CodeMeter als Token

Private Schlüssel und Zertifikate für digitale Authentifizierungslösungen mobil und sicher aufbewahrt

Die CodeMeter-Technologie von WIBU-SYSTEMS bietet Datensicherheit und Datenschutz bei der digitalen Kommunikation über die Verwendung der CodeMeter-Bauformen als Token.
Neben gewohnt sicherem Schutz und der effektiven Lizenzkontrolle von Software und digitalen Inhalten, bewahrt der Token private Schlüssel und Zertifikate sicher auf. Über die Middleware CSSI des bekannten Herstellers Charismathics, verfügbar für Windows, Mac OS X und Linux Betriebssysteme, eröffnen sich für Anwendungen, die Microsoft CSP und PKCS#11 unterstützen, viele Einsatzmöglichkeiten im Bereich digitaler Authentifizierungslösungen.
Mit dem optionalen Flash-Speicher, der die Installation mobiler Anwendungen auf dem Token erlaubt, werden die CodeMeter Bauformen damit zum einzigartigen, unvergleichbaren Allrounder: Token, Dongle und Speichermedium in einem.

Datenkommunikation: vertraulich, verbindlich und authentisch

Die Sicherheitsanforderungen an Authentifizierungslösungen sind mit CodeMeter über asymmetrische Schlüsselpaare kryptologisch abgedeckt. Jedes Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel (private und public key). Der private Schlüssel ist nur dem Benutzer bekannt und sicher im CodeMeter Token aufbewahrt.

PKI-Token-Anwendungen:

- **Verschlüsseln und Signieren von E-Mails**
- **Verschlüsseln von Daten bei Remote Access**
- **Zugangskontrolle (starke Zwei-Faktor-Authentifizierung)**
- **Zertifikatsbasiertes Windows-Login**
- **Webbasierte Anwendungen (Software as a Service, SaaS)**
- **Unternehmensweites Single-Sign-On (Windows)**
- **Virtual Private Networks (VPN)**

Der Allrounder: Token, Dongle und Speichermedium

- Vollständige Implementierung von Microsoft CSP und PKCS#11
- Aktivierung durch PIN-Eingabe
- Aufbewahrung von privaten Schlüsseln (16 X.509 Zertifikate für mehrere Anwendungen einsetzbar)
- Asymmetrische Verschlüsselung (RSA 1024)
- Erzeugung von Signaturen
- Softwareschutz für viele Betriebssysteme (Windows, Windows Embedded, Windows CE, Mac OS X, Linux, Sun Solaris) und Programmiersprachen (.NET, Java)
- Viele Bauformen: USB, PC-Card, ExpressCard, CF-Card, SD-Card, µSD-Card
- Optionaler Flash-Speicher

WIBU SYSTEMS

CodeMeter als Token

Asymmetrische Verschlüsselung

Die Vertraulichkeit der Datenkommunikation wird gewährleistet, da Daten, die mit dem privaten Schlüssel verschlüsselt wurden, ausschließlich mit dem zugehörigen öffentlichen Schlüssel wieder entschlüsselt werden können und umgekehrt. Sämtliche Ver- und Entschlüsselungsvorgänge finden sicher im CodeMeter Token statt.

