Publikation der Entscheide des deutschen Bundesverfassungsgerichtes im Internet (Wolfgang Rohrhuber, Leiter der Abteilung EDV und Dokumentation)

I. Problematik

Zunehmend nutzen öffentliche Stellen - und damit auch die Gerichte – die Möglichkeit, amtliche Dokumente über das Internet zu publizieren. Damit kommt der Frage, wie die Authentizität dieser Dokumente sichergestellt werden kann, immer größere Bedeutung zu.

Untersucht man die Veröffentlichungspraxis auf den gerichtseigenen WWW-Seiten, so zeigt sich bezüglich dieses Problems der Absicherung der Integrität der öffentlichten Texte ein äußerst heterogener Befund:

- Die Mehrzahl der Gerichte in Deutschland negiert dieses Problem und veröffentlicht Entscheidungen ohne weitere Sicherheitsvorkehrungen
- Einige Gerichte weisen auf die Problematik hin und erklären einen ausdrücklichen oder versteckten Haftungsausschluss oder erklären die Internetveröffentlichung nicht für verbindlich.
- Sicherung der Authentizität und Integrität der amtlichen Texte durch digitale Signaturverfahren, d. h.: Sicherstellen, daß eine Datei nicht unbemerkt von dritter Seite verändert wird.

II. Die Sicherung der Authentizität der aufliegenden Urteile durch eine digitale Signatur

1. technische Voraussetzungen – Prinzip der digitalen Signatur

Beim Bundesverfassungsgericht wird zur Zeit das Public-Key- oder asymmetrisches kryptographisches Verfahren angewendet. Dieses basiert auf der Verwendung eines privaten und eines öffentlichen elektronischen Schlüssels. Der private Schlüssel dient dabei zur Verschlüsselung der Nachricht auf der Sender-Seite, der dazugehörige öffentliche Schlüssel wird zur Entschlüsselung durch den Empfänger benötigt.

