



# OPENLiMiT® SignCubes

**Monika Burmester**

**e-Mail: [monika.burmester@openlimit.com](mailto:monika.burmester@openlimit.com)**

Software and Services  
for Digital Signature and Encryption




## Allgemeine Informationen - Firmenprofil

- OPENLiMiT ist ein **Technologieunternehmen**
- OPENLiMiT **entwickelt** Software zur Anwendung elektronischer Signaturen, und Verschlüsselungstechnologien
- Die **zentrale Aufgabe** der OPENLiMiT Softwareprodukte ist, die Beweiskraft, Sicherheit und Effizienz von elektronischen Geschäftstransaktionen, Workflow, Kommunikationsprozessen und Daten zu steigern
- OPENLiMiT ist ein Technologielieferant und **vermarktet** ihre Produkte durch strategische Marketingpartner, wie z.B. Adobe, Fujitsu Siemens Computers, Trust Center und Systemhäuser
- OPENLiMiT ist ein Schweizer Unternehmen. Die Softwareentwicklung und das Testing finden in Deutschland (Berlin) statt.
- OPENLiMiT beschäftigt derzeit ca. 45 Mitarbeiter (Stand September 2008)

Kommunikation  
ohne Verschlüsselung  
und Signatur ist  
wie das Versenden  
vertraulicher  
Information auf **mit**  
**Maschine**  
**geschriebenen**  
**Postkarten!**

Kommunikations-  
partner

Kto-Nr	
1231120	
PIN	<input type="text"/>
1234	<input type="text"/>

Kommunikations-  
partner

# Elektronische Signatur

## Elektronische Signatur ist der **Schlüssel für den medienbruchfreien, sicheren digitalen Prozess**

- Sie identifiziert eindeutig den Unterzeichner eines elektronischen Dokuments oder Daten und macht Datenmanipulation ersichtlich
  - für den Einsatz in **allen Workflowprozessen** geeignet
  - Rechtsverbindliche Dokumente und Prozesse (Rechnungen, e-Banking, Belege, Verträge usw.)
  - Elektronische **Formulare**, Elektronische (**Langzeit-)**Archivierung
  - Authentisierung an Internet Plattformen (e-Banking), Server und Computer
  - eMail, ERP-Systeme, Scanning, Sicherheit

Der **volkswirtschaftliche Nutzen** für die EU ist ein höherer dreistelliger Milliarden Euro-Betrag pro Jahr

# :: Gesetzgebung

- **EU:** Richtlinie für elektronische Signaturen, 1999
- **EU-Mitgliedstaaten:** Umsatz der Richtlinie in nationale Gesetze, 2001

## Deutschland:

- Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz--**SigG**)-- 16. Mai 2001
- Verordnung zur elektronischen Signatur (Signaturverordnung--**SigV**)-- 16. November 2001
- Änderung des Bürgerlichen Gesetzbuches vom 15. Juni 2001
- Anpassung des SigG – 01/2005 (1. Änderung des SigG)

# :: Def. Elektronische Signatur nach SigG

1. **“elektronische Signaturen”** Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,
  
2. **“fortgeschrittene elektronische Signaturen“** elektronische Signaturen nach Nummer 1, die
  - a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
  - b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
  - c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
  - d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,
  
3. **“qualifizierte elektronische Signaturen”** elektronische Signaturen nach Nummer 2, die
  - a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
  - b) mit einer sicheren Signaturerstellungseinheit erzeugt werden,



# Artikel 1 Änderung des BGB

Das Bürgerliche Gesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 400-2, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 2 Abs. 25 des Gesetzes vom 25. Juni (BGBl. I S. 1206), wird wie folgt geändert:

2. § 126 wird wie folgt geändert:

a) Nach Absatz 2 wird folgender Absatz 3 eingefügt:

„(3) Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.“

3. Nach § 126 werden folgende §§ 126a und 126b eingefügt:

## „§ 126a

(1) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten Signatur nach dem Signaturgesetz versehen.

(2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.“

# Einführung PKI - Struktur

Elektr. Geschäftsprozesse  
erfordern Vertrauen in die...

