Servicebeschreibung

SecDocs Archive Service

Digital Signature and Preservation Services

Basisdienst für die beweiswerterhaltende Langzeitarchivierung auf Basis offener Standards

Digitale Langzeitarchivierung

Die Archivierung von Dokumenten in digitaler Form bietet viele Vorteile gegenüber papiergebundenen Archiven: Die Aufbewahrung ist kostengünstiger und die Dokumente können erheblich schneller und billiger transportiert werden. Digitale Dokumente unterliegen auch keiner physikalischen Alterung, die zum Beispiel durch Zerfall von Papier und Tinte Dokumente unlesbar machen kann.

Damit digitale Archive die papiergebundenen Archive vollwertig ersetzen können, müssen zwei technische Voraussetzungen erfüllt sein. Zunächst müssen die Formate der digitalen Dokumente langfristig garantiert und unabhängig von einer bestimmten Service-Landschaft lesbar bleiben. Diese Anforderung kann durch akzeptierte Standarddokumentenformate wie PDF-A oder TIFF ausreichend erfüllt werden. Außerdem muss der Nachweis der Integrität und Authentizität digitaler Dokumente während der gesamten Aufbewahrungsfrist möglich sein. Digitale Signaturen und manipulationssichere Speichermedien bieten hier jeweils nur einen endlichen Schutz: Die Lebensdauer von Speichermedien ist begrenzt, und digitale Signaturen werden durch den technischen Fortschritt zunehmend schwächer.

...mit Erhaltung der Beweiskraft

Hier setzt SecDocs Archive Service an und erlaubt die Archivierung von Dokumenten in einer Form, die deren Beweiskraft über einen beliebig langen Zeitraum garantiert. SecDocs Archive Service stützt sich dabei auf Ergebnisse der Projekte ArchiSig (digitale Übersignaturen) und ArchiSafe (sichere Langzeitspeicherung), die vom Bundesministerium für Wirtschaft gefördert wurden.

SecDocs Archive Service ist als Middleware-Dienst ausgelegt, der über SOAP Web Services genutzt wird und dadurch leicht in bestehende IT-Verfahren und Prozesse integriert werden kann. Als Speichersystem dienen Data Protection Appliances ETERNUS CS8000 von Fujitsu mit Virtual Network Storage oder auch andere NAS-Filer. Optional können die Speichersysteme so konfiguriert werden, dass sie mit dem SoftWORM-Feature zusätzlichen Schutz gegen versehentliche oder absichtliche Manipulation der archivierten Dateien bieten.

Den Sicherheitskern von SecDocs Archive Service bildet die Fujitsu Digital Signature Engine (DSEngine), die auf der Open-Source Referenzimplementierung der Europäischen Kommission beruht. Die Sicherheitsvorgaben umfassen Elemente aus der Technischen Richtlinie TR-03125 (Beweiswerterhaltung kryptographisch signierter Dokumente).

Merkmale und Nutzen

HAUPTMERKMALE	NUTZEN
DAUERHAFTER SCHUTZ DER DOKUMENTENINTEGRITÄT	
■ Versiegelung durch digital signierte Zeitstempel ■ Prüfung von digitalen Signaturen zum Dokument ■ Beweiswerterhaltung durch digitale Übersignatur	■ Portable, vom Speicherort unabhängiger Nachweis der Unverfälschtheit digitaler Dokumente ■ Dauerhafter Nachweis korrekter Signaturen, auch nach Ablauf von Gültigkeitsfristen
SCHNITTSTELLEN	
■ Sowohl die Nutzung des Archivs als auch die Administration erfolgen über SOAP Webservices ■ Anbindung über HTTP(S)	■ Leichte Integration in bestehende IT-Verfahren ■ Service auch in der Cloud realisierbar
ROLLENKONZEPT UND MANDANTENFÄHIGKEIT	
■ Mehrere Mandanten können abgeschottet voneinander ein Archiv nutzen	■ Zentrale Archivierung möglich, auch für Mandanten, die mit unterschiedlichen IT-Verfahren arbeiten
NUTZUNG OFFENER STANDARDS	
■ Die Integrität der Dokumente wird über RFC 4998-konforme Evidence Records und zusätzlich auch in der TR-ESOR Profilierung gewährleistet ■ Speicherung der Dokumente wahlweise mit anwenderdefinierten XML-Schemata oder im XAIP-Format entsprechend der Technischen Richtlinie TR-03125	■ Die Dokumentenintegrität kann mit Hilfe des Evidence Records auch außerhalb des Archivs und unabhängig vom SecDocs Archive Service nachgewiesen werden ■ Flexible Definition von Dokumententypen und Metadaten
ANPASSBARKEIT IM BEZUG AUF KOSTEN UND NUTZUNG	
■ Flexible Konditionen gemäß dem Bedarf der Projektsituation.	■ Ausdehnung der Archivierung auf neue IT-Verfahren oder Reduktion des Archivumfangs sind jederzeit möglich
ZERTIFIZIERBARER SICHERHEITS-KERN	
■ Eine Zertifizierung nach der Technischen Richtlinie TR-03125 ist im Rahmen eines Projekts möglich und erleichtert die Zertifizierung als Bewahrungsdienst.	■ BSI-zertifizierbare Sicherheit

