Originalveröffentlichung in: Museumskunde 77 (2012), Nr. 1, S. 77-86

Integrität, Authentizität und Vertrauenswürdigkeit des digitalen kulturellen Erbes

Hans Dieter Huber

Was ist Authentizität?

Der Begriff der Authentizität ist ein sehr komplexer, in verschiedenen Redeweisen, Kontexten und Diskursen verwendeter Begriff. Es lohnt sich, diesen Begriff genauer zu hinterfragen, um sich Klarheit über seinen Gebrauch zu verschaffen. Oft kann man einen *klassischen* von einem *kritischen* Gebrauch unterscheiden.

In der Geschichtswissenschaft ist Authentizität eine Eigenschaft, die Aussagen, Quellen, Dingen oder Orten zukommt, um ihre Echtheit, Glaubwürdigkeit oder Zuverlässigkeit zu kennzeichnen.[1] Die Eigenschaft der Authentizität kann sowohl der Quelle als ganzer als auch einzelnen Aussagen zukommen. Nach Hans-Jürgen Pandel beruht die Forderung nach der Authentizität eines historischen Dokuments auf unserem Geschichtsbewusstsein. Es stelle bestimmte Authentizitäts- und Wahrheitsansprüche an die überlieferten Aussagen, Quellen, Dinge und Orte der Vergangenheit. Denn wir wollen wissen, ob und wie etwas tatsächlich der Fall gewesen ist. Im Allgemeinen wird dabei zwischen der Authentizität eines Objekts, einer Person oder einem authentischen Erlebnis unterschieden.[2]

Die Denkmalpflege besitzt eine Jahrhunderte alte Tradition in der Bewahrung des historischen Erbes und in der Beantwortung der Frage, ob und wie man etwas konservieren, restaurieren, ergänzen oder rekonstruieren darf. Die Ergebnisse dieser Diskussionen sind für die Frage nach der Langzeiterhaltung digitaler Medien nicht unwichtig.

So gab das Deutsche Nationalkomitee für Denkmalschutz am 8. November 1985 folgende Erklärung heraus: *„Jedes Kulturdenkmal, das heute zugrunde geht, ist für alle Zeit verloren. Was wir jetzt nicht retten, kann nie mehr gerettet werden. Was wir jetzt versäumen, kann keine künftige Generation nachholen. Vor dieser Aufgabe gibt es kein Ausweichen. Nicht der Glanz einiger durchrestaurierter Großobjekte darf in dieser Zeit oberstes Ziel der Denkmalpflege sein, sondern allein die Substanzerhaltung möglichst vieler historischer Zeugnisse über eine Periode höchster Gefährdung hinweg."*[3]

Die Worte sprechen eine klare und deutliche Sprache. Sie verleihen auch der Langzeiterhaltung unseres digitalen kulturellen Erbes das nötige Gewicht.

In der *Charta von Venedig* aus dem Jahr 1964 heißt es, dass Denkmäler eine geistige Botschaft der Vergangenheit an die Gegenwart vermitteln. Die Menschheit habe daher die Verpflichtung, *„die Denkmäler im ganzen Reichtum ihrer Authentizität weiterzugeben."* Heute dagegen sei alles authentisch, was von irgend jemandem hergestellt wurde, meint der ehemalige Generalkonservator und Vorsitzende der Welterbe-Kommission, Michael Petzet.[4] Der Kult des Authentischen mache auch nicht vor dem Menschen selbst Halt, wie etwa vor dem *„authentischen Eingeborenen, der als authentische Staffage einer authentischen Kulturlandschaft herhalten muss"*.[5]

Authentizität ist Echtheit. Sie wird durch Prüfung des Inhalts und der Form sowie durch die Zeugnisse Anderer festgestellt. Das heißt wiederum, dass Authentizität *nicht* von vorne herein – per se – existiert, etwa als eine „objektive Eigenschaft" eines Gegenstands, sondern erst in einem komplizierten Beweissicherungs- und Beweiswürdigungsverfahren durch Experten ermittelt und dem Objekt zugeschrieben werden muss. Authentizität beruht daher nicht nur auf der Materie oder Originalsubstanz eines Objekts, sondern auch auf seiner durch die jeweilige Technik einer Zeit geschaffenen Form und Gestalt.[6] Für Petzet ist ein Denkmal mehr als nur ein aus einem bestimmten Material bestehender „Gegenstand." Er bezieht auch die Form, die Gestalt, die Funktion und den Ort eines Objekts in seine Überlegungen zur Authentizität des kulturellen Erbes ein.

Die *Spuren* eines Denkmals verdichten sich in seiner Entstehungs- und Wirkungsgeschichte.[7] Die Aura eines Objekts kann selbst dann noch gegenwärtig sein, wenn von

der historischen Substanz nichts mehr oder kaum mehr etwas übrig geblieben ist.[8]

