Elektronische Signaturen

Das Gesetz über Rahmenbedingungen für elektronische Signaturen und die Auswirkungen auf die Vertrauenswürdigkeit und Anwendung der elektronischen Signatur

Dr. Thomas Schöller
Referent beim Bundesamt für Sicherheit in der Informationstechnik
Referat: Zertifizierung und Zulassung
Bestätigung von technischen Komponenten nach dem Signaturgesetz
Tel: 0228 9582-115 Fax: -455 / Thomas.Schoeller@bsi.bund.de

Historie

- Informations- und Kommunikationsdienste-Gesetz -IuKDG vom 22.07.1997; Artikel 3

  Gesetz zur digitalen Signatur (Signaturgesetz) vom 01. August 1997
- Signaturverordnung vom 01.11.1997
- Erlass der Richtlinie 1999/93/EG des europäischen Parlaments und des Rates „über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“ erfolgte am 13. Dezember 1999
- Anpassung des - Gesetzes zur digitalen Signatur - vom 01. August 1997 an die EU-Richtlinie

Historie

- Das „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“ tritt am 22.05.2001 in Kraft
- Die dazugehörige Signaturverordnung wurde am 24.10.2001 vom Kabinett beschlossen und wird voraussichtlich im Dezember 2001 am Tag nach der Veröffentlichung im Bundesanzeiger in Kraft treten

Signaturvorgang

☆ **Welche Anforderungen stellen wir an ein unterschriebenes Dokument?**

Der Empfänger muss sich sicher sein, dass das Dokument authentisch ist und die Unterschrift (als Willenserklärung des Unterzeichners) den Unterzeichner eindeutig identifiziert.

🕐 **Elektronische Umsetzung der Unterschrift!**

Über das Dokument (oder beliebige Bitfolge) wird ein Hash-Wert (Fingerabdruck des Dokumentes) gebildet. Mit dem privaten (geheimen) Schlüssel wird der Hash-Wert signiert (verschlüsselt).

Versendet oder gespeichert (archiviert) wird: Das Dokument im Klartext, die Signatur (verschlüsselter Hash-Wert) und das Zertifikat (amtliche Bindung zwischen der natürlichen Person und seinem öffentlichen Schlüssel) und ggf. weitere Anhänge.

Verifizieren von elektronischen Signaturen

- **Echtheitsprüfung des Dokuments**

  Das Klartext-Dokument wird mit dem entsprechenden Hashalgorithums gehasht.

  Der mitgelieferte signierte Hashwert wird mit dem öffentlichen Schlüssel (aus Zertifikat) entschlüsselt.

  Vergleich der beiden Hash-Werte.

- **Identität des Unterzeichners**

  Der Name wird aus dem Zertifikat entnommen.

- **Echtheits- und Gültigkeits-Prüfung des Zertifikats**

  Online-Prüfung des Zertifikats bei dem ausstellenden Zertifizierungsdiensteanbieter.

Sicherheits-Anforderungen an die PKI (SigG)

- **Zertifizierungsdiensteanbieter**

  Ein Zertifizierungsdiensteanbieter ist eine Stelle oder eine juristische oder eine natürliche Person, die Zertifikate ausstellt oder andere Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt.

  - Schlüsselgenerierung

  Erzeugung und Übertragung von Signaturschlüsseln

  Eignung, Einmaligkeit, Geheimhaltung, Speicherung nur auf der sicheren Signaturerstellungseinheit (z.B. Chipkarte)

  - Vergabe von qualifizierten Zertifikaten

  Personen zuverlässig identifizieren

  Zuordnung eines Signaturprüfschlüssels zur id Person bestätigen

  qualifizierte Zertifikat nachprüfbar und abrufbar (nach Zustimmung) halten (Sperrlisten führen)

  - Ausstellen von qualifizierten Zeitstempeln

Sicherheits-Anforderungen an die PKI (SigG)

- **sichere Signaturerstellungseinheiten**

  müssen gewährleisten

  - dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrischer Merkmale angewendet werden kann.
  - keine Preisgabe des Signaturschlüssels
  - keine Möglichkeit des Duplizierens des Signaturschlüssels
  - bestimmte Eigenschaften an das Schlüsselpaar (siehe Vortrag von Herrn Dr. Niedermeyer)

Sicherheits-Anforderungen an die PKI (SigG)

- **Signaturanwendungskomponenten**

  müssen gewährleisten, dass

  bei der Erzeugung einer qualifizierten elektronischen Signatur

  - die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden
  - eine Signatur nur durch die berechtigt signierende Person erfolgt
  - die Erzeugung einer Signatur vorher eindeutig angezeigt wird.

