

Die elektronische Signatur und Kartenchips

was ist das - wie geht das - wer
braucht das - ist es sicher?

Thilo Schuster

[thilo.schuster NIXSPAM web.de](http://thilo.schuster.NIXSPAM.web.de)

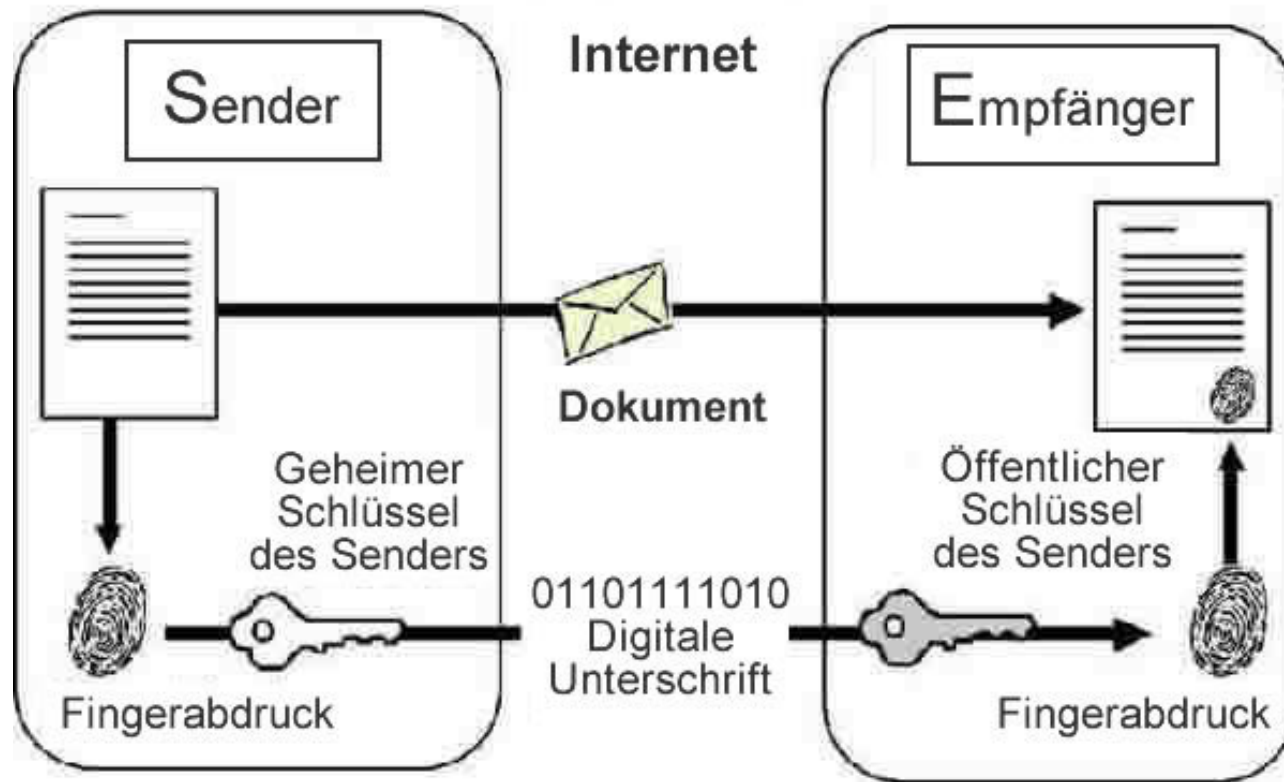
Fragen

- Was ist eine elektronische Signatur?
- Wie funktioniert die Signatur?
- Was ist eine PKI?
- Wie sieht die rechtliche Seite aus?
- Welche Komponenten werden benötigt?
- Was ist eine SmartCard, wie funktioniert sie?
- Wie sieht es mit der Sicherheit aus?
- Welche Zertifizierungsdiensteanbieter gibt es, was ist in der Planung?
- Welche Anwendungen gibt es bereits?
- Warum hat sich das bisher nicht so richtig durchgesetzt?
- Brauchen wir das ganze überhaupt?

Was ist eine elektronische Signatur?

- Sicherstellen von Integrität und Authentizität von elektronisch vorliegenden Daten mittels kryptographischer Algorithmen
- Erfolgt mit Hilfe eines elektronischen Zertifikats einer vertrauenswürdigen Stelle, welche die Identität des Zertifikatsinhabers kennt
- Ein Zertifikat ist eine Datenstruktur, welches Informationen über den Inhaber und seine kryptographischen Schlüssel enthält
- Das Zertifikat kann auf einer Chipkarte untergebracht werden und mittels PIN gesichert sein
- Qualifizierte elektronische Signaturen schaffen Rechtsverbindlichkeit in der elektronischen Kommunikation

Wie funktioniert die Signatur?