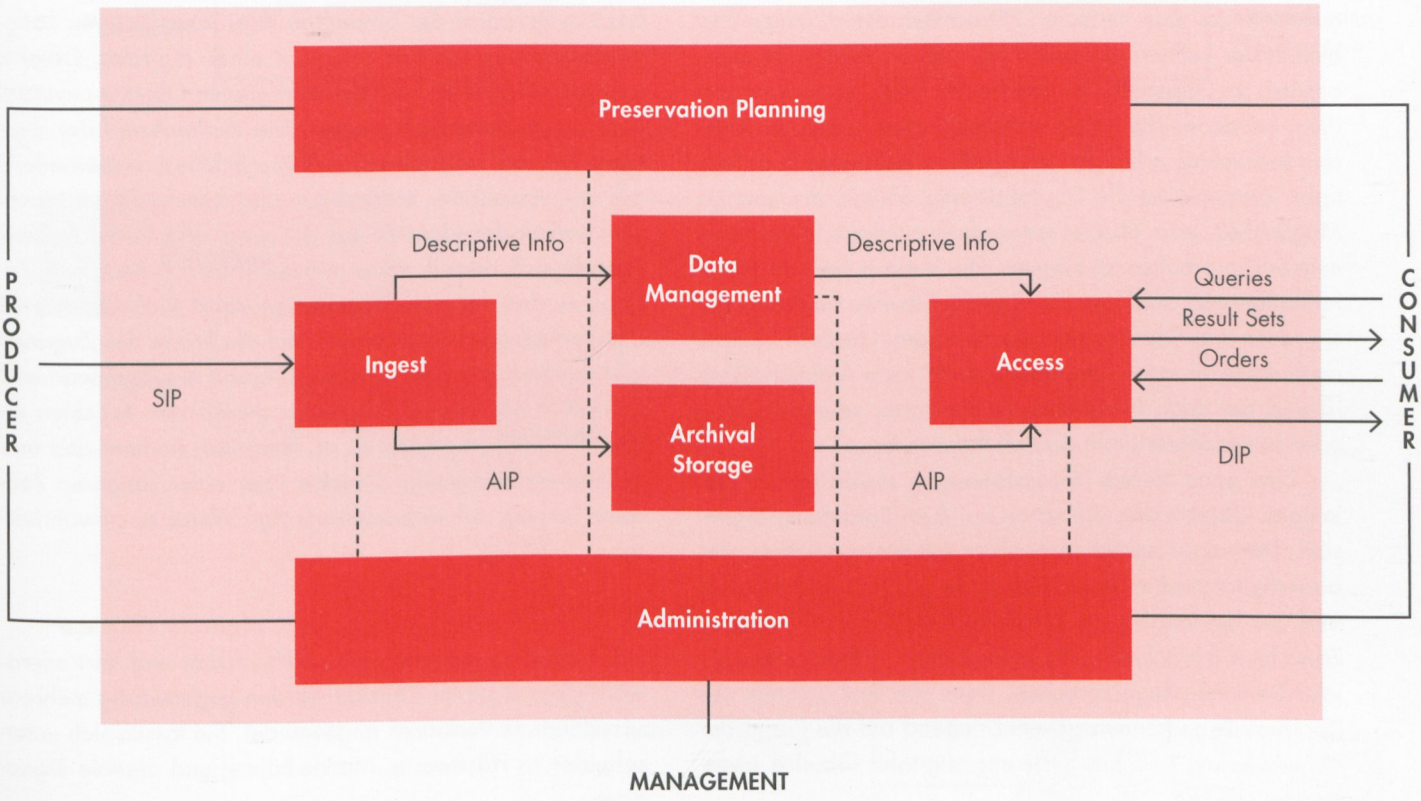
Dies ist ein wichtiger Hinweis auf die Rolle der historischen Substanz in der frühen Computerkunst, die in den letzten Jahren auf vielfältigste Weise diskutiert wurde. Denn wenn das Argument von Petzet richtig ist, dann wäre die Aura, die Ausstrahlung oder die Atmosphäre, die von einem originalen, historischen Computerkunstwerk ausgeht, selbst dann noch vorhanden, wenn von der originalen Substanz nichts mehr oder nur noch wenig übrig geblieben wäre. Es handelt sich hierbei um einen außerordentlich interessanten Gedanken, den ich jedoch nicht ohne Einschränkungen teile.

Die Frage nach Integrität, Authentizität und Vertrauenswürdigkeit von digitalen Daten, Objekten und Archiven ist von einer grundsätzlichen Bedeutung für unsere Gesellschaft. Sie steht in Zusammenhang mit dem langfristigen Erhalt unseres digitalen, kulturellen Erbes für die Nachwelt.

Frauenkirche, Dresden am 6. Oktober 2011, Rekonstruktion 1994–2005. Foto: Hans Dieter Huber.

Der technologische Wandel von analogen zu digitalen Produktionsweisen, Präsentationsformen und Archivierungsstrategien stellt einen tiefgreifenden, kulturellen und gesellschaftlichen Umbruch dar, der in seinem gesamten Ausmaß bisher noch nicht vollständig erkannt worden ist. Neue Medien altern paradoxerweise viel schneller als alte Medien. Dies erfordert ein grundsätzliches Umdenken aller traditionellen Erhaltungsmaßnahmen. Die Interessen der Softwareindustrie stehen der Bewahrung und der Nachhaltigkeit des kulturellen Erbes entgegen. Die Abhängigkeit von Unternehmensstrategien und kurzfristigen Gewinninteressen stellt eine akute Bedrohung des digitalen kulturellen Gedächtnisses dar. Hier muss durch eine Änderung der Gesetzgebung ein neues Rechtsbewusstsein für den Erhalt des digitalen kulturellen Erbes geschaffen werden.

Denkt man beispielsweise nur an die Korrespondenz von Künstlern oder Schriftstellern. Was für eine spannende Quelle stellten solche Briefe in der Vergangenheit dar. Mit der Erfindung der E-Mail ist die Briefkorrespondenz zwischen Künstlern oder Schriftstellern heute zu einem fast ausgestorbenen Kommunikationsmittel geworden. Selbst das noch so junge Medium der E-Mail ist heute schon durch Chat, Facebook, Skype oder Twitter vom kulturellen Vergessen bedroht. Das Literaturarchiv Marbach wird in Zukunft die E-Mail-Nachlässe von Schriftstellern für die Nachwelt bewahren müssen, wenn sie nicht schon lange vorher durch Unachtsamkeit oder Unwissen vernichtet wurden. In einer Fallstudie, die das Literaturarchiv mit dem alten Atari des früh verstorbenen Schriftstellers Thomas Strittmatter durchgeführt hat, wurden die Dateien auf vorbildliche Weise aus ihrem ursprünglichen Format ausgelesen und als Image-Dateien langzeitarchiviert. Aber wie archiviere ich die E-Mails eines berühmten Architekten, eines Künstlers oder eines Designers? Wie bewahre ich seine digitalen Fotografien, seine Handy-Videos, seine 3-D-Entwürfe und digitalen Konstruktionspläne am besten für die Nachwelt auf? Das sind schwierige Fragen, die in Zukunft von den Experten unserer Gesellschaft zu lösen sind. Sie betreffen die kulturelle Identität einer Gesellschaft, die auf den authentischen, historischen Objekten basiert, welche sie selbst geschaffen hat und die sie für wichtig erachtet. In der zuverlässigen Langzeiterhaltung Neuer Medien liegt daher ein tiefgreifender Konflikt. Auf der einen Seite ist das kulturelle Gedächtnis einer Gesellschaft auf Langlebigkeit und Verlässlichkeit angelegt. Auf der anderen Seite unterliegt die Funktionsfähigkeit digitaler Objekte einer immer kurzfristigeren Anpassung.



Original der Abbildung in: *Commitee for Space Data Systems: Recommendation for Space Data System Standards. Reference Model for an Open Archival Information System (OAIS). CCSDS 650.0 – B-1. Blue Book*, January 2002.

Was ist ein digitales Objekt?

Der Begriff des digitalen Objekts ist aus dem von NASA und ESA 1999 entwickelten *Open Archival Information System* (OAIS) entnommen.[9] Ein digitales Objekt wird dort als ein *„object composed of a set of bit sequences"* definiert, also als ein aus einer Reihe von Bit-Sequenzen zusammengesetztes Objekt.[10] Alles das, was mit einem Computer gespeichert und verarbeitet wird, kann als ein digitales Objekt bezeichnet werden. Es kann sich dabei um einfache Text- oder Bilddateien, aber auch um komplexe Multimedia-Applikationen, interaktive digitale Systeme oder um komplette Betriebssysteme handeln.

