Grundkonzepte rechtssicherer Transformation signierter Dokumente*

Stefanie Fischer–Dieskau§
s.fischer-dieskau@uni-kassel.de

Thomas Kunz, Andreas U. Schmidt, Ursula Viebeg**
{Thomas.Kunz,Andreas.U.Schmidt,Ursula.Viebeg}@sit.fraunhofer.de

Abstract: Umwandlungen signierter Dokumente werfen Fragen auf, die für die Anwendung erhebliche Unsicherheiten begründen. Dieser Beitrag untersucht den Themenkomplex unter rechtlichen, technischen und organisatorischen Aspekten. Es werden Grundkonzepte sicherer Transformationen erläutert, die Transformation als Prozess analysiert und Lösungsansätze präsentiert.

1 Einleitung

Der Einsatz elektronischer Informations- und Kommunikationstechniken beherrscht immer stärker nicht nur die unternehmens-, justiz- oder verwaltungsinterne Bearbeitung von Geschäftsvorfällen, sondern auch den Rechts- und Geschäftsverkehr, das heißt die Kommunikation mit der Außenwelt. Das elektronische Dokument und die elektronische Akte lösen das Papier als Trägermedium aller Informationen ab. Durch den Austausch elektronischer Dokumente sollen elektronische Kommunikationsprozesse realisiert werden, die die Grenzen von Anwendungsbereichen, bestehender technischer Systeme und auch Staaten überwinden. Die Verwendung geeigneter elektronischer Signaturverfahren soll dabei nicht nur die Integrität und Authentizität der Daten nachvollziehbar machen, sondern auch Formerfordernisse erfüllen und zu einer Beweissicherheit führen.

Allerdings kann nicht unterstellt werden, dass auch in den nächsten Jahren oder gar Jahrzehnten alle Kommunikationspartner vollelektronisch arbeiten werden. Daher wird es auf nicht absehbare Zeit notwendig sein, Papierdokumente in elektronische und elektronische in Papierdokumente umzuwandeln. Eine Umwandlung ist jedoch auch erforderlich, wenn elektronische Dokumente von einem Format in ein anderes übertragen werden sollen. Dies kann sich dadurch ergeben, dass unterschiedliche Nutzdaten- und Signaturformate

*Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des *Bundesministerium für Wirtschaft und Arbeit* unter den Förderkennzeichen 01 MS 401 – 01 MS 405 im Rahmen des Projekts TransiDoc — Rechtssichere Transformation signierter Dokumente gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

§Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel

**Fraunhofer-Institut für sichere Informationstechnologie SIT, Dolivostrasse 15, 64293 Darmstadt

in den Anwendungen verwendet werden oder aber Technologieentwicklungen, wachsende Ansprüche an neue Medien oder geänderte Geschäftspolitiken der Softwarehersteller einen Formatwechsel bedingen. Es handelt sich hierbei um eine technisch bedingte Umwandlung eines Ausgangsdokuments in ein Zieldokument, unabhängig vom jeweiligen Trägermedium.

Umwandlungen können jedoch auch durch andere Gründe erforderlich sein. So sieht beispielsweise § 42 Abs. 3 BeurkG vor, dass Auszüge von umfassenden Dokumenten beglaubigt werden können. Ein anderes Beispiel ergibt sich aus der Verpflichtung zur Wahrung des Daten- sowie Geheimnisschutzes. Es kann erforderlich sein, Dokumente zum Beispiel zur Nutzung für Forschungszwecke zu anonymisieren oder aber schützenswerte Geheimnisse vor der Weitergabe der Dokumente unkenntlich zu machen. Die Bedeutung dieser Umwandlung wird insbesondere mit der Verabschiedung des Informationsfreiheitsgesetzes wachsen[1]. Danach wird die Verwaltung verpflichtet, Einsichtsrechte in die Unterlagen allen Bürgern zu gewähren. Allerdings hat sie dabei die informationelle Selbstbestimmung der Beteiligten, sowie deren Geheimnisse zu wahren. Eine Umwandlung wäre hierbei nicht technisch bedingt, sondern ergäbe sich aus dem Anwendungskontext.

In all diesen Fällen geht durch die Umwandlung des Ausgangsdokuments, sei es durch Scannen oder Ausdrucken oder durch reine Konvertierung der Daten, die bisherige technische Sicherung durch die Verkörperung und Unterschrift oder durch die elektronische Signatur verloren [Ro03]. Ob es dieser Sicherung bedarf, hängt von der jeweiligen Zielsetzung ab, die mit dem Dokument verfolgt wird. In den meisten Fällen wird dies allerdings zu bejahen sein. Unabhängig von dieser Fragestellung steht jedoch das Bedürfnis, dass eine entsprechend der Zielsetzung der Umwandlung verfolgte Übereinstimmung des Ziel- mit dem Ausgangsdokument erreicht wird. Daher ist es erforderlich, Instrumente vorzuhalten, die den Verlust der technischen Sicherung ausgleichen, um insbesondere den rechtlichen Wert des Dokuments, der durch die technische Sicherung gerade geschaffen wurde, auch für das Zieldokument zu wahren und die erforderliche inhaltliche Entsprechung sicherstellen.