Quelle: Bundesamt für Sicherheit in der Informationstechnik
<http://www.bsi.bund.de/literat/faltbl/F10ElektronischeSignatur.htm>

Was ist eine PKI?

- Zur elektronischen Signatur wird ein Schlüsselpaar (privater und öffentlicher Schlüssel) benötigt und ein Zertifikat mit den Daten des Inhabers
- Aufgabe einer PKI ist
 - Die Verwaltung von öffentlichen Signaturschlüsseln
 - die Sicherstellung, dass der öffentliche Schlüssel zu der Person gehört, die als Eigentümer des öffentlichen Schlüssel (und des damit zugehörigen privaten Schlüssels) ausgewiesen ist (Beglaubigung bzw. Zertifizierung)
 - Zu einer PKI gehören eine oder mehrere Zertifizierungsinstanzen (CA), welche sich der gleichen Policy unterworfen haben
- Eine PKI ist in der Regel hierarchisch organisiert im Gegensatz zu PGP

Wie sieht die rechtliche Seite aus?

- Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (1. Version von 1997)
- Signaturverordnung vom 16. November 2001 erläutert explizit die Verfahren
- EU-Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen vom 13.12.1999 vereinheitlicht die Kommunikation und den Rechtsverkehr auf EU-Ebene
- Mit § 126a BGB wird die elektronische Form zur Alternative für die eigenhändige Unterschrift
- Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001 (BGBl. I, S. 1542)
- Durch die Nutzung qualifizierter elektronischer Signaturen in der Verwaltung und bei ihren Kommunikationspartnern kann die Rechtsverbindlichkeit signierter elektronischer Dokumente bei Anwendungen mit Schriftformerfordernis erreicht werden

Wie sieht die rechtliche Seite aus?

(2)

- Diese Gesetze regeln, dass die Schriftform durch die mit einer qualifizierten elektronischen Signatur verbundene elektronische Form ersetzt werden kann
- Bei Anwendungen ohne Formerfordernis kann weiterhin jede Form elektronischer Kommunikation verwendet werden

