so dass die weitere Verarbeitung der Daten beim Empfänger gezielt unterstützt werden kann.

### **1. Zielgruppen**

Zielgruppen zur Nutzung von XJustiz sind z.B.

- Partner der Justiz im elektronischen Rechtsverkehr (z.B. Notare, Anwälte) ,
- Entwickler/Softwarehäuser, die für diese Partner Software entwickeln,
- Facharbeitsgruppen der Justiz und der Verwaltung,
- Entwicklerverbünde der Justiz und der Verwaltung und
- Entwickler/Softwarehäuser der Justiz und Verwaltung.

---

<sup>32</sup> Vgl. Fn.24

## 2. Aufbau von XJustiz

Die XML-Schemata von XJustiz setzen sich zusammen aus einem **Grundmodul**, mehreren **Fachmodulen** und zugehörigen **Wertelisten**.

Die Schema-Datei für den Grunddatensatz wird mit „XJustiz.Kern“ bezeichnet, die fachspezifischen Erweiterungen mit „XJustiz.Xxx“, z.B. „XJustiz.Familie“, „XJustiz.Register“, „XJustiz.Mahn“ oder „XJustiz.Straf“.

Das **Grundmodul XJustiz.Kern** definiert die Grundstrukturen und stellt diese als Sammlung von Bausteinen zur Verfügung, auf die die einzelnen Fachmodule (z.B. XJustiz.Straf, XJustiz.Mahn, XJustiz.Familie, etc.) zurückgreifen können.

Die **Fachmodule** sind der unmittelbare Anknüpfungspunkt für den Aufbau eines auszutauschenden XML-Dokuments (eines so genannten Instanzdokuments). Sie enthalten die formalen Regeln, nach denen ein Instanzdokument aufgebaut sein muss. Zur Definition dieser Regeln greifen die Fachmodule auf die im Grundmodul definierten Bausteine zurück. Je nach fachlichem Zusammenhang enthalten sie darüber hinaus Änderungen oder Ergänzungen der im Grundmodul enthaltenen Definitionen.

**Wertelisten** enthalten vordefinierte Inhalte für Elemente, die typischerweise nur bestimmte Werte enthalten können. Typische Beispiele sind Elemente wie „Familienstand“ oder „Staatsangehörigkeit“. Durch die Definition von XML-basierten Wertelisten wird es möglich, einen XJustiz-Datensatz bereits mit marktgängigen XML-Werkzeugen darauf zu überprüfen, ob die betroffenen Felder einen zusätzlichen Wert enthalten. Um dennoch ein Mindestmaß an Flexibilität zu bewahren, kann in den Instanzdokumenten durch einen bestimmten Befehl angezeigt werden, dass ausnahmsweise ein nicht in der Werteliste enthaltener Wert übermittelt wird.

## 3. Anpassungen und Erweiterungen von XJustiz

Anpassungen und Erweiterungen von XJustiz erfolgen abgestimmt über die BLK (Bündelung, Prüfung, Integration der Änderungen und Vorschlag der Freigabe durch AG-IT). Dabei werden Festlegungen aus anderen Bereichen (z.B. KOOPA ADV und AG XöV im Rahmen von Deutschland online) berücksichtigt. Mit der technischen Führung und Dokumentation ist die OSCI-Leitstelle beim KoopA ADV beauftragt.

#### **4. Informationen zu XJustiz**

Der XJustiz-Leitfaden, der die Philosophie und den Aufbau von XJustiz näher beschreibt, ist den OT-Leit-ERV als der Anlage 2 beigelegt.

Die aktuelle Dokumentation zu XJustiz kann unter [www.xjustiz.de](http://www.xjustiz.de) und [www.osci.de](http://www.osci.de) abgerufen werden.

