DuD
Datenschutz und Datensicherheit

Signiertes XML und das Präsentationsproblem

Andreas U. Schmidt

Eines der gravierendsten Probleme, die sich einer breiten öffentlichen Anwendung digitaler Signaturen in den Weg stellt, ist das Problem der zurechenbaren und beweiskräftigen Präsentation signierter Dokumente.[1] Im vorliegenden Beitrag wird untersucht, welchen Lösungsbeitrag hierzu die Extensible Markup Language (XML) als universelles Datenformat und der XML-Signaturstandard, der zurzeit vom World Wide Web Consortium (W3C) spezifiziert wird, leisten können.

Dr. phil. nat.
Andreas U. Schmidt

Postdoktorand im Themenbereich Marktplatz Internet (MINT) des Instituts für sichere Telekooperation (SIT) der GMD in Darmstadt. Arbeitsschwerpunkt: Umsetzung digitaler Signaturen in XML und E-Commerce Protokollen.

E-Mail: aschmidt@darmstadt.gmd.de

[1] Siehe Fox, DuD 7/1998, S. 386 ff., und Pordesch, DuD 2/1999, S. 89 ff.

Einleitung

Seit zweieinhalb Jahren ist mit dem deutschen Signaturgesetz (SigG) und der zugehörigen Signaturverordnung (SigV) eines der weltweit ambitioniertesten Regelwerke zu digitalen Signaturen in Kraft. Hervorgehoben wird meist zu Recht die Rechtssicherheit, die das SigG für die digitale Signatur als *sekundärem* Authentifizierungsmedium neben der eigenhändigen Unterschrift schafft. In der langfristigen Perspektive ist der Anspruch des Gesetzes aber sehr viel weitreichender: Die digitale Signatur soll prinzipiell in der Lage sein, die handschriftliche zu ersetzen. Dies wird auch deutlich im Evaluierungsbericht der Bundesregierung zum IuKDG,[2] der am 16. Juni 1999 vorgelegt wurde:

„Digitale Signaturen können in nahezu allen Lebensbereichen alternativ zur eigenhändigen Unterschrift eingesetzt werden."[3]

Und speziell in Bezug auf Vorgänge, bei denen die Schriftform gefordert ist:

„Fälschungssichere digitale Signaturen nach dem SigG bilden die Basis für die Einführung der 'elektronischen Form' als Alternative zur gesetzlichen Schriftform."

Wer sie nutzt hat die „Sicherheitsvermutung" (Roßnagel [Roßnagel_98]) nach § 1 Abs. 1 SigG für sich. Er kommt daher in den Genuss einer Beweiserleichterung, die eine vergleichbare Rechtssicherheit wie die herkömmliche Schrifturkunde bietet.[4]

Das von der Bundesregierung vorgelegte Aktionsprogramm „Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts" hat in den Teilen, die sich auf die digitale Signatur beziehen, die gleiche Stoßrichtung:

„Durch den mit der gesetzlichen digitalen Signatur möglichen weitgehenden Umstieg vom Papierdokument auf das elektronische Dokument wird ein erhebliches volks- und betriebswirtschaftliches Rationalisierungspotenzial erschlossen."[5]

Zurzeit bereitet das Bundesjustizministerium eine Anpassung des bürgerlichen Gesetzbuches zur Einführung einer 'elektronischen Form' gleichrangig neben der klassischen Schriftform vor.[6]

Zwar ist nicht zu erwarten, dass digitale Signaturen innerhalb der nächsten Jahre tatsächlich auf breiter Front den Platz der handschriftlichen Unterschrift einnehmen, die Zitate machen aber klar, dass die Erreichung dieses Zieles von Seiten der Politik eingefordert wird und technische Überlegungen dem Rechnung tragen sollten.[7] Zugleich wirft ein so allgemeiner Geltungsanspruch aber eine Reihe von Problemen auf, wie z. B. die von Ulrich Pordesch [Pordesch_00, ausführlicher in der Studie Pordesch_99] aufgezeigten. Vergleicht man die dortigen Ergebnisse mit dem in der Einleitung geschilderten hohen Anspruch, so lassen sie erhebliche Zweifel an der Annahme einer Beweiskraft digital signierter Dokumente aufkommen.

Allgemein gesprochen liegt das zentrale Problem darin, dass digitale Daten in ihrer inneren Struktur und in der Form, in der sie Menschen präsentiert werden, eine viel größere Variabilität aufweisen, als Schrift oder auch Zeichnungen auf Papier. Signierte digitale Daten stehen in einem Kontext, in dem ihre 'gerichtsfest' nachvollziehbare

[2] Informations- und Kommunikationsdienstegesetz; Art. 3 ist das Signaturgesetz.

[3] Siehe [IuKDG-Bericht], Abschnitt 2.4.

[4] Siehe [IuKDG-Bericht], Abschnitt 1.

[5] Siehe [Aktionsprogramm], S. 44.

[6] Siehe [BMJ_99].

[7] Das gilt auch dann, wenn aus der Sicht einer speziellen Anwendung, wie etwa dem E-Commerce, nicht klar sein mag, warum die hohen Anforderungen an digitale Signaturen des SigG erforderlich sind. Das SigG lässt ja digitale Signaturen mit geringerem Anspruch – und dementsprechend möglicherweise geringerem Beweiswert – ausdrücklich zu. Dies wird auch explizit im Entwurf der europäischen Signaturrichtlinie ausgedrückt, die sogenannte 'einfache' Signaturen mit gegenüber dem SigG erheblich schwächeren Anforderungen einführt.

