

eArchive Module

mit der geprüften und bestätigten Signaturanwendungskomponente SLMBC 3.0.20

Verwendung & Einsatzbereich

Das AuthentiDate eArchive Module ermöglicht die rechtskonforme, massenhafte Prüfung von qualifizierten Signaturen innerhalb von Archiv- und Dokumenten-Management-Systemen.

Als wesentliches Leistungsmerkmal ist hierbei die Konformität zu den Standards X.509v3 (qualifiziert) und Common PKI Version 1.1 und 2.0 zu nennen. Dadurch können extern, d.h. durch Drittanwendungen erzeugte Signaturen mit hoher Sicherheit geprüft werden.

Das eArchive Module ist speziell für den Zweck der Integration in andere Software-Produkte entwickelt worden. Durch seine serviceorientierte Architektur (SOA) kann das Modul einfach und auf Basis aller gängigen Programmiersprachen verwendet werden. Die Integration des Moduls erfolgt auf Basis gängiger Programmierschnittstellen. Somit ist die Integration der Modulfunktionalität in bestehende Software-Produkte mit geringem

Aufwand und größtmöglicher Flexibilität gegenüber vorhandenen Software-Architekturen und Basistechnologien möglich.

Mittels eines auf Zustandsmaschinen basierenden Jobmanagements gewährleistet das Modul auch im Fall sehr hoher Transaktionsvolumina eine sichere und ordnungsgemäße Datenverarbeitung.

Das eArchive Module ist eine Software-Komponente, die lokal oder auf einem separaten Rechner im lokalen Netzwerk betrieben werden kann. Es basiert auf der Signaturgesetz-konformen "AuthentiDate SLM Base Component". Eine unabhängige, für die Prüfung vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannte Prüfstelle hat die Software geprüft. Anschließend hat eine von der Bundesnetzagentur zugelassene Bestätigungsstelle die entsprechende Bestätigung nach Signaturgesetz (SigG)



ausgestellt. Die Anforderungen des Deutschen Signaturgesetzes an Produkte für qualifizierte Signaturen sind somit erfüllt.

Funktionsbeschreibung

Das AuthentiDate eArchive Module dient der massenhaften Prüfung qualifizierter Signaturen unter Einhaltung der Anforderungen des Signaturgesetzes - nachgewiesen durch eine Bestätigung nach dem deutschen Signaturgesetz.

Die massenhafte Prüfung qualifizierter Signaturen erfolgt in konfigurierbaren Prüftiefen. Das Ergebnis der Prüfung einer Signatur wird hierbei als so genannter "Evidence Record" in Form eines XML-Dokumentes an die aufrufende Applikation zurückgegeben. Mit der Speicherung und Archivierung dieses XML-Dokumentes können Signaturprüfungen auf einfache Weise und in langfristig lesbarer Form dokumentiert werden.

Auf Anforderung werden alle relevanten Zertifikate sowie Nachweise zu Existenz und Sperrstatus bereitgestellt. Diese Nachweise und Zertifikate können zur

Archivierung verwendet werden. Bei einer späteren, erneuten Prüfung kann optional auch auf die archivierten Nachweise und Zertifikate zurückgegriffen werden, anstatt diese Informationen erneut über Online-Zugriffe einzuholen. Dieser Aspekt ist insbesondere im Bereich der langfristigen Archivierung von signierten Daten relevant.

Abhängig von der gewählten Prüftiefe wird ferner die Zahl der erforderlichen Online-Verzeichnisdienstzugriffe durch einen Caching-Mechanismus minimiert. Beim Caching prüft das eArchive Module, ob zu den zu überprüfenden Zertifikaten bereits anwendbare Statusinformationen im Cache vorliegen. Hierdurch wird die Verarbeitungsgeschwindigkeit bei der Überprüfung großer Mengen von Signaturen i.d.R. deutlich erhöht.

Die Prüfung qualifizierter Zeitstempel wird vollständig unterstützt. Dies umfasst

sowohl die Prüfung separater Zeitstempel, als auch solcher, die in Signaturcontainer als Nachweis zum Signaturerstellungszeitpunkt eingebettet sind. Hierdurch wird das Nachsignieren von Signaturen, und somit der langfristige Erhalt der Gültigkeit von Signaturen unterstützt. Entsprechend ist auch die Implementierung eines Systems zur langfristigen Aufbewahrung elektronisch signierter Dokumente gemäß dem international anerkannten ETSI-Standard (ETSI TS 101 733) möglich. Ebenso kann das eArchive Module für die Prüfung von Signaturen und Zeitstempeln in Archiven, die bspw. ERS oder ArchiSig für die langfristige Beweiswerterhaltung nutzen, verwendet werden.



Zusammenfassung der Funktionen

- ▶ Massenhafte Prüfung von qualifizierten Signaturen in Archiv-, und Dokumenten-Management-Systemen
- ▶ Unterstützung von qualifizierten Attributzertifikaten
- ▶ Unterstützung qualifizierter Zeitstempel – separat und in Signaturen eingebettet
- ▶ Unterstützung begleitender und integrierter Signaturen (TIFFv6, PDF)
- ▶ Unterstützung von Parallel- und Gegensignaturen
- ▶ Transaktions- und Datensicherheit durch skalierbares Job-Management (eine Zustandsmaschine je Job)
- ▶ Dokumentation der Prüfergebnisse über Evidence Records
- ▶ Variable Konfiguration der Prüftiefe im Verifikationsprozess
- ▶ Bestätigung nach deutschem Signaturgesetz



Standards und Schnittstellen

- Signaturgesetz:
Bestätigung nach Signaturgesetz, ausgestellt am 17.08.2009*. Herstellererklärung der verwendeten Signaturanwendungskomponente (SLMBC) wurde von der Bundesnetzagentur im Amtsblatt 02/2010 am 27.01.2010 veröffentlicht.
- Zertifikatsformat X.509v3 (qualifiziert), Common PKI V. 1.1, V. 2.0
- Signaturformat Cryptographic Message Syntax (CMS), beigefügt oder als integrierte Signatur (für TIFF, PDF)
- OCSP, LDAP, RFC3161
- Unterstützung von RSA 2048, SHA-256, SHA-384 und SHA-512

Systemvoraussetzungen

- Hardware-Mindestanforderungen: Intel Pentium Prozessor 3.0GHz; min. 1GB RAM; 100 GB HD
- Unterstützte Betriebssysteme: Das Modul ist grundsätzlich plattformunabhängig und läuft in der Java Runtime Environment 1.4.2. Herstellerseitig werden folgende Betriebssysteme und Versionen unterstützt:
 - Microsoft Windows XP ab ServicePack 3 (SP3),
 - Microsoft Windows 2003 Server ab ServicePack 1 (SP1),
 - Red Hat Enterprise Server (Kernel Versionen ab 2.6.9),
 - Suse Enterprise Server (Kernel Versionen ab 2.6.9)
- Transparente Netzwerkverbindung zum Verzeichnis- und Zeitstempeldienst der Zertifizierungsdiensteanbieter (OCSP, LDAP, RFC3161)

Lieferumfang

- Auslieferung der Software und Dokumentation erfolgt auf CD oder elektronisch per Email/FTP.
- Auslieferung der Lizenzschlüssel erfolgt elektronisch per Email oder FTP.

Verwandte Produkte

- Signature Check Server
- Signature Check Webservice
- eBilling Connector für SAP

* Die Bestätigung nach Signaturgesetz setzt bestimmte Hardware- und Softwarekomponenten voraus. Details sind im Prüfbericht verfügbar.