Beschreibung

Funktionsweise

SecDocs Archive Service archiviert Dokumente jeglicher Art und versiegelt sie mit einem Zeitstempel, der von einem externen Vertrauensdiensteanbieter digital signiert wurde. SecDocs Archive Service selbst benötigt dafür kein „Geheimnis" in Form eines eigenen privaten Schlüssels, der vor unberechtigtem Zugriff geschützt werden muss. Für die gelagerten Dokumente kann so der Nachweis erbracht werden, dass das Dokument seit seiner Archivierung nicht verändert worden ist.

Zeitstempel für dauerhaften Beweiswert

Die Verwendung von Zeitstempeln anstatt herkömmlicher digitaler Signaturen ermöglicht dabei eine dauerhafte Erhaltung des Beweiswerts: Alle kryptografischen Algorithmen verlieren im Lauf der Zeit durch die ständig steigende Leistungsfähigkeit der CPUs und Fortschritte in der Kryptoanalyse an Sicherheit, bis hin zu dem Punkt, an dem die mit ihnen erstellten digitalen Signaturen nicht mehr fälschungssicher sind. Mit einer Übersignatur im Sinn des ArchiSig-Konzepts, wiederum mit einem Zeitstempel, kann ein Dokument neu versiegelt werden, bevor der ursprüngliche Zeitstempel fälschbar geworden ist. Die dabei entstehende Kette von Zeitstempeln dient dann dem Nachweis, dass jede Versiegelung zu einem Zeitpunkt erfolgt ist, zu dem die verwendeten Algorithmen ausreichende Sicherheit geboten haben.

Erhaltung des Beweiswerts digitaler Dokumentensignaturen

SecDocs Archive Service bietet auch Mehrwert für die Archivierung von Dokumenten, die digital signiert sind. Die Algorithmen dieser digitalen Signaturen altern ebenfalls und werden schwächer, aber SecDocs Archive Service bewahrt den ursprünglichen Beweiswert dieser Signaturen für die gesamte Aufbewahrungsfrist. Dazu werden die digitalen Signaturen zum Zeitpunkt der Archivierung geprüft und die resultierenden Prüfberichte zusammen mit dem Dokument mit Zeitstempel versiegelt.

Beweiswert ohne Bindung an den Speicherort

Mit Hilfe der digital signierten Zeitstempel, die von SecDocs Archive Service im standardisierten Format eines „Evidence Record" (RFC 4998) aufbewahrt werden, kann die Unversehrtheit eines Dokuments völlig unabhängig vom Ablageort (zum Beispiel auf Speichermedien, die vor Überschreiben geschützt sind) nachgewiesen werden. Ein Dokument und der dazugehörige Evidence Record können aus dem Archiv entnommen und weitergegeben werden. Auch ohne jeglichen Zugriff auf das Archiv und ohne Prüfung der Sicherheit des Archivbetriebs während der Aufbewahrungszeit kann, allein mit Hilfe des Evidence Records, die Integrität eines Dokuments ab dem Zeitpunkt seiner Versiegelung zweifelsfrei nachgewiesen werden.

Architektur

SecDocs Archive Service ist als selbständige, über das Netz ansprechbare Komponente zur Integration in bestehende IT-Verfahren konzipiert. Die Nutzung zur Archivierung und Versiegelung von Dokumenten und die Verwaltung im laufenden Betrieb erfolgen über Web Services-Schnittstellen (SOAP).
Die archivierten Dokumente legt SecDocs Archive Service auf einem NFS-Dateisystem ab, wobei optional eine WORM-Funktion genutzt werden kann. Zur performanten Verwaltung interner Daten wird eine aktuelle Oracle Database Enterprise Edition benötigt.

Service-orientierte Architektur

Die Bedienung von SecDocs Archive Service über Webservices und das Transport-Protokoll HTTPS erlauben es, SecDocs Archive Service als Archivierungsdienst zentral bereitzustellen. Die nutzenden SOAP-Anwendungen können auf dem gleichen Server installiert werden, oder innerhalb des internen Netzes in einem Unternehmen oder auch weltweit verteilt sein. Eine Authentisierungsfunktion stellt sicher, dass nur berechtigte Nutzer den Archivservice in Anspruch nehmen können.