Präsentation entscheidend für ihre Würdigung als Beweismittel in Streitfällen wird.

Das *Präsentationsproblem* entwickelt sich auf mehreren Bedeutungsebenen. In [Pordesch_99] werden unter diesem Begriff speziell die unmittelbare Darstellung der signierten Daten sowie die darauf aufbauende Interaktion des Benutzers mit ihnen subsumiert. Im Zusammenhang mit XML wird außerdem die der Präsentation zugrundeliegende Syntax der Daten wichtig werden.

In diesem Beitrag werden die Teile des *Kontextproblems* dargestellt, die sich durch die Implementation von digitalen Signaturen in XML erschließen. Der Leitgedanke ist dabei, für die relevanten Bestandteile eines signierten XML-Dokuments und seines Kontextes die jeweilige Bedeutung in Bezug auf das Kontextproblem zu untersuchen und darauf abgestimmte Lösungsvorschläge zu machen.

1 Kontextproblem bei XML-Signaturen

XML[8] ist zur Zeit ein häufig gehörtes Akronym im IT-Business. An das universelle Datenformat knüpfen sich große Hoffnungen im Hinblick auf die Lösung des Problems der Interoperabilität unterschiedlicher Datenwelten.[9]

Auf den ersten Blick ähnelt XML sehr der bekannten Textauszeichnung in HTML. Ein XML-Abschnitt sieht gewöhnlich so aus:

```
<Element>
 Inhalt
</Element>
```

Diese sogenannten *Tags* umschließen den Inhalt des Dokuments als bezeichnete Klammern. Durch die Verschachtelung dieser Elemente entsteht eine komplexe Syntax, die durch Querverweise ergänzt werden kann.

Während aber HTML eine SGML-*Anwendung* darstellt, das heißt eine vordefinierte Menge von Tags mit festgelegter Bedeutung für einen speziellen Kontext (die Darstellung im Browser), ist XML eine *Untermenge* von SGML. Insbesondere ist die Menge möglicher Tags, die sogenannten Elemente eines XML-Dokuments, nicht vorbestimmt und im Prinzip unbegrenzt – XML legt nur die Syntax ihrer Verwendung fest. Somit lassen sich in XML prinzipiell alle möglichen Datenstrukturen darstellen, fzum Beispiel auch die von HTML, das somit selbst als eine XML-Anwendung verstanden werden kann.[10]

Um XML mit Leben zu füllen hat das World Wide Web Consortium (W3C) verschiedene Aktivitäten und Standardisierungsgruppen ins Leben gerufen. Diese haben inzwischen etliche XML-Anwendungen und ihre Semantik festgelegt, die in anwendungsspezifischen Dokumenten Verwendung finden können. So gibt es auch eine Arbeitsgruppe, die sich mit der Definition einer Semantik und der zugehörigen Syntax für digitale Signaturen in XML beschäftigt und deren Entwürfe schon fast bis zur Anwendungsreife gediehen sind.[11]

Im Folgenden wird die allgemeine Struktur eines signierten XML-Dokuments, wie sie sich nach den gegebenen und in Arbeit befindlichen Standards darstellt, in Bezug auf die verschiedenen Ebenen des Kontextproblems analysiert. Dabei zeigt sich, dass diese anhand vier verschiedener und paarweise zueinander orthogonaler Komponenten beschrieben werden können.

1.1 Syntax und Darstellung

Der erste Schritt zur Festlegung des Kontextes für XML-Dokumente innerhalb einer bestimmten Anwendung ist die Definition des *syntaktischen Kontextes*. Das heißt, die zulässige Syntax der zur intendierten Anwendung gehörigen Dokumente muss gegenüber der allgemeinen XML-Syntax konkretisiert und damit die zulässigen Datenstrukturen festgelegt werden. Das Instrument hierzu verbirgt sich in XML hinter dem allgemeinen Konzept des Schemas. In einem *XML-Schema* lassen sich die zulässigen Elementnamen, die Baumstruktur, die die Elemente bilden können und der Datentyp des Elementinhalts festlegen. Als Schemasprache ist zunächst einmal die *Dokumententypdefinition* (DTD) vorgesehen. DTDs bieten aber nicht alle nötigen Ausdrucksmittel, um Datenstrukturen für alle Anwendungen hinreichend stark fixieren zu können. Die XML-Schema-Arbeitsgruppe des W3C arbeitet deshalb an einer wesentlich ausgefeilteren Schemasprache.

Ein XML-Dokument, das den in einem bestimmten Schema festgelegten Regeln genügt, heißt *gültig* (im Unterschied zum Begriff der *Wohlgeformtheit* eines Dokuments, der nur aussagt, dass das Dokument der grundlegenden XML-Syntax genügt). Zukünftig soll jede XML-fähige Anwendung nicht nur die Wohlgeformtheit, sondern auch die Gültigkeit von XML-Dokumenten prüfen.

