

Archivierung  
von Dokumenten der  
elektronischen Nachweisführung  
(eANV)

Consist ITU  
Environmental Software GmbH  
23.02.2009

Für die elektronischen Dokumente gemäß Nachweisverordnung sind qualifizierte elektronische Signaturen vorgeschrieben, die auch gemäß den gesetzlichen Regelungen archiviert werden müssen.

Die Dokumente haben eine Aufbewahrungsfrist von mindestens acht Jahren. Die Aufbewahrungsfrist ergibt sich aus einer bis zu fünfjährigen Laufzeit für Entsorgungsnachweise und der minimalen Registrierungsdauer für registerpflichtige Belege von drei Jahren gemäß Nachweisverordnung (§25 Abs. 1). Außerdem sind die Dokumente Handelsbriefe, für die ebenfalls nach Handelsgesetzbuch (HGB §257) eine Archivierungspflicht von zehn Jahren besteht.

Die ordnungsgemäße Archivierung bedingt dabei die Erhaltung der Gültigkeit der elektronischen Signaturen nach den Anforderungen des SigG und der SigV.

## 1 Modawi-Lösung

Da die Erhaltung der Gültigkeit von Signaturen nicht uneingeschränkt nachträglich erfolgen kann, beinhaltet die Modawi-Lösung ein Langzeitarchiv für Signaturen nach ArchiSig. Der im Leistungsumfang von Modawi enthaltene Signaturserver SecPKI archiviert automatisch alle über ihn signierten oder geprüften Signaturen nach ArchiSig. Durch eine regelmäßige Übersignatur der Wurzeln der Hashbäume mit qualifizierten Zeitstempeln wird die Integrität der archivierten Signaturen sichergestellt. Die notwendigen qualifizierten Zeitstempel müssen von einem Trustcenter oder einem anderen geeigneten Zeitstempeldienst bezogen werden.

Modawi stellt beim Empfang von Dokumenten sicher, dass die enthaltenen Signaturen geprüft und damit ins Signaturarchiv aufgenommen werden.

Beweisdokumente zur Gültigkeit von Signaturen können bereits mit der aktuellen Version über die entsprechenden Werkzeuge generiert werden bzw. die Nachweisinformationen als Evidence Record (nach RFC 4998) bereitgestellt werden. Eine Prüfung von „alten“ Signaturen ist damit auch Dritten möglich. Natürlich kann die Modawi-Lösung auf dieser Basis auch „alte“ Signaturen prüfen. Künftige Modawi-Versionen werden die Generierung von Beweisdokumenten auch komfortabel in der Modawi-Schnittstelle anbieten.

In der BMU-Schnittstelle ist der Austausch dieser Evidence-Records aber derzeit noch nicht genau spezifiziert, so dass hier Anpassungen wahrscheinlich sind.

Da die Dokumente in der Abfallwirtschaft bereits im XML-Format vorliegen, ist ein zusätzlicher XML-Container nach ArchiSafe nicht notwendig.

Modawi stellt eine umfassende Lösung zur Bearbeitung und Archivierung von elektronisch signierten Dokumenten zur Verfügung, bei deren Einsatz wir gerne unterstützen.

## 2 Hintergrundinformationen

### 2.1 Archivierung von elektronisch signierten Dokumenten

Zur Archivierung elektronisch signierter Dokumente, müssen sowohl die Dokumente sicher gespeichert, als auch die Signatur archiviert werden. Das Signaturarchiv erfüllt drei Aufgaben:

- 1) Dokumentation der Signaturzertifikatsgültigkeit zum Zeitpunkt des Erhalts
- 2) Erhaltung der Signaturgültigkeit durch Übersignatur mit qualifizierten Zeitstempeln
- 3) Erzeugen von Nachweisen, dass die Signatur im Archivierungszeitraum immer gültig war (Integritätsnachweis)

Die Signaturarchivierung muss zunächst dokumentieren, dass die Signatur mit einem gültigen Signaturzertifikat erstellt wurde. Da Trustcenter immer nur über den aktuellen Status der ausgegebenen Zertifikate Auskunft geben, ist es also notwendig, eine erhaltene Signatur und deren Zertifikat schnellstmöglich zu prüfen und dieses zu dokumentieren. In der Praxis speichert man das Ergebnis der Zertifikatsprüfung, die man in signierter Form mit Zeitangabe vom Trustcenter erhält (signierter OCSP-Response) im Signaturarchiv.

