

## Scan Signature Module

mit der geprüften und bestätigten Signaturanwendungskomponente SLMBC 3.0.20

### Verwendung & Einsatzbereich

Das Scan Signature Module ermöglicht die rechtskonforme, massenhafte Erzeugung und Prüfung von qualifizierten elektronischen Signaturen in der Beleg-erfassung (Scanprozess).

Durch die Verwendung qualifizierter elektronischer Signaturen kann in Scan-Prozessen bei entsprechenden rechtlichen Rahmenbedingungen eine Gleichstellung von Papierdokumenten und ihren digitalen Abbildern erreicht werden. Diese Gleichstellung bietet Scan-Lösungsanbietern ein erweitertes Anwendungsfeld, in dem die Rechtssicherheit für gescannte Daten gefordert ist.

Das Konzept des Scan Signature Modules ermöglicht es Anbietern von Scan-Lösungen, qualifizierte elektronische Signaturen in die existierenden Software-komponenten mit geringem Aufwand und unter größtmöglicher Beibehaltung der vorhandenen Prozesse und Basistechnologien zu integrieren. Bestandskunden können darüber hinaus ohne größere Änderungen der eingesetzten Infrastruktur und der bereits etablierten Prozesse die erweiterte Funktionalität durch eine Migration auf ein neues Software-Release der Scan-Anwendung nutzen.

### Funktionsbeschreibung

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

Signaturkarten können Mandanten- oder Signaturzweck-bezogen gruppiert werden. Signaturkarten werden hierbei unabhängig von den angeschlossenen Chipkartenterminals anhand des Zertifikates identifiziert und den konfigurierten Gruppen zugeordnet. Die Zahl der verwendeten Chipkartenterminals und Signaturkarten ist praktisch nur durch die Leistungsgrenzen des zugrunde liegenden Systems begrenzt.

Ebenfalls kann der zwingende Gebrauch von Attributzertifikaten, mit denen beispielsweise der Signaturwert auf den Anwendungsfall der Dokumentation des Medienbruchs beschränkt werden kann, vorkonfiguriert werden.

Das Scan Signature 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 Zustandsmaschinen-basierenden Job-Managements gewährleistet das Modul auch im Fall sehr hoher Transaktionsvolumina eine sichere und ordnungsgemäße Daten-verarbeitung. Das Scan Signature Module ist eine Software-Komponente, die lokal oder auf einem separaten Rechner im lokalen Netzwerk betrieben werden kann. Es basiert auf der signaturgesetzkonformen "AuthentiDate SLM Base Component". Eine unabhängige, für die Prüfung vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannte Prüfstelle hat die Software geprüft.

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



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 entsprechend erfüllt.

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-Verzeichnisdienst-Zugriffe durch einen Caching-Mechanismus minimiert. Beim Caching prüft das Scan Signature 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.


**Zusammenfassung der Funktionen**

- ▶ Massenhafte Erzeugung von qualifizierten und fortgeschrittenen Signaturen zur Dokumentation des Medienbruchs
- ▶ Massenhafte Prüfung von qualifizierten und fortgeschrittenen Signaturen
- ▶ Mandanten- oder Signaturzweck- bezogene Gruppierung von Signaturkarten
- ▶ Unterstützung von qualifizierten Attributzertifikaten
- ▶ Unterstützung begleitender und integrierter Signaturen (TIFFv6, PDF)
- ▶ Unterstützung von Parallel- und Gegensignaturen
- ▶ Transaktions- und Datensicherheit durch skalierbares Job-Management (eine Zustandsmaschine je Job)
- ▶ Chipkartenterminal-basierender Dialog zur Aktivierung von Signaturkarten
- ▶ Dokumentation der Prüfergebnisse über Evidence Records
- ▶ Variable Konfiguration der Prüftiefe im Verifikationsprozess
- ▶ Stapelbezogene Aktivierung von Signaturkarten gemäß technischer Richtlinie des BSI (BSI-TR-03115)
- ▶ Lizenzabhängige Transaktionsvolumen je Zeitintervall
- ▶ 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)
- USB Port zum Anschluss von Chipkartenterminals
- Signaturgesetz-konforme Signaturkarten nach DIN-NI 17.4 und mit Unterstützung des Open Card Frameworks (OCF)
- OCSP, LDAP, RFC3161
- Unterstützung von RSA 2048, SHA-256, SHA384 und SHA-512