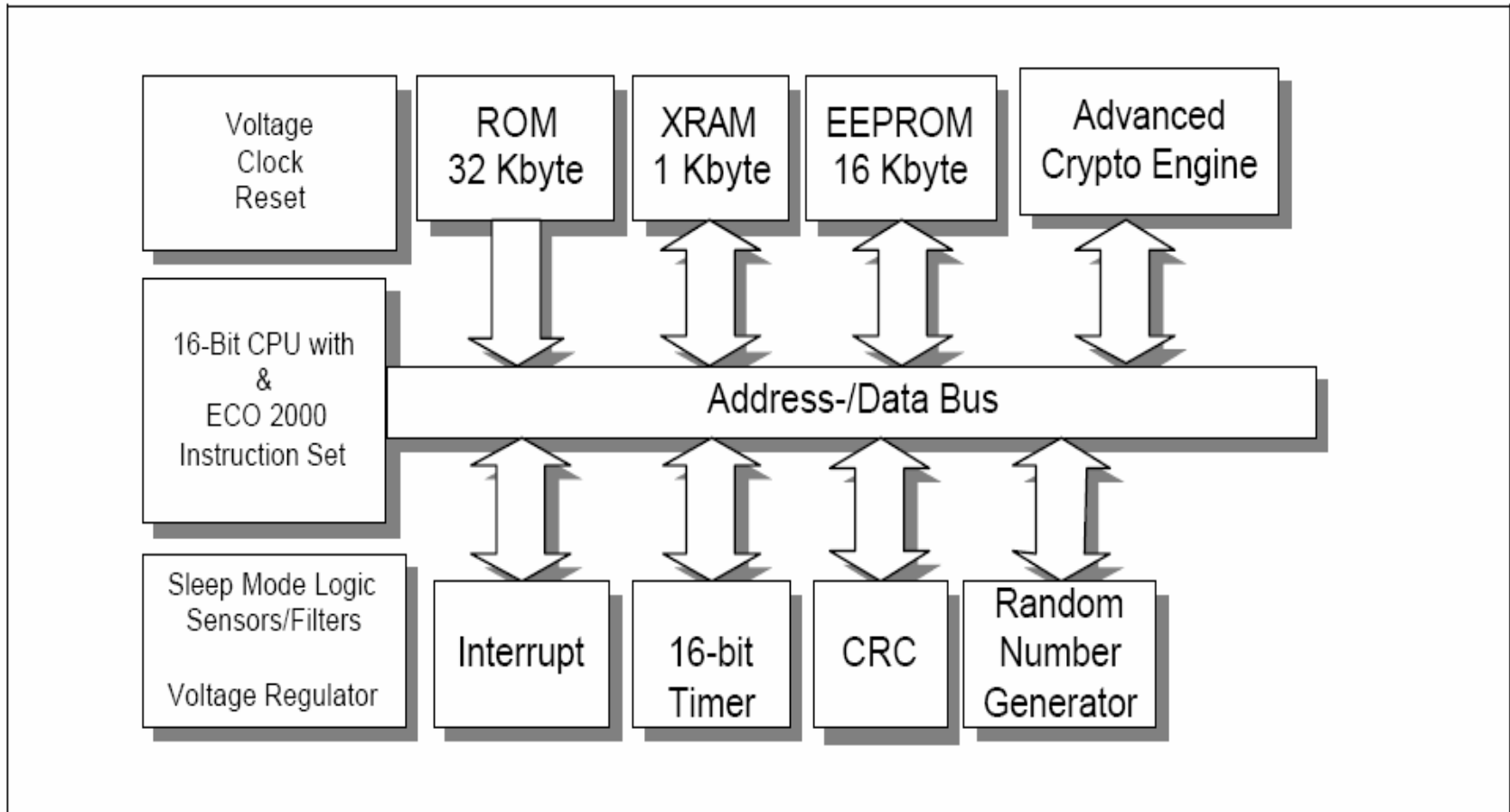
Qualifizierte Signatur

- Produkte für qualifizierte elektronische Signaturen sind
 - sichere Signaturerstellungseinheiten
 - technische Komponenten für Zertifizierungsdiensteanbieter
 - Signaturanwendungskomponenten

Was ist eine SmartCard, wie funktioniert sie?

- Im Gegensatz zu Speicherkarten verfügen SmartCards über einen vollständigen Rechner mit CPU, Speicher, Peripherie und Betriebssystem (z.B. SLE66CX160S – 4 KB EEPROM, 32 KB ROM, 1024 Byte RAM, CryptoEngine, Timer, etc.)
- SmartCards haben verschiedene Speicherbereiche, auf denen Daten abgelegt werden können
- SmartCards können Berechnungen wie z.B. die Verschlüsselung durchführen
- Teilweise können auch Schlüssel auf der Karte erzeugt werden
- Es gibt verschiedene Hersteller (z.B. Infineon, G&D, GemPlus) und unterschiedliche Betriebssysteme (z.B. CardOS, TCOS, StarCOS)
- SmartCards unterstützen Standard-Schnittstellen (ISO 7816 für den physikalischen Zugriff), PKCS#11 oder OCF bzw. PKCS#15 für den Zugriff auf die Objekte und Funktionen und auf das Dateisystem

Architekturbeispiel (Quelle: Infineon)



Wie sieht es mit der Sicherheit aus?

- Komplexes Gesamtsystem, die Sicherheit hängt von allen Einzelgliedern ab
- Unterschiedliche Sicherheitsniveaus lt. SigG
 - Einfache Signatur
 - Fortgeschrittene Signatur
 - Qualifizierte Signatur
 - Qualifizierte Signatur mit Anbieterakkreditierung
- Sicherheitsaspekte der qualifizierten Signatur werden definiert durch Gesetze und Verordnungen
- Es folgen einige Definitionen, die aus folgender Veröffentlichung übernommen wurden:
<http://www.bsi.bund.de/literat/faltbl/F10ElektronischeSignatur.htm>

Technische Sicherheit qualifizierter Signaturen (Quelle: BSI)

- Die technische Sicherheit qualifizierter elektronischer Signaturen beruht vor allem auf folgenden Faktoren:
 - sichere kryptographische Verfahren
 - einmalige Signaturschlüsselpaare
 - zuverlässige Bindung der geheimen, privaten Signaturschlüssel an die rechtmäßigen Nutzer
 - Ausschluss nicht gewollter digitaler Signaturen
 - zuverlässige Nachprüfung der Gültigkeit von Zertifikaten

Signaturerstellungseinheiten (Quelle: BSI)