### **V. Authentisierung und Verschlüsselung**

#### **1. Basisverfahren**

Auf dem Markt werden Produkte verschiedener Hersteller für den sicheren Datenaustausch angeboten. Dies ist aus Konkurrenz- und Wirtschaftlichkeitsgründen auch erwünscht. Die mit diesen Produkten durchgeführten Verschlüsselungen sowie die erzeugten Unterschriften dürfen nicht produktspezifisch sein, sie sollen interoperabel sein. Die von verschiedenen Herstellern abgestimmte Common-PKI-Spezifikation<sup>33</sup>) verfolgt dieses Ziel. Daneben wird das Ziel verfolgt, eine offene und zertifizierte Profilierung der zugrunde liegenden internationalen Standards (S/MIME, X.509, PKIX, PKCS#)<sup>34</sup> zu schaffen, die nicht durch teilweise nicht prüfbare firmeninterne oder länderspezifische Vorschriften (z.B. US-Geheimnisse oder Exportbeschränkungen) geschützt ist.

Speziell für die Umsetzung von E-Government wurde das Nachrichtenprotokoll OSCI (Online Service Computer Interface) entwickelt. OSCI spezifiziert eine Sicherheitsinfrastruktur, nach der sowohl Formulare, transaktionsorientierte Internetanbindungen von Fachverfahren als auch Fremdformate aus Drittsystemen sicher und ggf. signiert (mit unterschiedlichen Niveaus) über das Internet übermittelt werden können. Mit OSCI kann die Nachricht sicher über ungesicherte Verbindungen (TCP/IP) gesendet werden. Dies wird durch die Übermittlung eines Datencontainers über einen Intermediär ermöglicht, wobei der Datencontainer nach dem Prinzip des „doppelten Umschlags“ konzipiert ist, und eine strikte Trennung der eigentlichen Inhalte von Transportdaten vorsieht. Damit wird sichergestellt, dass von Dritten im Internet keine Kommunikationsprofile erstellt werden können und die Vertraulichkeit der Inhalte auch gegenüber dem Intermediär gewährleistet ist.

<sup>33</sup> Die „Common-PKI-Spezifikation“ (Version 2.0 vom 20.01.2009) beschreibt ein Profil über international verbreitete und anerkannte Standards für elektronische Signaturen, Verschlüsselung und Public-Key-Infrastrukturen. Das Profil wurde von T7 und Teletrust verabschiedet (früher ISIS-MTT). Die „Industrial Signature Interoperability Specification“ der führenden deutschen Trustcenter war zunächst als reiner Signaturstandard konzipiert und im Herbst 2001 mit dem E-Mail Standard „Mail-TrusT 2.0“ zu „ISIS-MTT“ verbunden worden.  
S.a. im Internet unter: <http://www.common-pki.org>.

Die kryptographischen Mechanismen zur Sicherstellung von Vertraulichkeit, Integrität und Authentizität wurden im Hinblick auf Interoperabilität festgeschrieben und basieren auf internationalen und nationalen Standards (W3C XML-Signature und –Encryption, X509, Common-PKI etc.). OSCI ist sowohl auf der Ebene der Transport- als auch auf der Ebene der Inhaltsdaten eine XML-Anwendung. Somit ist die Möglichkeit einer standardisierten Strukturierung der Nachrichteninhalte und einer medienbruchfreien Weiterverarbeitung gegeben. Die OSCI-Architektur sieht als zentralen Mittler einen sogenannten Intermediär vor, der aufwändige kryptographische Funktionen zentralisiert zur Verfügung stellt (z.B. Zertifikatsprüfungen) und Mehrwertdienste erbringen kann (z.B. Zwischenspeicherung von Nachrichten, Kommunikationsprotokolle bzw. -bestätigungen).

Im Rahmen des elektronischen Rechtsverkehrs sind folgende Basisverfahren verbindlich und gemäß der Common-PKI-Specification zu profilieren:

### **ITU<sup>35</sup>-Empfehlung X.501**

Das allgemeine Format für Namen wird in der ITU-T Empfehlung [ITU-T X.501] durch den *distinguished name*-Typ festgelegt. Der *distinguished name* besteht aus einer Folge von *AttributeType*-und *AttributeValue*-Paaren. Spezielle Typen für *AttributeType* werden in der ITU-T Empfehlung [ITU-T X.520] definiert.

