Fraunhofer
SIT

Warum digitale Signaturen altern und wie man trotzdem ihren Wert erhält

ArchiSoft-Dokumentation, Band 1

Version 2.5 vom 18. Juni 2009

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Rheinstraße 75
64295 Darmstadt

`http://www.sit.fraunhofer.de/archisoft/Whitepaper.pdf`

Zusammenfassung

Handschriftlich geleistete Signaturen unterliegen einem Alterungsprozess. Digitale Signaturen können zwar nicht verblassen, doch auch sie altern und verlieren dadurch an Wert. Dieser Wertverlust wird spätestens nach sechs Jahren signifikant. Alle Anwender, die Signaturen auch danach noch beweissicher verifizieren wollen, müssen rechtzeitig und regelmäßig Gegenmaßnahmen ergreifen.

Dieses Whitepaper erläutert die Hintergründe des Alterns und zeigt, wie digitale Signaturen dennoch über Jahrzehnte in ihrem Wert erhalten werden können. Grundlage dafür ist das Programmpaket ArchiSoft, das am Fraunhofer-Institut für Sichere Informationstechnologie entwickelt wurde. Die Software lässt sich leicht in Dokumentenmanagementsysteme integrieren und übernimmt selbständig alle Schritte, die zu einem Werterhalt digitaler Signaturen notwendig sind.

Das Thema ist hochaktuell, da alle Signaturen, die auf kurzen Schlüsseln basieren, nur noch bis zum 31.3.2008 als uneingeschränkt sicher galten, so die offizielle Bekanntgabe der Bundesnetzagentur. Dazu gehören alle Signaturen, die bis Ende 2007 mit signaturgesetzkonformen Karten geleistet wurden. Signaturen, die nicht rechtzeitig erneuert wurden, sollten so schnell wie möglich, einen Erneuerungsprozess durchlaufen. Besser ist es jedoch, Prozesse so zu gestalten, dass Signaturerneuerung ein integraler Bestandteil ist.

Die Kapitel 1 bis 5 dieses Papiers richten sich an alle, die sich mit der Archivierung digital signierter Dokumente beschäftigen.

Die folgenden Kapitel beschreiben technische Details der ArchiSoft-Lösung. Sie richten sich an Softwarearchitekten, welche die Integration von ArchiSoft in ein Dokumentenmanagementsystem planen.

Verfasser:
MICHAEL HERFERT, THOMAS KUNZ, URSULA VIEBEG.
Die Autoren sind über ArchiSoft@sit.fraunhofer.de zu erreichen.
An früheren Versionen dieses Papiers haben mitgewirkt:
SUSANNE OKUNICK

1 Prolog vor Gericht

Donnerstag, 29.10.2020. Heute hat Katharina S. ihren vierten Gerichtstermin. Es geht um Ansprüche aus einem Vertrag, den sie im Jahr 2005 geschlossen hat. Katharina S. hat damals zu den ersten Anwendern gehört, welche digitale Signaturen durchgängig eingesetzt haben, um Medienbrüche konsequent zu vermeiden. Ihre Firma profitiert noch heute von den erzielten Einsparungen. Sie war sich ganz sicher, das der Prozess eine Lapalie sei, schließlich sind ihre Ansprüche eindeutig formuliert und sie hatte seinerzeit Komponenten eingesetzt, welche die strengen Anforderungen des deutschen Signaturgesetzes erfüllten. Ihr Prozessgegner legte dann aber eine ganz andere Version des Vertrags vor, die ebenfalls digital signiert ist. Das Gericht stellt fest, dass die damalige Signatur heute jeder Taschencomputer brechen könne. Sie habe dadurch ihren kryptographischen Beweiswert verloren. Die Beteiligten hätten gemäß §6 SigG und §17 SigV dafür sorgen sollen, dass die Signatur nicht „kryptographisch verblasse“ . Nun müsse der Streit auf Basis anderer Indizien entschieden werden. Der Ausgang ist offen.

2 Archivierung digitaler Dokumente

Zurück zum heutigen Tag.
In vielen Anwendungsbereichen gibt es Anforderungen an Aufbewahrungs- fristen für digitale Dokumente. Das betrifft insbesondere den Gesundheits- bereich, das eGovernment, das Steuerwesen und den Bankenbereich. Dabei sind die folgenden prinzipiellen Probleme zu lösen:

1. Wie erreicht man, dass der Datenträger auch nach Jahrzehnten noch lesbar ist?
2. Wie erreicht man, dass das Dokumentenformat auch nach Jahrzehnten noch verarbeitet werden kann?
3. Wie erreicht man, dass digitale Signaturen auch nach Jahrzehnten noch beweiskräftig sind?