Sicherheits-Anforderungen an die PKI (SigG)

Signaturanwendungskomponenten

müssen gewährleisten, dass

bei der Prüfung einer qualifizierten elektronischen Signatur

- die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und
- eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

Sicherheits-Anforderungen an die PKI (SigG)

☆ Technische Komponenten für Zertifizierungsdienste

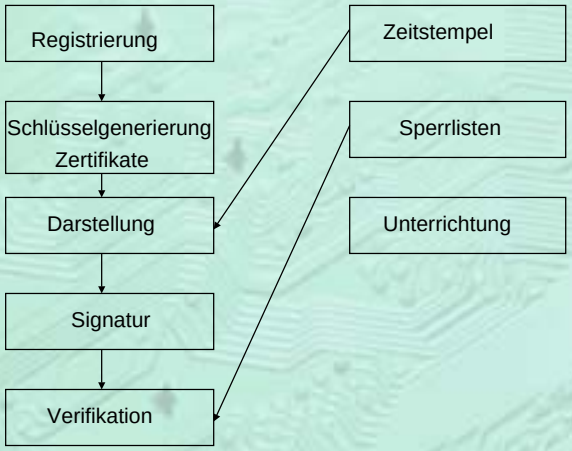
müssen gewährleisten, dass

- die Sperrung eines qualifizierten Zertifikats nicht unbemerkt rückgängig gemacht wird und
- die Auskünfte auf ihre Echtheit überprüft werden können
- die zum Zeitpunkt der Erzeugung des qualifizierten Zeitstempels die gültige gesetzliche Zeit unverfälscht in diesen aufgenommen wird

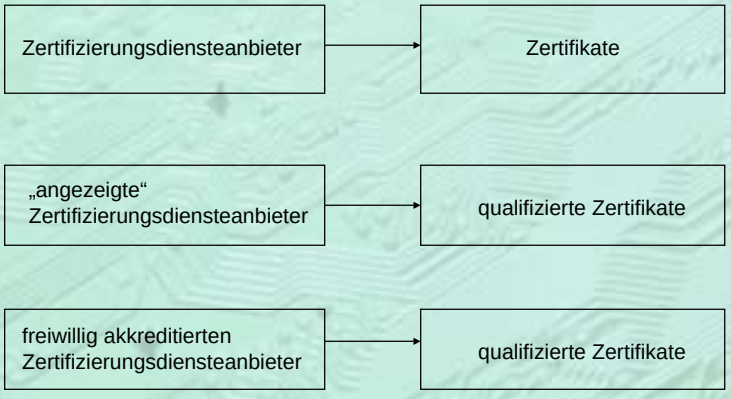
Hinweis zu den Auskünften:

Die Auskünfte müssen beinhalten, ob die nachgeprüften qualifizierten Zertifikate im Verzeichnis der qualifizierten Zertifikate zum angegebenen Zeitpunkt vorhanden und ob sie nicht gesperrt waren. Nur nachprüfbar gehaltene qualifizierte Zertifikate dürfen nicht öffentlich abrufbar sein.