In unserem Zusammenhang können wir zwei verschiedene Arten digitaler Objekte unterscheiden. Die erste Gruppe sind Digitalisate von analogen Objekten, zum Beispiel von Fotografien, Filmen, Videos oder Tonbändern. Wenn wir zum Beispiel ein analoges Magnetvideoband der 1970er-Jahre vor uns haben, das sich in seine Bestandteile aufzulösen beginnt und zu dem man schon heute kaum mehr ein Abspielgerät findet, in welches man dieses Band einlegen kann, schreitet man zur Digitalisierung des Inhaltes.

Heute wird alles, was obsolet geworden ist, digitalisiert, als sei diese Maßnahme die Lösung aller Probleme. Dabei tauchen aber neue Probleme auf, die viel schneller

auftreten, als man vermutet. Hinsichtlich dieser neuen Problematiken kennen wir bisher nur relativ wenige Lösungsansätze im Gegensatz zu den traditionellen, analogen Medien, bei denen die Konservierungserfahrungen schon mehrere Jahrzehnte oder gar Jahrhunderte betragen. Zum heutigen Zeitpunkt ist die Digitalisierung oftmals die einzige Möglichkeit, eine obsolet gewordene analoge Information mittelfristig erhalten zu können. Die Vorteile bei der Transformation von analogen in digitale Objekte bestehen darin, dass man immer noch ein analoges Original besitzt, auch wenn es unter Umständen nicht mehr funktionsfähig ist und nur noch hinsichtlich seiner Form, seines Designs oder seiner Materialität studiert werden kann.

Eine ganz andere Herausforderung stellen jedoch diejenigen Objekte dar, die schon bei ihrer Entstehung digital sind. Deswegen sprechen wir hier seit einigen Jahren von *born-digital media*. Auch hier geht es in zunehmendem Maß um die langfristige Erhaltung dieses genuin digitalen Erbes für die Nachwelt. Wir könnten hier durchaus von digitaler Denkmalpflege sprechen. Denn die Diskussionen der Denkmalpflege können gewinnbringend auf die Frage der Konservierung und Restaurierung digitaler Objekte angewendet werden.

Die Vertrauenswürdigkeit digitaler Langzeitarchive

Im Zusammenhang mit der Langzeitarchivierung oder Musealisierung digitaler Objekte stellt sich in verstärktem Maß die Frage nach der Vertrauenswürdigkeit digitaler Langzeitarchive. Im *Internet Security Glossary* wird Vertrauenswürdigkeit (engl. *trustworthiness*) als die Eigenschaft eines Systems definiert, gemäß seinen Zielen und Spezifikationen zu operieren, also genau das zu tun, was es zu tun vorgibt und dies auch in geeigneter Weise glaubhaft zu machen.[11] Die Prüfung und Bewertung der eingesetzten Erhaltungsmaßnahmen, mit denen die Risiken und Bedrohungen minimiert werden, denen digitale Langzeitarchive durch Zerfall, Verlust und Manipulation der Daten ausgesetzt sein können, erbringen den Nachweis der Vertrauenswürdigkeit der Archive und damit der in ihnen archivierten digitalen Objekte. Die Informationen, die durch digitale Objekte repräsentiert werden, sind in ihrer Langzeiterhaltung durch Einbußen in ihrer *Integrität, Authentizität, Vertraulichkeit* sowie im gänzlichen oder teilweisen Verlust ihrer *Verfügbarkeit* und Benutzbarkeit bedroht.

Man erkennt daran, dass die „Authentizität" eines digitalen Objekts nur ein einziger Gesichtspunkt von mindestens vier verschiedenen Aspekten drohender Obsoleszenz beziehungsweise der Strategien ihrer zuverlässigen Langzeitbewahrung ist. Die *Integrität* eines digitalen Objekts sagt etwas darüber aus, ob die digitalen Objekte unverändert und vollständig vorliegen. Die *Authentizität* der digitalen Objekte bezieht sich auf ihre Echtheit, insbesondere auf den Aspekt der eindeutigen und zweifelsfreien Nachweisbarkeit der Identität des Urhebers. Die *Vertraulichkeit* bezieht sich darauf, dass unberechtigten Dritten kein Zugang zu den digitalen Objekten gewährt wird. Der Aspekt der *Verfügbarkeit* bezieht sich auf die Frage des Zugangs und der Benutzbarkeit digitaler Objekte in Gegenwart und Zukunft.[12] Sie können bereits an diesen vier Aspekten erkennen, wie kompliziert es ist, Integrität, Authentizität und Funktionalität digitaler Objekte über einen längeren Zeitraum hinweg auf vertrauenswürdige Weise zu gewährleisten.