Die ersten beiden Punkte sind nicht Gegenstand dieses Papiers. Als Institut für sichere Informationstechnologie konzentrieren wir uns auf die Beweiswerterhaltung digitaler Signaturen. Dazu ist zunächst zu erläutern, warum digitale Signaturen trotz ihrer immateriellen Natur überhaupt einem Alterungsprozess unterliegen.

3 „Verblassende“ digitale Signaturen

Digitale Signaturen basieren üblicherweise auf einem zweistufigen Prozess. Der Signierer erzeugt zunächst mittels einer kryptographischen Hashfunktion einen Fingerabdruck des Dokuments. Dieser Fingerabdruck hat eine feste Länge, typischerweise 20 bis 32 Bytes, unabhängig von der Länge des Dokuments. Im zweiten Schritt wird der Fingerabdruck mittels eines Public-Key-Verfahrens „verschlüsselt“ . Dafür wird der private Schlüssel des Signierers benutzt. Jeder, der über den assoziierten öffentlichen Schlüssel verfügt, kann verifizieren, dass der Hashwert mit dem privaten Schlüssel des Signierers verschlüsselt wurde. Um für eine Signatur geeignet zu sein, muss die Hashfunktion so gestaltet sein, dass es praktisch unmöglich ist, aus einem Hashwert auf das Urbild zu schließen. Diese Eigenschaft lässt sich nicht streng beweisen, vielmehr wird ein Hashverfahren als geeignet angesehen, wenn es von renommierten Kryptographen empfohlen wird. Gleichzeitig arbeiten andere Kryptographen daran, die Hashfunktion zu brechen, indem sie einen Weg suchen, doch auf das Urbild zu schließen oder zumindest zwei Urbilder zu finden, die auf denselben Hashwert abgebildet werden. Ein Public-Key-Verfahren beruht auf mathematischen Problemen, die in einer Richtung sehr leicht lösbar sind, in der anderen aber sehr schwierig sind. Im Falle des RSA-Verfahrens, das am häufigsten eingesetzt wird, bedeutet dies, dass es sehr einfach ist, zwei Zahlen zu multiplizieren, aber sehr schwierig, eine große Zahl in ihre Faktoren zu zerlegen. Auch hier arbeiten Kryptographen daran, die Signatur zu brechen, indem sie nach effizienten Wegen suchen, eine große Zahl zu faktorisieren. Dadurch wäre es einem Angreifer möglich, eine fremde Identität anzunehmen. Beachtet man noch die steigenden Rechenleistungen, so erhält man drei Faktoren, die maßgeblich zur zeitlichen Schwächung digitaler Signaturen beisteuern:

1. Fortschritte in der Kryptographie bedrohen essentielle Eigenschaften von Hashalgorithmen und Public-Key-Verfahren.
2. Durch die zunehmende Rechenleistung lassen sich selbst über einfache brute force-Attacken immer bessere Ergebnisse erzielen.
3. Auch die massive Vernetzung trägt zum steigenden Erfolg von brute force-Attacken bei.

Derartige Schwächungen sind keine akademischen Illusionen, sondern sie finden tatsächlich statt. Jüngstes Beispiel ist der Hashalgorithmus SHA1, dessen Schwä-

chung im Februar 2005 bekannt wurde. Zuvor wurde schon MD5 so weit attackiert, dass er heute praktisch unbenutzbar ist. Auch die Faktorisierung großer Zahlen macht Fortschritte. 1994 hat die Zerlegung eines 426 bit langen Schlüssels noch 5000 MIPS-Jahre erfordert. Zwei Jahre später, nach bahnbrechenden Ergebnissen des Kryptographen POLLARD, gelang die Faktorisierung eines 432 bit langen Schlüssels, dessen Schlüsselraum $2^6 = 64$ mal größer ist, in nur 750 MIPS-Jahren. Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (ehemals RegTP) gibt im Januar jedes Jahres eine Übersicht über geeignete Algorithmen für Hashfunktionen und Public-Key- Verfahren heraus. Der Prognosezeitraum erstreckt sich über sechs Jahre. Alle Anwender, die Signaturen auch danach noch beweissicher verifizieren wollen, müssen sich um die Beweiswerterhaltung bemühen. Sie tun gut daran, dies hinreichend häufig (z.B. jährlich) zu tun, denn die Gültigkeit über sechs Jahre ist eine Schätzung, keine Garantie.