Mit dem 3. Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften hat der Gesetzgeber eine erste diesbezügliche Regelung eingeführt. § 33 Abs. 4 Nr. 3 und 4 VwVfG sieht für die drei Formen der Umwandlung die Möglichkeit der amtlichen Beglaubigung vor. Dabei prüft der zuständige Bedienstete neben der Übereinstimmung des Ziel- mit dem Ursprungsdokument eine Signatur und erzeugt einen Beglaubigungsvermerk mit einzelnen Angaben aus den Signaturzertifikaten. Das transformierte elektronische Dokument und der Beglaubigungsvermerk sind im Anschluss von ihm elektronisch zu signieren oder das elektronische Dokument und der Beglaubigungsvermerk auszudrucken und handschriftlich zu unterschreiben.

Diese ersten gesetzlichen Regelungen sind jedoch in mehrerer Hinsicht noch nicht hinreichend spezifiziert [F-D03]: Es wird lediglich verlangt, dass die Zertifikatsdaten aufzuzeichnen sind. Die notwendige Unterscheidung in wichtige inhaltliche und unwichtige technische Daten fehlt. Wichtige Angaben, die nicht in Zertifikaten, sondern in den Signaturen enthalten sind, wie zum Beispiel Zeitstempeldaten, werden nicht berücksichtigt.

[1] Siehe zum derzeitigen Stand der Gesetzeslage www.informationsfreiheit.de

Der Umstand, dass die Ergebnisse der Signaturverifikation vom Zeitpunkt der Prüfung (beispielsweise Ablauf der Zertifikatsgültigkeit versus Ablauf der Algorithmeneignung) und der gewählten Prüfpolitik (zum Beispel Erfordernis bzw. Nicht-Erfordernis von Zeitstempeln) abhängen können, wird noch nicht bedacht. Die potenzielle Mehrdeutigkeit der Präsentation und Interpretation elektronischer Dokumente (etwa aktive Elemente, verborgene Texte, externe Dokumentvorlagen, *et cetera*) bleibt unberücksichtigt [Po00]. Anforderungen an die Überprüfung technischer Komponenten und technisch-organisatorischer Verfahren fehlen. Würden alleine auf dieser Basis transformierte Dokumente beglaubigt, so wäre zu erwarten, dass in Gerichtsprozessen zahlreiche berechtigte Einwände gegen so beglaubigte Dokumente vorgebracht werden.

Eine von der Zielsetzung her vergleichbare Regelung zur amtlichen Beglaubigung soll durch das derzeit als Kabinettsentwurf vorliegende Justizkommunikationsgesetz für Notare eingeführt werden. Nach §§ 39a, 42 Abs. 4 BeurkG-E sollen auch Notare als originär für Beglaubigungen zuständige Rechtspflegeorgane transformierte Dokumente beglaubigen können; detaillierte Vorgaben, die in den Beglaubigungsvermerk aufzunehmen sind, sind aber nicht vorgesehen.

Sowohl die amtliche wie auch die öffentliche Beglaubigung sind von ihrer Funktion her auf eine persönliche Beglaubigung ausgelegt, weil jedes Dokument vom Zuständigen einzeln geprüft und beglaubigt werden muss. Aus diesem Grunde ist das Instrument der Beglaubigung zwar geeignet, dem transformierten Dokument grundsätzlich ein dem Ursprungsdokument vergleichbaren rechtlichen Wert zukommen zu lassen, allerdings ist sie für das Massenverfahren untauglich. Somit gilt es, ein Instrument zu entwickeln, dass einerseits rechtliche Anforderungen erfüllen kann, andererseits aber auch massentauglich ist. Das Ziel sollte es dabei sein, Konzepte zu entwickeln, die lediglich in ihrer technischen Umsetzung in Abhängigkeit zur jeweiligen Form der Umwandlung differieren, im Übrigen jedoch allen Formen zugrunde gelegt werden können und auch anwendungsunabhängig einsetzbar sind.

2 Sichere Dokumenttransformationen

Viele Anwendungskontexte, insbesondere auch der rechtliche, besitzen eigene, starke Systeme vorbelegter Begriffe, aus denen sich Bewertungskriterien für Transformationen ergeben können. In einem allgemeinen Grundkonzept für sichere Transformationen sind diese Begriffe zu meiden. Andererseits variieren die Eigenschaften, die eine Dokumenttransformation und ihre Ergebnisse haben müssen, um den intendierten Zweck zu erfüllen, von Bereich zu Bereich und in jedem Bereich von Anwendung zu Anwendung stark. Eine Transformation mag zum Beispiel aus Gründen des Datenschutzes oder der Geheimhaltung durchgeführt werden. Ebenso kann das Ergebnis der Transformation etwa nach Gesichtspunkten des monetären oder ideellen Wertes eines Dokuments (und dessen Erhaltung) beurteilt werden.

Der Anwendungskontext bestimmt letztlich auch, was im konkreten Fall unter „Sicherheit“ zu verstehen ist, weshalb auch dieser Begriff sehr verschieden aufgefasst werden

kann. Die im vorigen Abschnitt beschriebenen rechtlichen Aspekte stellen eine besonders wichtige Ausprägung von Sicherheit dar, da rechtliche Regelungen die meisten Bereiche des Zusammenlebens betreffen.