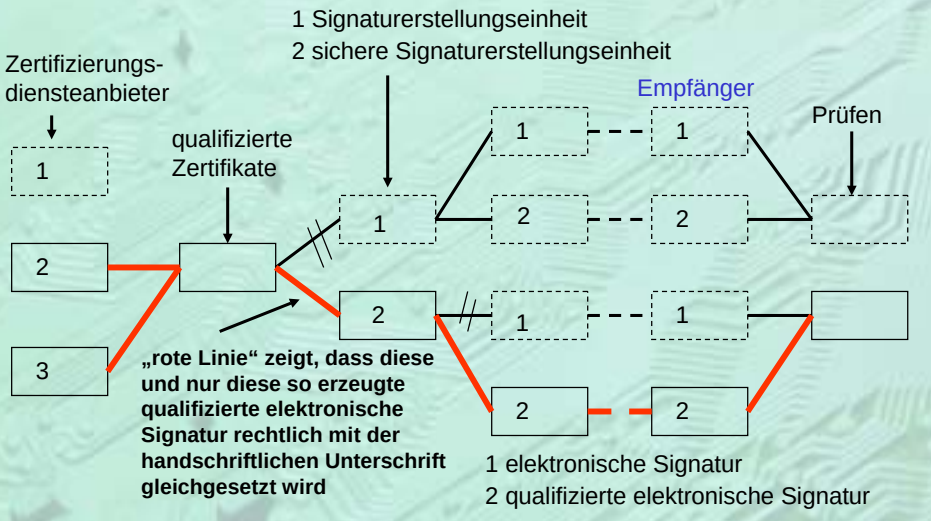
Kette der Sicherheit



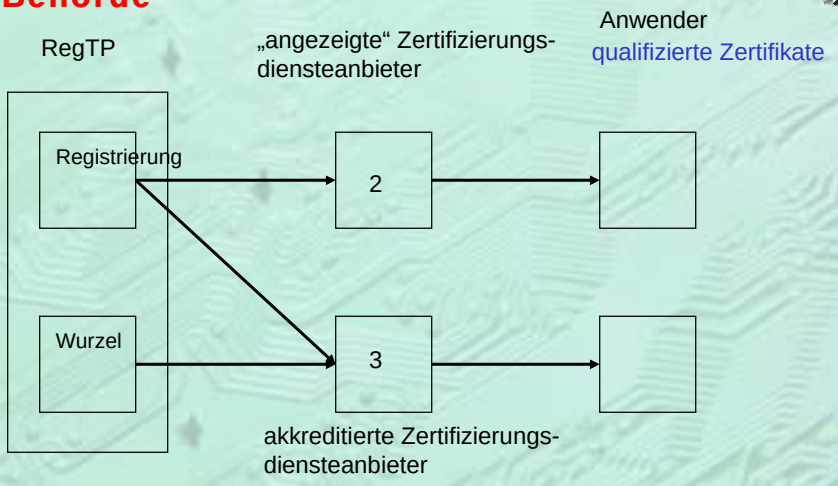
Zertifizierungsdiensteanbieter nach SigG



Realisierungsmöglichkeiten nach SigG



Registrierung bei der „zuständigen Behörde“



Prüfungen der technischen Komponenten (Nachweise der Anforderungen)

Technische Komponenten für akkreditierte Zertifizierungsdiensteanbieter

- Erzeugen und Laden von Schlüsseln — EAL 4-hoch+ / E3-hoch
- sichere Signaturerstellungseinheiten — EAL 4-hoch+ / E3-hoch
- Darstellung, Erzeugung und Überprüfung — EAL 3-hoch+ / E2-hoch+
- **die außerhalb eines besonders gesicherten Bereichs (TC) eingesetzt werden**
- Nachprüfbarhalten von Zertifikaten — EAL 4-hoch+ / E3-hoch+
- Erzeugen von Zeitstempeln — EAL 4-hoch+ / E3-hoch
- **die innerhalb eines besonders gesicherten Bereichs (TC) eingesetzt werden**
- Nachprüfbarhalten von Zertifikaten — EAL 3-hoch+ / E2-hoch+
- Erzeugen von Zeitstempeln — EAL 3-hoch+ / E2-hoch

Prüfungen der technischen Komponenten (Nachweise der Anforderungen)

Technische Komponenten für „angezeigte“ Zertifizierungsdiensteanbieter

- Erzeugen und Laden von Schlüsseln — EAL 4-hoch+ / E3-hoch
- sichere Signaturerstellungseinheiten — EAL 4-hoch+ / E3-hoch

- Nachprüfbarhalten von Zertifikaten
- Erzeugen von Zeitstempeln
- Darstellung, Erzeugung und Überprüfung

Herstellererklärung

\+ **ergänzend:** es ist gegen ein hohes Angriffspotential zu prüfen und eine vollständige Missbrauchsanalyse durchzuführen.

hoch Widerstand gegen ein hohes Angriffspotential

Prüfungen der technischen Komponenten (Nachweise der Anforderungen)

Technische Komponenten für Anwender qualifizierter Zertifikate

- sichere Signaturerstellungseinheiten EAL 4-hoch+ / E3-hoch

Signaturanwendungskomponenten

- Darstellung, Erzeugen und Prüfen von Signaturen

  Herstellererklärung ist ausreichend, es kann mindestens EAL 3-hoch+ / E2-hoch geprüft und bestätigt werden

Ausblick und Hinweise

- Alle Realisierungsmöglichkeiten der elektronischen Signatur werden im Markt ihre Anwendung finden.
- Die qualifizierten elektronischen Signaturen (rechtliche Gleichsetzung mit der handschriftlichen Unterschrift) werden zunächst dort Anwendung finden, wo sie gesetzlich vorgeschrieben wird.
- Jeder Anwender sollte sich über die Rechtswirkung seiner elektronischen Signatur im Klaren sein und

  sollte Prüfen, ob die technische und administrative Einsatzumgebung **genau** den Angaben der Bestätigung oder des Herstellers entspricht.

Quellen

- BSI http://www.bsi.bund.de, SigG,
- RegTP http://www.regtp.de, Zertifizierungsstellen, bestätigte Produkte
- BMWi http://www.iid.de/iukdg, SigG, SigV, SigVBr.
- ISIS Industrial Signature Interoperability Specification
  http://www.dud.de
- EESSI European Electronic Signature Standardization Initiative
  http://www.ict.etsi.org/eessi/