4 Prinzipien der Beweiswerterhaltung

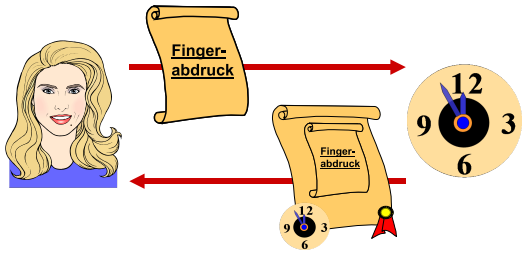

Abbildung 1. *Idee: Der Zeitstempeldienst bestätigt, dass ein Dokument zu einer gegebenen Zeit in dieser Form vorlag.*

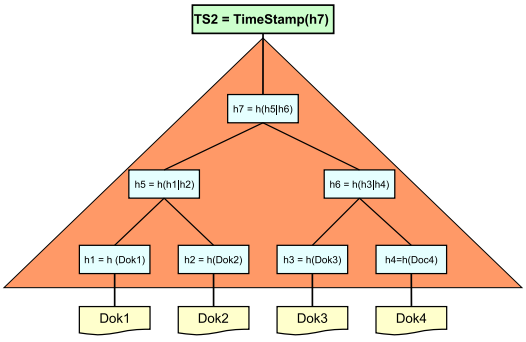

Abbildung 2. *Optimierung: Ein Hashbaum fasst sehr viele Dokumente zusammen. Die Wurzel (hier h7) repräsentiert alle Dokumente. Nur für sie wird ein Zeitstempel (TS1) eingeholt.*

Die Idee zur Werterhaltung digitaler Signaturen besteht darin, sie rechtzeitig zu erneuern. Die Erneuerung braucht dabei nicht durch den ursprünglichen Signierer zu erfolgen, sondern kann von einer Maschine geleistet werden. Nahe liegend ist die Benutzung eines Zeitstempeldienstes (Abb. 1), welcher den Hashwert eines Dokuments empfängt, die aktuelle Zeit hinzufügt und das so entstandene Konstrukt

mit seiner eigenen, auf aktuellen Algorithmen und Schlüssellängen beruhenden, digitalen Signatur versieht. Das Verfahren lässt sich optimieren, indem nicht jedes Dokument einzeln behandelt wird, sondern zunächst sehr viele Dokumente in einem Hashbaum zusammengefasst werden, dessen Wurzel alle Dokumente repräsentiert (Abb. 2). Nur für sie wird dann ein Zeitstempel eingeholt, der die Signaturen aller Dokumente erneuert. Der Zeitstempel ist ein signiertes Datum, unterliegt also auch einem Alterungsprozess. Aus diesem Grund wird er in den Archivierungsprozess integriert und seinerseits fortwährend erneuert. Das Verfahren ist massentauglich, effizient, kostengünstig und erfüllt die Anforderungen des Signaturgesetzes. Das hat der renommierte Rechtswissenschaftler Prof. Roßnagel in einem Gutachten festgestellt [3]. Es schützt sowohl gegen schwächer werdende Hashfunktionen als auch gegen Public-Key-Verfahren, die an Sicherheitseignung verlieren. Eine geschwächte Hashfunktion erfordert die Generierung neuer Hashwerte. In diesem (seltenen) Fall fordert ArchiSoft die Dokumente vom DMS an, um sie mit einer neuen Hashfunktion zu hashen. Für den häufiger vorkommenden Fall, dass Schlüssellängen an Wert verlieren, braucht das DMS nicht einbezogen zu werden, da lediglich die betroffenen Zeitstempel erneuert werden. Wichtig ist, dass die Signaturerneuerung stets rechtzeitig durchgeführt wird, bevor die eingesetzten Algorithmen ihre Beweiskraft verlieren. Nur dadurch lässt sich eine kryptographie-basierte Argumentationslinie aufrechterhalten. Die Beweiswerterhaltung digitaler Signaturen ist damit nicht durch einen einmaligen Vorgang erledigt, sondern ist ein kontinuierlicher Prozess. Einige Dokumentenformate bieten die Möglichkeit, einen Zeitstempel in das Dokument zu integrieren. Auf diese Weise lässt sich der Beweiswert der Signatur auch erhalten, allerdings steigen die Kosten mit der Anzahl der Dokumente stark an. Tabelle 1 vergleicht das dateibasierte Verfahren mit dem von ArchiSoft (s. Kap. 6) praktizierten Baumverfahren:

Anzahl Dokumente	Kosten pro Zeitstempel	Kosten ohne ArchiSoft	Kosten mit ArchiSoft
1.000.000	0,50	500.000	0,50
1.000.000	0,001	1.000	0,50

Tabelle 1. *Bei der Signaturerneuerung reduziert ArchiSoft die Kosten erheblich, weil für sehr viele Dokumente nur ein einziger Zeitstempel notwendig ist.*

In der zweiten Zeile wurde ein sehr großer Mengenrabatt für die Zeitstempel zugrunde gelegt. Selbst in diesem Fall erhält man mit ArchiSoft eine Kostenreduktion um den Faktor 2000 (!).

5 Revisionssicherheit

Das ArchiSoft-Baumverfahren lässt sich auch mit unsignierten Dokumenten sinnvoll verwenden. Diese Variante ist insbesondere dann indiziert, wenn in einem Anwendungskontext die Notwendigkeit besteht, alle Dokumente mit einem Zeitstempel zu versehen. Hier kann ArchiSoft als optimierender Zeitstempelclient eingesetzt werden, indem ArchiSoft einen Baum erzeugt und nur für dessen Wurzel einen Zeitstempel einholt. Die folgende Tabelle zeigt das dabei entstehende Einsparpotenzial:

Dokumente pro Tag	Kosten pro Zeitstempel	Kosten pro Tag ohne ArchiSoft	Kosten pro Tag mit ArchiSoft	Ersparnis pro Jahr
1.000	0,10	100	0,50	35.820
10.000	0,05	500	0,50	179.820

Tabelle 2. *Auch in Bezug auf Revisionssicherheit erzielt ArchiSoft durch das Baumverfahren eine starke Reduktion der Kosten.*

Selbst bei 1000 Dokumenten pro Tag bewirkt ArchiSoft eine starke Reduktion der Kosten.

6 Beweiswerterhaltung durch ArchiSoft

SIT hat mit ArchiSoft eine Software geschrieben, welche das oben beschriebene, hocheffektive Baumverfahren praktisch umsetzt. ArchiSoft lässt sich auf einfache Weise mit einem DMS verbinden und steuert selbständig den gesamten Erneuerungsprozess. Das Prinzip ist einfach (Abb. 3): Der DMS-Server wird um ein Plugin erweitert, das ihn in die Lage versetzt, mit ArchiSoft zu kommunizieren. Wenn er ein neues Dokument erhält, schickt er eine Nachricht an ArchiSoft. Das System sorgt in der Folge dafür, dass rechtzeitig Hashbäume gebildet und Zeitstempel angefordert werden.

Nachdem ein Hashbaum gebildet wurde, kann ArchiSoft zu jedem Dokument ein *Evidenzdokument* (evidence record, kurz eRecord) liefern. Dieses enthält den Ausschnitt des Baumes, der notwendig ist, um das Dokument zu verifizieren, sowie weitere Daten (OCSP-Auskünfte, Sperrlisten, Zertifikate), welche in die spä-

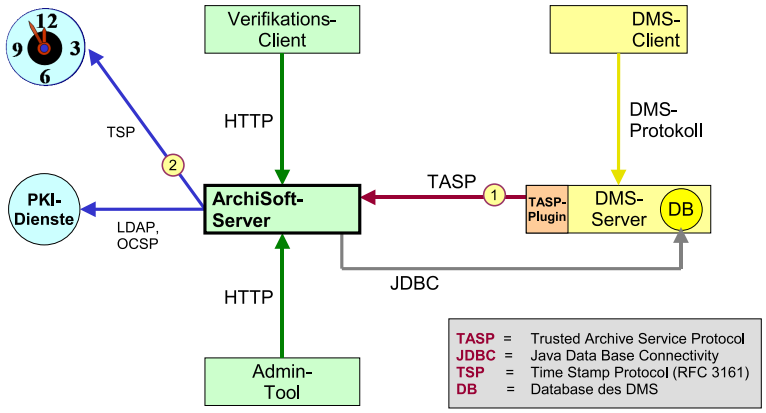

Abbildung 3. *Anbindung von ArchiSoft an ein DMS: Der DMS-Server informiert ArchiSoft über ein neues Dokument, indem er eine Referenz und den Hashwert sendet (1). Nachdem ArchiSoft einen Baum aufgebaut hat, fordert der Server einen Zeitstempel für die Wurzel an und erneuert damit die Signaturen aller Dokumente auf einmal (2).*