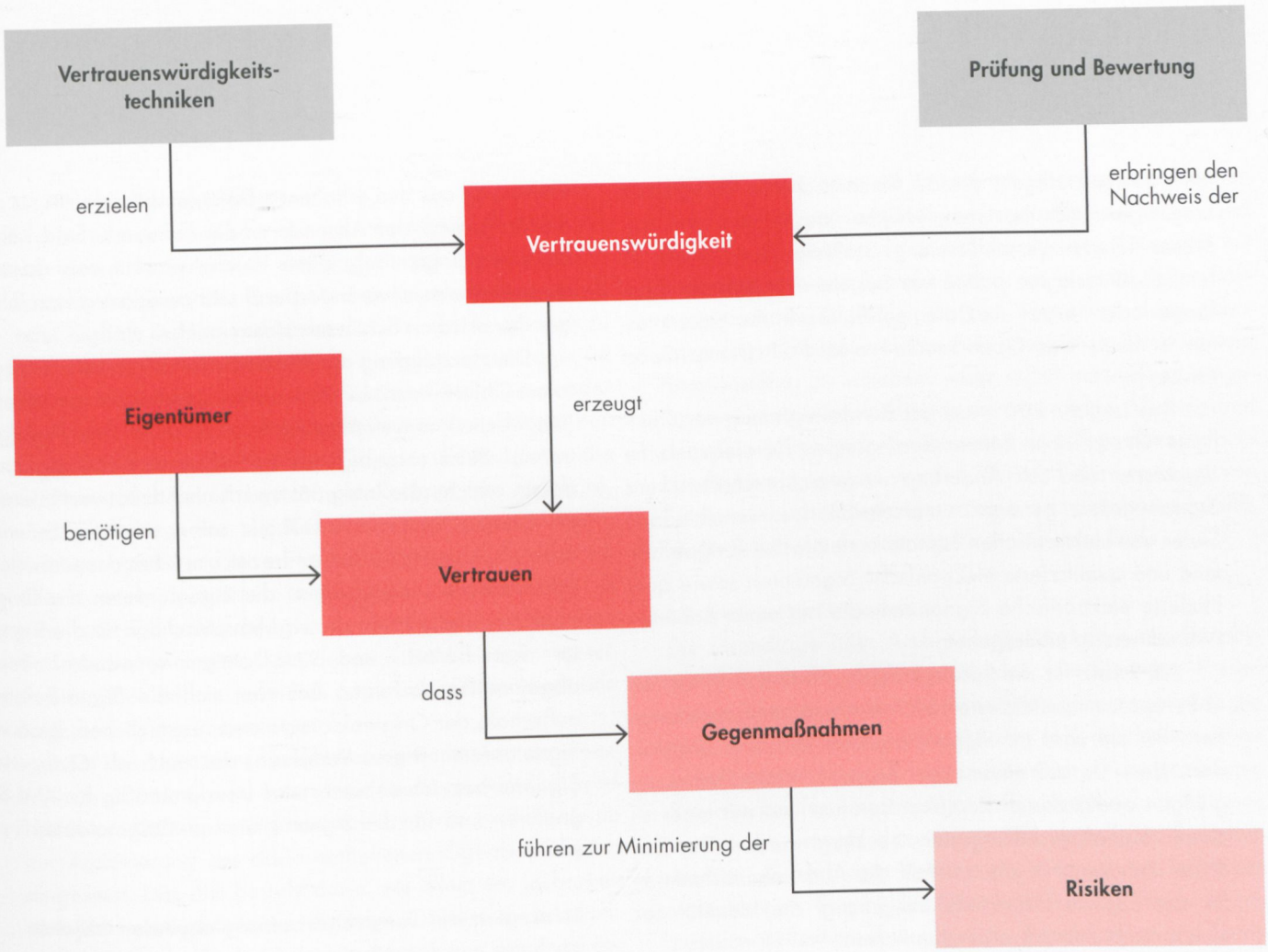
Die Integrität und Authentizität digitaler Objekte

Zur Sicherung der Integrität, Authentizität und Vertrauenswürdigkeit digitaler Objekte werden gegenwärtig mehrere verschiedene Verfahren angewendet. Sie lassen sich unterscheiden in Hashwerte, Merkle-Bäume und digitale Signaturen.

Der Nachweis der unveränderten *Integrität* eines digitalen Objekts wird mit Hilfe von Hashwerten erbracht. MD-5 Prüfsummen gelten dagegen als nicht zuverlässig. Mit Hilfe kryptografisch sicherer Hashfunktionen werden eindeutige digitale „Fingerabdrücke" von Datenobjekten berechnet und zusammen mit den Objekten versandt oder gespeichert. Anhand eines solchen digitalen „Fingerabdrucks" ist der Empfänger oder Nutzer in der Lage, die Integrität eines digitalen Objekts zu überprüfen beziehungsweise unautorisierte Modifikationen zu entdecken. Eine Hashfunktion ist eine mathematisch definierte Funktion, die einen Eingabewert von variabler Länge auf einen kürzeren Ausgabewert fester Länge, den so genannten Hashwert, abbildet. Das Ziel liegt darin, einen „Fingerabdruck" der Eingabe zu erzeugen, der eine Aussage darüber erlaubt, ob eine bestimmte Eingabe aller Wahrscheinlichkeit nach mit dem Original übereinstimmt oder nicht.

Besonders interessant für digitale Langzeitarchive sind so genannte Merkle-Bäume, die eingesetzt werden, um über große Mengen von Daten oder Dokumenten hinweg einen zusammenfassenden Hashwert zu bilden.[13]

Der Merkle-Baum wurde 1979 von dem amerikanischen Verschlüsselungsmathematiker Ralph C. Merkle erfunden, der auch ein Public-Key-Kryptografie-Verfahren vor-



Original der Abbildung in: *nestor Handbuch. Eine kleine Enzyklopädie der digitalen Langzeitarchivierung*, Version 2.3, Göttingen 2010, Kap. 5:3, Abb. 2. Quelle: Bundesamt für Sicherheit in der Informationstechnik 2006.

geschlagen hat. In einem Merkle-Baum können hierarchisch übereinander angeordnete Hashwerte von Hashwerten von Hashwerten gebildet werden, sodass man am obersten Hashwert sofort erkennen kann, ob ein Dokument in einem großen, digitalen Archiv manipuliert wurde oder nicht. Wenn man sich für den obersten Hashwert einen akkreditierten Zeitstempel holt, kann man beweisen, dass die von ihm erfassten digitalen Objekte existieren und seitdem nicht manipuliert wurden. Dies ist eine der wichtigsten Voraussetzungen für den Nachweis der unveränderten Integrität digitaler Objekte und der Vertrauenswürdigkeit eines digitalen Langzeitarchivs als Ganzem.

Die *Authentizität* digitaler Objekte wird dagegen mit Hilfe von elektronischen Signaturen überprüft. Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung im elektronischen Rechts- und Geschäftsverkehr dienen.[14] Ihre Funktion ist die eindeutige und zweifelsfreie Identifizierung des Urhebers der Daten, also der Nachweis, dass die Daten tatsächlich vom Urheber selbst stammen (Echtheitsfunktion) und dass dies auch vom Empfänger oder Nutzer der Daten überprüft werden kann (Verifikationsfunktion). Beides lässt sich heute auf der Grundlage kryptografischer Authentifizierungssys-

teme bewerkstelligen, die auf einem sicheren Verschlüsselungsalgorithmus basieren, welcher aus einem privaten, personifizierten Verschlüsselungs-Schlüssel sowie einem öffentlich hinterlegten *public key* besteht, mit dem der Empfänger oder Nutzer die Daten entschlüsselt. Am bekanntesten ist heute das Open-Source-Project PGP (*Pretty Good Privacy*).

Das im Jahr 2001 von der Bundesregierung veröffentlichte *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften* kurz *Signaturgesetz* genannt, unterscheidet vier verschiedene Stufen von elektronischen Signaturen: einfache, fortgeschrittene und qualifizierte elektronische Signaturen sowie qualifizierte elektronische Signaturen, die mit einer Anbieter-Akkreditierung einhergehen.

Als Ersatz für die handschriftliche Unterschrift werden in Europa nur qualifizierte elektronische Signaturen akzeptiert. Für sie wird im *Signaturengesetz* (§ 2, Nr. 3) gefordert, dass sie auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt wurden. Das Zertifikat übernimmt in diesem Fall die Authentizitätsfunktion für das digitale Objekt. Es bescheinigt die Identität der elektronisch unterschreibenden Person.