- ...**Identität** des Partners
- ...**Integrität** der Nachricht
- ...**Verbindlichkeit** der  
Nachricht



# Public Key Infrastruktur (PKI) - das Modell „Trustcenter“

Zertifikatsinhaber ↔ Trustcenter ↔ Bundesnetzagentur

- **Ausstellen von Zertifikaten**
  - Identität und öffentlicher Schlüssel
  - Attribute
  - Pseudonyme
  - Gültigkeitszeit
- **Zeitstempeldienst**
- **Verzeichnisdienst**
  - Abfrage
  - Sperrung



# :: Signatur allgemein

private key

public key



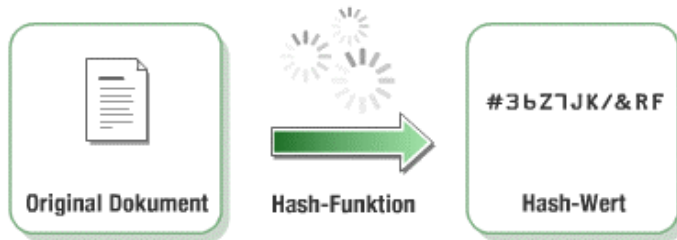
SparkassenCard (Bild 1) und Kontounabhängige GeldKarte (Bild 2) mit Vorbereitung für die elektronische Signatur



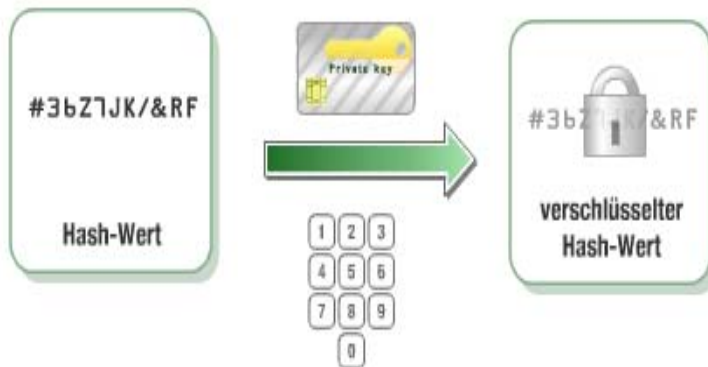
Sowohl bei der Signatur als auch bei der Verschlüsselung kommen asymmetrische Verschlüsselungsverfahren zum Einsatz:

Es werden immer zwei verschiedene Schlüssel verwendet, der private Schlüssel (private key) und der öffentliche Schlüssel (public key), die sich gegenseitig ergänzen und miteinander „verknüpft“ sind. Daten, die mit dem einen Schlüssel "zugeschlossen" wurden, können nur mit dem anderen wieder "aufgeschlossen" werden.

# :: Signatur allgemein

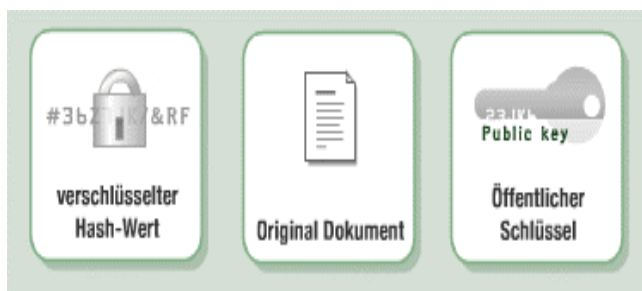


1. Berechnung des Hashwertes mit Hilfe einer Hashfunktion



2. Übergabe des Hashwertes an den Chip der Karte und Verschlüsselung des Hashwertes mit 2048 bit (RSA) Schlüssel. Damit ist gesichert, dass der **private Schlüssel** die Karte nie verlässt. Der private Schlüssel ist zusätzlich durch eine PIN (personal identification number) geschützt.

(Das Asymmetrische Verschlüsselungsverfahren **RSA** ist benannt nach den Entwicklern Ron **R**ivest, Adi **S**hamir und Len **A**dleman)



3. Rückgabe des verschlüsselten Hashwertes mit dem öffentlichen Schlüssel und dem Zertifikat an den PC und speichern

4. Versendet oder archiviert werden:

- der verschlüsselten Hashwert,
- das Originaldokument,
- der Öffentliche Schlüssel

# :: Signatur allgemein

**Empfänger: Folgende Punkte sind bei der Prüfung wichtig:**

1. Ist das Dokument unverändert angekommen?



Das Dokument wird erneut gehasht. Der alte Hashwert wird entschlüsselt und mit dem neuen verglichen: Sind beide Hashwerte identisch, ist bewiesen, das Dokument ist unverändert.

2. Ist der Signaturinhaber „echt“?

Authentizität des Inhabers, geprüft anhand der Authentifizierungskette/PKI Infrastruktur.