### **ITU-Empfehlung X.509 V3, Zertifikate**

Als generelles Format für Zertifikate wurde 1997 von der ITU-T (telecommunication standardization sector of the international telecommunication union) die Empfehlung [ITU-T X.509] als Bestandteil der X.500-Directory-Serie verabschiedet, die in der Zwischenzeit durch zwei weitere Versionen ergänzt wurde. Das ursprüngliche X.509-Standardformat wird heute als X.509 v1-Zertifikatsformat bezeichnet und diente als Grundlage für die Entwicklung des Internet-Reports für sichere elektronische Post (PEM, privacy enhanced mail) [RFC 1422 93].

### **API PKCS #11**

In dem "Cryptographic Token Interface Standard" [PKCS#11] wird eine Programmierschnittstelle (Application Programming Interface, API) festgelegt. Diese Schnittstelle wird als "cryptographic token interface" (Cryptoki) bezeichnet. Über diese Schnittstelle können Anwendungsprogramme auf Geräte, so genannte "kryptographische Token", zugreifen. Ein kryptographisches Token ist eine Abstraktion der Eigenschaften von Smartcards. Die Anwendung muss die genauen Zugriffsmethoden und Fähigkeiten eines kryptographischen Token nicht im Voraus kennen. Über die Schnittstelle kann die Anwendung die Fähigkeiten des Tokens erfragen und Operationen (also etwa die Verwendung eines privaten Schlüssels in einer kryptographischen Berechnung) auslösen. PKCS#11 soll auch dafür sorgen, dass mehrere Anwendungen Zugriff auf das kryptographische Token haben können, ohne sich gegenseitig zu stören. PKCS#11 ist als Schnittstelle in der Programmiersprache C entwickelt und ist insofern nicht nur eine konzeptionelle Definition sondern bietet auch Kompatibilität auf Ebene des Programmquellcodes. Damit ist es möglich, dass Anwendungsprogramme beliebige PKCS#11 Module verwenden können.

<sup>34</sup> S/MIME: Secure Multipurpose Internet Mail Extensions, X.509: Standard: Public Key Infrastructure auf Basis des Verzeichnisdienstes X.500 (RFC 2459), PKIX: Arbeitsgruppe zur Festlegung der X.509 Standards, PKCS: Public Key Cryptography Standards

<sup>35</sup> International Telecommunication Union, früher CCITT

### Austauschformat PKCS #7<sup>36</sup>

Der "PKCS#7 Cryptographic Message Syntax Standard (CMS)" [PKCS#7 93] beschreibt allgemeine Datenstrukturen zur Speicherung und Übertragung von digital signierten oder verschlüsselten Inhalten. Die Datenstrukturen sind rekursiv aufgebaut, so dass beispielsweise eine digital signierte Nachricht zusätzlich auch verschlüsselt werden kann. Die Verschlüsselung wird dann "außen" um die "innere" signierte Nachricht angebracht. Es können beliebige Attribute zu den Nachrichten ergänzt werden. In einer stark vereinfachten Form können PKCS#7 konforme Nachrichten zum Transport und zur Verteilung von Zertifikaten und Sperrlisten verwendet werden.

## **2. Elektronische Signatur nach SigG und Attribute**

Nach dem Signaturgesetz (SigG) sind Signaturschlüsselpaare für Signaturen nur natürlichen Personen zuzuordnen, da sie das elektronische Äquivalent zur eigenhändigen Unterschrift bilden. Im elektronischen Rechtsverkehr mit Behörden und Gerichten kommt es für Bürgerinnen und Bürger jedoch i.a. weniger auf die ausfertigende Person an, als auf die ausstellende Behörde. Das SigG sieht dafür Attribute vor (entspricht Dienstsiegeln), die entweder als Attributfelder in einem qualifizierten Signaturzertifikat oder als eigenes Attributzertifikat beispielsweise mit der Organisationsbezeichnung gefüllt werden können, wobei die gesonderten Attributzertifikate stets nur in Verbindung mit einem persönlichen Signaturzertifikat gültig sind .