Wie erwähnt besitzt das eigentliche XML im Gegensatz zu HTML keine eingebauten Methoden zur Festlegung der Darstellungsform von Dokumenten. Um diesem Mangel abzuhelfen, hat das W3C mit den XML-Anwendungen *Extensible Stylesheet Language* (XSL) und *XSL Transformations* (XSLT) zwei mächtige Werkzeuge geschaffen, die in ihrer Flexibilität und Mächtigkeit weit über das von HTML und auch *Cascading Stylesheets* Bekannte hinausgehen. XSLT ist eine selbst wieder in XML formulierte Sprache, die es erlaubt, XML-Dokumente auf nahezu beliebige Weise in andere XML-Dokumente umzuwandeln und ihre Baumstruktur zu manipulieren.[12] Das Standardbeispiel für eine solche Transformation ist die Umwandlung von anwendungsspezifischen XML-Dokumenten in HTML-Seiten zur Darstellung im Browser. Jedoch ist auch eine Umwandlung in alle XML-basierten oder andere Darstellungsformate möglich, zum Beispiel Speech ML (zur Sprachausgabe) oder *Rich Text Format*. Seine volle Stärke bei der seitenorientierten Darstellung entfaltet XML aber, wenn das Ziel der Transformation eines Dokuments die XSL-eigene Formatierungssprache ist. Diese erfüllt alle wesentlichen Anforderungen an ein professionelles Layout, das sich mit ihr bis in feine Details beschreiben lässt. Inzwischen entstehen Tools, mit denen sich diese Formatierungsanweisungen in PDF-Dokumente übersetzen lassen.
Mithilfe von XSL kann also der Darstellungskontext eines signierten XML-Dokuments für alle seitenorientierten Aus-

[8] Extensible Markup Language.

[9] Es gibt inzwischen eine ganze Reihe dickleibiger Abhandlungen über XML und seine Anwendung, die im Kontrast zur Jugend dieses Standards stehen. Auf den WWW-Seiten des World Wide Web Consortiums (www.w3c.org) kann sich zudem jeder Interessierte, der bereit ist etwas Zeit zu investieren, sehr aktuell und dennoch ziemlich allgemeinverständlich informieren.

[10] In der unter www.w3.org/TR/xhtml zu findenden 'W3C Proposed Recommendation' wird dieser XHTML genannte Standard beschrieben.

[11] Siehe den Spezifikationsentwurf [XMLDSig] und die Homepage www.w3.org/Signature der Arbeitsgruppe .

[12] XSLT hat in der Version 1.0 inzwischen den Status einer 'Proposed Recommendation' und damit einen stabilen Zustand erreicht. XSL ist dagegen noch ein 'Working Draft' und wird wahrscheinlich, obwohl schon sehr umfangreich, noch um einiges erweitert werden.

gabegeräte einer Klasse (Bildschirmfenster eines XSL-fähigen Browsers, Drucker etc.) einheitlich festgelegt werden, jedenfalls sofern sich das Gerät an den Standard hält.

1.2 Anwendung und Signatur

Betrachten wir ein einfaches Beispiel für ein zu signierendes XML-Dokument:

```
<Dokument>
 <Titel>
 Mein Dokument.
 </Titel>
 <Inhalt>
     Mein Text.
 </Inhalt>
</Dokument>
```

Die Signatur 'unter' diesem Dokument könnte nach dem vorläufigen Standardentwurf [XML-Dsig] grob vereinfacht[13] etwa so aussehen:

```
<dsig:Signature>
 <dsig:SignedInfo>
 ...
 <dsig:ObjectReference>
 <dsig:Location
URI=„http://www.Dokument.de
/“>
 ...
 </dsig:ObjectReference>
 ...
 </dsig:SignedInfo>
 <dsig:Signaturevalue>
 ...
 </dsig:Signaturevalue>
</dsig:Signature>
```

Was hier gegenüber unseren bisherigen Beispielen ins Auge fällt, ist der Namensraum-Präfix '`dsig`'. Der technische Zweck der Namensräume ist es zunächst einmal, Kollisionen zwischen den Elementnamen verschiedener Anwendungsbereiche zu vermeiden. Es ist klar, dass sie darüberhinaus verschiedene Anwendungskontexte trennen und somit eine wichtige semantische Funktion haben.

Namensräume müssen bei ihrer ersten Verwendung eindeutig definiert werden, was im Allgemeinen durch Angabe einer WWW-Ressource geschieht, unter der die entsprechende Spezifikation zu finden ist. In unserem Fall könnte dies zum Beispiel so aussehen:

```
<dsig:Signature xmlns:dsig=
„http://www.w3.org/Signature/
Drafts/WD-xmldsig-core-
200001281“>
 ...
</dsig:Signature>
```

Hinter dieser Adresse kann sich wie in [XML-Dsig] eine für Menschen lesbare Spezifikation der Anwendungssemantik oder ein dazugehöriges Schema zur Definition der Syntax der Anwendung verbergen.

Im Element `SignedInfo` der Signatur sind dann alle zur Signatur gehörenden Daten enthalten, insbesondere ein oder mehrere `ObjectReference`-Elemente, die auf das zu signierende XML-Dokument durch Angabe des 'Universal Resource Identifiers' (URI) im Attribut `URI` des Elements `Location` verweisen.

