Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Dipl.-Inform. Michael Herfert
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-329
Fax 06151 869-322
michael.herfert@sit.fraunhofer.de
www.sit.fraunhofer.de/archisoft

ARCHISOFT

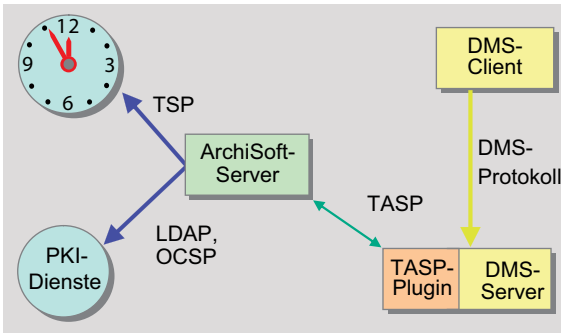
LANGZEITARCHIVIERUNG VON ELEKTRONISCHEN DOKUMENTEN

Elektronische Geschäftsprozesse in Wirtschaft und Verwaltung brauchen sichere und dauerhafte elektronische Signaturen für Dokumente – nur so wird eine papierlose und dennoch revisionssichere Abwicklung erst möglich.

Zum Teil sind extrem lange Aufbewahrungspflichten solcher Dokumente vom Gesetzgeber vorgeschrieben, zum Beispiel 30 Jahre im Gesundheitswesen. Das gilt auch für die elektronischen Signaturen – diese aber können veralten, »verblassen«, weil sie eventuell mit Verfahren erzeugt wurden, die aufgrund des technischen Fortschritts nicht mehr sicher genug sind. In einem Streitfall kann dies dazu führen, dass die Signatur vor Gericht ihren kryptographischen Beweiswert verliert. Mit »ArchiSoft« jedoch behalten Signaturen und damit Dokumente ihren Wert und können in Streitfällen weiter zuverlässig vor Gericht eingesetzt werden.
Das vom Fraunhofer-Institut SIT entwickelte Softwarepaket ArchiSoft aktualisiert Signaturen bei Bedarf, bevor sie veralten. Besonders kostengünstig wird es durch die Einbindung in vorhandene Dokumentenmanagement-Systeme (DMS): Es bündelt vorhandene Dokumente samt ihren Signaturen zu einem Baum und teilt ihnen gemeinsam eine neue, schwerer als bisher zu brechende Signatur zu, statt jedes einzeln zu signieren. Diese Methode ist international akzeptiert und wurde in der Norm RFC 4998 unter der Mitwirkung des SIT festgelegt. RFC 4998 spezifiziert weiterhin sogenannte Evidenzdokumente. Diese Evidenzdokumente werden aus dem Baum extrahiert und beglaubigen die Gültigkeit der digital signierten Dokumente. Schon bei konservativer Schätzung sind durch die Bündelung Kosteneinsparungen um den Faktor 2000 möglich, in der Praxis wahrscheinlich eher mehr. Außer für DMS steht ArchiSoft auch als Dienstleistung und als Mailserver-Bestandteil zur Verfügung.

Professionelles Softwarepaket

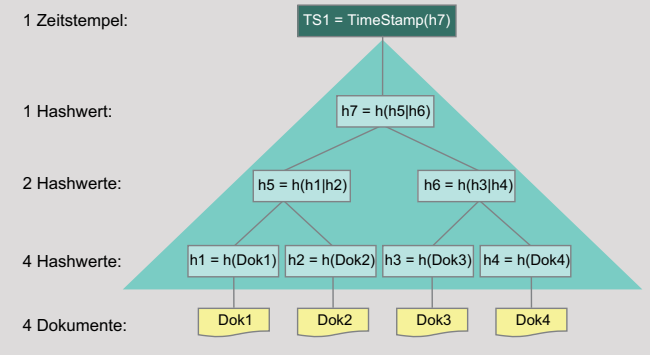
Das Softwarepaket ArchiSoft sorgt dafür, dass digitale Signaturen auch über Jahrzehnte beweissicher sind, gleichgültig, ob es sich um die Signaturen eigener Dokumente oder die von Geschäftspartnern handelt. ArchiSoft ist in Java geschrieben und läuft daher auf allen wesentlichen Plattformen. SIT vermarktet ArchiSoft zusammen mit gewerblichen Partnern, die den notwendigen Support und Hotline zu dem professionellen Software-Produkt bieten.



ArchiSoft arbeitet hervorragend mit Dokumentenmanagement-Systemen zusammen.

Einfache Integration in DMS

ArchiSoft lässt sich sehr einfach mit den allermeisten DMS-Servern verbinden. Dazu muss auf der Seite des DMS-Servers nur ein kleines Plug-In ergänzt werden, das sehr einfach zu programmieren ist. Es kommuniziert über das TASP-Protokoll (Trusted Archive Service Protocol) mit dem ArchiSoft-Server. Nachdem der DMS-Server einmalig die Existenz eines Dokumentes an ArchiSoft gemeldet hat, kann er das Problem der »verblassenden« Signaturen von seiner Agenda streichen – ArchiSoft übernimmt die Steuerung des kompletten Zyklus.



