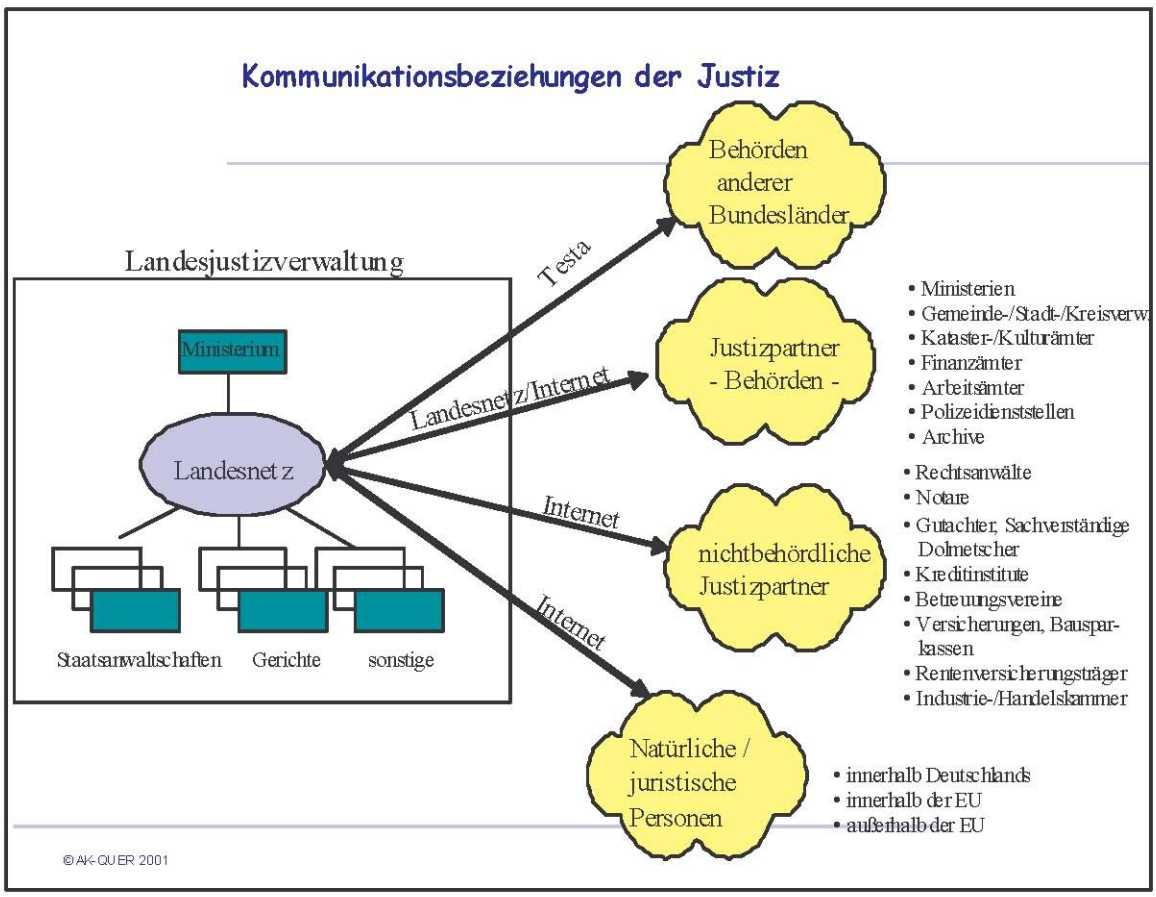
Technische Rahmenvorgaben
für den elektronischen Rechtsverkehr

Stand: ... Mai 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[1] 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 tief greifende 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.

[1] Auf verbindlich vorzugebende Standards wird im Folgenden durch entsprechende Formulierungen im Text hingewiesen. Tabellarisch werden sie auch in der Inhaltsübersicht aufgeführt.

Versionsnummern von Dateiformaten (z.B. Word v 2003) haben ihre Berechtigung in Rechtsverordnungen nach § 130a ZPO, um die tatsächliche Bearbeitbarkeit eines Eingangs durch das Gericht sicherstellen und 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.