Es ist also notwendig, ein eigenes begriffliches Grundgerüst für „sichere Transformationen“ aufzubauen, das von den Anwendungsbereichen unabhängig, aber gleichzeitig flexibel genug ist, damit sich unter seinem Dach die verschiedenen Anwendungsbereiche einpassen können. Hierfür ist ein gewisser Abstraktionsgrad unerlässlich. Ein zweites Ziel des hier vorgestellten Konzepts der sicheren Transformationen ist es, die Schnittstelle zwischen dem „realweltlichen“ Kontext, in dem Dokumente letztlich von Menschen interpretiert und ihrer Bedeutung nach bewertet werden und dem formal fassbaren Prozess einer sicheren Transformation, der letztlich einer technischen Lösung zugeführt werden soll, möglichst genau herauszuarbeiten. Dies zeigt die Grenze für die Formalisierbarkeit der angestrebten Sicherheitseigenschaften und der Automatisierbarkeit ihrer Umsetzung auf.

Unter einer **Transformation**[2] wird die Umwandlung eines Ausgangsdokuments mit einer bestimmten Bedeutung in ein Zieldokument mit einer gewünschten Bedeutung verstanden. Die **Bedeutung** eines Dokuments wird pragmatisch durch dessen Verwendungsmöglichkeiten bestimmt, also die Zuschreibungen möglicher Verwendungen zum Dokument, die sich in einem gegebenen Kontext auch wirklich umsetzen lassen (mit anderen Worten: Zutreffende Interpretationen der Gültigkeit). Im Prinzip kann das Zieldokument den gleichen, geringeren oder umfassenderen Bedeutungsumfang als das Ausgangsdokument haben, jedoch ist abgesehen von diesen drei grundlegenden Fällen im Allgemeinen der Bedeutungsumfang von Ausgangs- und Zieldokument nicht direkt vergleichbar. Der **Zweck** einer Transformation ist, ein Zieldokument mit einer bestimmten Bedeutung zu erhalten. Diese Bedeutung des Zieldokuments wird dabei stets von der des Ausgangsdokuments abhängen, insbesondere dadurch, dass das Ausgangsdokument die möglichen Verwendungen des Zieldokuments einschränkt. An dieser Stelle wird noch nicht zwischen Inhalt und Signatur/Unterschrift differenziert. Beides gilt gleichermaßen als Inhalt, der bedeutungstragend, zweckdienlich und zweckbestimmend sein kann. Die drei grundlegenden Fälle gleichen, geringeren und größeren Bedeutungsumfangs entsprechen ebenso grundlegenden Zwecken:

- Ist der Zweck einer Transformation, das Ausgangsdokument komplett durch ein **Ersatzdokument** zu ersetzen, muss das Zieldokument eine so weit als möglich identische Bedeutung haben wie das Ausgangsdokument. ***Beispiel:*** Beglaubigte Kopien von Papierdokumenten[3]; P→E Transformationen zur elektronischen Weiterbearbeitung; Die Sicherung der Lesbarkeit eines Dokuments für den Adressaten erfordert häufig Änderungen von Dokumentformaten, zum Beispiel bei der Einreichung eines Antrages bei einer Behörde.

- Ist eine **Teilkopie** des Ausgangsdokuments zu erstellen, wobei die Verwendbarkeit

[2] Dieser Begriff umfasst sowohl die Umwandlung von elektronischen in elektronische (E→E), als auch solche, die Papierdokumente involvieren (P→E und E→P).

[3] Bei E→E Transformationen macht eine identische Kopie eines signierten Dokuments als Transformation keinen Sinn, weil die Kopie verlustfrei erfolgt und sich die Frage des Erhalts der Gültigkeit der enthaltenen Signaturen nicht stellt. Ersatzdokumente werden also bei E→E Transformationen nicht schlichte Kopien sein, sondern Änderungen gegenüber dem Original aufweisen.

des Zieldokuments auf bestimmte Bereiche eingeschränkt sein kann, so ist der Bedeutungsumfang des Zieldokuments im Allgemeinen geringer als der des Ausgangsdokuments. ***Beispiele:*** Auszüge aus amtlichen Registern für bestimmte Verwendungszwecke; Entpersonalisierte Fassung aus Datenschutzgründen, zum Beispiel im Medizinbereich die Anonymisierung von Patientenakten zur Weiterverwendung für wissenschaftliche Studien, wobei die Zurechenbarkeit des Dokuments zu einem Arzt (Signatur) erhalten bleiben soll.

- In bestimmten Fällen kann eine **Aufwertung** eines Dokumentes erfolgen, also die Bedeutung des Zieldokuments größer sein als die des Ausgangsdokuments. Es wird hier aber nur der Fall betrachtet, dass keine bedeutungstragenden Inhalte hinzugefügt werden (s.u.), das heißt weitere semantische Informationen, die im gewählten Anwendungskontext eigene Bedeutungen haben. ***Beispiele:*** Ein einfaches aber praktisch relevantes Beispiel ist die Migration eines Datensatzes auf ein neues Format durch Hinzufügung eines leeren, für spätere Verwendungen vorgesehenen Feldes; wird ein Zeichensatz oder ein anderes Druckformat gewählt, so kann ein Dokument beispielsweise auch Sehbehinderten zugänglich gemacht werden.

Der Begriff der Transformation ist hier noch zu allgemein. So würden zum Beispiel auch Vorgänge, bei denen Inhalte hinzugefügt, mehrere Dokumente zusammengefasst oder in komplizierten Bearbeitungsschritten ein neues Dokument erstellt wird, darunter fallen. Solche Vorgänge, die zum Beispiel verwaltungsrechtlich gesehen als *Vorgangsbearbeitung* gelten und informationstechnisch durch Workflow-Systeme abgedeckt werden, sollen hier nicht betrachtet werden. Eine Bedeutungserhöhung, die durch ein Anfügen oder Ergänzen von Inhalten oder Signaturen erreicht wird, wird daher nicht als Transformation angesehen.