ArchiSoft vergibt Zeitstempel für mehrere Dokumente gemeinsam und senkt damit Kosten.

ArchiSoft als Service

Unternehmen, die nicht in einen eigenen ArchiSoft-Server investieren möchten, können bei SIT-Partnern ArchiSoft als Service nutzen. Das Prinzip ist einfach: Der Kunde erzeugt Hashwerte seiner Dateien und schickt sie an den Dienstleistungspartner, der mit Hilfe von ArchiSoft Hashbäume erzeugt, aus denen schließlich Evidenzdokumente generiert werden. Die Evidenzdokumente werden zurück an den Nutzer geschickt.

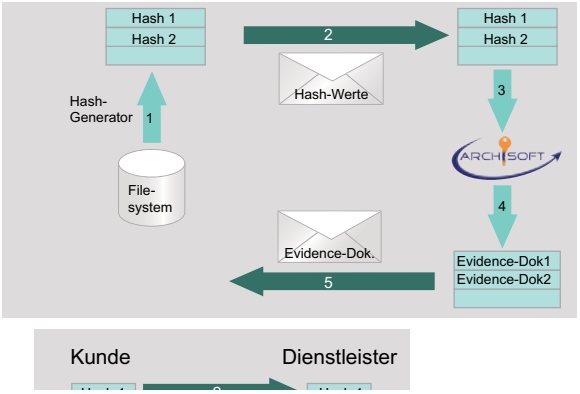
Eine Verifikationssoftware erlaubt es dem Nutzer, aus den Evidenzdokumenten und den dazugehörigen eigentlichen Dokumenten den Beweiswert seiner Dokumente zu belegen. Ein Richter oder ein Gutachter kann unabhängig von dem Nutzer den Beweiswert selbständig nachvollziehen. Alle Beweise beruhen auf kryptographischen Argumenten. Dadurch ist die Beweiskette sehr viel stärker, als sie es wäre, wenn man sich bei der Echtheit der Signaturen allein auf den ordnungsgemäßen Betrieb zertifizierter Systeme berufen würde.

ArchiSoft im Mailserver

Auch für unsignierte Dokumente ist der Einsatz von ArchiSoft sinnvoll. Hier trägt ArchiSoft zur Revisionssicherheit bei, ganz ohne teure Spezialhardware. Durch die Integration in einen Mailserver sind auch revisionssichere Mailarchive mit wenig Aufwand möglich.

Zeitstempel schützen Signaturen

ArchiSoft schützt Signaturen durch die Integration von Zeitstempeln. Dazu greift das System auf externe Zeitstempelserver zurück. ArchiSoft holt aber nicht für jedes einzelne Dokument einen Zeitstempel ein – das wäre ineffizient –, sondern baut aus



ArchiSoft als Service ist ein Angebot an Unternehmen, die ArchiSoft nicht selber betreiben möchten.

vielen Dokumenten einen »Baum« auf, dessen Wurzel für alle Dokumente steht. Nur für die Wurzel, die sehr viele Dokumente repräsentiert, wird ein Zeitstempel eingeholt. Da die Wurzel aus einem Hashwert besteht, erfährt der Betreiber des Zeitstempelservers absolut nichts über die Inhalte der so signierten Dokumente. Auch die Kosten des Zeitstempels fallen damit kaum noch ins Gewicht.

Alte Signaturen haben ihren Sicherheitsstatus verloren

Am 31.3.2008 verloren Signaturen, die mit Schlüsseln der Länge 1024 Bit geleistet wurden, ihren bisherigen Sicherheitswert. Das hat die dafür zuständige Bundesnetzagentur in einer amtlichen Veröffentlichung festgelegt.

Damit gelten alte Signaturen, die bis Ende 2007 mit signaturgesetzkonformen Karten geleistet wurden, jetzt als »kryptographisch verblasst«. Das Signaturgesetz schreibt aber vor, dass Signaturen zu erneuern sind, wenn sie ihren Beweiswert behalten sollen. ArchiSoft nimmt diese Erneuerung vor, kostengünstig und effizient. Wer noch nicht gehandelt hat, sollte jetzt schnellstmöglich seine Signaturen mit ArchiSoft auffrischen.

SYSTEMVORAUSSETZUNGEN

Prozessor:
empfohlen Intel Core 2 Duo mit 2,0 GHz

Arbeitsspeicher:
empfohlen mind. 2 GB

Festplatte:
mind. 110 MB für die Installation

Betriebssysteme:
Windows Server 2008, Windows Server 2003, Windows XP Professional, Windows Vista, Linux, Solaris

Java Runtime Environment: Benötigt wird eine Java Runtime Environment (JRE) Version 5 oder 6

Datenbanken:
Microsoft SQL Server 2008, Microsoft SQL Server 2005, Microsoft Server 2000, Oraces 9i, Oracle 10g, MySQL 5, PostgresSQL 8 sowie prinzipiell jede Datenbank mit JDBC-Schnittstelle

Schnittstellen:
Java-API und WebService-Schnittstelle zu Dokumentenmanagement-System bzw. Archiv

Zeitstempeldienste:
RFC3161 (TSP) -konforme Zeitstempeldienste mit optionaler Authentifizierung über HTTP(S) oder CMS-Signatur