Das Konzept personengebundener qualifizierter Signaturen stößt dann an seine Grenzen, wenn aus Fachverfahren heraus Bescheide in großer Zahl authentisiert werden sollen. Hier erscheint ein Rückgriff auf personengebundene Signaturen nicht mehr angemessen. Sachgerecht wäre vielmehr eine automatisiert anzubringende „Behördensignatur“ ohne Personenbezug.<sup>37</sup>

Während in den ersten Jahren nach Verabschiedung des Signaturgesetzes die Inkompatibilität elektronischer Signaturen unterschiedlicher Hersteller noch einem sorglosen Einsatz im Wege stand<sup>38</sup>, steht mit der „Common-PKI“ inzwischen ein Profil zur Verfügung, das Interoperabilität gewährleistet. Zertifizierungen zur Common-PKI-Konformität wurden in 2009 an die einschlägigen Anbieter elektronischer Signaturen in Deutschland ausgestellt.

<sup>36</sup> Nachdem Profile für XML-Signature und XML-Encryption in die Kernspezifikation des Common-PKI-Profiles aufgenommen wurden (vgl. aktuelle Fassung vom 16.3.2004, Teil 8), ist es zulässig, diese Signatur/Verschlüsselungsformate an Stelle des PKCS#7-Formats zu verwenden. Nach Möglichkeit sollen Signaturanwendungskomponenten sowohl PKCS#7-konforme Signaturen als auch Signaturen gemäß Common-PKIXML-Profil validieren können.

<sup>37</sup> Entsprechende Gespräche mit der Bundesnetzagentur und anderen wurden insbesondere von der „Gemeinsamen ERV-Kommission“ des Deutschen EDV-Gerichtstages aufgenommen. – Siehe auch unter „4. Fortgeschrittene SignaturFortgeschrittene elektronische Signatur“, Seite 26.

Die OT-Leit-ERV bestimmen unter Nr. 6.4, Attribute würden nur in den gesetzlich vorgesehenen Fällen ausgewertet. Diese Regelung ist zum einen dem Umstand geschuldet, dass die Einträge in Attributfeldern nicht standardisiert sind und daher nicht maschinell ausgewertet werden können und zum anderen interpretationsbedürftig bleiben und damit ohne Not Konfliktpotential eintragen können.<sup>39</sup>

Ein anderer Weg der Zuordnung bestimmter Attribute zu elektronischen Identitäten eröffnet sich mit dem Identitätsmanagement-Konzept S.A.F.E.<sup>40</sup>. Wenn Vertrauensstellungen zu Domänen aufgebaut werden, die geschlossene Benutzergruppen bilden (bspw. das Notarnetz der BNotK) oder die für Gruppen von Mitgliedern bestimmte Eigenschaften verlässlich prüfen und mit einheitlichen Attributen versehen, können diese Kennzeichnungen künftig auch automatisiert ausgewertet und zur Steuerung der weiteren Datenverarbeitung herangezogen werden. Die Entwicklung bleibt aber insoweit noch abzuwarten.