Durch leistungsfähigere Rechner und Fortschritte in der Kryptoanalyse werden Signaturen im Laufe der Zeit unsicher. Die Signatur besteht aus einem Hashwert über das Dokument und der Verschlüsselung des Hashwertes mit dem Private-Key des Signierenden.

Ein Signaturarchiv stellt nun durch Übersignieren mit aktuellen Verschlüsselungsfunktionen per Zeitstempel sicher, dass die Integrität der Ursprungssignatur nachgewiesen werden kann. Wird jedoch die Hashfunktion unsicher, so müssten auch die Hashwerte über die Dokumente erneuert werden.

Unsicher werden der Hashfunktion ist mit der aktuell verwendeten SHA256-Hashfunktion sehr unwahrscheinlich und auch mangels einer geeigneten Alternative zurzeit nicht absicherbar. Neue Hashfunktionen sind in der Entwicklung, werden aber nicht vor 2012 bereitstehen. Außerdem wird es wirtschaftlicher sein, sich geeignete Verfahren zur Signaturabsicherung zu überlegen, wenn sich eine nennenswerte Unsicherheit abzeichnet (Information der BNetzA zu Kryptoalgorithmen). Es ist sehr wahrscheinlich, dass man nicht jedes Dokument neu hashen muss, sondern größere Blöcke bilden kann. Die Voraussetzung für ein Absicherungsprojekt ist ein vom Dokumentenarchiv getrenntes Signaturarchiv mit gültigen Signaturen.

## 2.2 Lösungsansätze

Für die Archivierung von signierten Dokumenten bestehen auf dem Markt unterschiedliche Lösungsansätze: das Konzept ArchiSig, die Software ArchiSoft des SIT und das Projekt ArchiSafe:

Bereits 2004 wurde im Rahmen des ArchiSig-Projektes ein Verfahren vorgestellt, wie man Signaturen sehr effizient erhalten kann. Es werden die Hashwerte mit den OCSP-Responses (Zertifikatsprüfungen) in sogenannten Hashbäumen gespeichert und die Werte darin wiederum durch Hashwerte gesichert. Durch die Baumstruktur müssen nun nur die Wurzeln der Hashbäume mit Zeitstempeln übersigniert werden. Mit wenigen Zeitstempeln kann so die Signaturerhaltung für viele Dokumente erfolgen. Das Verfahren ist durch ein Rechtsgutachten („Rechtsgutachten zur Signaturgesetzkonformität des Standardisierungsvorschlags „Long-Term Conservation of Electronic Signatures für die ISIS-MTT Spezifikation vom 30.06.2004“ (ArchiSig) vom 20.07.2004“ von Prof. Dr. Alexander Roßnagel) abgesichert. Das ArchiSig-Konzept wird auch in der Modawi-Lösung verwendet.

Auf Basis von ArchiSig hat das Fraunhoferinstitut für Sicherheit in der Informationstechnologie (SIT) die Software ArchiSoft entwickelt.

ArchiSafe ist ein Projekt der Physikalisch Technischen Bundesanstalt (PTB), welches ein Verfahren für die Langzeitarchivierung von Dokumenten (auch elektronisch signierter Dokumente) zum Ergebnis hatte. Langzeitarchivgeeignete Dokumente (TIFF, PDF/A, Text) werden mit Metainformationen in XML-Containern archiviert, und es erfolgt Signaturerhaltung nach ArchiSig. Das Projekt adressiert neben der Signaturarchivierung auch, dass die langfristige Wiedergabe der Dokumente gesichert sein muss. Deshalb erfolgt eine Beschränkung auf wenige geeignete Formate. Ferner werden die Anforderungen der Behörden berücksichtigt, die im DOMEA-Konzept für elektronische Akten definiert sind. ArchiSafe hat 2008 auch ein Protection Profile für derartige Systeme beim BSI veröffentlicht. Es ist jedoch bisher kein System dokumentiert, welches danach geprüft wurde.