3. Ist das Zertifikat gültig? Zertifikatsstatus wird geprüft anhand der

- Sperrlisten (das sind Listen, die die Trustcenter regelmäßig veröffentlichen und in denen die gesperrten Zertifikate erfasst werden)
- Online Abfrage bei dem Trustcenter

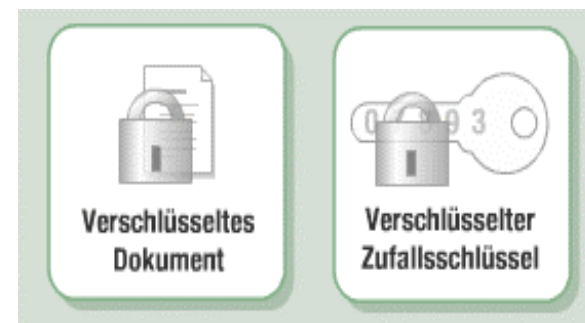
# :: Verschlüsselung allgemein

Das Dokument wird mit einem Zufallsschlüssel im Triple DES Verfahren verschlüsselt. Das heißt, das Dokument wird dreimal hintereinander mit 192 bit verschlüsselt.



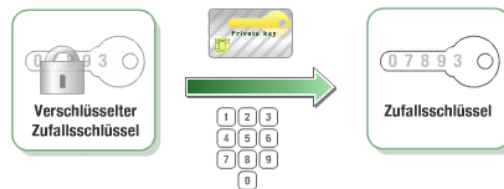
Der Zufallsschlüssel wird dann mit dem **öffentlichen Schlüssel** der Empfänger verschlüsselt. Hier kommt die 1024bit RSA-Verschlüsselung zum Einsatz.

Das verschlüsselte Dokument und der verschlüsselte Zufallsschlüssel werden dann zusammen archiviert oder per e-Mail an die Kommunikationspartner versandt, für die verschlüsselt wurde.



# :: Entschlüsselung allgemein

Um das Dokument wieder entschlüsseln zu können, wird zunächst der **Zufallsschlüssel** mit dem **privaten Schlüssel** (PIN Eingabe notwendig) des Empfänger entschlüsselt.



Mit dem **Zufallsschlüssel** wird das gesamte Dokument entschlüsselt.



Durch dieses Verfahren ist gesichert, dass nur der **Karteninhaber mit seiner PIN** (Haben und Wissen) das Dokument entschlüsseln und lesen kann.

# :: Verschlüsselung allgemein

Wo kommt der **öffentliche Schlüssel** her?