Beispiele: Eine weitere Unterschrift einer Akte im Umlauf. Ausfertigung eines Gerichtsurteils zur Vollstreckung - der Vermerk, der das Urteil vollstreckbar macht, ist eine inhaltliche Ergänzung, der außerdem noch eine weitere Signatur trägt.

Um einem Zweck zu entsprechen, muss eine Transformation gewisse Eigenschaften haben, die mit dem Begriff **Inhaltstreue** zusammengefasst werden. Dies ist hier zu verstehen als „Inhalte dem Zweck getreu umwandeln“, kann also im Einzelfall eine gezielte, das heißt dem Zweck entsprechende „Untreue“ beinhalten. Inhaltstreue bezieht sich auf die Eigenschaften aller für die Transformation relevanten Bestandteile des Ausgangs- und Zieldokuments einschließlich der Signaturen. Charakteristisch für die Unterscheidung der Inhaltstreue von dem nicht gut formal fassbaren — weil im realen Kontext liegenden — Bedeutungsübergang zwischen Ausgangs- und Zieldokument, ist die *Überprüfbarkeit* der Eigenschaften, die sie ausmachen, anhand des Ausgangsdokuments und Zieldokuments sowie der durchgeführten Transformation selbst. Diese Eigenschaften bestimmen den Grad der Inhaltstreue. Was genau zu seiner Feststellung geprüft werden *muss*, richtet sich im Einzelfall stark nach dem Zweck der Transformation. Was geprüft werden *kann*, richtet sich aber auch nach den tatsächlich vorliegenden Ausgangs- und Zieldokumenten.

Beispiele: Inhaltstreue kann auf unterschiedlichen Ebenen bewertet werden. Es kann reichen, die Auflösung und Farbtiefe eines Scanners festzuhalten, aber auch nötig sein, Dokumente auf Buchstabenebene zu vergleichen. Gegebenenfalls ist die Eignung des Ausgangs-

formats für die Transformation zu prüfen, zum Beispiel ein Papierdokument auf hinreichende Druckqualität. Auch inhaltliche Eigenschaften können relevant werden, beispielsweise eine Kontrolle, dass der Transformationsalgorithmus die Namen von Personen im Dokument tatsächlich alle entfernt hat. Wesentlich für die Inhaltstreue kann insbesondere bei E→E, aber auch bei P→E Transformationen sein, ob die Formate von Ausgangs- und Zieldokument geeignet sind, alle signierten Daten richtig darzustellen. Zur Überprüfung der Inhaltstreue sind daher geeignete Viewer zu verwenden, um das bekannte Darstellungsproblem digital signierter Dokumente in angemessener Weise zu berücksichtigen, vgl. [Po00, Sc00].

Ohne geeignete Sicherheitsmaßnahmen besteht im Nachhinein keine Möglichkeit festzustellen, ob die angestrebte Inhaltstreue wirklich erreicht wurde. Eine **sichere Transformation** liegt dann vor, wenn das Zieldokument die durch den Zweck der Transformation bestimmte Art der Inhaltstreue zum Ausgangsdokument aufweist und dies in einer vertrauenswürdigen Form vermerkt wurde. **Vertrauenswürdigkeit** bedeutet hier, dass nachträglich überprüfbar ist, was für eine Transformation durchgeführt wurde, dass die Inhaltstreue geprüft und bewertet wurde und wer diese Prüfung durchgeführt hat und für ihr Ergebnis verantwortlich zeichnet. Die *a posteriori* Nachvollziehbarkeit, die entscheidend für die Sicherheit der Transformation ist, stellt insbesondere an einem Punkt hohe Anforderungen an die Vertrauenswürdigkeit: Das Zieldokument muss in vielen, wenn nicht den meisten Fällen, die gewünschten Bedeutungen erreichen, *selbst wenn das Ausgangsdokument nicht mehr vorliegt.*

Verschiedene Instanzen können die Vertrauenswürdigkeit einer Transformation im Transformationsprozess bewerten und an seinem Ende garantieren. In einem Massenverfahren bestätigt das Transformationssystem selbst, dass ein bestimmter Algorithmus angewandt und im Dokument enthaltene Signaturen positiv überprüft wurden. Bei Beglaubigungen ist es hingegen nötig, dass eine autorisierte Person, etwa ein Notar, Inhaltstreue prüft und Vertrauenswürdigkeit durch Vermerk des Prüfergebnisses herstellt und durch seine Signatur verantwortet.