**Systemvoraussetzungen**

- Hardware-Mindestanforderungen: Intel Pentium 4-kompatibler Prozessor mit 3.0 GHz oder vergleichbares Modell ; min. 1GB RAM; 100 GB HD
- Unterstützte Betriebssysteme: Das Modul ist grundsätzlich plattform-unabhängig. Es werden jedoch nur 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)
- Schnittstellen: USB Port je angeschlossenem Chipkartenterminal

- Chipkartenterminals: Reiner SCT, Cherry SmartBoard xx44, Smart Terminal ST-2xxx, SCM Microsystems SPR532
- Chipkarten: Signaturgesetz-bestätigte Versionen der TeleSec Signaturkarten PKS-Card, E4KeyCard, E4NetKey-Card sowie der D-Trust multcard.
- Transparente Netzwerkverbindung zum Verzeichnisdienst 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.

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



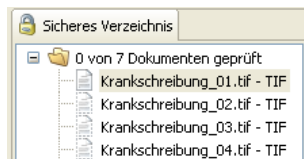
## AuthentiView Version 1.2

### Mit AuthentiView in drei Schritten zur qualifizierten Signatur!

**AuthentiView ist der neue „Trusted Viewer“ von AuthentiDate, mit dem sie zu signierende und signierte Dokumente jederzeit sicher anzeigen und prüfen können. Aber AuthentiView kann noch mehr: Es dient als Steuerungszentrale für die Signaturerstellung und die Signaturprüfung. Mit nur drei einfachen Schritten ermöglicht es Ihnen AuthentiView, auf ihrem Arbeitsplatzrechner qualifizierte Signaturen zu ihren Dokumenten zu erstellen. Es sind keinerlei technische Vorkenntnisse notwendig!**

Die Vorgehensweise ist denkbar einfach: AuthentiView wird automatisch mit den gewünschten Dokumenten aus Ihrer Anwendung aufgerufen. Ausgewählte Dateien können Sie sich vor der Signaturerstellung anschauen und prüfen. Mit einem Klick auf den „Signieren“-Button starten sie den Signaturprozess und werden zur Eingabe ihrer PIN am Kartenleser aufgefordert. Schon wird die Signatur erzeugt.

#### 1 Dokumente sichten & prüfen,



#### 2 PIN eingeben,



#### 3 Fertig!



##### Signaturinformationen:

Signatur wurde erstellt durch: CN=DAKCA2TestCMPRequestor  
Datum und Uhrzeit der Signaturerstellung: 6. Januar 2009 09:23:42 CET  
Hash-Algorithmus: SHA-256  
Einschränkungen laut Attributzzertifikat: kein Attribut Zertifikat gefunden

### Umfangreiche Zusatzfunktionen rund um die Signatur enthalten

AuthentiView bietet darüber hinaus eine Vielzahl an hilfreichen Funktionen, die die tägliche Arbeit mit qualifizierten und fortgeschrittenen Signaturen wesentlich vereinfachen. Zum Beispiel stehen Ihnen diese Funktionen zur Verfügung:



**1. Dokument-Prüfung nach Vorgabe der Bundesversicherungsanstalt (BVA):** AuthentiView bietet die Möglichkeit, vor der Signaturerstellung zwei Prozent der Dokumente entsprechend der aktuellen Vorgabe der BVA zu überprüfen und erst anschließend für die Signaturerstellung freizugeben.



#### 2. Signaturen und Prüfergebnisse im Klartext:

Der Inhalt der Signaturen und Prüfergebnisse können jederzeit auf dem Bildschirm angeschaut werden. Die wichtigen Inhalte und die Prüfergebnisse werden leicht verständlich dargestellt– sie benötigen keinerlei technisches Know-How.



#### 3. Signaturprüfung jederzeit möglich:

AuthentiView unterstützt sie bei der Prüfung von Signaturen. Dabei spielt es keine Rolle, ob sie Signaturen direkt nach ihrer Erstellung oder zu einem späteren Zeitpunkt prüfen möchten. AuthentiView erlaubt ihnen, beide Fälle mit nur einem Mausklick durchzuführen.



