



Consulting



Projects



Solutions

Tembit



Neue Features für Kunden der Version 1:

- Windows Vista und Windows 7 Support
- Unabhängigkeit von Sun's Applet Installer
- Vollständige Steuerung über JavaScript
- Signaturen gemäß A005 / A006

Digitale Signatur in Web-Applikationen ohne lokale Installation.

bc:sign 3.0.

Mit bc:sign 3.0 können Transaktionen in Web-Anwendungen auf Basis hochsicherer Smartcard-basierter Kryptographie durchgeführt werden.

Mögliche Einsatz-Szenarien sind:

- Signatur von Banktransaktionen wie Überweisungen
- sicheres Login
- Autorisierung von Geschäftstransaktionen im eCommerce wie z.B. Bestellungen
- Signatur von Rechtsgeschäften mit der öffentlichen Verwaltung



Bei Verwendung der mIDentity Smartcard-Reader (Kobil Systems) ist ein installationsloser Betrieb möglich, der keine Administrator-Rechte auf dem Rechner des Anwenders erfordert.

Applet.

Da die gegenwärtigen Browser keine Signatur via Smartcard unterstützen, besteht die einzige praktikable Lösung in der Nutzung eines Java Applets, das von der jeweiligen Webseite auf den Rechner des Anwenders geladen wird.

Das Applet kommuniziert über definierte Schnittstellen mit dem Kartenleser und kann alle wesentlichen Funktionen rund um die Smartcard ausführen wie z.B.:

- Auslesen von öffentlichen Schlüsseln
- Änderung der PIN
- Sperre der PIN mit der SuperPIN aufheben
- Challenge/Response-Verfahren
- Hashing von Nachrichten
- Signatur von Nachrichten

Die mit bc:sign erzeugte fortgeschrittene elektronische Unterschrift kann z.B. zur Signatur von Aufträgen im Geschäftsverkehr mit Banken eingesetzt werden. Dazu entspricht das Plugin u.a. den Anforderungen der

A004-, A005- und A006-Standards des Zentralen Kreditausschusses (ZKA).

Das Applet wird über einen Satz von Parametern so gesteuert, dass es sich optimal in vorhandene HTML-Seiten integriert. Es kann auf eine unsichtbare Größe verkleinert und vollständig von außen über JavaScript angesteuert werden.

Authentication Server.

Das Gegenstück zum Applet auf der Server-Seite bildet der Authentication Server mit folgenden Funktionen:

- Speicherung von Public Keys
- Prüfung von digitalen Signaturen
- sichere Protokollierung aller Prüfungen
- Sperren und Freischalten von Kunden

Der Authentication Server ist selbst als Web-Anwendung realisiert, um die öffentlichen Schlüssel der Kunden zu administrieren und deren Beziehung zu den operativen Systemen zu verwalten.

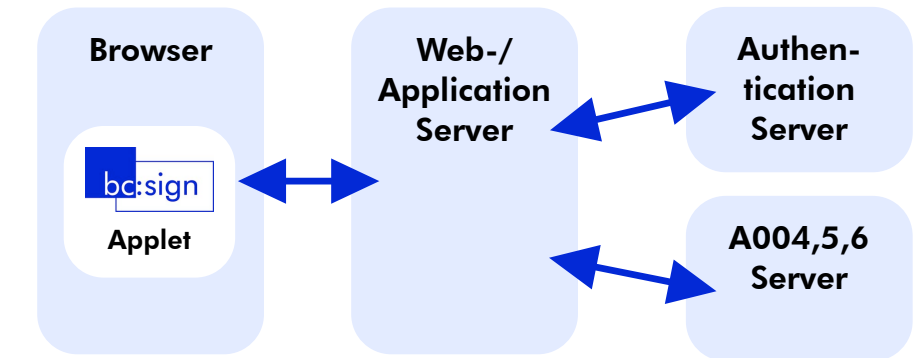


Durch eine hochgradig skalierbare Architektur ist der Authentication Server für den massiv parallelen Einsatz ausgelegt und damit auch für eine sehr grosse Zahl von Transaktionen pro Zeiteinheit ausgelegt.

Ausserdem ist er im Rahmen der Java EE-Technologie als hochverfügbares System konzipiert, das auch bei Ausfällen von einzelnen Servern verfügbar bleibt.

Leistungsspektrum.

bc:sign ist ein Plugin für bestehende IT-Infrastrukturen (IBM WebSphere, Bea WebLogic, JBoss, Inubit IS u.a.) mit folgenden Eigenschaften:



- Elektronische Unterschrift im Browser über ein Java-Applet
- Elektronische Unterschriften für Electronic Banking, eCommerce, Rechtsgeschäfte mit der öffentlichen Verwaltung uvm.
- Erzeugen von Schlüsselpaaren
- Auch ohne den Authentication Server einsetzbar, z.B. im Kontext von EBICS und A004/A005/A006, wenn signaturprüfende Anwendung vorhanden ist.
- Installationsloser Betrieb mit bestimmten Kartenlesern von Kobil Systems, auch ohne Administratorrechte.

Version 3.0

Neu in Version 3.0 ist die Unterstützung der Signatur nach A005 und A006 parallel zur Signatur nach A004 sowie ein umfangreiches Testframework, um das Applet im Kontext der zugrundeliegenden Webseite maschinell testen zu können.

Dies kann bei Abnahmetests mit unterschiedlichsten Betriebssystem und Java Plattformen sehr hilfreich und zeitsparend sein.

Technik

bc:sign ist ein Plugin, das auf Server-Seite in die gängigen Application und Integration Server integriert werden kann. Auch eine Integration in Applikationen, die nicht Application/Integration-Server-basiert sind, ist möglich.

Die Server-Seite von bc:sign ist gemäß dem Java EE-Standard implementiert, die Client-Seite in Form eines Java-Applets.

Systemvoraussetzungen

bc:sign kann Server-seitig in beliebige J2EE-basierte Applikationen integriert werden und wird laufend unter den Application-Servern IBM WebSphere, Bea WebLogic und JBoss getestet.

Durch Einsatz der Java-Technologie ist bc:sign plattformunabhängig und sowohl auf Windows ab XP als auch unter Linux und Mac verfügbar. bc:sign ist kompatibel zu den führenden Kartenlesegeräten.