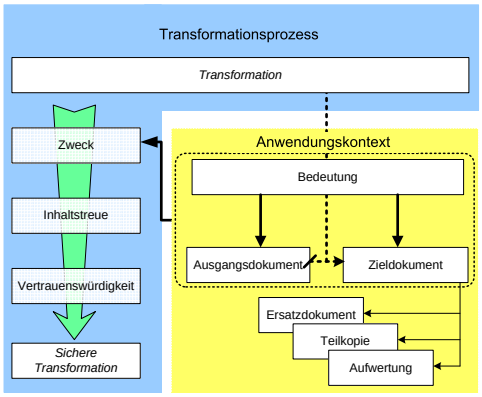

Abbildung 1: Grundbegriffe sicherer Transformationen

Abbildung 1 zeigt die Grundbausteine des Begriffssystems für sichere Transformationen

und ist so zu verstehen: Eine sichere Transformation wird gewährleistet durch die Vertrauenswürdigkeit der Inhaltstreue für einen bestimmten Zweck. Der Zweck ist die Transformation eines Ausgangsdokuments mit einer bestimmten Bedeutung in ein Zieldokument mit einer bestimmten Bedeutung. Ein Kernergebnis, das sich hieraus ableiten lässt ist, dass Anwendungskontext und Transformationsprozess an genau einer Stelle verknüpft sind: Die Festlegung des Zwecks einer Transformation durch den angestrebten Bedeutungsübergang. Hier liegen, wie im Folgenden erkennbar werden wird, die Hauptschwierigkeiten für die Formalisierung und praktische Realisierung sicherer Transformationen.

3 Rechtssicherheit transformierter Dokumente

Dokumente werden stets zu einem oder mehreren Zwecken erstellt. Unabhängig vom konkreten Zweck ihrer Entstehung dienen Dokumente stets zum Nachweis eines bestimmten Handelns oder Unterlassens oder eines Handlungsverlaufs. Die Beweissicherung ist dabei nicht allein prozessrechtlich zu verstehen, sondern umfasst ebenso die Möglichkeit des Nachvollziehenkönnens, das heißt für sich selbst oder für Dritte zum Beispiel ein bestimmtes Vorgehen, ein Handeln, eine Vereinbarung oder aber auch eine Bestandsaufnahme durch ein Foto für ein zukünftiges Ereignis transparent zu machen. Das Dokument wird jedoch nur dann als geeignet zum Nachweis herangezogen werden, wenn eine Sicherheit darüber besteht, dass das Dokument authentisch ist, es sich um das ursprünglich erstellte Dokument handelt, es „echt“ ist.

Insbesondere wenn dem Dokument eine rechtlich relevante Bedeutung zukommt bzw. zukommen kann, steht die Sicherung der Echtheit grundsätzlich in Abhängigkeit zu dieser Bedeutung. Der Einsatz bestimmter technischer Sicherungen wie qualifizierte elektronische Signaturen oder Papier und Unterschrift dienen nicht nur dazu, gesetzliche oder vereinbarte Schriftformerfordernisse zum Beispiel gemäß § 126 BGB oder § 3a Abs. 2 VwVfG zu erfüllen, sondern insbesondere erlaubt ihr Einsatz durch beweisrechtliche Privilegierungen eine vereinfachte Ermittlung der Echtheit. Erreicht wird letztere durch die Beweisregeln für Urkunden und den Anscheinsbeweis des § 292a ZPO für qualifiziert signierte Dokumente. Gerechtfertigt sind diese Privilegierungen durch die Anforderungen, die an die technischen Sicherungen gestellt werden. Das Trägermedium Papier und die Unterschrift als biometrisches Merkmal erlauben, im Regelfall mit großer Sicherheit, Fälschungen erkennen zu können. Bei qualifiziert signierten Dokumenten kann aufgrund der hohen technisch-organisatorischen Sicherheitsanforderungen an ihre Erstellung die Echtheit festgestellt werden. Damit stehen Gestaltungsmittel zur Verfügung, deren Verwendung den Dokumenten eine hohe formelle Beweiskraft geben und dadurch eine Beweissicherheit schaffen.

Die Beweissicherheit ist dabei wesentliches Kriterium der Rechtssicherheit. Letztere beinhaltet das Gebot, dass Unsicherheiten bei der Anwendung des Rechts vermieden werden müssen. Daraus ergibt sich, dass jeder erkennen können muss, welche Rechtsnormen von ihm zu beachten sind und was von ihm verlangt wird, damit er sich danach richten und sicher sein kann, nicht versehentlich das Recht zu verletzen [SG00]. Die Vorhersehbarkeit spielt daher eine wesentliche Rolle. Übertragen auf das hier vorliegende Problem bedeutet

dies, dass es für den Anwender vorhersehbar sein muss, wie seine Rechtsstellung ist, wenn ein Dokument transformiert wird. Sein Ziel wird es grundsätzlich sein, dass die Beweissicherheit bestehen bleibt.

Führt eine Transformation nun dazu, dass die Sicherung verloren geht, ist zu fragen, wie die Beweissicherheit erhalten bleiben kann. Denn gelingt das, besteht auch mit dem transformierten Dokument eine Rechtssicherheit, da die erforderliche Vorhersehbarkeit gegeben ist. Grundsätzlich ergibt sich die Beweissicherheit als Kriterium der Rechtssicherheit durch das Ergebnis, also durch das Dokument. Allerdings muss diesem Ergebnis ein Verfahren zugrunde liegen, dass diese Zuordnung der Eigenschaft rechtfertigt. Rechtliche Anforderungen sind daher an dieses Verfahren zu stellen, um zu gewährleisten, dass das Ersatzdokument die rechtlich bedeutsamen Eigenschaften des Ausgangsdokumentes aufweisen kann. Handelt es sich, wie hier zu entwickeln, um ein vorwiegend technisches Verfahren, dürfen somit nicht beliebige Formatkonverter eingesetzt werden, Prüfergebnisse entsprechend einem gerade zur Verfügung stehenden Prüfprogramm aufgezeichnet und Dokument und Prüfergebnisse durch eine gewöhnliche Signatur ergänzt werden. Notwendig sind vielmehr spezielle Transformationsverfahren, die rechtliche Anforderungen durch geeignete technische und organisatorische Maßnahmen erfüllen.