Dokumentenformate

Für die Archivierung von Dokumenten in SecDocs Archive Service können kundenspezifische XML-Schemata registriert werden. Jedes zu archivierende Dokument wird anhand der registrierten Schemata validiert. Dabei werden auch vom Kunden vorgegebene Elemente direkt ausgewertet (Metadaten, digitale Signaturen). Binäre Inhalte, wie zum Beispiel PDF-A-Dateien, können in Base64-Kodierung eingebettet werden. SecDocs Archive Service erkennt dabei, wenn innerhalb eines PDF-Dokuments digitale Signaturen eingebettet sind, und prüft diese.

Mandantenfähigkeit und Rollenkonzept

In einem Archiv können Dokumente mehrerer Mandanten vollständig voneinander abgeschottet archiviert werden. Für jeden Mandanten gibt es die Rolle eines Mandantenadministrators, der z.B. die Dokumententypen registriert, und die eines Archivars, der die Dokumente einlagert und gegebenenfalls wieder ausliest.

Technische Details

Technische Voraussetzungen Hardware	
Server	x86 Server, 64 Bit
RAM	mindestens 16 GB; mindestens 24 GB, wenn Oracle Database auf demselben Server installiert wird
Speicher-System	NAS Filer, optional mit WORM-Funktion; bevorzugt: Fujitsu ETERNUS CS8000 mit ViNS

Technische Voraussetzungen Software	
Betriebssystem	Suse Linux Enterprise Server (x86-64)
Datenbank	Oracle Database Enterprise Edition
Andere Plattformen auf Anfrage	

Schnittstellen	
Archivierung	Web Services mit SOAP V1.1 über HTTP(S)
Dokumententypen	Beliebig durch vom Kunden vorgegebene XML-Schemata; XML formatted Archival Information Package (XAIP)
Administration	Web Services mit SOAP V1.1 über HTTP(S)

Unterstützte Algorithmen	
Hashalgorithmen	SHA-1 (nur für Validierung), SHA-224 (nur für Validierung), SHA-256, SHA-384, SHA-512, RIPEMD-160 (nur für Validierung)
Signaturtypen	PAdES (EN 319 142-1/2), CAdES (EN 319 122-1/2), weitere auf Anfrage
Validierungsreport:	ETSI BB (EN 319 102-1) und ETSI-VR (TS 119 102-2)

Dokumentation	
https://github.com/fujitsu-dsps/secdocs	SecDocs Archive Service Benutzerhandbuch

Weitere Informationen

Fujitsu Plattform Lösungen

Zusätzlich zu Fujitsu SecDocs Archive Service bietet Fujitsu eine Vielzahl an Plattformlösungen. Diese kombinieren leistungsstarke Produkte von Fujitsu mit optimalen Servicekonzepten, langjähriger Erfahrung und weltweiten Partnerschaften.

Dynamic Infrastructures
Mit dem Konzept Fujitsu Dynamic Infrastructures, bietet Fujitsu ein komplettes Portfolio aus IT-Produkten, Lösungen und Services. Dieses reicht von Endgeräten bis zu Lösungen im Rechenzentrum sowie Managed Infrastructures- und Infrastructure-as-a-Service-Angeboten. Sie entscheiden, wie Sie von diesen Technologien, Services und Know-how profitieren wollen: Damit erreichen Sie eine völlig neue Dimension von IT-Flexibilität und Effizienz.

Computing products
www.fujitsu.com/global/services/computing/

- PRIMERGY: Industrial standard server
- SPARC Enterprise: UNIX server
- PRIMEQUEST: Mission-critical IA server
- ETERNUS: Storage system

Software
www.fujitsu.com/software/

- Interstage: Application infrastructure software
- Systemwalker: System management software

Weitere Informationen

Für weitere Informationen über Fujitsu SecDocs, kontaktieren Sie bitte Ihren persönlichen Ansprechpartner.

Fujitsu Green Policy Innovation

Fujitsu Green Policy Innovation ist unserweltweites Projekt, um negative Umwelteinflüsse zu reduzieren. Mit Hilfe unseres globalen Wissens, suchen wir Lösungen, um die Energieeffizienz von IT zu maximieren.
Weitere Informationen:
https://www.fujitsu.com/de/about/csr/

Copyright

Haftungsausschluss

Kontakt

Fujitsu Services GmbH
Mies-van-der-Rohe-Str. 8, 80807 München, Deutschland
E-Mail: secdocs@fujitsu.com
Website: http://www.fujitsu.com/emeia
04.10.2022, DE