Dies kann ein lokaler, also auf einen Teil des Gesamtdokuments bezogener Verweis sein, der die Signatur enthält, aber es sind auch externe Verweise auf allgemeine WWW-Ressourcen möglich. Die eigentliche digitale Signatur wird dann über das Element `SignedInfo` und seine Unterelemente gebildet, wobei die Integrität der zu signierenden Daten durch einen digitalen Fingerabdruck innerhalb des `ObjectReference`-Elements geschützt wird.

Man sieht: Bei signiertem XML ist das unterzeichnete Dokument auf dreierlei Weise von der Signatur getrennt:

- Syntaktisch durch Verwendung eines eigenen Namensraums und Schemas,
- eventuell physisch – durch externe Verweisung – und schließlich auch
- technisch dadurch, dass nur der Inhalt von `SignedInfo` tatsächlich digital signiert wird.

1.3 Kontext-Komponenten

Im Kontext von signiertem XML lassen sich also einerseits die semantischen Ebenen Syntax und Darstellung und andererseits der Anwendungs- vom Signaturkontext unterscheiden. Damit lassen sich vier sowohl von ihrer Bedeutung als auch technisch trennbare XML-Komponenten festhalten, die bei digitalen Signaturen relevant werden:

- Das *Signaturschema* legt die Syntax der XML-Signaturen fest. Es wird durch die Standardisierung im W3C für alle digital signierten XML-Dokumente einheitlich sein.
- Das *Anwendungsschema* kann dasselbe für die jeweilige Anwendung leisten.
- Ein *Signatur-Stylesheet* kann verwendet werden, um die in der XML-Signatur enthaltenen Informationen darzustellen, während
- ein *Anwendungs-Stylesheet* die signierten Daten sichtbar machen kann.

Bei den letzten drei Komponenten heißt „kann“ natürlich, dass sie explizit vorhanden sein müssen (und nicht etwa 'festverdrahtet' sind), wenn obige Aufteilung stimmen soll. Die Abbildung zeigt eine

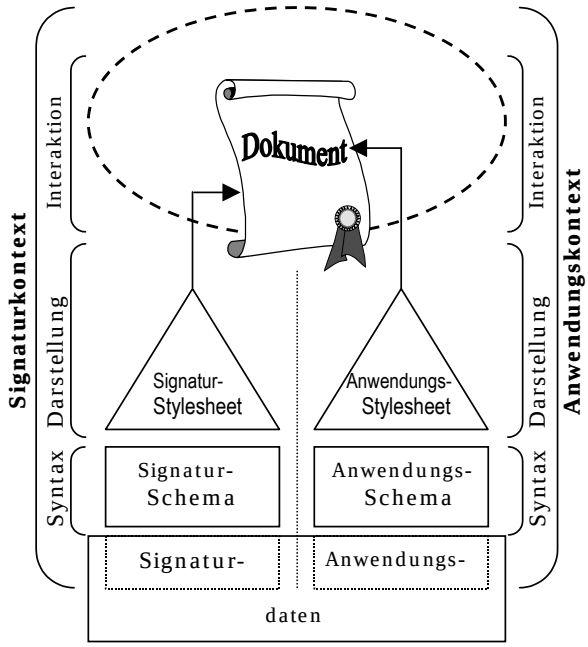

Abb.: Der Kontext eines signierten XML-Dokuments.

[13] Hier wird insbesondere weggelassen: Der vorgeschriebene digitale Fingerabdruck des Dokuments, die Angabe von Signatur- und Hashalgorithmen, Informationen über Signierer und Schlüssel sowie Kodierungs und Kanonisierungsinformationen.

schematische Darstellung der beschriebenen Strukturen.

Im folgenden Abschnitt wird gezeigt, wie sich diese Komponenten in Lösungsansätze für das Kontextproblem einbringen lassen.

2 Wie hilft XML?

Die Universalität von XML scheint zunächst ein zusätzliches Problem zu sein, denn die Vielzahl von möglichen Anwendungskontexten bedingt eine Vielzahl zugehöriger Kontextprobleme. Dies bringt offenbar jedes Datenformat mit sich, das so universell ist wie XML.

Signiertes XML macht aber einige der Problembestandteile explizit und damit handhabbar. Das wird deutlich, wenn man versucht, Anforderungen an die genannten Komponenten zu stellen, um die Beweiskraft eines signierten XML-Dokuments zu erhöhen und sich dabei z. B. an den rechtlichen Anforderungen und praktischen Gestaltungszielen, die in [Pordesch_99] formuliert wurden, orientiert. Leitlinie ist dabei die Grundforderung, dass Inhalt und Präsentation des signierten Dokuments dem Unterzeichner *zurechenbar* gemacht werden sollen.

Zunächst ist festzuhalten, dass sich der Signaturkontext in Bezug auf die rechtliche Verantwortung, die ein Unterzeichner für ihn übernehmen kann, grundsätzlich vom Anwendungskontext unterscheidet. Der XML-Signaturkontext wird durch einen Standard unabhängig vom Unterzeichner definiert. Er bildet daher das eigentliche Medium der digitalen XML-Signatur. Der Unterzeichnende kann nur begrenzt Verantwortung für die Funktionsweise dieses Mediums übernehmen, wie er auch beim Papier in gewissem Maße auf die Funktion des Mediums vertrauen muss. Der Anwendungskontext ist dagegen im Allgemeinen ‘proprietär’: Er kann sowohl vom Unterzeichner als auch vom Verifizierer eines signierten Dokuments oder auch von einem Dritten geschaffen worden sein.