4 Transformation als Prozess

Eine sichere Transformation zeichnet sich dadurch aus, dass sie einen bestimmten Zweck erfüllt, sowie nachträglich überprüfbar und vertrauenswürdig ist. Hierzu muss feststellbar sein, welche Transformation durchgeführt wurde, dass die dem Zweck der Transformation entsprechende Inhaltstreue überprüft wurde und wer diese Prüfung durchgeführt und das Prüfungsergebnis erstellt hat. Um diese Anforderungen zu erfüllen, genügt es nicht, lediglich die Inhalte des Ausgangsdokuments in ein Zielformat zu konvertieren. Es sind zusätzliche Schritte und Vorkehrungen erforderlich, die über die reine (Format-) Konvertierung von Daten hinausgehen. Dieser Prozess einer sicheren Transformation ist in einzelne, sequentiell zu durchlaufende **Transformationsphasen** zu unterteilen, die diese Schritte widerspiegeln. Im Folgenden werden die einzelnen Phasen einer sicheren Transformation unabhängig von der Art der Transformation (P→E, E→E oder E→P) auf eine generische Weise näher beschrieben. Die Reihenfolge, in der die Phasen beschrieben werden, entspricht im Prinzip ihrer Ausführung, kann jedoch in manchen Anwendungsfällen modifiziert werden (z.B. durch Wegfallen einzelner Phasen). In Abbildung 2 stellt den Prozess schematisch dar.

Zu Beginn des Transformationsprozesses müssen die überprüfbaren Eigenschaften von Ausgangsdokument, Zieldokument und der Transformation selbst, die die Inhaltstreue ausmachen, festgelegt werden. Dies geschieht in der ersten Phase einer sicheren Transformation, der **Klassifikationsphase**. Hier wird nicht nur bestimmt, welche Eigenschaften des Ausgangsdokuments für die zur erzielende Inhaltstreue mit dem Zieldokument herangezogen werden, sondern auch, wie die Inhaltstreue im Transformationsprozess erreicht, geprüft und vertrauenswürdig bestätigt werden soll.

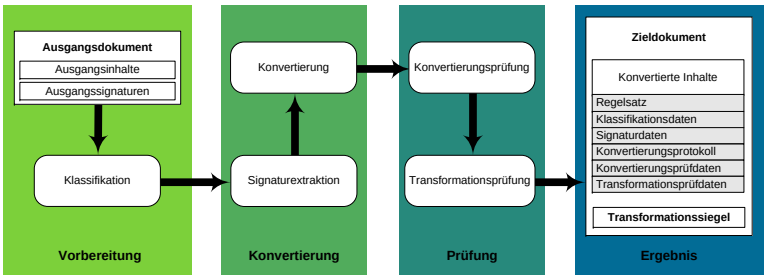

Abbildung 2: Phasen einer sicheren Transformation

Beispiel: Handelt es sich bei dem Ausgangsdokument um eine Bauzeichnung und ist der Zweck der Transformation die Erstellung eines Ersatzdokuments, so gehört beispielsweise der Erhalt der Farben und der Größenverhältnisse zu den Eigenschaften, die zur Inhaltstreue und deren Prüfung herangezogen werden müssen. Die Inhaltstreue und deren Überprüfbarkeit sollen dabei durch die Qualität der verwendeten Geräte und Softwarekomponenten, sowie den daran vorgenommenen Einstellungen garantiert werden. Eine Bestätigung, dass die geforderte Inhaltstreue geprüft und festgestellt wurde, soll durch eine elektronische Signatur einer autorisierten Person zu der gewünschten Vertrauenswürdigkeit des Transformationsprozesses führen.

Die Klassifikation des Ausgangsdokuments und der Zweck der Transformation bestimmen somit die Vorgehensweise im Transformationsprozess. Darauf basierend wird ein **Regelsatz** zusammengestellt, dessen Regeln im gesamten anschließenden Transformationsprozess eingehalten werden müssen. Die Einhaltung des Regelsatzes stellt sicher, dass die angestrebte Vertrauenswürdigkeit der Transformation erreicht wird. Um den Verlauf der Transformation nachvollziehbar und überprüfbar zu gestalten, entsteht während des Transformationsprozesses sukzessive eine so genannte **Transformationsakte**, bestehend aus Metadaten, die in den einzelnen Transformationsphasen erzeugt werden. Der Regelsatz stellt einen der Bestandteile der Transformationsakte dar.

Klassifikation. In dieser Phase wird das Ausgangsdokument klassifiziert, das heißt seine Bedeutung, wie etwa „technische Zeichnung“ oder „Word-Dokument“ wird dem Zweck der Transformation entsprechend möglichst genau ermittelt. Dies kann zum Beispiel per Augenschein anhand von äußeren Merkmalen, wie dem Titel oder dem Typ des Dokuments, oder voll automatisiert anhand eines zugeordneten XML-Schemas erfolgen. Das Klassifikationsergebnis und der Zweck der Transformation bestimmen das Vorgehen im Transformationsprozess. Es wird festgelegt,

- welche Eigenschaften und Bestandteile des Ausgangsdokuments für die zu erzielende Inhaltstreue mit dem Zieldokument herangezogen werden müssen,
- wie die Inhaltstreue erreicht und geprüft werden soll,
- wie die Inhaltstreueprüfung und deren Ergebnis vertrauenswürdig vermerkt und bestätigt werden sollen.