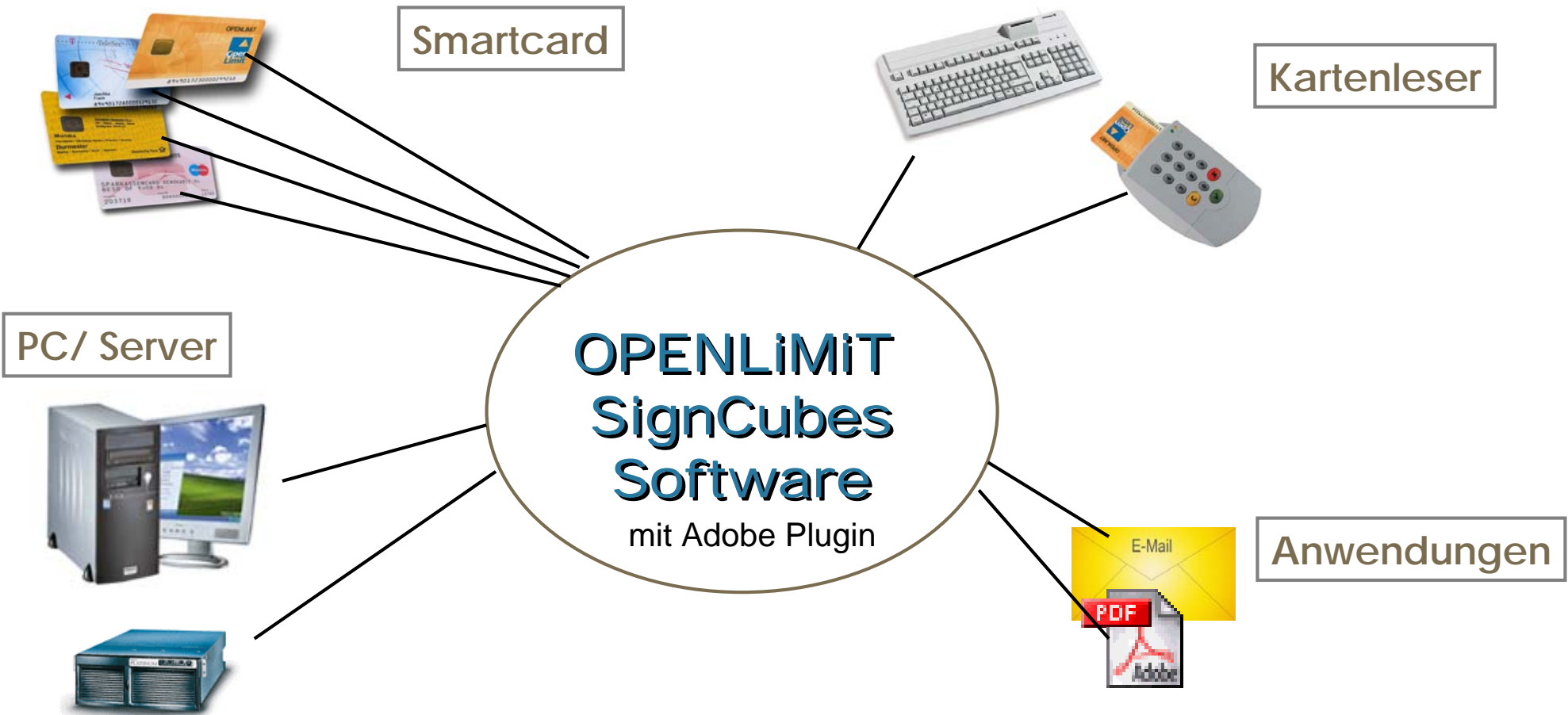
**Empfänger**



durch  
Export  
aus  
seiner  
Chipkarte

Verzeichnisdienst des  
Zertifizierungsdiensteanbieters

# :: Lösung



OPENLiMiT® CC Sign ist die universelle Clientanwendung für die Erzeugung und Prüfung qualifizierter Signaturen und für die Nutzung von Signatur-, Verschlüsselungs- und Authentisierungsfunktionen in zahlreichen Mail-Clients oder Browsern auf Windows Systemen.

Mit Batch 25 können bis zu 25 Dokumente durch einmalige Pin Eingabe signiert werden. Automatische TIFF Konvertierung und Versand per e-Mail ergänzen das Produkt.

# :: Signaturanwendung OPENLiMiT

## Trust Center

- unabhängig, d.h. unterstützt Trustcenter, die in Deutschland für die Ausgabe qualifizierter Zertifikate bestätigt sind

## Signaturkarten

- Unterstützung alle in Deutschland bestätigten Signaturkarten, die mit einem RSA-Algorithmus arbeiten.
- D-TRUST, Gemplus-mids, Gisecke & Devrient, Siemens, Signtrust, STARCOS, S-TRUST, Telesec und weitere.

## Kartenlesegeräte

- Unterstützung verschiedener Kartenleser (mit sicherer PIN - Eingabe) der Unternehmen Cherry, Kobil, Omnikey, Reiner SCT, SCM Microsystems.



# Schwerpunkt: Technologie Heute – Zulassungen / Interoperabilität



Common Criteria Arrangement  
for components up to EAL4

- Die OPENLiMiT® Basiskomponenten sind nach Common Criteria EAL4+ evaluiert



- Die OPENLiMiT® Basiskomponenten sind nach SigG und SigV vom Bundesamt für Sicherheit in der Informationstechnik bestätigt



- Die OPENLiMiT® Basiskomponenten besitzen das ISIS-MTT-Siegel



- Die OPENLiMiT-Software in einer Adobe Anwendungsumgebung ermöglicht, bei sachgerechter Anwendung, eine den in Deutschland geltenden Grundsätzen ordnungsmäßiger Buchführung entsprechende Erzeugung elektronischer Signaturen bzw. deren Verifikation. Dies wurde von PricewaterhouseCoopers testiert

## Ausblick – eCard API Framework (2)

- Umsetzung der technischen Richtlinie BSI-TR-03112 (eCard-API Framework) -> OPENLiMiT Version 3
- Veröffentlichung der Spezifikation Version 1.0 erfolgte am 05.03.2008 auf der CeBIT in Hannover
- Bereitstellung einer einheitlichen Middleware-Komponente für die Ansteuerung von:
  - Sicher Signaturerstellungseinheiten
  - ePA (Elektronischer Personalausweis)
  - eGK (Elektronische Gesundheitskarte) etc.
- Validierung elektronischer Signaturen
- Dokument Ver- und Entschlüsselung
- OPENLiMiT hat die Konformitätsprüfung der Implementierung beim BSI bereits angemeldet

### Plattformen

- Microsoft Betriebssysteme ab Windows 2000
- Linux ab Linux Kernel v2.6
- SUN Solaris ab Solaris 10
- Mac ab MacOS X (Intel)

### Technische Schwerpunkte

- Einfache Integration neuer Signaturhardware über sog. CardInfo-Files
- Aufbauend auf internationalen Standards
- Internationale Interoperabilität