Eine wesentliche Eigenschaft dieser asymmetrischen kryptografischen Authentifizierungssysteme, die mit einem geheimen *private key* und einem öffentlich in einem Verzeichnis hinterlegten *public key* arbeiten, liegt darin, dass es praktisch unmöglich ist, den privaten Schlüssel aus dem öffentlichen Schlüssel abzuleiten. Er wird durch eine so genannte Einwegfunktion aus dem privaten Schlüssel errechnet. Da die Signatur das Ergebnis einer Verschlüsselungsfunktion ist, sind die signierten Daten nachträglich nicht mehr veränderbar beziehungsweise eine Änderung sofort erkennbar. Zusätzlich kann der Autor oder Absender der Daten seine Urheberschaft nicht mehr leugnen, weil ausschließlich er selbst über den privaten Signaturschlüssel verfügt.

Es wäre viel zu aufwändig, das gesamte digitale Objekt zu verschlüsseln und zu entschlüsseln. Deshalb wird aus den Daten eine eindeutige Prüfsumme in Form eines Hashwertes erzeugt. Diese wird dann verschlüsselt und dem Originaldokument beigefügt. Der mit dem privaten Schlüssel codierte Hashwert garantiert sowohl die Integrität als auch die Authentizität des digitalen Objekts. Der Empfänger oder Nutzer bildet nach demselben Verfahren, das heißt mit demselben Hash-Algorithmus, ebenfalls eine Prüfsumme aus den erhaltenen Daten und vergleicht sie mit der Prüfsumme des Absenders oder Urhebers. Sind beide Prüfsummen identisch, dann ist dies ein Hinweis darauf, dass die Daten unverändert sind und zuverlässig vom Inhaber des privaten Schlüssels stammen.[15]

Die Hinzufügung der elektronischen Signatur zum digitalen Objekt kann auf drei Arten geschehen: *enveloped* (eingebettet), *enveloping* (einbettend) und *detached* (getrennt). Beim eingebetteten Verfahren sind die Signaturdaten, welche die Integrität und Authentizität verifizieren, als Element im digitalen Objekt selbst erhalten. Es wird auch als *Inbound-Verfahren* bezeichnet. Bei der einbettenden Methode „umschließen" die Signaturdaten die Originaldaten. Diese Methode wird hauptsächlich für die Signatur von E-Mails und XML-Dateien verwendet. Beim abgetrennten Verfahren befinden sich die Signaturdaten außerhalb der Originaldatei in einer zusätzlichen, binären Signaturdatei. Dieses Verfahren, das auch als *Outbound-Signatur* bezeichnet wird, wird standardmäßig für XML-Signaturen und für die Signatur binärer Originaldaten verwendet.

Strategien der Langzeiterhaltung digitaler Objekte

Ich habe nur die gängigsten Methoden und Verfahren erläutert, die wir heute benutzen, um die Integrität und Authentizität digitaler Objekte zu bewahren. Worüber wir allerdings noch gar nicht gesprochen haben, ist die Frage nach einer Perspektive für die Langzeiterhaltung unseres digitalen kulturellen Erbes. Erstaunlicherweise altern neue Medien nämlich wesentlich schneller als alte Medien. Nach drei bis vier Jahren muss man damit rechnen, dass Festplatten ihren Dienst versagen und ernsthafte Datenverluste erzeugen, wenn man keine regelmäßige Backupstrategie entwickelt hat. Integrität, Authentizität und Vertrauenswürdigkeit digitaler Objekte sind in ihrer Langzeitperspektive vor allem durch das Obsoletwerden der verwendeten Datenträger, der zugehörigen Software und Betriebssysteme sowie der Hardware-Obsoleszenz massiv in ihrem Erhalt gefährdet. Generell werden heute fünf bis sechs verschiedene Strategien zur Langzeiterhaltung digitaler Objekte diskutiert. Nicht jede dieser Strategien ist für jeden Objekttyp gleichermaßen geeignet. Auch die Integrität und Authentizität digitaler Objekte werden durch die verschiedenen Erhaltungsstrategien in unterschiedlicher Weise verändert. Die verschiedenen Strategien lauten: *Hardware Preservation, Bitstream Preservation, Migration, Emulation, Rekonstruktion.*

Hardware Preservation

Die Standardstrategie für die meisten Museen besteht darin, eine Arbeit physisch einzulagern, egal ob dies darin besteht, ausgewähltes Equipment in Regale zu verpacken oder digitale Dateien auf Bändern, CDs oder Festplatten zu archivieren. Was bedeutet diese Einlagerungsstrategie im Fall von digitalen Objekten? Was könnte ein Museum oder ein Archiv im Fall eines digitalen Kunstwerkes physisch einlagern? Es müsste die digitalen Objekte, die Festplatte, die Software, das Betriebssystem, die Rechner, die Monitore, die Peripheriegeräte, die Kabel, die Interfaces einlagern. Kurz gesagt, müsste ein vertrauenswürdiges Archiv einfach alles zusammen in seiner ursprünglichen Funktionalität als eine heterogene Mischung aus verschiedenen Materialien und Medien einlagern, von denen jedes im ungünstigsten Fall unterschiedliche und sich gegenseitig ausschließende Lagerbedingungen benötigt.

Bei der Hardware Konservierung kann man zwei verschiedene Intentionen unterscheiden. Im ersten Fall wird Hardware-Konservierung von Archiven als eine Strategie zur Archivierung der darin enthaltenen digitalen Objekte eingesetzt. Das Ziel besteht darin, vor allem die Lesbarkeit und die Funktionalität der digitalen Objekte zu erhalten, nicht dagegen die originale Hardware. Aus diesen Gründen versucht man, die Hardware- und Software-Plattform so lange wie möglich am Laufen zu halten und tauscht sie dann aus. Bei der zweiten Strategie, die insbesondere von Technik-, Design- oder Medienmuseen verfolgt wird oder, besser gesagt, verfolgt werden sollte, ist auch die Erhaltung der ursprünglichen Hardware- und Software-Plattform ein zentrales Anliegen konservatorischer Bemühungen.[16] Während bei der ersten Erhaltungsstrategie Reparaturen und Ersatzteile in erster Linie dem Erhalt der Funktionsfähigkeit der digitalen Objekte dienen, fallen in diesem Sammlungsbereich auch ethische und ästhetische Gesichtspunkte der originalen Hardware und ihrer authentischen Erhaltung ins Gewicht. Die Erhaltung der Funktionsfähigkeit der digitalen Objekte ist nicht mehr das einzige Kriterium. Vielmehr sollen möglichst historisch adäquate Geräte und Bauteile verwendet werden, um eine authentische ästhetische Erfahrung mit einer historischen Computer-Plattform machen zu können. Die Vorteile liegen auf der Hand. Keine andere Strategie kann so viel vom intrinsischen Wert historischer, originaler, digitaler Objekte vermitteln. Der *Look and Feel* einer solchen funktionsfähigen Einheit ist an Authentizität und an ästhetisch-historischen Erfahrungsmöglichkeiten nicht zu überbieten.