### 3. Gesetzeskonformität von Signaturanwendungskomponenten

In §§ 17 und 15 Abs. 7 SigG werden die technischen Anforderungen sowohl an sichere Signaturerstellungseinheiten als auch an Signaturanwendungskomponenten definiert. Konstitutiv für rechtswirksame qualifizierte elektronische Signaturen - mit oder ohne Anbieter-Akkreditierung - ist aber nur die Verwendung gesetzeskonformer Signaturerstellungseinheiten. Denn lediglich die sichere Signaturerstellungseinheit, nicht aber die sichere Signaturanwendungskomponente wird von der Legaldefinition des § 2 Ziff. 3 SigG in Bezug genommen und nur ihr Besitz ist nach § 15 Abs.7 Ziff. 2 SigG (freiwillig akkreditierte Trust-Center) bzw. § 5 Abs. 6 SigG i.V.m. § 5 Abs. 2 SigV-E Voraussetzung für die Vergabe bzw. das Nachprüfbarhalten qualifizierter Zertifikate durch die Trust-Center. Hinsichtlich sicherer Signaturanwendungskomponenten bestehen lediglich Hinweispflichten der Trust-Center gemäß § 15 Abs.7 Ziff.3 (freiwillig akkreditierte Trust-Center) bzw. § 6 Abs. 1 SigG i.V.m. § 6 Ziff. 3 SigV-E und eine "Soll"-Vorschrift für den Einsatz durch die Signaturschlüssel-Inhaber (§ 17

---

<sup>38</sup> Eine mögliche Lösung dieses Problems bestand in der Entwicklung einer herstellernerutralen Client-Software, wie z.B. Govello oder EGVP, die unabhängig von der spezifischen Software eines Trustcenters selber signieren und Signaturprüfungen durchführen kann.

<sup>39</sup> So geschehen z.B. in einem Verfahren vor dem FG Münster, in dem darüber gestritten wurde, ob die Eintragung einer Wertgrenze im Attributfeld der Signatur auf den Streitwert der Sache oder auf die für das Verfahren fällige Gerichtsgebühr zu beziehen sei mit der Folge, dass entweder eine Frist gewahrt oder wegen eines Formfehlers (ungültige Signatur) versäumt wurde.

Abs. 2 S.4 SigG).<sup>41</sup>

Das bedeutet: Eine elektronische Signatur, die mit einer gesetzeskonformen Chipkarte erstellt wurde, ist rechtlich auch dann wirksam, wenn der Anwender vor der Unterschrift nicht mehr sehen konnte, welche Inhalte er unterschreibt.

Auch wenn die Gesetzeskonformität der eingesetzten Signaturanwendungskomponenten keine Voraussetzung dafür ist, rechtswirksame qualifizierte elektronische Signaturen erzeugen zu können, ist sicherzustellen, dass im elektronischen Rechtsverkehr nur gesetzeskonforme Signaturanwendungskomponenten eingesetzt werden.

Die Gesetzeskonformität von Signaturanwendungskomponenten, die bei der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen eingesetzt werden, ist wahlweise durch eine nach § 18 SigG anerkannte Bestätigungsstelle oder durch den Hersteller zu bestätigen (§ 17 Abs. 4 SigG). Soweit es um die Erzeugung oder Prüfung qualifizierter elektronischer Signaturen mit Anbieter-Akkreditierung geht, muss die Bestätigung sogar zwingend durch eine anerkannte Bestätigungsstelle vorgenommen werden (§ 15 Abs. 7 SigG). (Bei den Signaturerstellungseinheiten ist die Gesetzeskonformität konstitutiv für die Erzeugung rechtswirksamer qualifizierter elektronischer Signaturen und folgerichtig bestimmen §§ 15 Abs. 7, 17 Abs. 4 SigG, dass die Erfüllung der Anforderungen an die Signaturerstellungseinheiten stets durch eine nach § 18 SigG anerkannte Bestätigungsstelle zu bestätigen ist. Eine Substitution der Bestätigung durch eine Herstellererklärung ist nicht möglich.)

---

<sup>40</sup> „Secure Access to Federated E-Government/E-Justice“. Der Auftrag zur Entwicklung wurde vergeben. Das System kann frühestens in der zweiten Hälfte 2010 zur Verfügung stehen.

<sup>41</sup> Auch die amtliche Begründung zu § 17 Abs. 2 S. 4 SigG geht davon aus, "dass die Verwendung von geeigneten Signaturanwendungskomponenten nicht Voraussetzung für die Erzeugung einer qualifizierten elektronischen Signatur ist." (Gesetzesentwurf der Bundesregierung, BR-Drucksache 496/00 vom 18.8.2000, S. 67).