In der Klassifikationsphase muss insbesondere bestimmt werden, inwieweit das Ausgangsdokument und sein Format für eine sichere Transformation geeignet ist und welche Maßnamen beispielsweise zur Vermeidung von Mehrdeutigkeiten (Präsentationsproblem) ergriffen werden müssen. Liegt das Ausgangsdokument in einem Format vor, das auf verschiedene Arten darstellbar ist, so besteht die Unsicherheit, welche Variante signiert, das heißt dem Signierer präsentiert wurde. Zudem ist zu berücksichtigen, wie mit Randnotizen, Streichungen, Korrekturen im Text oder ähnlichem umgegangen werden soll. In solchen Fällen müssen entsprechende Maßnahmen vorgesehen werden, wie etwa dass bestimmte Dokumente nur unter bestimmten Voraussetzungen automatisiert transformiert werden dürfen, oder dass Personen in den Transformationsprozess einzubeziehen sind. Anhand dieser Anforderungen werden Regeln ausgewählt und bestimmt, nach denen in den folgenden Transformationsphasen vorgegangen werden muss, um eine sichere Transformation zu gewährleisten. Diese Regeln werden zu einem Regelsatz zusammengefasst und liegen in allen Phasen der sicheren Transformation vor. Falls es der Regelsatz erfordert, können bereits in dieser Phase entsprechende Prüfungen des Ausgangsdokuments durchgeführt werden, die beispielsweise die Prüfung der Einhaltung von geltenden Formvorschriften, wie das Schriftlichkeitsgebot oder die Existenz einer Signatur, umfassen können. Das Ergebnis der Prüfungen bildet zusammen mit der Klassifizierung des Dokuments und dem Zweck der Transformation die so genannten Klassifikationsdaten, die mit dem Regelsatz der Transformationsakte hinzugefügt werden.

Signaturextraktion. Während der Signaturextraktion werden den Signaturen des Ausgangsdokuments Informationen entnommen und für die Transformationsakte als Signaturdaten zusammengestellt. Bei diesen Signaturen, im Folgenden kurz „Ausgangs-signaturen“ genannt, kann es sich im Falle von Papierdokumenten um handschriftliche Unterschriften handeln oder aber auch um elektronische Signaturen.

Der in der Klassifikationsphase erzeugte Regelsatz bestimmt, ob und wie die Ausgangssignaturen geprüft werden sollen und welche Signaturdaten für das Zieldokument relevant sind. Sollen die Ausgangssignaturen geprüft werden, legt der Regelsatz die zu prüfenden Eigenschaften und die Prüftiefe fest. Beispielsweise könnte der Regelsatz fordern, dass das Ausgangsdokument mehrere Signaturen oder eine notarielle Beglaubigung enthält. Im Falle eines elektronischen Dokuments könnte der Regelsatz die Validierungs-Policy vorgeben. Das Prüfergebnis wird ebenfalls in der Transformationsakte festgehalten.

Konvertierung. In der dritten Phase wird die eigentliche Konvertierung der Inhalte des Ausgangsdokuments in das Zielformat vorgenommen. Die Regeln zur Einstellung oder Auswahl der Konvertierungsmethode und zugehöriger Parameter, wie etwa Farbtiefen und die Auflösung, werden durch den Regelsatz bestimmt. Es wird ein Konvertierungsprotokoll erstellt, das den Verlauf der Konvertierung wiedergibt und in der Transformationsakte abgelegt wird.

Konvertierungsprüfung. In dieser Phase wird die Korrektheit der zuvor durchgeführten Konvertierung überprüft. Hierzu werden die Inhalte des Ausgangsdokuments mit den konvertierten Inhalten verglichen. Regeln zur Feststellung der Inhaltstreue, wie zum Beispiel Anforderungen an Systeme zur Darstellung der Inhalte der Ausgangsdokumente und der konvertierten Inhalten sowie an Vorgehensvorschriften bei der Prüfung werden durch den Regelsatz festgelegt. Falls es der Regelsatz vorsieht, wird nach erfolgreicher Prüfung der

Konvertierung das Ausgangsdokument aus dem weiteren Transformationsprozess entfernt.

Transformationsprüfung. In der letzten Phase des Transformationsprozesses werden die Ergebnisse der vorangegangenen Transformationsphasen überprüft. Der Regelsatz definiert die vorzunehmenden Prüfungen und die dabei einzuhaltenden Regeln und Vorgehensweisen. Hierzu könnte beispielsweise die Feststellung gehören, ob alle erforderlichen Phasen der Transformation durchlaufen wurden, oder die Prüfung der konvertierten Inhalte auf die Formvorschriften, die für die angestrebte Bedeutung des Zieldokuments notwendig sind. Schließlich wird dem Regelsatz entnommen, wie die Prüfergebnisse vertrauenswürdig vermerkt und bestätigt werden sollen.

Im Transformationsprozess werden Daten verarbeitet, erzeugt und an folgende Transformationsphasen weitergegeben. Eine Manipulation dieser Daten könnte zur Folge haben, dass dem Zieldokument eine Bedeutung zukommt, die nicht beabsichtigt ist. Dies wiederum könnte zu Verlust oder Manipulation von Informationen und Betrug führen. In einer sicheren Transformation müssen daher die Integrität, Authentizität und richtige Zuordnung der Daten zueinander gewährleistet sein. Beispielsweise muss in allen Phasen derselbe Regelsatz vorliegen und angewandt werden.