Um eine Datei oder ein Programm in seiner spezifischen Funktionalität und originalen Umgebung aus Hard- und Software zu erhalten, ist es notwendig, den Computer mit dem ursprünglichen Betriebssystem, der ursprünglichen Software und den originalen Dateien sowie den dazu gehörigen Schnittstellen und Peripheriegeräten vollständig und funktionsfähig zu erhalten. Aber selbst massenhaft eingelagerte Ersatzteile unterliegen der natürlichen Alterung und dem physischen Verfall, auch wenn sie völlig unbenutzt und nagelneu eingelagert wurden.[17] Wenn die Lagerung von Ersatzteilen als Erhaltungsstrategie nicht mehr weiterhilft, ist die Erhaltung des Bitstreams die nächste Stufe.

Bitstream Preservation

Die Grundlage aller Archivierungstätigkeiten ist der physische Erhalt der digitalen Objekte, die *Bitstream Preservation*. Hierbei werden Speicherstrategien eingesetzt, die eine redundante Datenspeicherung auf mindestens zwei verschiedenen Speichermedien vorsehen. Die verwendeten Speichermedien werden regelmäßig durch neuere Systeme ersetzt, um sowohl dem physischen Verfall der Speichermedien als auch dem Veralten der eingesetzten Techniken vorzubeugen. Es gibt vier Arten von Bitstream Preservation, nämlich *Refreshment, Replication, Repackaging* und *Transformation*.[18] Beim Refreshment werden einzelne Datenträger gegen neue, gleichartige Datenträger ausgetauscht. Die Dateien, beispielsweise eine DVD, werden direkt auf einen neuen DVD-Datenträger kopiert, die Daten einer CD auf eine neue CD und die Daten einer Festplatte auf eine neue Festplatte von gleicher Größe. Es wird also lediglich ein älterer durch einen gleichartigen, neueren Datenträger ausgetauscht.[19]

Bei der *Replication* werden zwar auch Daten von einem älteren Datenträger auf einen neuen kopiert. Allerdings kann es sich hier auch um einen Datenträger eines anderen oder neueren Typs handeln. *Replication* findet zum Beispiel dann statt, wenn man die Daten von mehreren CDs oder DVDs auf eine einzige Blue-Ray-Disc kopiert. Der neue Datenträger kann daher in der Regel nicht mehr den Platz des alten einnehmen. Im Unterschied zum *Refreshment* finden hier Veränderungen in der physischen Speicherstruktur statt.

Das *Repackaging* ist ein Konservierungsvorgang, bei dem das Archivpaket verändert wird. Die Änderung betrifft nicht die Dateninhalte, sondern nur eine Veränderung in der Struktur des Archivpakets.[20] Die Daten werden neu verpackt und angeordnet. *Transformation* ist dagegen ein

Migrationsprozess, bei dem auch die Inhaltsdaten eines Archivpakets verändert werden. Dies findet zum Beispiel dann statt, wenn man eine alte Word-Datei ins RTF-Format konvertiert, um sie für künftige Word-Versionen leichter lesbar zu halten oder eine JPEG-Datei in das für Langzeitarchivierung geeignete TIFF-Format konvertiert.

Migration

Durch Migration soll erreicht werden, dass Bild-, Text- oder Sounddateien zusammen mit ihren Kontext- und Erschließungsinformationen über längere Zeiträume hinweg im Umfeld ihrer jeweils zeitbezogenen Hard- und Softwarearchitektur verfügbar und lesbar bleiben. Was bedeutet die Strategie der Migration für die Bewahrung von digitalen Objekten? Migration stellt kein größeres Problem dar, solange das archivierte Objekt auf einem jüngeren Betriebssystem und mit jüngerer Software in seiner ganzen Funktionalität erhalten bleiben kann. Aber wir kennen bereits jetzt zahlreiche digitale Objekte, zum Beispiel komplexe Webseiten aus der *net.art*, die von einem ganzen Bündel von Steuerelementen, Skripten und Protokollen abhängen, die heute kaum mehr benutzt werden oder welche neuere Formate wie Flash nicht mehr verarbeiten können und dadurch Fehlermeldungen produzieren. Die nächste Lösung, wenn die Strategien der Bitstream Preservation und der Migration an ihr Ende gelangt sind, ist Emulation.

Emulation

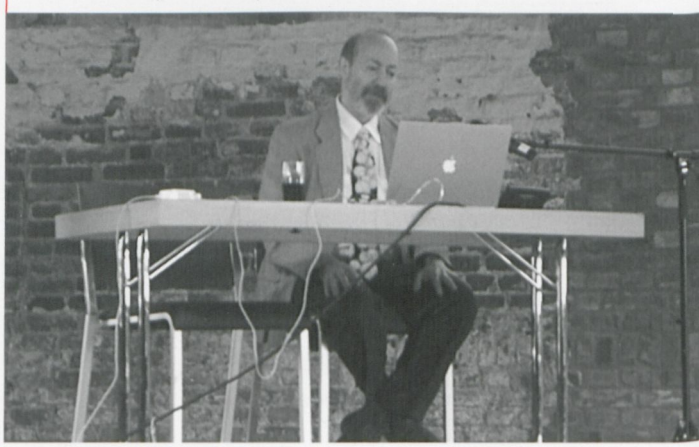
Das Emulationskonzept wurde 1995 von Jeff Rothenberg von der *Rand Corporation* vorgeschlagen, der das Migrationskonzept langfristig für zu unsicher hielt. Prinzipiell beruht das Konzept eines Emulators darauf, die Funktionalität eines Betriebssystems aus derjenigen Zeit, in welcher das archivierte, digitale Objekt entstanden ist, nachzubilden. Das heißt, es soll eine nicht mehr vorhandene Hardware- und Betriebsystemumgebung so simuliert werden, dass die digitale Information in ihrer ursprünglichen Softwareumgebung und damit auch in ihrer ursprünglichen Funktionalität und Ästhetik in späteren Zeiten noch zugänglich gemacht und erhalten werden kann.