Übersicht:

	Verbindliche Standards	Seite
I. Organisatorischer Rahmen	SAGA	**5**
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
II. Medien und Anlagengröße		**8**
1. Anlagengröße bei E-Mails	max. 5 MB	8
2. CD-ROM		8
3. DVD	(Einsatz nicht empfohlen)	8
III. Dokumentenformate		**9**
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	14
5. Langfristige Speicherung, Archivierung		14
IV. Übergabe strukturierter Daten, (Xjustiz)	XJustiz	**17**
1. Zielgruppen		17
2. Aufbau von XJustiz		17
3. Anpassungen und Erweiterungen von XJustiz		18
4. Informationen zu XJustiz		18
V. Authentisierung und Verschlüsselung		**19**
1. Basisverfahren	X.501, X.509 V3, PKCS#7 (alternativ: ISIS-MTT XML-DigSig/Encryption), PKCS#11	19
2. Elektronische Unterschrift nach SigG und Attribute		21
3. Interoperabilität und Gesetzeskonformität von Signaturanwendungskomponenten	ISIS-MTT V 1.1	23
4. Fortgeschrittene elektronische Signatur		25
5. Verschlüsselung		25
VI. Übertragungswege		**26**
1. E-Mail	SMTP	26
2. Nutzung von Webservern/Portalen		27
a) Zugang über Browser	SSL, S-HTTP	27
b) Zugang über Applikationen	OSCI V 1.2	27
VII. Elektronische Akte	(Abstimmung mit XDOMEA	28

I. Organisatorischer Rahmen

1. Übergreifende Standards

SAGA[2] 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).

[2] Standards and Architectures for e-government Applications, derzeit Version 2.0

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. Virenschutzprogrammme 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 Firewallsystemen auszustatten. Dabei sind die Firewallsysteme 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 dieser 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"[3] festgelegt. Ergänzende Festlegungen finden sich im sogenannten Joliet-Standard[4], 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. Derzeit kann noch keine allgemein gültige Empfehlung gegeben werden, welcher DVD-Standard eingesetzt werden sollte.

---

[3] Das „Orange Book“ ist eines von mehreren „Bunten Büchern“ (vgl. „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“).

[4] Zu „Joliet“ vgl. „http://whatis.techtarget.com/definition/0,,sid9_gci212402,00.html (Überblick) sowie weiterführend „http://bmrc.berkeley.edu/people/chaffee/jolspec.html“.

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 Virenscanner bzw. virenfreie Systeme verfügen, die derartig ausführbaren Code auf bekannte Schadwirkungen prüfen können.[5]

[5] Ein Schaden kann aber schon darin gesehen werden, dass ggf. über den fristwahrenden 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[6]

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[7], 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.[8] Ältere Softwareversionen können dabei häufig neuere Dateiformate nicht direkt bearbeiten.[9]

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. Dateibeschreibungen 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.[10]

Obwohl verschiedene Word-Formate wegen ihrer Verbreitung auch von einigen anderen Programmen erkannt und zum Teil auch erzeugt werden können, kann von einer plattformübergreifenden

---

[6] Als „codiert“ werden hier Daten bezeichnet, bei denen die Informationen zeichenorientiert übermittel 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.

[7] 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“).

[8] 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.

[9] 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.

[10] Vgl. c’t magazin für computertechnik, Heft 3 / 2002 S.172, Dokumente durchleuchtet: Was Office-Dateien verraten können.

Verfügbarkeit nicht gesprochen werden. Archivverwaltungen, die sich grundsätzlich der Übernahme digitaler Daten öffnen, haben Word-Formate daher bisher als nicht archivierungsfähig bezeichnet.

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[11] sowie die europastämmige ECMA International[12] für eine Anerkennung von OOXML als ISO-Standard ausgesprochen hatten.[13]

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[14]. 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[15] - 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 niedrigschwelliger Teilnahmevoraussetzungen abgesehen.[16]

---

[11] DIN: Deutsches Institut für Normung

[12] ECMA International: ursprünglich: “European Computer Manufacturers Association”; ECMA-Standard 376

[13] 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.

[14] Vgl. Übersicht in Wikipedia: http://de.wikipedia.org/wiki/OpenDocument#Einsatz_des_OpenDocument-Formats_bei_.C3.B6ffentlichen_Stellen

[15] Kommunikation von Bürgern („Citizen“) bzw. Unternehmen („Business“) mit staatlichen Stellen („Government“)

[16] 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.

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[17] an. Alle Einträge einschließlich der Formatierungsanweisungen werden in Klartext aufgelöst und können im Klartext von einem ASCII[18]-Editor angezeigt werden. Das RTF-Format gibt das Layout z.B. von Word-Dateien wieder, kennt jedoch keine Makros.[19]

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 „**P**ortable **D**ocument **F**ormat“ (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[20] 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).[21] 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.[22]

---

[17] „**O**pen **D**ocument **A**rchitecture“ / „**O**pen **D**ocument **I**nterchange **F**ormat“

[18] „**A**merican **S**tandard **C**ode of **I**nformation **I**nterchange“

[19] 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“

[20] DTP: Desk Top Publishing

[21] 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)

[22] PDF/A kann von Adobe Acrobat ab der Version 8.0 und auch über weitere Tools erzeugt werden.

