



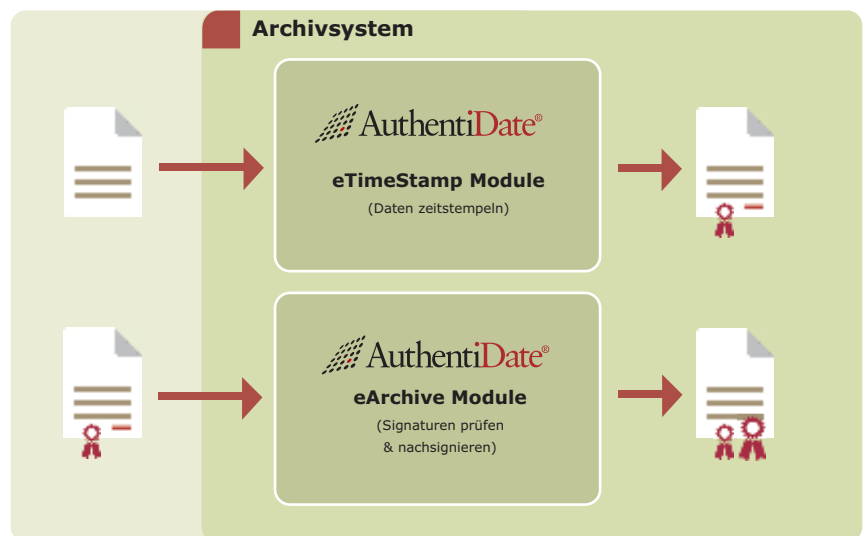
Rechtssichere Langzeitarchivierung

Signaturen & Zeitstempel zur Ergänzung von Archivsystemen nach europäischem ETSI Standard

Der Geschäftsprozess

Das Archivsystem nimmt in vielen Unternehmen und Behörden eine zentrale Rolle ein. Daten müssen langfristig sicher und zugleich schnell wieder auffindbar abgelegt werden. Dies gilt insbesondere für Daten, die bereits in anderen Prozessen signiert wurden.

Qualifizierte Zeitstempel ermöglichen die gesetzeskonforme, langfristige, rechtssichere Archivierung. Auch Aufbewahrungszeiten von mehr als 30 Jahren können abgebildet werden.



Die Umsetzung

AuthentiDate Produkte ergänzen Archivsysteme, je nach Anforderung, um verschiedene Funktionen.

■ Nachsignieren

Im Archivsystem abgelegte, bereits signierte Daten werden hierbei erneut mit einem qualifizierten Zeitstempel signiert. Das Nachsignieren mit Zeitstempeln ist vom Gesetzgeber vorgeschrieben, wenn die beim Signieren verwendeten Algorithmen schwach werden. Ohne ein Nachsignieren könnte nicht mehr 100-prozentig sichergestellt werden, dass bereits erzeugte Signaturen vor Manipulationen geschützt sind. Das Nachsignieren läuft automatisch und transparent für die Anwender ab.

■ Prüfen

Signaturen können automatisch bei Ablage der signierten Daten im Archivsystem geprüft werden. Das Ergebnis der Signaturprüfung wird automatisch mit archiviert. Fehler in der Signaturprüfung werden sofort und automatisch reportet, um die optimale Qualität archivierter Daten zu sichern.

■ Dokumentieren

Daten aller Art können automatisch und zentral im Archivsystem mit qualifizierten Zeitstempeln signiert werden. Hierbei kann individuell definiert werden, wann und welche Daten durch die Zeitstempel eingefroren werden sollen. Sie sind anschließend sicher vor unbemerkten Manipulationen geschützt. Dieser Prozess ist z.B. auch für LogFiles, im Rahmen von SOX-Prozessen realisierbar.



Produkte für diese Lösung

sind einzeln oder kombiniert nutzbar

- **eArchive Module**
- **eTimeStamp Module**

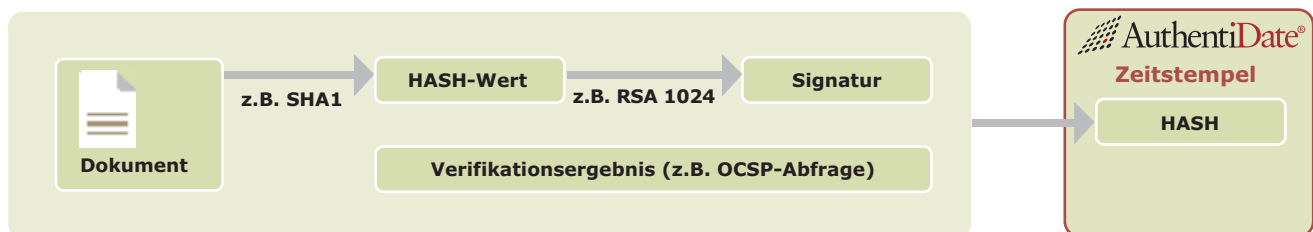


Uneingeschränkte Archivsystem – Funktionalität

durch Berücksichtigung des europäischen ETSI Standards

Zur Erstellung einer Signatur werden grundsätzlich zwei verschiedene Algorithmen verwendet. Ein Algorithmus wird zur Erstellung des Hash-Wertes genutzt und ein weiterer zur Verschlüsselung des Hash-Wertes. Hieraus ergibt sich die eigentliche Signatur.

Die AuthentiDate Produkte sind daher so konzipiert, dass die Signaturen beim Nachsignieren automatisch davor geschützt werden, dass einer oder beide Algorithmen schwach werden. Somit ist das Archivsystem mit nur einer technischen Lösung für alle Algorithmenwechsel gerüstet. Dieses Verfahren wurde auch im europäischen ETSI (European Telecommunication Standard Institute) TS 101 733 Standard definiert.



▪ Standardkonformität

Durch Anwendung des europäischen ETSI Standards können einzelne Dateien, einschließlich aller verbundenen Elemente (z.B. HASH-Werte und Signaturen) auch nach dem Nachsignieren vollständig aus dem Archiv gelöscht werden. Überflüssige Daten belasten somit nicht mehr das Archivsystem. Jede Datei wird als ein eigenständiges Element behandelt. Neue Dateien können hinzugefügt und ebenfalls nachsigniert werden. Eine Prüfung der nachsignierten Dateien, z.B. durch Richter, Wirtschaftsprüfer, etc., kann jederzeit auch ohne Zugriff auf das Archivsystem erfolgen.

Gleichzeitig können, wie z.B. im ArchiSig - Konzept definiert, Elemente zusammengefasst und somit die Anzahl der Zeitstempel minimiert werden.

Steckbrief

- ▶ **Automatisches „Nachsignieren“ durch qualifizierte Zeitstempel, wie gesetzlich vorgegeben**
 - Einsatz gesetzeskonformer Algorithmen
 - Wenige Zeitstempel durch Batch-System erforderlich
- ▶ **AuthentiDate Verfahren berücksichtigt ArchiSig-Konzept und zusätzlich europäischen ETSI (European Telecommunication Standard Institute) Standard.**
 - Extraktion, vollständige Löschung und Hinzufügen von Daten auch nach dem Nachsignieren
 - Nachsignierte Daten fügen sich transparent in bestehende Archivstruktur ein
 - Kein zusätzlicher Aufwand bei schwach werden des HASH-Algorithmus
- ▶ **Massenweise Prüfung (=Verifikation) von personenbezogenen Signaturen und/oder Zeitstempeln im Archiv**
- ▶ **Standardmäßig bei den marktgängigen Archivsystemen vorinstalliert und verfügbar**