Es gibt auf diesem Gebiet verschiedene Arten von Emulationen. Sie kann auf der Ebene der Anwendersoftware, auf der Ebene des Betriebssystems, aber auch auf der Ebene der Hardware eingesetzt werden. So kann zum Beispiel die ursprüngliche Hardware eines digitalen Objekts als Software mit einem Emulatorenprogramm nachgebildet werden, welches das archivierte Betriebssystem und die darauf aufbauenden Softwarekomponenten laden kann. Ein Beispiel für die Emulation von Betriebssystemen wäre zum Beispiel ein MS-DOS-Emulator, der die Programme für dieses veraltete Betriebssystem auf zeitgenössischen, aktuellen Rechnern ausführen kann. Ein Beispiel für Software-Emulation wäre etwa ein Programm zum Anzeigen und Bearbeiten von sehr alten Microsoft-Word-Dateien, welche die aktuelle Word-Software nicht mehr lesen kann.[21]

Im Gegensatz zur Migration, bei der jeweils eine neue und aktuellere Version des digitalen Objekts selbst erzeugt wird, werden die originalen Objekte bei der Emulation nicht verändert.[22] Mittlerweile gibt es jedoch einen elaborierteren Ansatz, der für die Zukunft der Emulation sehr vielversprechend zu sein scheint, nämlich der so genannte *Universal Virtual Computer* (UVC) von IBM. Der UVC ist ein gut dokumentierter virtueller Computer, der auf unterschiedlichen, auch zukünftigen Computerarchitekturen, nachgebildet werden kann. Auf diesem virtuellen Computer aufbauend, können weitere Programme oder Emulatoren geschrieben werden, mit denen man ältere digitale Objekte öffnen und bearbeiten kann.

Die Vorteile der Emulation liegen darin, dass die Originalobjekte unverändert bleiben. Eine Konvertierung ist nicht notwendig. Außerdem wird weniger Speicherplatz benötigt, da keine migrierten Objekte zusätzlich zu den Originalen gespeichert werden müssen. Die Nachteile liegen darin, dass für komplizierte digitale Objekte oder Systeme Emulatoren technisch schwer zu implementieren sind. Zusätzlich entsteht ein hoher Aufwand für jeden Hardware-Generationswechsel. Denn das grundlegende Problem von Emulation besteht darin, dass der Emulator selbst von

Jeff Rothenberg am 22. Juni 2003 auf der *404 – Object Not Found Conference* in Dortmund. Foto: Hans Dieter Huber.



einem bestimmten Betriebssystem abhängig ist und nur auf diesem Betriebssystem läuft. Das Problem des Emulators liegt darin, dass er selbst auch altert und man dann einen Emulator für einen Emulator schreiben muss. Es müssen also für jede neue Plattform neue Emulatoren entwickelt werden. Neben dem UVC existieren jedoch auch Ansätze, Emulatoren in plattformunabhängigen Sprachen, wie Java, zu verfassen, die dann auf mehreren Betriebssystemen oder Hardwarearchitekuren lauffähig sind.[23]

Wenn also auch Emulation keine mögliche Lösung für die Langzeitbewahrung mehr darstellt, besteht zum gegenwärtigen Zeitpunkt die letzte Möglichkeit in der radikalen Neuinterpretation oder Rekonstruktion des Werkes.

Joan Jonas, *Organic Honey's Visual Telepathy* (1972 – 1999), Installation in der Rijksakademie van beeldende kunsten, Amsterdam, Juni 2010. Foto: Hans Dieter Huber.

Rekonstruktion

Die radikalste Bewahrungsstrategie besteht darin, eine Arbeit jedes Mal, wenn sie aufgebaut, gezeigt oder vorgeführt wird, neu zu rekonstruieren. Ion Ippolito von der *Variable Media Initiative* in New York hat diese Strategie unter dem Begriff Re-Interpretation für bestimmte Arbeiten wie Performances, Installationen oder vernetzte Arbeiten vorgeschlagen. Er ist aber selbst hinsichtlich der Neuinterpretation sehr skeptisch. Denn er schreibt: *„Die radikalste Bewahrungsstrategie besteht darin, die Arbeit jedes Mal, wenn sie neu aufgebaut wird, zu reinterpretieren.* [...] *Reinterpretation ist eine gefährliche Technik, wenn sie nicht durch den Künstler autorisiert ist, aber es kann die einzige Weise sein, Kunstwerke wie eine Performance, eine Installation oder ein vernetztes Kunstwerk neu zu erschaffen, die entworfen worden sind, um sich mit dem jeweiligen Kontext zu verändern."*

Die Rekonstruktion oder Wiederaufführung einer Arbeit sollte auf einer möglichst genauen Notation, Handlungsanweisung oder ausführlichen Dokumentation beruhen. Die Rahmendaten einer Re-Konstruktion sollten in einem gemeinsamen Gespräch mit dem Künstler festgehalten werden. Man muss eine Übereinkunft darüber erlangen, was genauso bleiben muss und nicht verändert werden darf sowie darüber, was variieren oder durch andere Bestandteile ersetzt werden kann. Denn dann ist eine Rekonstruktion autorisiert. Die *Variable Media Initiative* hat hierzu einen umfangreichen Fragenkatalog entwickelt, in dem durch eine genaue Befragung des Künstlers die feststehenden und variablen Parameter einer Arbeit für die Nachwelt dokumentiert werden können.[24] Der heutige Stand in den Konservierungswissenschaften geht dahin, eines oder mehrere so genannte *extended interviews* mit dem Künstler hinsichtlich einer autorisierten Wiederaufführung oder der Re-Installation durchzuführen und zu dokumentieren. Das Stedelijk Museum in Amsterdam hat dies 2010 mit dem Hauptwerk von Joan Jonas *Organic Honey's Visual Telepathy / Organic Honey's Vertical Roll*, das in mehreren Performances und Installationsversionen im Zeitraum von 1972 bis etwa 1994 entstanden ist, durchgeführt und die festen und variablen Parameter der Arbeit zusammen mit der Künstlerin selbst erarbeitet und dokumentiert.[25]

Zusammenfassung

Authentizität ist ein vielfältiger Begriff, der auf Objekte, Personen und Ereignisse bezogen werden kann. Die Authentizität eines Objekts ist das Resultat eines komplexen und langwierigen Zuschreibungsprozesses. Auch im Bereich unseres digitalen kulturellen Erbes sind Fragen der Integrität, Authentizität und langfristigen Erhaltung digitaler Artefakte von großer Bedeutung. Die gegenwärtig diskutierten Ansätze zur langfristigen Erhaltung unseres digitalen Erbes lauten *Hardware Preservation, Bitstream Preservation, Migration, Emulation* und *Rekonstruktion*

Die Integrität digitaler Objekte wird gegenwärtig vor allem durch digitale Fingerabdrücke wie Prüfsummen oder Hashwerte festgestellt. Die Authentizität eines digitalen Objekts wird dagegen mit Hilfe elektronischer Signaturen überprüft, die meistens mit einem öffentlichen und einem privaten Schlüssel funktionieren. Dieselben Fragen, die den langfristigen Umgang mit unserem kulturellen Erbe in Form von Denkmälern betreffen, lassen sich auf den Bereich unseres digitalen, kulturellen Erbes ausdehnen und erweitern, das von Jahr zu Jahr immer stärker anwächst. Man könnte von hier aus ein neues Fach entwickeln, nämlich eine Art von digitaler Denkmalpflege.