5 Lösungsansatz „Transformationssiegel“

In Abschnitt 2 wurde festgestellt, dass das Endergebnis einer Transformation häufig auch dann sicher sein muss, wenn das Originaldokument nicht mehr zum Vergleich herangezogen werden kann. Dies führt zu der Notwendigkeit, die während des oben beschriebenen Transformationsprozesses aufgezeichneten relevanten Daten in vertrauenswürdiger Form festzuhalten. Als grundlegendes Ergebnis einer sicheren Transformation sollte dazu am Ende des Transformationsprozesses ein **„Transformationssiegel“**[4] erzeugt werden. Dieses „Transformationssiegel“ muss die geforderte Vertrauenswürdigkeit auch dann garantieren, wenn das Ausgangsdokument nicht mehr vorliegt. Mit ihm wird bestätigt, dass der Ablauf des Transformationsprozesses geprüft und als korrekt angesehen wird und dass die mit der Transformation angestrebte Inhaltstreue zwischen Ausgangsdokument und Zieldokument erreicht ist. Dazu muss die während der Transformation erstellte Transformationsakte kryptografisch gesichert werden, damit der Ablauf der Transformation nachträglich feststellbar und überprüfbar wird. Die Vertrauenswürdigkeit der Prüfergebnisse wird durch deren Zurechenbarkeit erreicht, das heißt es ist nachprüfbar festzuhalten, wer die Prüfung durchgeführt hat. Schließlich muss das „Transformationssiegel“ in eindeutiger und unverfälschbarer Weise an das Zieldokument gebunden werden.

Technisch gesehen könnte das „Transformationssiegel“ als Datencontainer realisiert werden, der die Transformationsakte und das Zieldokument (oder einen eindeutigen Verweis darauf, zusammen mit einem Hashwert) umfasst und durch eine elektronische Signatur dem Transformationsprüfer zurechenbar gemacht wird.

[4] „Siegel“ ist natürlich nicht dahingehend zu verstehen, dass sein Bruch zu einem Siegelbruch im Sinne des § 136 Abs. 2 StGB führt.

6 Ausblick

Die Ausgestaltung rechtssicherer Transformationen stellt, wie die obige Analyse zeigt, eine Herausforderung dar. Ihre Bewältigung erfordert eine interdisziplinäre Herangehensweise, die organisatorische Maßnahmen mit technischen Lösungen vereint, um im konkreten Anwendungsfall die jeweiligen rechtlichen Anforderungen zu erfüllen. Im Einzelfall ist zu fragen, ob bestehende rechtliche Regelungen ausreichen oder insoweit angepasst werden müssen, damit eine rechtssichere Transformation erst ermöglicht wird. Das Projekt TransiDoc stellt sich diesen Herausforderungen und entwickelt auf Grundlage der hier dargestellten Konzepte konkrete Lösungen für ein breites Anwendungsspektrum. Dazu gehören ein Katalog von Handlungsanweisungen, Vorgehensbeschreibungen und technischen Vorgaben ebenso wie generische Software-Komponenten für die Durchführung des Transformationsprozesses und der Erzeugung des „Transformationssiegels“.

Ein Kernpunkt der Forschung ist die Ausgestaltung der Regelsätze für sichere Transformationen. Hier sind insbesondere die Grenzen der Automatisierbarkeit zu berücksichtigen: Aufgaben, die ein Transformationssystem nicht selbst in sicherer Weise durchführen kann, müssen in kontrollierter Weise auf menschliche Eingriffe und Kontrollen zurückverwiesen werden. Dazu müssen Regelsätze entsprechende Regeln enthalten, die vom Transformationssystem ergonomisch umzusetzen sind.

Neben der Sicherung der Langzeitaufbewahrung elektronisch signierter Dokumente[5] ist die Lösung der Frage ihrer rechtssicheren Transformation notwendige Grundlage für Systemgrenzen überschreitenden elektronischen Rechts- und Geschäftsverkehr. Die Brisanz dieser Problematik wurde anscheinend in Wissenschaft und Anwendung bisher kaum erkannt. Dies macht das beschriebene Forschungs- und Entwicklungsprogramm zu einem der drängendsten im Umfeld elektronischer Signaturen.

Literatur

[Bo03] Borghoff, U. M. et al. Langzeitarchivierung. dpunkt Verlag, Heidelberg, 2003.

[F-D03] Fischer–Dieskau, S.: Der Referentenentwurf zum Justizkommunikationsgesetz aus Sicht des Signaturrechts, MultiMedia und Recht 6 (11) 701–705 (2003).

[Po00] Pordesch, U.: Der fehlende Nachweis der Präsentation signierter Daten, Datenschutz und Datensicherheit 24 (2) 89–95 (2000)

[Ro03] Roßnagel, A.: Das elektronische Verwaltungsverfahren - Das Dritte Verwaltungsverfahrensänderungsgesetz, NJW 469–474 (2003).

[Sc00] Schmidt, A. U.: Signiertes XML und das Präsentationsproblem, Datenschutz und Datensicherheit 24 (3) 153–158 (2000).

[SG00] Stein, E.; Götz, F.: Staatsrecht, 17. Auflage, 2000.

[5] Dies wurde im Vorläuferprojekt ArchiSig intensiv untersucht. Siehe www.archisig.de und vergleiche [Bo03].