Textformat (ASCII und UNICODE)

Der „**A**merican **S**tandard **C**ode of **I**nformation **I**nterchange“ 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 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 „E**x**tensible **M**arkup **L**anguage“, 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 „**D**ocument **T**ype **D**efinition“ (DTD) oder in einer XML Schema Datei beschrieben werden. Die Dateiinhalte sind als ASCII-Zeichen oder im UniCode[23] 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 Textverarbeitungs-systemen 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.

[23] UniCode ist der (16bit) Nachfolger des ASCIII-Zeichensatzes, mit dem auch länderspezifische Alphabete dargestellt werden können.

4. Formate für nicht-codierte Daten

Zum Austausch nicht-codierter Daten soll entweder das TIFF-Format[24] in der Version 6.0, CCITT/TSS Gruppe 4, verwendet werden oder eine Umwandlung in eine PDF/A Datei erfolgen.

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[25].

Unabhängig von den für die Aktenbildung eingesetzten Systemen und ihren gegebenenfalls spezifischen Anforderungen sollen die eingesetzen Dateiformate für eine langfristige Speicherung und Bearbeitbarkeit[26] 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.

---

[24] TIFF ("**T**ag **I**mage **F**ile **F**ormat")

[25] 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.).

[26] DerBegriff 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 Beiziehung der Akte - noch erforderlich sein.

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 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.[27] In diesem Falle enthält das Anzeigeprogramm (Adobe’s Acrobat) einen Menüpunkt, über den die Signaturprüfung und die Anzeige des Ergebnisses angestoßen werden kann.[28] 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.[29]

---

[27] Die Signatur kann auch in dem PDF/A-Format aufgenommen werden.

[28] 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 Authentitäts-prüfungen erforderlichen Root-Zertifikate können aber gesondert importiert werden.

[29] Die revisionssichere Speicherung von Daten ist eine klassische Aufgabe öffentlich-rechtlicher Rechenzentren. Die dazu erforderlichen Techniken werden laufend fortentwickelt.

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[30], 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 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.

[30] Vgl. bspw. §§ 105 (1), 164 (4), 315 (3), 319 (2), 320 (4), 734, 813 (2) ZPO

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[31] 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.

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.

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. XJusiz.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 Philosophie und Aufbau näher beschreibt, ist in der Anlage 2 beigefügt.

Die aktuelle Dokumentation zu XJustiz kann unter www.xjustiz.de und www.osci.de abgerufen werden.

---

[31] Ein Schaden kann aber schon darin gesehen werden, dass ggf. über den fristwahrenden Eingang einer Erklärung gestritten wird, die von einem Virusscanner entfernt wurde. Dateiformate, die keine aktiven Elemente kennen, tragen daher zur Eindeutigkeit der Kommunikation bei.

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 ISIS-MTT-Spezifikation (ISIS-MTT v 1.0.1[32]) verfolgt dieses Ziel. Daneben wird das Ziel verfolgt, einen offenen und zertifizierten Standard zu schaffen, der nicht durch teilweise nicht prüfbare firmeninterne oder länderspezifische Vorschriften (z.B. US-Geheimnisse oder Exportbeschränkungen) geschützt ist.

Der MailTrusT-Standard [MTT], der in ISIS-MTT v. 1.1 integriert ist, wurde von dem Tele-Trust-Verein [TTT] entwickelt, dem alle führenden deutschen Hersteller von kryptographischen Produkten, sowie weitere Stellen wie z.B. der TÜV-IT, das BSI oder das Bundeskriminalamt angehören. Der Standard berücksichtigt internationale Normen (S/MIME, X.509, PKIX, PKCS#).[33]

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 einen Datencontainer ermöglicht, der nach dem Prinzip des „doppelten Umschlags“ konzipiert ist, und eine strikte Trennung der eigentlichen Inhalte von Transportdaten vorsieht. 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, ISIS MTT, etc.). OSCI ist sowohl auf der Ebene der Transport- als auch auf der Ebene der Inhaltsdaten eine

[32] Der „**I**ndustrial **S**ignature **I**nteroperability **S**pecification“ der führenden deutschen Trustcenter wurde zunächst als reiner Signaturstandard konzipiert. Er wurde im Herbst 2001 verbunden mit dem E-Mail Standard „**M**ail-**T**rus**T** 2.0“ zu „ISIS-MTT“.

[33] 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

XML-Anwendung. Somit ist die Möglichkeit einer standardisierten Strukturierung der Nachrichteninhalte und somit 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, zertifizierte Zeitstempeldienste, etc.).