Der vorliegende Text erscheint in Kürze im Band: Wolfgang COY und Jens-Martin LOEBEL (Hrsg.), *Zuverlässige Langzeitarchivierung – Tagungsband*, Stiftungsreihe der Alcatel-Lucent-Stiftung für Kommunikationsforschung, Band SR 98, Stuttgart 2012.

Anmerkungen

1 Hans-Jügen PANDEL, „Authentizität", in: Ulrich MAYER, Hans-Jürgen PANDEL, Gerhard SCHNEIDER u. a. (Hrsg.), *Wörterbuch Geschichtsdidaktik*, Schwalbach/Taunus 2009, S. 30–31, hier S. 30.

2 Eva Ulrike PIRKER und Mark RÜDIGER, „Authentizitätsfiktionen in populären Geschichtskulturen: Annäherungen", in: Eva Ulrike PIRKER und Mark RÜDIGER u. a. (Hrsg.), *Echte Geschichte. Authentizitätsfiktionen in populären Geschichtskulturen*, Bielefeld 2010, S. 11–30, hier S. 18.

3 DEUTSCHES NATIONALKOMITEE FÜR DENKMALSCHUTZ, „Zur Substanzerhaltung umweltgefährdeter Denkmäler, Frankfurt am Main, 8. November 1985", in: DEUTSCHES NATIONALKOMITEE FÜR DENKMALSCHUTZ (Hrsg.), *Denkmalschutz. Texte zum Denkmalschutz und zur Denkmalpflege*, 4. Auflage, Band 52, Bonn 2007, S. 156–157, hier S. 157.

4 1995 hat der Generalkonservator des Bayerischen Landesamts für Denkmalpflege, Michael PETZET, auf der Konferenz in Nara, Japan, über *Authenticity in Relation to the World Heritage Convention* einen bemerkenswerten Vortrag über Authentizität gehalten, in welchem er unter Anderem den vorherrschenden Kult der Authentizität kritisiert hat. Siehe: Knut Einar LARSEN (Red.), *Nara Conference on Authenticity in Relation to the World Heritage Convention. Nara, Japan 1–6 November 1994, UNESCO World Heritage Center*, Trondheim 1995, S. 85–99.

5 Michael PETZET, „Was heißt Authentizität? Die authentische Botschaft des Denkmals", in: Ulrike BESCH (Hrsg.), *Restauratorenbuch 1998*, München 1997, S. 141–162, hier S. 142.

6 Ebd., S. 214.

7 Ebd., S. 146.

8 Siehe hierzu auch DEUTSCHES NATIONALKOMITEE FÜR DENKMALSCHUTZ (Hrsg.), *Rekonstruktion in der Denkmalpflege. Überlegungen – Definitionen – Erfahrungsberichte*, 2. Auflage, Band 57, Bonn 1998; Winfried NERDINGER (Hrsg.), *Geschichte der Rekonstruktion – Konstruktion der Geschichte*, Ausst. Kat. Architekturmuseum der Moderne in der Pinakothek der Moderne, 22. Juli – 31. Oktober 2010, München u. a. 2010.

9 CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (2001), *Reference Model for an Open Archival Information System* (OAIS), CCSDS 650.0-B-1, BLUE BOOK, online unter public.ccsds.org/publications/archive/650x0b1.pdf (letzter Aufruf am 12. April 2012).

10 Stefan E. FUNK, „Digitale Objekte und Formate", in: Heike NEUROTH, Achim OSSWALD u. a. (Hrsg.), *nestor Handbuch. Eine kleine Enzyklopädie der digitalen Langzeitarchivierung*, Version 2.3., Göttingen 2010, Kap. 7:3 – 7:8. Online unter nestor.sub.uni-goettingen.de/handbuch/nestor-handbuch_23.pdf (letzter Aufruf am 12. April 2012);

11 Zit. nach Susanne DOBRATZ und Astrid SCHOGER, „Grundkonzepte der Vertrauenswürdigkeit und Sicherheit", in: NEUROTH, OSSWALD u. a. 2010 (wie Endnote 10), Kap. 5:3.

12 Ebd., Kap 5:3.

13 Siegfried HACKEL, Tobias SCHÄFER und Wolf ZIMMER, „Praktische Sicherheitskonzepte", in: NEUROTH, OSSWALD u. a. 2010 (wie Endnote 10), Kap. 5:9 – 5:19, hier Kap. 5:9.

14 Ebd., Kap 5:13. Siehe ferner: Sebastian BÖSING, *Authentifizierung und Autorisierung im elektronischen Rechtsverkehr. Qualifizierte Signaturschlüssel- und Attributszertifikate als gesetzliche Instrumente digitaler Identität*, Baden-Baden 2005.

15 HACKEL, SCHÄFER, ZIMMER (wie Endnote 13), Kap. 5:16.

16 Karsten HUTH, „Computermuseum", in: NEUROTH, OSSWALD u. a. 2010 (wie Endnote 10), Kap. 8:24 – 8:31, hier Kap. 8:25.

17 Wir besitzen an unserer Kunstakademie die wunderbare Video-Installation *Two Way Communication* von Nam June Paik aus dem Jahr 1996 mit 84 Monitoren. Fünf Ersatzmonitore wurden bei der Erstinstallation mitgeliefert. Als wir diese vor ein paar Jahren aus dem Lagerraum holten, waren bereits zwei originalverpackte Monitore defekt, ohne dass sie jemals in Betrieb genommen worden waren.

18 Dagmar ULLRICH, „Bitstream Preservation", in: NEUROTH, OSSWALD u. a. 2010 (wie Endnote 10), Kap. 8:3 – 8:9, hier Kap. 8:3.

19 Ebd., Kap. 8:5.

20 Ebd., Kap. 8:6.

21 Stefan E. FUNK, „Emulation", in: NEUROTH, OSSWALD u. a. 2010 (wie Endnote 10), Kap. 8:16 – 8:23, hier Kap. 8:16.

22 Ebd.

23 Diesen Hinweis verdanke ich freundlicherweise Jens-Martin Loebel, Berlin.

24 Die *Filmmaker Datenbank* mit dem Fragenkatalog ist unter variablemediaquestionnaire.net zu finden (letzter Aufruf am 12. April 2012).

25 Siehe unter www.incca.org/cawc-programme/day-3/670-decision-making (letzter Aufruf am12. April 2012).