2.1 Allgemeine Anforderungen

Die grundsätzlichste Anforderung wurde schon erwähnt: Die vier Kontextkomponenten sollten einzeln vorhanden sein, damit sie zur Lösung des Kontextproblems verwendbar werden. Auf der technischen Ebene ist außerdem sicherzustellen, dass sie (als Web-Ressourcen) für Unterzeichner und Verifizierer verfügbar sind und dass die gegebene XML-Signaturanwendung sie auch verwendet (und nicht etwa durch eigene Komponenten ersetzt).

Um dies sicherzustellen und für den Empfänger des Dokuments auch sicher nachvollziehbar zu machen, ist wiederum eine eindeutige Bindung der Komponenten an das Dokument notwendig. Das bedeutet, dass mindestens mitunterzeichnete Verweise auf die entsprechenden Web-Ressourcen existieren müssen. XML-verarbeitende Anwendungen müssen (durch diese Verweise oder sonstwie) angewiesen werden, die bezeichneten Komponenten zu verwenden.

Dies ist für alle Anwendungen, die den entsprechenden XML-Standards des W3C genügen, prinzipiell in einheitlicher Weise möglich: Stylesheets und DTDs werden über sogenannte *Processing Instructions* (spezielle Tags, die keine Elemente darstellen) an Dokumente gebunden, Schemata können auf definierte Weise über das Attribut `schemaName` (entsprechend `xmlns:...` für Namensräume) einer Gruppe von Elementen zugewiesen werden. Die Bindung an bestimmte Kontext-Komponenten muss dabei freiwillig durch den Unterzeichner erfolgen, um der rechtlichen Anforderung der *Willenserklärungsfreiheit* Rechnung zu tragen. Ihre Auszeichnung dient dann der *Bestimmtheit* der Präsentation und die – für Menschen lesbare – Angabe eines Stylesheets trägt zu ihrer *Transparenz* bei.

Ist die Bindung der Komponenten an das Dokument vollzogen, können Schema und Stylesheet des jeweiligen Kontextes auf ihre gegenseitige Konsistenz überprüft werden: Tauchen etwa im Schema keine Elemente auf, die nicht auch über den Stylesheet dargestellt werden, so gibt dies einen Hinweis auf die *Vollständigkeit* der Darstellung. Umgekehrt sollte auch der Stylesheet nicht signifikant mehr Darstellungsbestandteile enthalten als es unterschiedliche Datenlemente im Schema gibt, um als darstellungstreu gelten zu dürfen. Treue und Vollständigkeit einer Darstellung – zusammengefasst im Gestaltungsziel der *Abgeschlossenheit* bezüglich der signierten Daten – sind dabei wesentliche Grundforderungen an jeden Präsentationskontext signierter Dokumente. Das bedeutet, dass der Signatur-Stylesheet die Darstellung der im Signaturschema definierten Datenstrukturen so detailliert wie möglich festlegen muss. Eine Konsistenzprüfung zwischen Stylesheet und Schema muss daher Teil einer Prüfung des XML-Kontextes im Hinblick auf die Beweiskraft der in ihm signierten Dokumente sein. Die XML-Komponenten bieten hier einen möglichen Ansatz zur teilweisen Automatisierung, auf jeden Fall aber eine (Beweis-) Erleichterung.

Als Beispiel für eine technische Forderung, die sich aus den obigen Punkten ableiten lässt, kann die durchgehende Verwendung dedizierter Namensräume für Signatur- und Anwendungskontext beziehungsweise die zugehörigen Schemata genannt werden. Insbesondere sollten im Dokument keine Elemente vorkommen, deren syntaktischer Kontext nicht durch einen Namensraum identifiziert wird – der sogenannte Default-Namensraum (Elementnamen ohne Präfix) sollte gemieden werden.

Eine weitere Forderung, die man sonst im Zusammenhang mit den Hoffnungen, die auf XML hinsichtlich Interoperabilität gesetzt werden, hört, ist, dass XML-Dokumente für Menschen leicht lesbar sein sollen. Zum Beispiel sollen die Namen von Elementen entsprechend ihrer Bedeutung in natürlicher Sprache gewählt werden. Diese Forderung, die das W3C explizit an alle Entwickler von XML-Anwendungen stellt, ist auch für signierte Dokumente relevant, denn es erleichtert enorm die rechtliche Würdigung der Kontext-Komponenten und der signierten XML-Dokumente selbst – zum Beispiel durch Sachverständige vor Gericht. Dieses leicht umsetzbare Gestaltungsziel für signierte XML-Dokumente unterstützt so die wichtige rechtliche Anforderung der *Fairness*: In einem Prozess sollen allen Beteiligten die Beweismittel leicht zugänglich sein.

Ein eklatantes Gegenbeispiel ist der Entwurf für die DIN-Norm 16557-4, die einen Standard für die Umsetzung von UN/EDIFACT-Daten in XML beschreibt. Er spiegelt die EDIFACT-Syntax eins zu eins in XML wieder und vergibt so die Möglichkeit, den Inhalt von XML-EDI Nachrichten auch für technische Laien verständlich und überprüfbar zu machen.

