

Langzeit-Beweiswerterhaltung elektronischer Dokumente



gesetzeskonforme Langzeit-
Beweiswerterhaltung
elektronisch signierter
Dokumente

Nachweis von
Veränderungen elektronisch
archivierter Dokumente

Basis: ArchiSig & internatio-
naler LTANS/ERS-Standard

schnelle Verarbeitung
großer Dokumentenmengen
durch effizientes
Hash-Baum-Verfahren

Elektronische Signaturen werden auf Basis
kryptographischer Algorithmen erstellt, die
eine bestimmte Stärke bzw. Sicherheit
besitzen. Mit dem technischen Fortschritt
nimmt diese Stärke ab, z.B. bei schnelleren
Rechnern.

Um eine ggfs. notwendige Langzeit-Beweis-
werterhaltung bestimmter Daten und Doku-
mente (z.B. Akten im Sozialversicherungsw-
esen, Patientenakten in Einrichtungen des ge-
sundheitswesens) zu gewährleisten, müssen
digitale Signaturen regelmäßig mittels aktu-
eller, 'geeigneter' Algorithmen erneuert wer-
den. Dieser Vorgang wird allgemein als
„Übersignieren“ bzw. „Nachsignieren“ be-
zeichnet und ist in Deutschland gesetzlich in
§17 Signaturverordnung (SigV) geregelt.

Dauerhafte Beweiswerterhaltung auf Basis internationaler Standards

Die Softwarelösung digiSeal® archive von
secript signiert auf Basis des ArchiSig-Konzepts
vorhandene signierte Daten rechtzeitig, sicher
und effizient nach.

Dabei setzt sie den internationalen LTANS/ERS-
Standard (Long-Term Archive and Notary Servi-
ces / Evidence Record Syntax) der IETF (Internet
Engineering Task Force) ein und verwendet je-
weils gesetzeskonforme amtliche Zeitstempel.
Diese beruhen auf Algorithmen, die das Bundes-
amt für Sicherheit in der Informationstechnik
(BSI) als geeignet und sicher einstuft.

So ermöglicht digiSeal® archive dauerhafte Be-
weiswerterhaltung und Manipulationsschutz von
digitalen Daten in Kombination mit Archiv- und
Dokumenten-Management-Systemen (DMS).

Leistungsmerkmale

- automatisierter Hintergrunddienst
- Umsetzen des internationalen
LTANS/ERS-Standards der IETF
- Dokumentation aller durchgeführten
Prozessschritte in einer Logdatei
- Aufbringen von Zeitstempeln der folgen-
den akkreditierten Anbieter:
D-TRUST (Bundesdruckerei), Telesec
(T-Systems), Signtrust (Deutsche Post)
- Verwaltung von Hash-Bäumen,
(Zeitstempel-) Signaturinformationen und
Datenstrukturen in Standard-Datenbank