Das Ziel der Interoperabilität ist noch nicht erreicht, entsprechende Tests des BSI werden jedoch mittelfristig abgeschlossen sein (s.u. Firmenabstimmung am 28. März 2002 in Stuttgart).

Um an den Arbeiten zu einer Interoperabilität zukünftig aufsetzen zu können, sind folgende Basisverfahren für Produkte, die eingesetzt werden, verbindlich:

ITU[34]-Empfehlung X.501

Das allgemeine Format für Namen wird in der ITU-T Empfehlung [ITU-T X.501] durch den *distinguished nam*e-Typ festgelegt. Der *distinguished name* besteht aus einer Folge von *AttributeType*-und *AttributeValu*e-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.

[34] International Telecommunication Union, früher CCITT

Austauschformat PKCS #7[35]

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 SigG sind Signaturschlüsselpaare für Signaturen nur natürlichen Personen zuzuordnen. Keine Aussage trifft das Signaturgesetz über die Zuordnung von Verschlüsselungsschlüsseln. In der Praxis befindet sich auf den von den Trustcentern ausgegebenen Smartcards aber regelmäßig auch ein Verschlüsselungsschlüsselpaar, das dem Signaturschlüsselinhaber zugeordnet ist (personalisierter Verschlüsselungsschlüssel). Der öffentliche Verschlüsselungsschlüssel kann weitergegeben werden, um das Verschlüsseln von Nachrichten für den Schlüsselinhaber zu ermöglichen. Nur der Schlüsselinhaber kann die für ihn verschlüsselte Nachrichten mit Hilfe des auf seiner Smartcard befindlichen privaten Schlüssels entschlüsseln.

Solange noch nicht alle Trustcenter ihre Praxis geändert haben und eine behördenbezogene Verschlüsselung auf ihren Karten anbieten, ist eine behördenbezogene gesicherte Übertragung mit SigG-konformen Produkten zu Poststellen der Gerichte zunächst nicht ohne Weiteres möglich. Für bestimmte Personen -z.B. an der/den Posteingangsstelle(n) – muss deren öffentlicher Schlüssel als für den Eingang relevant bekannt gegeben werden. Vertretungen würden aber an der Nichtübertragbarkeit der Signatur scheitern.[36]

---

[35] Nachdem Profile für XML-Signature und XML-Encryption in die Kernspezifikation des ISIS-MTT-Standards 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 ISIS-MTTXML-Profil validieren können.

[36] In einer Hilfskonstruktion könnte eine Person (z.B. der Geschäftsleiter) neben seiner persönlichen, unter seinem bürgerlichen Namen firmierenden Signatur sich eine zweite Signatur unter einem Pseudonym (z.B. als „Poststelle Amtsgericht Hamburg“) erteilen lassen. Der zu dieser Signatur gehörende öffentliche Verschlüsselungsschlüssel könnte für die vertrauliche Kommunikation mit dem AG bekannt gegeben werden.
Die Chipkarte würde in der Posteingangsstelle von den jeweils Zuständigen zum „Öffnen“ der Post (Entschlüsseln) benutzt und (mindestens) ebenso sorgfältig verwahrt und ggf. weitergegeben wie ein Dienstsiegel. Diese Hilfskonstruktion mag in kleinen Dienststellen bzw. bei begrenzten Pilotierungen funktionieren. Bei großen Dienststellen, in denen mehrere Mitarbeiter die Eingangspost parallel entgegennehmen und weiterleiten müssen, scheitert ein solches Konstrukt. In jedem Falle bleibt die sachlich nicht begründete Bindung des Kommunikationsschlüssels einer Institution an eine natürliche Person.

Damit eingegangene Sendungen auch bei Urlaub, Krankheit oder bei Verlust der Karte in jedem Fall entschlüsselt werden können, empfiehlt es sich, die zur Entschlüsselung beim Gericht verwendete Karte wie folgt zu behandeln:

- Die zur Signatur vorgesehenen Zertifikate werden sofort nach Ausgabe der Karte widerrufen. Damit kann nur noch das Verschlüsselungszertifikat genutzt werden. Die SigG-relevanten Funktionen sind lahm gelegt. Einer Weitergabe von Karte und PIN stehen deshalb keine Bedenken entgegen.
- Bei Beantragung der Karte werden sofort eine oder mehrere identische Ersatzkarten beantragt. Eine Ersatzkarte wird an sicherer Stelle (Tresor) aufbewahrt. Intern muss der private Verschlüsselungs-Schlüssel der Poststelle mehreren Personen zur Verfügung stehen (für paralleles Abarbeiten des Posteingangs oder bei Vertretungen), während diese Weitergabe für Signaturen nicht in Betracht kommen kann.