- **Sichere Signaturerstellungseinheiten** müssen unabhängig vom Einsatz und der Anwendung nach den Sicherheitskriterien "Common Criteria for Technology Security Evaluation" (CC) mit der Prüftiefe EAL 4 gegen ein hohes Angriffspotential und einer vollständigen Missbrauchsanalyse oder nach den "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (ITSEC) mit der Prüftiefe E3 und in beiden Fällen mit der Mechanismenstärke "hoch" durch eine akkreditierte Prüf Stelle geprüft und durch eine Bestätigungsstelle bestätigt werden.

technische Komponenten (Quelle BSI)

- Technische Komponenten für Zertifizierungsdiensteanbieter sind Software- oder Hardwareprodukte, die bestimmt sind:
 - Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen,
 - qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar zu halten oder
 - qualifizierte Zeitstempel zu erzeugen als elektronische Bescheinigung, dass bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben
- Die technischen Komponenten zum Erzeugen oder Übertragen von Signaturschlüsseln müssen mindestens die Prüftiefe nach EAL 4 + oder E3 umfassen.

Signaturanwendungskomponenten (Quelle: BSI)

- Signaturanwendungskomponenten, bestehend aus Software- und Hardwareprodukten, die dazu bestimmt sind,
 - Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder
 - qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen,
- können mindestens nach den Stufen EAL 3+ oder E2 bei einer Mechanismenstärke "hoch" und gegen ein hohes Angriffspotential und einer vollständigen Missbrauchsanalyse geprüft und bestätigt werden. Eine Herstellererklärung reicht aus

Soweit die Theorie...

- In der Praxis hängt die Sicherheit von vielen Faktoren ab
- Immer das Kleingedruckte (z.B. die Einsatzbedingungen) lesen
- Sicherheit ist immer bezogen auf ein Sicherheitsziel
- Medienkompetenz ist durch keinen Stempel zu ersetzen

Welche qualifizierten Zertifizierungsdiensteanbieter gibt es?

- Deutsche Telekom / TeleSec
- Signtrust / Deutsche Post eBusiness
- Bundesnotarkammer
- DATEV eG
- Steuerberaterkammer Nürnberg
- Steuerberaterkammer Saarland
- Hanseatische Steuerberaterkammer Bremen
- Steuerberaterkammer München
- Steuerberaterkammer Berlin
- Steuerberaterkammer Stuttgart
- Rechtsanwaltskammer Koblenz
- Rechtsanwaltskammer Bamberg
- AuthentiDate
- TC Trustcenter
- D-Trust
- Hanseatische Rechtsanwaltskammer Hamburg
- Steuerberaterkammer Niedersachsen
- Wirtschaftsprüferkammer
- Rechtsanwaltskammer München
- Rechtsanwaltskammer Berlin
- Steuerberaterkammer Brandenburg

Welche Anwendungen gibt es bereits?

- In der Privatwirtschaft im Bereich des elektronischen Rechtsverkehrs (z.B. DATEV) verbreitet, ansonsten keine Massenanwendung
- In der öffentlichen Verwaltung:
 - Beantragung von Tierprämien
 - Virtuelle Poststelle
 - CITES-Online (BfN)
 - Handel mit Emissionszertifikaten
 - Virtuelles Bauamt
 - Elektronische Vergabe
 - Elektronischer Rechtsverkehr
 - Demnächst: BAföG-Beantragung
 - Etliche weitere (auch aus Media@Komm) vorhanden
 - Allerdings: längst noch keine Massenanwendung

Warum hat sich das bisher nicht so richtig durchgesetzt?

- Derzeit nur Anwendungen für geschlossene Zielgruppen
- Probleme für die Massenanwendung
 - Signaturen müssen gekauft, umständlich beantragt und installiert werden
 - technisch inkompatible Komponenten (ist in den letzten Jahren besser geworden, aber immer noch nicht wirklich gut)
 - Kreditwirtschaft sucht noch nach einem Geschäftsmodell
 - Staat möchte die Ausstattung der Bürger nicht bezahlen
 - Henne / Ei – Problem: keine Signaturkarten, keine Anwendungen – keine Anwendungen, keine Signaturkarten
- Media@Komm sollte Anwendungen erproben
- Signaturbündnis sollte als Ausweg etabliert werden

Brauchen wir das ganze überhaupt?

- Für viele Anwendung im Internet wird keine elektronische Signatur benötigt (z.B. Bücher kaufen)
- Für bestimmte Applikationen allerdings schon
- Die Sicherheit wird auf jeden Fall erhöht, alleine durch die Signatur allerdings nicht
- Rechtliche Verbindlichkeit gibt es nur mit elektronischer Signatur