# AuthentiView Version 1.2

## Verschiedenste Einsatzgebiete für AuthentiView

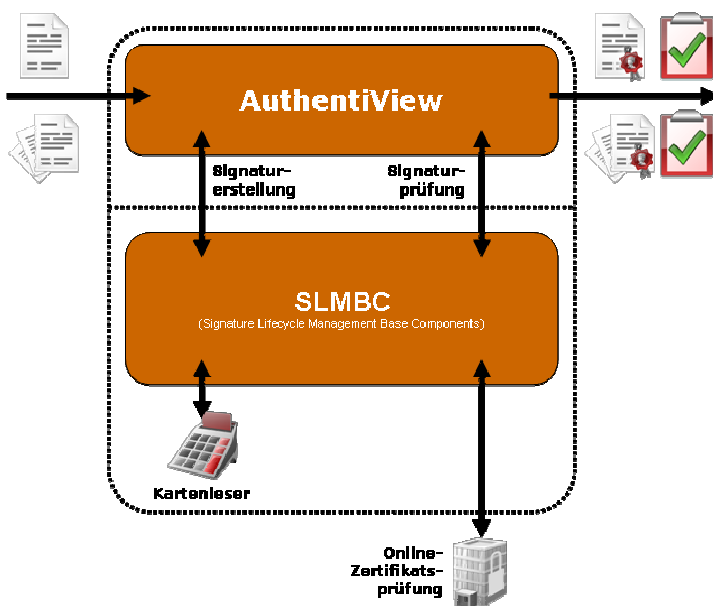
AuthentiView kann in unterschiedlichsten Einsatzgebieten genutzt werden. Weit verbreitet ist die Nutzung in der Massenbelegerfassung oder in Freigabeprozessen zur Dokumentation von Workflows. AuthentiView stellt in diesen Prozessen und für die entsprechenden Anwendungen die gewünschten Signaturfunktionen bereit. AuthentiView nimmt die zu signierenden Daten entgegen und erstellt je nach Einsatzgebiet – gesteuert durch die Prozessanwendung – entweder Einzel- oder Stapelsignaturen.

## Flexibel und anpassbar – bequeme und einfache Integration

Eine Integration in andere Anwendungen ist sehr einfach möglich: Dazu steht ein Software Development Kit (SDK) auf Java-Basis zur Verfügung, mit dem eine detaillierte Steuerung von AuthentiView möglich ist. Alternativ kann AuthentiView über Kommandozeilen-Parameter angesteuert werden. So können die Signaturfunktionen genau an die gewünschten Unternehmensprozesse angepasst werden.

## Stabile Basis durch jahrelang bewährte Technologie

AuthentiView baut auf die jahrelang bewährte und zertifizierte Signatur-Technologie (SLMBC) von AuthentiDate auf. Damit wird die sichere und performante Signaturfunktionalität nun auch im Einzelarbeitsplatz-Umfeld verfügbar. Auf jedem PC können die Signaturfunktionen so genutzt werden wie dies sonst nur in besonders geschützten Umgebungen von Rechenzentren oder Server-Umgebungen möglich ist. Auch große Stapelsignatur-Aufträge werden so in kürzester Zeit abgearbeitet und sorgen für eine spürbare Beschleunigung der Arbeitsprozesse.



Architektur-Überblick AuthentiView

### Systemvoraussetzungen:

- Intel Pentium IV-kompatibler Prozessor
- 1 GB RAM
- 80 GB Festplatte
- Grafikkarte mit 32 MB Speicher
- Windows XP Service Pack 2 oder höher
- JRE 1.5 (im Lieferumfang enthalten)
- Unterstützter Chipkarten-Leser mit seriellem oder USB-Anschluß entsprechend AuthentiDate-Vorgabe (bspw. ReinerSCT)
- Signaturkarten:
  - TSI T-Telesec PKS Chipkarten (TCos 2&3)
  - Swisscom Diamant
  - D-Trust multiscard
- Transparente Netzwerk-Verbindung und DNS-Anbindung

### Signaturgesetz-Konformität:

- Herstellererklärung nach SigG

### Im Lieferumfang von folgenden Produkten enthalten:

- Scan Signature Module
- eArchive Module
- eSign Client Module
- eTimeStamp Module SLMBC