Über entsprechende Anzeigekomponenten wird sichergestellt, dass das Prinzip WYSIWYS (What You See Is What You Sign) eingehalten wird.
Falls die – signierte – Visualisierung nicht weiterverarbeitbar ist (z.B. tiff), soll die Übersendung einer weiterverarbeitbaren Datei entsprechend den oben aufgestellten Vorgaben zu den Formaten erfolgen. Beide Dateien sollen mit einer Klammersignatur[37] versehen werden.

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

[37] Hier wird wegen der Darstellungsproblematik die Klammersignatur i.d.R. nur eine „fortgeschrittene elektronische Signatur“ sein können, was ausreichend ist.

(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 Abs. 2 S.4 SigG).[38]

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.

3. **Interoperabilität und Gesetzeskonformität von Signaturanwendungskomponenten**

Aus wirtschaftlichen Gründen ist es gewünscht, vielen Anbietern von TrustCenter-Diensten und von technischen Produkten für elektronische Signaturen den Marktzugang zu eröffnen. Damit stellt sich das Problem der Interoperabilität.

Über die ISIS-Spezifikation (Industrial Signature Interoperability Specification) in der aktuellen Version 1.1 (ISIS-MTT v. 1.1), die auch den Mailtruststandard inkorporiert, wird angestrebt, Interoperabilität zwischen TrustCentern bzw. zwischen technischen Produkten für elektronische Signaturen herzustellen. Die ISIS-MTT-Konformität und die Interoperabilität wird, so haben die Abstimmungen ergeben, von allen Bietern, die in der T7[39]-Gruppe vertreten sind (SignTrust, TeleSec, DATEV, Bundesdruckerei) angestrebt, faktisch realisiert ist sie noch nicht. Insbesondere können in den gängigen Mailclients (z.B. Outlook) nicht mehrere PlugIns verschiedener Hersteller parallel integriert werden

Die Abstimmungen und Tests des BSI hierzu sind noch nicht abgeschlossen. Eine Produktentscheidung verhindert daher u.U. derzeit noch eine Interoperabilität mit anderen Produkten.

[38] 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.” (Gesetzentwurf der Bundesregierung, BR-Drucksache 496/00 vom 18.8.2000, S. 67).

[39] Homepage der Gruppe: „http://www.t7-isis.de/index.html“.

Firmenabstimmung am 28. März 2002 in Stuttgart

Die Trustcenterbetreiber Telesec (mit dem Softwarehaus SECUonline), SignTrust, Datev, Bundesdruckerei mit D-Trust haben in einer Veranstaltung am 28. März 2002 in Stuttgart verbindlich eine Erklärung dahin abgegeben, dass die Interoperabilität (Interoperabilität der Anwender-Komponenten nach ISIS-MTT und der Interoperabilität auf Zertifikatsebene) bis spätestens November 2002 vollständig sichergestellt sei.

Eine schriftliche Bestätigung ist daher Formsache und auf keinen Fall unbillig.

Von Seiten der Betreiber wurde weiterhin zugesichert, jederzeit auf Anforderungen einzugehen und die Anwendungskomponenten an die Erfordernisse der Justiz anzupassen. Damit soll erreicht werden, dass eine weitere Verbreitung des elektronischen Rechtsverkehrs im Rahmen der jeweiligen Landessystemkonzepte möglich ist.

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.)

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 wird z.Zt. 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.

An die Produkte und Hersteller sind dieselben Anforderungen wie unter V. 2. beschrieben zu stellen.

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[40] 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.

[40] Das „**S**imple-**M**ail-**T**ransport-**P**rotocol“ ist der E-Mail-Standard im Internet.

2. Nutzung von Webservern/Portalen

Neben der Sicherung des Mailverkehrs wird der authentisierte 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 hat 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, hat 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. Die aktuelle Version Governikus 2.0 implementiert

den Standard OSCI-1.2 und stellt sowohl einen Intermediär, als auch entsprechende Client-Bibliotheken für die Programmierung von OSCI-fähigen Applikationen zur Verfügung.
Im Rahmen des Projektes Media@Komm wird eine OSCI-Komponente auf Open-Source-Basis angeboten.

VII. Elektronische Akte

Mit dem JKomG ist die breite Einführung der elektronischen Akte möglich.

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)[41].

[41] Im Jahre 2005 ist bei der OSCI-Leitstelle mit einer Abstimmung von Datenstrukturen zwischen XJustiz und XDOMEA begonnen worden.