#### **4. Fortgeschrittene elektronische Signatur**

Beim – nicht SigG-konformen – Mailaustausch basierend auf dem MailTrust-Standard kann eine PKI, die auch Behördenschlüssel umfasst, aufgebaut werden. Diese Lösung wurde in Zusammenarbeit mit dem BSI aus Kostengründen in verschiedenen Landesnetzen vorangetrieben. Sie ist in der nicht-formgebundenen, nicht an qualifizierte Signaturen gebundenen Kommunikation (z.B. gem. § 174 Abs. 3 ZPO) angemessen.

Der zum Entschlüsseln benötigte Schlüssel würde dann nicht auf einer Smartcard gespeichert, sondern würde – ggf. durch eine PIN gesichert – im Intranet so abgelegt, dass nur ein definierter Kreis von Berechtigten auf ihn zugreifen kann. Dies erleichtert im Vergleich zur Lösung mit Smartcards die interne Organisation. Daher sollen, wo zulässig, fortgeschrittene elektronische Signaturen, die Behördenschlüssel erlauben, eingesetzt werden.

#### **5. Verschlüsselung**

Wenn zusätzlich zur Signatur verschlüsselt werden muss, sind grundsätzlich die Verschlüsselungskomponenten des Signaturproduktes zu nutzen, um wirtschaftlich die entsprechende PKI zu nutzen.

Bilateral können im Einzelfall – nach einer entsprechenden Risiko- und Sicherheitsanalyse – Verschlüsselungsprodukte entsprechend Landesvorgaben etc. genutzt werden.

Verschlüsselungen sind nur als sicherer Transportcontainer auf unsicheren Kommunikationswegen einzusetzen und verschlüsselte Eingänge unmittelbar nach Empfang zu dekodieren. Scheitert die Entschlüsselung, so ist der Absender darüber zu informieren und auf ein geeignetes Verfahren hinzuweisen.

Nur entschlüsselte Dateien sollen gespeichert werden (ohne ihren „Transportumschlag“), um eventuellen Problemen bei späterer Dekodierung vorzubeugen.

## VI. Übertragungswege

Die Übermittlung von Dokumenten und Dateien im elektronischen Rechtsverkehr erfolgt grundsätzlich über Datenleitungen auf einem der drei Wege: SMTP, https oder OSCI.

Folgende Kommunikationsszenarios sind derzeit verfügbar und im ERV eingesetzt:

- E-Mail (SMTP)
- Nutzung von Webservern/Portalen
  - Zugang über Browser (SSL, https)
  - Zugang über Applikationen (OSCI)

Aufgrund der Beschränkung der Größe von E-Mail-Anlagen bei den verschiedenen Providern wird eine maximale Anlagengröße von 5 MB empfohlen.

### 1. E-Mail

E-Mail-Kommunikation bildet ein universelles Szenario ab, dessen Komponenten allgemein verfügbar sind.

Die Datenübermittlung erfolgt in -codierten oder nicht-codierten - Anhängen verschlüsselt und/oder signiert nach den hier dargestellten Standards. Zur Zuordnung der E-Mail sollen die wesentlichen Metadaten in den Feldern „Betreff“, „Absender“, „Empfänger“ genutzt werden.

Als Mailprotokoll ist SMTP<sup>42</sup> zu nutzen.

Es kann zweckmäßig sein, neben dem Mail-Zugang zusätzlich oder anstelle eines Mailzugangs eine Punkt-zu-Punkt Übertragungsart anzubieten, die eine sofortige Rückmeldung über Erfolg oder Misserfolg der Übertragung bietet und die Übermittlung prinzipiell beliebig großer Datenmengen erlaubt. Für solche Systeme ist das Protokoll http-s einzusetzen.

---

<sup>42</sup> Das „Simple-Mail-Transport-Protocol“ ist der E-Mail-Standard im Internet.

