

# digiseal® archive

## Langzeit-Beweiswerterhaltung elektronischer Dokumente im eArchiv

### Highlights

eIDAS ready

Gesetzeskonforme Langzeit-Beweiswerterhaltung Elektronisch signierter Dokumente

Nachweis von Veränderungen elektronisch archivierter Dokumente

Basis: ArchiSig & internationaler LTANS/ERS-Standard

Schnelle Verarbeitung großer Dokumentenmengen durch effizientes Hash-Baum-Verfahren



### Anforderung

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

Um eine gegebenenfalls notwendige Langzeit-Beweiswerterhaltung bestimmter Daten und Dokumente (z.B. Akten im Sozialversicherungswesen, Patientenakten in Einrichtungen des Gesundheitswesens) zu gewährleisten, müssen digitale Signaturen regelmäßig mittels aktueller, 'geeigneter' Algorithmen erneuert werden. Dieser Vorgang wird allgemein als ‚Übersignieren‘ bzw. ‚Nachsignieren‘ bezeichnet.

### Dauerhafte Beweiswerterhaltung auf Basis internationaler Standards

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

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

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

### Leistungsmerkmale

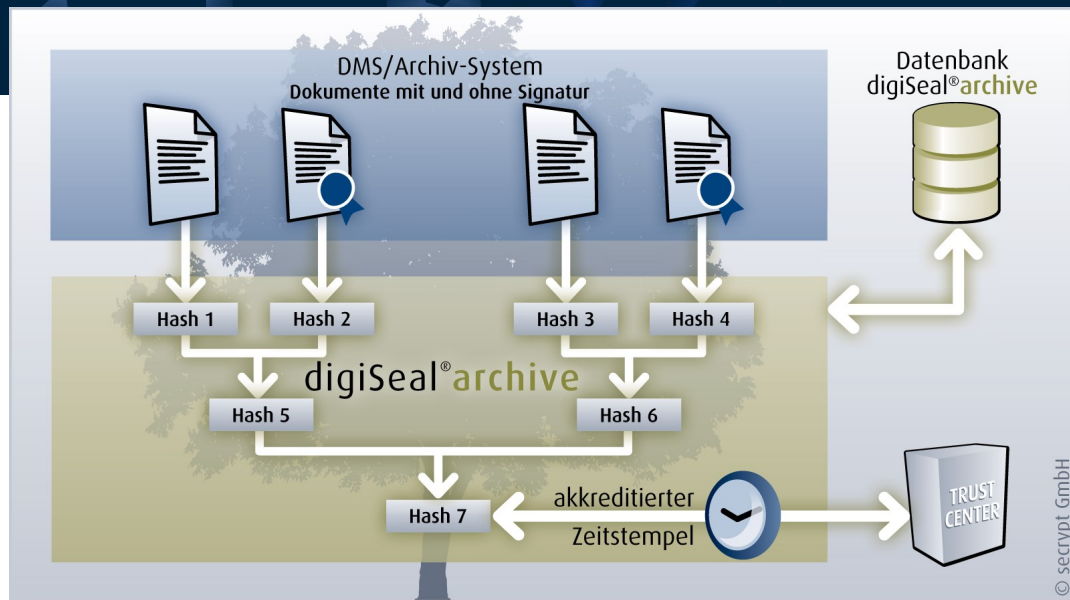
- Automatisierter Hintergrunddienst
- Umsetzen des internationalen LTANS/ERS-Standards der IETF
- Dokumentation aller durchgeführten Prozessschritte in einer Logdatei
- Aufbringen von Zeitstempeln akkreditierter Anbieter z.B. D-TRUST (Bundesdruckerei)
- Verwaltung von Hash-Bäumen, (Zeitstempel-) Signaturinformationen und Datenstrukturen in Standard-Datenbank

### Anwendungsbereiche (Beispiele)

- Patientenakten
- Nachweisdokumentationen (z. B. Pharma- & Flugzeugbranche)
- Personenstandsregister
- Grundbucheinträge
- Patentanträge
- Bau- und Konstruktionszeichnungen



# digiSeal®archive Dauerhafte elektronische Beweiswerterhaltung



## 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.

Somit wurden alle Signaturen erneuert und der Beweiswert der Dokumente voll erhalten — bei minimalen Zeitstempelkosten.

digiSeal®archive verwaltet sämtliche Hash-Werte, Hash-Bäume sowie Zeitstempelinformationen in einem Datenbanksystem, wie z.B. dem Microsoft SQL Server. 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 (x64)

Windows Server 2022 / 2019 / 2016 / 2014 / 2012 R2 / 2012  
Windows 11 / 10 / 8.1 / 8

### Betriebssysteme Linux (x64)

RedHat Linux Enterprise 7 / 8

### Prozessor

aktueller Prozessor

### Arbeitsspeicher (RAM)

mindestens 4 GB

### Festplatte

mindestens 500 MB freier Festplattenspeicher für Basis-Installationspaket

### Datenbank

Microsoft SQL Server 2005 / 2008 / 2012 / 2014 / 2016 / 2017 / 2019,  
Oracle 10g / 11g / 12c / 19c,  
MySQL 5.6 / 8.0

### 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

SecurITy  
made  
in  
Germany

TeleTrust Quality Seal  
www.teletrust.de/itsmig

© secript GmbH

Tel.: +49 30 7565978-0  
Fax: +49 30 7565978-18

sales@secript.de  
www.secript.de

Haftungsausschluss: Alle Rechte sowie Druckfehler, Irrtümer und Änderungen vorbehalten.  
Stand: 2023/05

Seite 2 / 2