2.2 Zurechenbarkeit im Signaturkontext

Die Bindung eines signierten XML-Dokuments an die Komponenten des Signaturkontexts entspricht also der Bindung an ein digitales Signaturmedium, für dessen Funktion im Detail der Unterzeichner nicht

verantwortlich gemacht werden kann. Mit der eindeutigen Bezugnahme auf die Komponenten des Signaturkontextes kann man hier erreichen, was zu erreichen ist, nämlich die Zurechenbarkeit der Verwendung eines vertrauenswürdigen Signaturkontextes. Technisch kann dies heißen, dass Signaturschema und -Stylesheet gar nicht mitunterzeichnet, sondern nur im unterzeichneten Dokument eindeutig bezeichnet werden sollten, weil sonst ein falscher Anschein von Verantwortlichkeit (für das Signaturmedium, s. o.) entstünde.

Wodurch kann nun (rechtlich haltbares) Vertrauen in den XML-Signaturkontext geschaffen werden? Das oben vorgebrachte Argument spricht dafür, dass hier eine Standardisierung möglich und hilfreich ist. Die Trennung der Kontexte von Signatur und Anwendung verhindert, dass damit eine unbeabsichtigte, restriktive Vereinheitlichung der zu signierenden Inhalte und ihrer Darstellung verbunden wäre.

Andererseits muss – wenn jedermann darauf vertrauen soll – das Signaturmedium ein 'öffenliches Gut' sein. Wenn auch nicht jeder den Herstellungsprozess oder die chemische Zusammensetzung von Papier und Tinte geschweige denn die entsprechenden DIN-Normen kennt, so sind diese Informationen doch frei verfügbar. Dies spricht stark dafür, die XML-Komponenten des Signaturkontextes in offenen Standards durch Gremien ohne partikuläre Interessen definieren zu lassen. Für das Signaturschema kann dies die XML-Signatur-Arbeitsgruppe des W3C leisten.

Da das digitale Signaturmedium aber im Detail deutlich komplexer ist als das papierne sein kann, wird es nötig sein, die standardisierten Komponenten von Experten erstellen und evaluieren zu lassen. Geeignete, allgemein formulierte Ausgestaltungskriterien hierzu sind beispielsweise in [SigI_A3] vom BSI veröffentlicht worden. Sie können zugleich Hinweise für das Design zum Beispiel eines Signatur-Stylesheets sein. Diese Behörde besitzt auch die Autorität, die Evaluierung durchzuführen oder eine andere Prüfinstanz damit zu beauftragen und ihr (positives) Ergebnis durch ein digitales Zertifikat zu bestätigen. Das Zertifikat sollte zugleich wie üblich die Integrität der jeweiligen Komponente sichern (was zum Beispiel Wasserzeichen im Papier nicht in dieser Stärke leisten können).

Bei Erfüllung dieser Forderungen können XML-Signaturen ein Gutteil zur beweiskräftigen Zurechenbarkeit eines vertrauenswürdigen Signaturkontextes zum Unterzeichner beitragen. Im Signaturkontext lässt sich somit die in [Pordesch_99] aufgestellte Forderung einer *einfachen Standardpräsentation* für signierte Dokumente am leichtesten ausgestalten.

2.3 Zurechenbarkeit im Anwendungskontext

Beim Anwendungskontext stellt sich die Lage erheblich komplizierter dar, was wiederum an der Variationsbreite möglicher XML-Anwendungen liegt. Im Prinzip ist es natürlich denkbar, eine Normdarstellung für digital signierte XML-Daten festzuschreiben. Das würde aber auch die zulässigen Datenstrukturen signierbarer Dokumente erheblich einschränken, denn in ihnen dürfte nur enthalten sein, was dem Standard gemäß auch dargestellt wird. Eine solche Normdarstellung darf dann nicht so verstanden werden, dass sie die Darstellungsform aller zukünftigen signierten XML-Dokumente präjudiziert und ihnen *per se* geringeren Beweiswert zuspricht, wenn sie von der Norm abweichen.

Man sollte bedenken, dass die gesamte Informations- und Kommunikationstechnik im (Arbeits-) Alltag noch sehr jung ist und wir daher vermutlich nicht genügend Fantasie besitzen, uns alle künftigen Präsentationsformen digitaler Daten und alle möglichen Signaturanwendungen vorzustellen.

Das folgende Beispiel ist vielleicht nicht weit hergeholt: Ingenieure eines Zulieferers und eines Automobilherstellers verhandeln in einer CAVE über die Gestaltung eines Bauteils und wollen das erzielte Einverständnis durch eine digitale Signatur bestätigen. (Die Daten könnten hier zum Beispiel in einem XML-basierten Nachfolgestandard von VRML vorliegen). Für die genaue rechtliche Bewertung dieser Übereinkunft ist im Prinzip die gesamte virtuelle Realität, in der sie getroffen wurde, einzubeziehen und gegebenenfalls wiederherzustellen, wenn zum Beispiel geklärt werden soll, ob ein Detail für einen der Unterzeichner möglicherweise verdeckt oder anderweitig (etwa durch ungünstigen Lichteinfall) schlecht zu erkennen war.