## **2. Nutzung von Webservern/Portalen**

Neben der Sicherung des Mailverkehrs wird der authentifizierte und gesicherte Online-Verkehr (Austausch von Formularen, Transaktionen) immer bedeutsamer. Formularserver/Upload-Verfahren bieten z.B. den Vorteil, Eingabedaten direkt zu überprüfen / plausibilisieren, die erforderlichen XJustiz-Daten strukturiert zu erfassen und Zeitpunkte des Einstellens oder Abholens von Informationen eindeutig in Justizhoheit feststellen zu können.

Die Verfahren müssen mit Standardbrowsern nutzbar sein. Wenn JAVA-Applets/Applikationen eingesetzt werden, müssen diese signiert sein. Die Nutzung unsignierter Applets/Applikationen und anderer aktiver Inhalte (z.B. JavaScript) ist grundsätzlich nicht gestattet.

### **a. Zugang über Browser**

In den entsprechenden Standardisierungsgremien des Internets sind Schnittstellen abgestimmt und festgelegt worden:

- SSL (Secure Socket Layer v 3.0)  
Schnittstelle für Internetbrowser, um über Plugins entsprechende Sicherheits-Produkte einzusetzen.
- S-HTTP (SecureHypertextTransferProtocoll)  
Protokollstandard zur gesicherten Übertragung via Internet/Intranet.

Es sind nur Produkte einzusetzen, die diese offenen Schnittstellen nutzen. Zulässig ist auch das Protokoll http in Verbindung mit anderen kryptographischen Mechanismen, die besonders zu vereinbaren sind („Containerverschlüsselung“) und die den gesicherten Transport über unsichere Netze ermöglichen.

### **b. Zugang über Applikationen**

Mit der eGovernment-Initiative BundOnline2005 hatte sich die Bundesregierung verpflichtet, alle internetfähigen Dienstleistungen des Bundes bis zum Jahr 2005 online bereitzustellen. Um die Behörden bei der Umsetzung des Programms zu unterstützen, hatte das Bundesministerium des Innern die Erstellung einer Basiskomponente Datensicherheit (= Virtuelle Poststelle) beauftragt. Diese Virtuelle Poststelle (VPS) ist Grundlage des Elektronischen Gerichts-und Verwaltungspostfachs (EGVP). Ein zentraler Baustein der VPS bzw. des EGVP ist die Software Governikus der bremen online services GmbH & Co. KG. Governikus implementiert OSCI-Transport und stellt sowohl einen Intermediär, als auch entsprechende Client-Bibliotheken für die

Programmierung von OSCI-fähigen Applikationen zur Verfügung.<sup>43</sup>

Im Rahmen des Projektes Media@Komm wird eine OSCI-Komponente auf Open-Source-Basis angeboten.

## VII. Elektronische Akte

Mit dem JKomG wurde bereits im Jahre 2005 die gesetzliche Grundlage zur Führung elektronischer Verfahrensakten in der Justiz geschaffen (ausgenommen lediglich der Bereich der StPO).

Die Konzeption und die Realisierungen stehen aber noch am Anfang. Daher erfolgen derzeit darüber hinaus keine weiteren Festlegungen. Insbesondere die Vorgabe von Strukturierungen für Ablage- und Suchkriterien, technische Rahmenbedingungen für die DMS und deren Workflow-Komponenten sind derzeit nicht möglich. Die in dieser Anlage 1 festgelegten Standards und Verfahren gelten auch im Grundsatz für den Aufbau elektronischer Akten (Dokumentenformate, XJustiz)<sup>44</sup>.

---

<sup>43</sup> Zum aktuellen Stand des Governikus siehe unter <http://www.bos-bremen.de/de/produkte/governikus/229415/>, hinsichtlich OSCI-Transport siehe unter <http://www1.osci.de/sixcms/detail.php?gsid=bremen02.c.1160.de> und für das EGVP unter [www.egvp.de](http://www.egvp.de).

<sup>44</sup> In Xjustiz wurde auf eine eigenständige Beschreibung von Dokumenten und Akten verzichtet und statt dessen XDOMEA eingebunden (zu XDOMEA s.u. [www.xdomea.de](http://www.xdomea.de)).