tere Prüfung einfließen. Für die Verifikation bietet ArchiSoft einen eigenen Client. Es ist aber durchaus alternativ möglich, das Verifikationsdokument auf einen Datenträger zu schreiben und es von einer anderen Stelle, z.B. einem gerichtlichen Gutachter, verifizieren zu lassen. Daten, die im Laufe der Archivierung anfallen, beispielsweise die Hashwerte der Dokumente, legt ArchiSoft in eigenen Tabellen ab, die in der Datenbank des DMS geführt werden. Die dazu erforderliche JDBC-Schnittstelle (Java Database Connectivity) wird von jeder relevanten Datenbank angeboten. ArchiSoft arbeitet mit jedem RFC 3161-konformen Zeitstempeldienst zusammen. Die Qualitätsanforderungen (z.B. Akkreditierung) an den Zeitstempeldienst werden durch den Anwendungskontext bestimmt.

7 ArchiSoft als Service

Einige Nutzer signierter Dokumente möchten Signaturen erneuern, ohne einen ArchiSoft-Server zu betreiben. Zu diesen Nutzern gehören sowohl Anwender mit sehr komplexen Dokumentenmanagementensystemen (DMS), als auch solche, die gar kein DMS betreiben. Sie alle können trotzdem ihre Signaturen erneuern, indem sie einen Dienstleister in Anspruch nehmen. Das Prinzip ist einfach (Abb. 4):

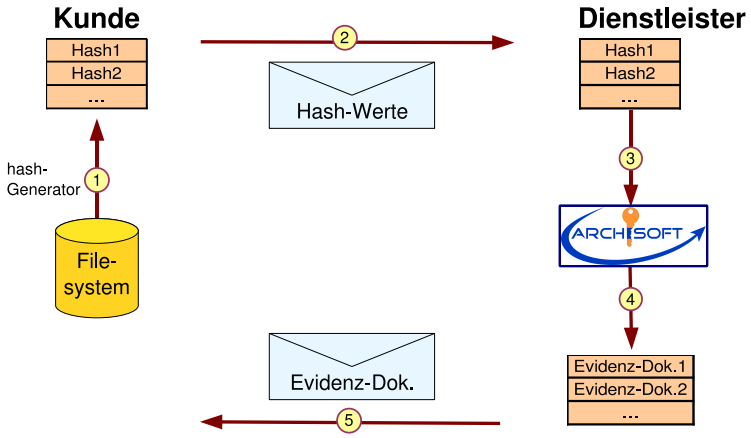

Abbildung 4. *ArchiSoft als Service: Der Kunde erzeugt (1) Hashwerte seiner Dateien, schickt (2) sie an den Dienstleister, der sie in ArchiSoft einliest (3), einen Baum bildet und Evidenzdokumente exportiert (4), die er schließlich an den Kunden sendet (5).*

Der Nutzer erzeugt Hashwerte seiner Dateien und schickt sie an den Dienstleister, der mit Hilfe von ArchiSoft Hashbäume erzeugt, aus denen schließlich Evidenzdokumente generiert werden. Die Evidenzdokumente werden zurück an den Nutzer geschickt. Eine Verifikationsapplikation erlaubt es ihm, aus den Evidenzdokumenten und den Dokumenten den Beweiswert seiner Dokumente darzulegen.

Wenn die Dateien des Kunden im Filesystem vorliegen, kann das von SIT bereitgestellte Tool *hashGenerator* die Hashwerte für ArchiSoft erzeugen. *hashGenerator* erhält ein Verzeichnis als Eingabeparameter und berechnet dann Hashwerte für alle Dateien in diesem Verzeichnis, sowie rekursiv für alle Dateien in Unterverzeichnissen. Mit weiteren Tools können Zeitstempel und ganze Hashbäume erneuert werden. Auf diese Weise kann die komplette ArchiSoft-Funktionalität genutzt werden, ohne dass der Kunde eine ArchiSoft-Installation benötigt. Für viele kleine und mittlere Unternehmen ist das eine optimale Lösung.

8 Zusammenfassung

ArchiSoft bietet die folgenden Leistungsmerkmale:

Kosteneffizienz ArchiSoft verwendet Zeitstempel äußerst effizient. Wo andere Lösungen 1.000.000 Zeitstempel benötigen, verwendet ArchiSoft einen einzigen. Die Kosten eines Zeitstempels werden dadurch irrelevant.