Es fällt schwer zu glauben, dass die XML-Komponenten eines solchen Anwendungskontextes in eine detaillierte Norm passen könnten, die heute aufgestellt würde. Das heißt aber natürlich nicht von vorneherein, dass sie notwendig weniger vertrauenswürdige Darstellungen bieten.

Das Problem scheint nur zugänglich, indem man sich in kleinen Schritten von sehr allgemein formulierten Anforderungen zu konkreteren für spezielle Anwendungsbereiche bewegt. Es wäre dementsprechend nützlich, für verschiedene Anwendungsbereiche standardisierte Stylesheets bereitzustellen, die gegenüber der 'vollen Darstellung' eine vereinfachte, vollständige Präsentation bieten. Diese Standard-Stylesheets können dann wiederum evaluiert und zertifiziert werden. Ein solches schrittweises Vorgehen wurde auch in [Fox_98] implizit mit dem Vorschlag einer Registrierung von Object Identifiern (OID) für 'signierfähige' Datenformate beschrieben. Es ist wohl denkbar, dass Anwender ihre XML-Präsentationsformate in eine solche Liste von OIDs eintragen lassen. Man sollte, wenn man in dieser Richtung vorgehen will, aber einige Bedenken in Betracht ziehen:

Wie gezeigt führt XML als semantisch extrem variables und kontextabhängiges Datenformat eine solche Registrierung ad absurdum, wenn man sie einfach als Eintrag von 'XML' in die Liste von OIDs versteht. Dieser wäre so gut wie bedeutungslos und würde sogar mehr schaden als nutzen, da er technische Laien (also auch die meisten Rechtsexperten) in falscher Sicherheit wiegen könnte. Um eine Registrierung mit Inhalt zu füllen, kann sie nur für einzelne XML-Anwendung erfolgen. Und hier stellt sich erneut das Problem der Variabilität: Man würde auf diesem Weg möglicherweise zu einer eskalierenden Regulierung einzelner XML-Anwendungen geführt. Beginnt man aber in der Hoffnung, vollkommene Sicherheit erreichen zu können, die semantische Ausdrucksfähigkeit von XML-Dokumenten und die Vielfalt der Darstellungsmöglichkeiten durch Stylesheets über Gebühr einzuschränken, wäre dies kontraproduktiv: Die breite Anwendung von XML als Format für digital signierte Dokumente wäre erschwert und damit im Endeffekt auch die Akzeptanz von digitalen Signaturen im allgemeinen. Die Hoffnungen, die in Bezug auf Interoperabilität zu Recht in XML gesetzt werden, wären zumindest zum Teil enttäuscht.

Das führt zu dem Schluss, das man die Schemata und Stylesheets einzelner XML-Anwedungen zunächst evaluieren und zertifizieren (registrieren) müsste, bevor eine breite Anwenderschicht ihnen Vertrauen schenken kann, dass dabei aber zugleich nicht zu restriktiv verfahren werden sollte.

Auch hier scheint einiges für offene (Anwendungs-) Standards zu sprechen.

2.4 Ausblick

XML ist ein junger Standard. Viele zugehörige Anwendungsstandards befinden sich noch 'im Fluss', und es ist auch längst nicht alles, was schon spezifiziert ist, auch implementiert. Dementsprechend sind einige der oben angesprochenen Methoden heute noch hypothetisch. Dies gilt insbesondere für XML-Schemata, die Formatierungssprache von XSL und die Bindung von Schemata und Stylesheets an Dokumente und Namensräume (wobei nicht zu vergessen ist, dass jeweils zwei davon parallel benutzt werden, was heute noch schwierig ist). Im übrigen ist auch der XML-Signaturstandard noch nicht in direkt verwendbarem Zustand. Es kann aber aus dem derzeitigen Spezifikationsentwurf schon ersehen werden, dass er im Prinzip ausreichend flexibel sein wird, um zur Lösung des Kontextproblems beizutragen.

Ein grundlegender Vorteil von XML sollte hier nicht übersehen werden: In XML lässt sich im Prinzip Bedeutung auf *jeder* Ebene formulieren, nicht nur auf denen der Syntax und Darstellung, für die jetzt schon die Gestaltungsmittel verfügbar sind, sondern auch auf höheren. So kann man in Anwendungsstandards den Ablauf einer Benutzerinteraktion oder die Aufeinanderfolge von Nachrichten in einem Geschäftsprozess mit XML-Elementen explizit und 'signierbar' machen. Mit dem XML-Standard RDF (*Resource Description Format*) steht dazu ein generisches Instrument, mit dem man 'Aussagen über Dokumente' in XML formulieren kann, zur Verfügung.

Fazit

Das Kontextproblem ist das schwerwiegendste, dass der Beweiskraft digital signierter Dokumente im Wege steht. Man könnte deshalb ein skeptisches Fazit ziehen: Die rechtliche Beweiskraft digitaler Signaturen ist in Gefahr, durch das Präsentationsproblem erheblich eingeschränkt zu werden. Im Unterschied zum Papier mit seiner relativ hohen Darstellungstreue verbergen sich in jedem digitalen Signaturmedium und so auch in XML vielfältige Verfälschungsmöglichkeiten. Daraus ergeben sich ebenso vielfältige Möglichkeiten, die Verbindlichkeit eines digital signierten Dokuments abzustreiten. Digitale Signaturen könnten dadurch in einen generellen Ruf der Unsicherheit geraten.