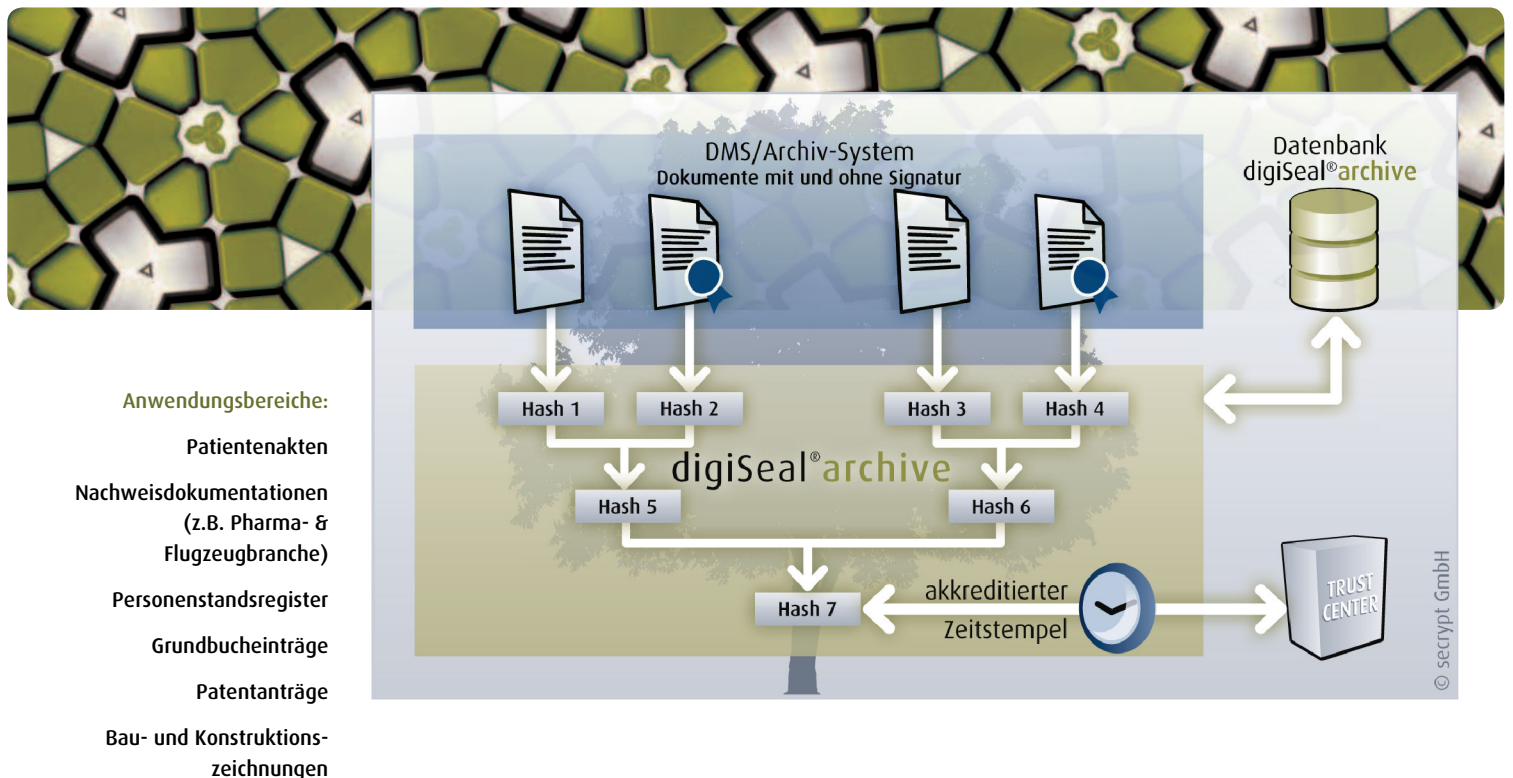


secript GmbH
Bessemerstraße 82
D-12103 Berlin

Fon: +49 (0)30.756 59 78-0
Fax: +49 (0)30.756 59 78-18

sales@secript.de
www.secript.de

Aus sicherer Quelle. **secript**



Verarbeitung vieler Dokumente mit effizientem Hash-Baum-Verfahren

Sämtliche Dokumente, die für das Erneuern ihrer Signatur zu verarbeiten sind, werden in einer effizienten Baumstruktur angeordnet. Über die Dokumente werden jeweils eindeutige kryptographische Prüfsummen (Hash-Werte) gebildet. Diese werden immer weiter zusammengefasst, so dass an der Wurzel des Baumes ein einziger Hash-Wert entsteht. Dieser Wert, der den gesamten Baum mit allen Dokumenten repräsentiert, wird mit einem einzigen Zeitstempel versehen. So hat man alle Signaturen erneuert und den Beweiswert der Dokumente voll erhalten - bei minimalen Zeitstempelkosten.

digiSeal® archive verwaltet sämtliche Hash-Werte, Hash-Bäume sowie Zeitstempelinformationen in einer separaten Standard-Datenbank. Die zugehörigen Dokumente verbleiben im DMS bzw. Archiv und sind über ein eindeutiges Identifikationsmerkmal (Dok-ID) mit den entsprechenden Hash-Bäumen verbunden.

Systemvoraussetzungen & Technik

Betriebssysteme Windows

Server: 2008 und 2003 / Windows® 7 SP1, Vista SP2, XP Professional SP3 / 2000 SP4

Betriebssysteme Linux

SUSE Linux Enterprise Server 10 und 11, openSUSE ab 11

Prozessor

aktueller Prozessor, z.B. Intel Core2Duo oder AMD Athlon ab 2,5 GHz

Arbeitsspeicher (RAM)

mindestens 2 GB

Festplatte

mindestens 50 MB freier Festplattenspeicher für Basis-Installationspaket

Datenbank

Oracle 10 und 11, MySQL 5.1, Microsoft SQL Server 2005 und 2008, DB2 mit 32-bit ODBC Schnittstelle

Schnittstelle

C- und JAVA-API-Schnittstelle zu Archiv- bzw. Dokumenten-Management-System

Ansprache der Zeitstempeldienste

per TSP mit optionaler Authentifizierung über HTTP, HTTPS, SSL und TLS; konform zu time-stamp protocol RFC 3161



ein Produkt der

secript GmbH
Bessemerstraße 82
D-12103 Berlin

Fon: +49 (0)30.756 59 78-0
Fax: +49 (0)30.756 59 78-18

sales@secript.de
www.secript.de