Vollständige Prozess-Steuerung Nachdem ArchiSoft einmalig durch den DMS-Server über die Existenz eines neuen Dokuments informiert wurde, übernimmt ArchiSoft die komplette Steuerung aller Signaturerneuerungszyklen. Dadurch wird die unerlässliche Kontinuität des Prozesses gewährleistet.

Integrierbarkeit in (fast) jedes DMS Über das TASP-Protokoll kann ArchiSoft sehr leicht mit einem DMS-Server verbunden werden. Java-fähige DMS-Systeme können darüberhinaus über die *Connection-API* innerhalb kürzester Zeit angebunden werden.

Erfüllung gesetzlicher Anforderungen ArchiSoft setzt die Anforderungen nach §6 SigG und §17 SigV um. Damit werden teure und aufwändige Streitfälle vermieden.

Eignung für große Datenmengen Die in ArchiSoft eingesetzten Hashbäume machen das System effizient, massentauglich und kostengünstig.

Verifikationsclient Von ArchiSoft generierte Evidenzdokumente können mittels des eigenen Verifikationsclients überprüft werden. Zusätzlich können sie für die Verifikation durch andere RFC4998-konforme Applikation als Dateien exportiert werden.

Administrationstool ArchiSoft besitzt ein eigenes Administrationstool, mit dessen Hilfe alle Parameter des Systems eingestellt werden können.

Formalisierung der Sicherheitseignung Die Bundesnetzagentur gibt einmal jährlich eine Bekanntmachung über die Sicherheitseignung von Hashfunktionen und Signaturverfahren heraus. ArchiSoft enthält ein Tool, um diesen Text in Interaktion mit einem Benutzer gemäß [2] zu formalisieren. Das so erzeugte maschinenverständliche XML-Dokument kann über das Administrationstool eingelesen werden.

Geschrieben in Java Durch die Implementierung in Java ist die Software plattformübergreifend einsetzbar und viele Fehler, etwa durch eine fehlerhafte Speicherverwaltung, können prinzipbedingt gar nicht erst auftreten. Zurzeit besteht ArchiSoft aus 700 Klassen, verteilt auf 152.000 Zeilen.

9 Über das Institut für Sichere Informationstechnologie SIT

SIT gehört zu den Pionieren auf dem Gebiet der IT-Sicherheit. Das Institut hat in zahlreichen nationalen und internationalen Projekten umfangreiche Expertise sowohl im konzeptionellen als auch im implementierungstechnischen Bereich erworben. ArchiSoft basiert auf Erkenntnissen aus dem ArchiSig-Projekt, das von SIT initiiert wurde. ArchiSig wurde durch das BMWi im Rahmen des VERNET-Programms gefördert. Die Ergebnisse wurden zusammen mit Richtern und Anwälten in fiktiven Gerichtsprozessen überprüft. SIT engagiert sich in der Standardisierung. Im nationalen Bereich hat SIT zur ISIS-MTT-Spezifikation beigetragen. Im internationalen Umfeld hat SIT zusammen mit den ArchiSig-Projektpartnern in [1] die Struktur für Evidenzdokumente festgelegt, die bereits von ArchiSoft umgesetzt wird. Zurzeit wird unter der Federführung von SIT ein IETF-Standard vorbereitet, der die Sicherheitseignung von Algorithmen formalisiert. Der Draft [2] ist weit fortgeschritten und wird in Kürze zum RFC werden.

Literatur

[1] T. GONDROM, R. BRANDNER und U. PORDESCH: *Evidence Record Syntax (ERS)*. RFC 4998, Internet Engineering Task Force, August 2007.

[2] T. KUNZ, S. OKUNICK und U. PORDESCH: *Data Structure for the Security Suitability of Cryptographic Algorithms (DSSC), INTERNET-DRAFT draft-ietf-ltans-dssc-09.txt, expires December 17, 2009*, Juni 2009.

[3] PROF. DR. ALEXANDER ROSSNAGEL: *Signaturgesetzkonformität des Standardisierungsvorschlages „Long-Term Conservation of Electronic Signatures“ für die ISIS-MTT Spezifikation vom 30.6.2004*. `http://www.teletrust.de/fileadmin/files/ag8_isis-mtt-gutachten-langzeitsig.pdf`, Juli 2004.