Die Allgegenwart der Informationstechnik darf dabei ebenso wenig wie ihr technischer Entwicklungsstand mit rechtlicher Sicherheit verwechselt werden. Letztere kann sich erst in der (Rechts-) Praxis herausbilden. Ihr kann mit technischen Mitteln nicht vorgegriffen werden. Man sollte aber das Medium digitaler Signaturen stets im Vergleich zum klassischen Medium – dem Papier – bewerten. In diesem Vergleich schneidet das digitale Medium nicht schlecht ab, bietet es doch zum Beispiel in Bezug auf Fälschungssicherheit erheblich stärkere Mittel als Papier.

Die Variationsbreite digitaler Daten und ihrer Präsentation sollte ebenfalls als positive Eigenschaft verstanden werden, auch wenn sie im Signaturkontext zu Problemen führt, die technisch und rechtlich qualitativ neue Lösungen erfordern. Aus den Gesetzes- und Verordnungstexten wird klar, dass der deutsche Gesetzgeber keine konkreten Vorgaben zur Lösung des Kontextproblems machen wollte. Dies könnte in der Absicht geschehen sein, dass sich das neue Signaturmedium in der täglichen Anwendungs- und Rechtsprechungspraxis bewähren und auf diese Weise etablieren soll. Das ist, was mit 'Etablierung des digitalen Signaturmediums' gemeint ist: Die Technologie digitaler Signatur soll auf allen Ebenen so weiterentwickelt werden, dass ihre Alltagssicherheit als mit der Unterschrift auf Papier vergleichbar angesehen wird – von Laien, Richtern und der Öffentlichkeit insgesamt. Auf der juristischen Ebene ist damit die Forderung nach der *Verkehrsfähigkeit* digitaler (XML-) Signaturen verknüpft. Diese Forderung schließt die Verwendung proprietärer Signaturstandards praktisch aus und liefert damit ein weiteres Argument für den Einsatz offener Standards wie XML-Signaturen.

Die Aufgabe, die Wissenschaft und Technologie hierbei erfüllen können, ist, da vollständige *Beweisbarkeit* nicht erreichbar sein wird, die einer umfassenden Hilfestellung. Sie kann zur rechtlichen *Bewertbarkeit* digitaler Signaturen beitragen, indem sie das Kontextproblem analysiert, für Teilbereiche jeweils angemessene Lösungsvorschläge macht und insbesondere auch persistente Probleme, die einer technischen Lösung prinzipiell oder aus pragmatischen Gründen nicht zugänglich sind, nicht verschweigt. Zudem müssen zunächst einmal passende Begriffe gefunden werden, um die völlig neuartigen Probleme überhaupt formulieren zu können (wie zum Beispiel das der zurechenbaren Präsentation).[14]

XML und XML-Signaturen können ein Mittel sein, für die in Abschnitt 1 aufgeschlüsselten Komponenten des Signatur- und Anwendungskontextes Zurechenbarkeit zu ermöglichen. Außerdem ist, wie in Abschnitt 2 gezeigt, XML selbst ein geeignetes Medium, um Sicherheitskriterien explizit zu formulieren und zu erfüllen. XML kann also trotz und wegen seiner Flexibilität einen wesentlichen Beitrag zur Etablierung digitaler Signaturen leisten.

Literatur

[Aktionsprogramm] Bundesministerien für Bildung und Forschung sowie für Wirtschaft und Technologie: *Aktionsprogramm Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts*. September 1999.

[BMJ_99] Bundesministerium der Justiz: *Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr*. Stand 19. Mai 1999 (www.dud.de)

[Fox_98] Fox, Dirk: *Zu einem prinzipiellen Problem digitaler Signaturen*. DuD 7/98, S. 386-388.

[IuKDG-Bericht] *Bericht der Bundesregierung über die Erfahrungen und Entwicklungen bei bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des IuKDG*. 16. Juni 1999.

[Pordesch_99] Pordesch, Ulrich: *Nachweis der Präsentation signierter Daten*. GMD-Report 68, November 1999.

[Pordesch_00] Pordesch, Ulrich: *Der fehlende Nachweis der Präsentation signierter Daten*. DuD 2/2000, S. 89-95.

[Roßnagel_98] Roßnagel, Alexander: *Die Sicherheitsvermutung des Signaturgesetzes*. Neue Juristische Wochenschrift (NJW), 45/98, S. 3312-3320.

[SigI_A3] BSI: *Signatur-Interoperabilitätsspezifikation. Abschnitt A3: Anwenderinfrastruktur*, Stand 15. Juni 1999.

[XML-DSig] *XML Signature Core Syntax*. W3C Working Draft 20-October-1999. www.w3.org/Signature/Drafts/WD-xmldsig-core-20000128.

[14] Die Dimensionen dieser Aufgabe gehen wohl weit über das hinaus, was normalerweise bei der Konzeption kommerzieller Anwendungen in Betracht gezogen wird. Ich bin daher der Meinung, dass die Bedeutung digitaler Signaturen – zumindest nach den rechtlichen Vorgaben in Europa – mehr im öffentlichen Raum und bei wichtigen Rechtsgeschäften als bei einfachen kommerziellen Anwendungen liegt.