Digitale Signaturen

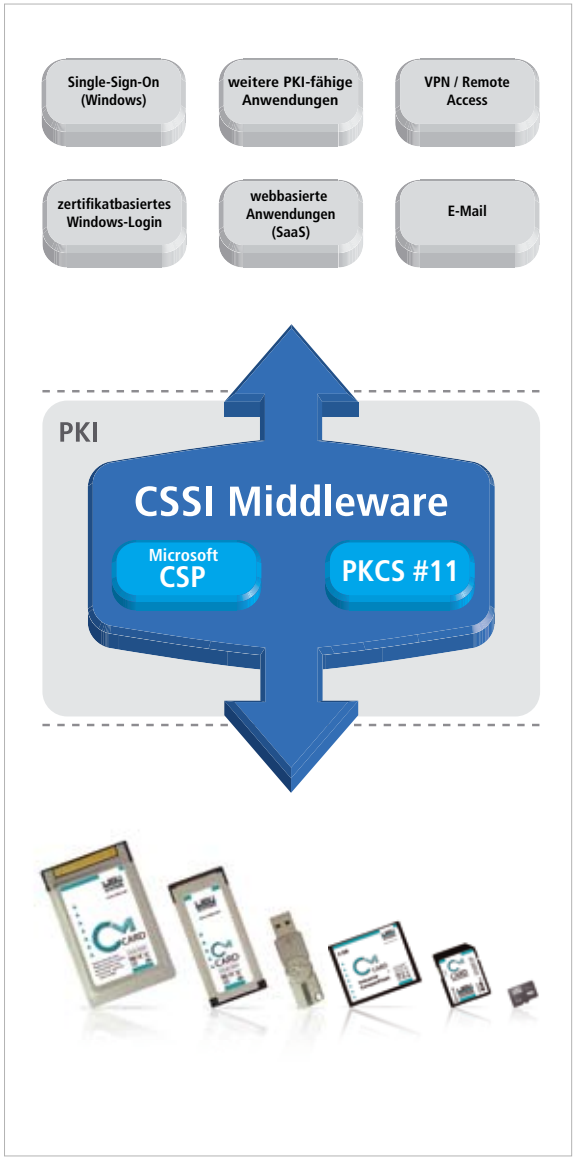
Zur Prüfung der Zugehörigkeit und Unveränderlichkeit der Daten setzt CodeMeter Signaturen ein. Die Signatur ist ein verschlüsselter „Fingerabdruck" (Hash-Wert) der Daten, der mit dem privaten Schlüssel im CodeMeter Token erzeugt wird. Bei der Signaturprüfung, die über die CSSI Middleware läuft, wird der öffentliche Schlüssel dazu genutzt, den verschlüsselten „Fingerabdruck" zu entschlüsseln und mit dem Ausgangswert zu vergleichen.

Digitale Zertifikate

Beim Einsatz von Signaturen kann Sicherheit aber nur gewährleistet werden, wenn sich ein öffentlicher Schlüssel eindeutig zu einem Benutzer zuordnen lässt und falsche Identitäten ausschließt. Diese Authentifizierung wird mit digitalen Zertifikaten erreicht, die u.a. die jeweiligen öffentlichen Schlüssel, Gültigkeitszeiträume sowie Inhaberangaben enthalten. Die Zertifikate werden von einer Zertifizierungsstelle erstellt, die Bestandteil einer Public Key Infrastructure (PKI) sein kann. Sie dienen als Art ‚elektronische Ausweise' zum Identitätsnachweis und sind im X.509 Format im CodeMeter Token sicher aufbewahrt.

CSSI Middleware

Die Middleware CSSI des Hersteller Charismathics stellt alle Dienste für Zugriff, Identifikation und Authentifizierung zur Verfügung und vermittelt die Funktionsaufrufe zwischen dem CodeMeter Token und Anwendungen über die Verwendung der Windows-proprietären CSP und der generische PKCS#11 Schnittstelle. Die Verwaltung der öffentlichen Schlüssel kann zusammen mit anderen Komponenten innerhalb einer Public Key Infrastruktur (PKI) organisiert werden.



WIBU-SYSTEMS ist nach DIN EN ISO 9001:2000 zertifiziert und Mitglied u.a. bei BITKOM e.V., VDMA PCMCIA, SD Card Association, USB Implementers Forum, SIIA und Microsoft Gold Certified and Embedded Partner.

WIBU-SYSTEMS – das heißt seit 1989 sichere Hard- und Softwaretechnologie für Digital Rights Management (DRM) bei Software, Dokumenten und Medien. DRM gehört zu den größten Wachstumsfeldern der nächsten Jahre und wird auch für den Erfolg Ihrer Produkte immer wichtiger. Über höchste Qualität und eine konsequente Nutzen- und Serviceorientierung haben wir uns eine Vorbildfunktion am Markt erarbeitet. Vorbildlich auch deshalb, weil wir als erfolgreiches Unternehmen auch unsere soziale Verantwortung ernst nehmen. Wir investieren in Ausbildung, unterstützen die Jugendarbeit und gehen mit unseren Lieferanten besonders fair um.

WIBU-SYSTEMS zählt heute zu den drei größten Anbietern für Software- und Dokumentenschutz. Dieser Erfolg ist Motivation genug, unsere technologische Führungsposition weiter auszubauen.

Auszeichnungen:

WIBU-SYSTEMS AG
Rüppurrer Straße 52-54
D-76137 Karlsruhe
Telefon: +49-721-93172-0
Fax: +49-721-93172-22
info@wibu.de | www.wibu.de

MEDIA ACCESS
PERFECTION IN SOFTWARE PROTECTION
DOCUMENT

5020-005-01/090916 © WIBU-SYSTEMS AG 2009