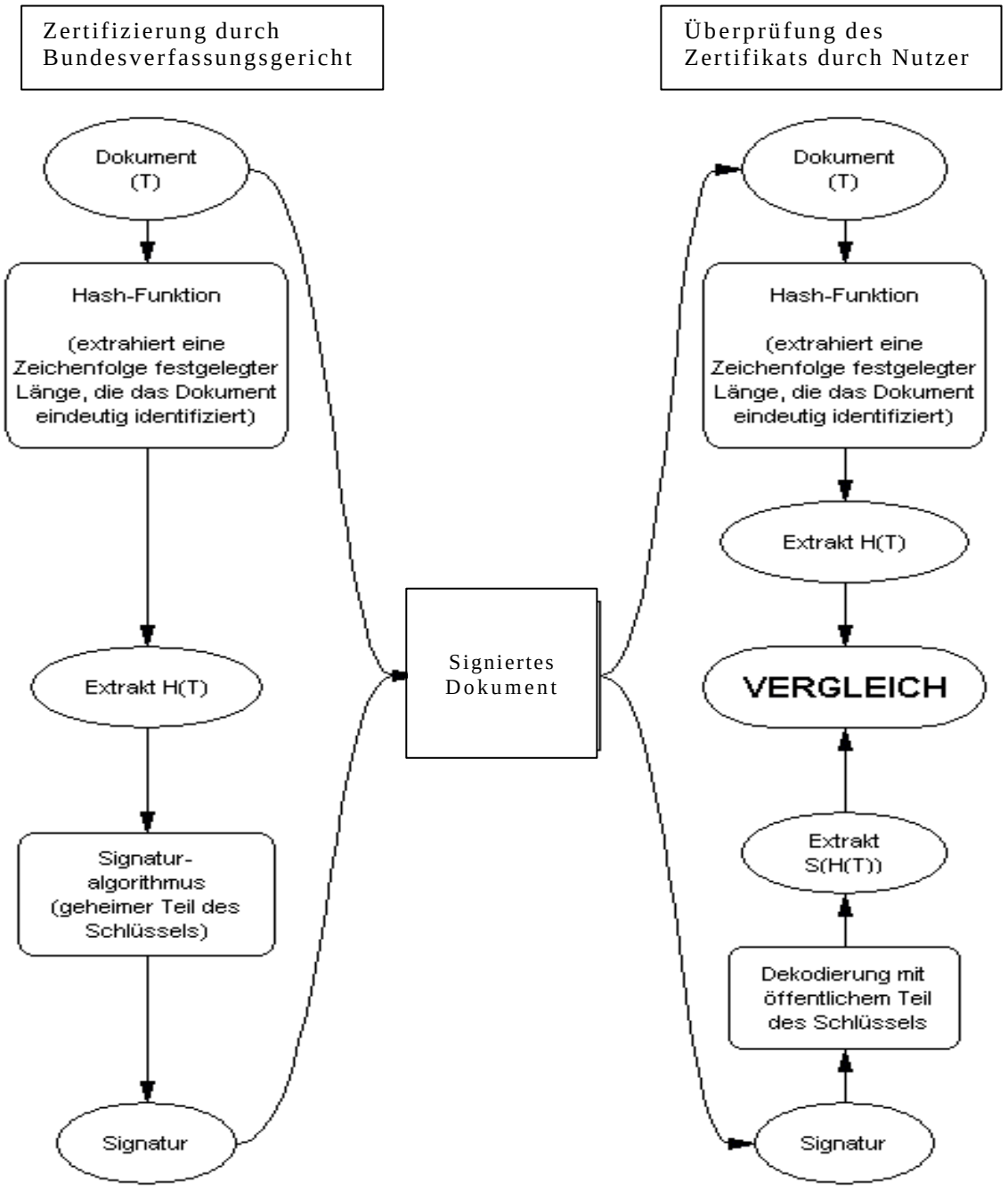
Voraussetzung für das Verfahren ist die Einschaltung sogenannter Trustcenter, die für die Generierung der Schlüsselpaare verantwortlich sind. Dieses geschieht unter strengen Sicherheitsmaßnahmen, die einer ständigen Überprüfung durch die Regulierungsbehörde unterliegen, da der private Schlüssel unbedingt geheim gehalten werden muss. Weiterhin darf kein Schlüssel-Code mehrmals ausgegeben werden, um eine eindeutige Identifizierung des Absenders gewährleisten zu können.

Eine weitere Aufgabe der Trustcenter ist die Zertifizierung des öffentlichen Schlüssels, d.h. die Trustcenter bescheinigen, dass der öffentliche Schlüssel auch wirklich zum Inhaber des Schlüsselpaares gehört. Zur Erstellung eines solchen Zertifikates werden lediglich die Angaben des ausgefüllten Antrages sowie eine Kopie des gültigen Personalausweises oder Reisepasses benötigt. Erst wenn der Antragsteller, der eine natürliche Person sein muss, auf diese

Weise identifiziert werden konnte, erhält er seine digitale Signatur, die dazugehörige PIN, die Software sowie die nötigen Komponenten. Das digitale Signieren jedes Zertifikates durch die Trustcenter ermöglicht es dem Empfänger, die Inhalte des Zertifikates auf ihre Richtigkeit zu überprüfen und somit den Absender zu identifizieren.

Weiterhin können einem Zertifikat Attribute hinzugefügt werden, die auf besondere Eigenschaften, eine bestimmte Stellung oder eine Beschränkung des Zertifikat-Inhabers hinweisen. Beispielsweise ist es möglich eine Berufsbezeichnung oder die Vertretungsmacht für eine andere Person aufzunehmen.

Im Ablaufmodell gewinnt das Ganze folgende Gestalt:



2. Der Mechanismus zur Überprüfung

Da für die Signatur auf Seiten des Gerichts das Programm PGP verwendet wird, muss dieses auch vom Nutzer, der die digitale Signatur überprüfen möchte, installiert sein.
Desweiteren müssen die Schlüssel derjenigen Mitarbeiter des Bundesverfassungsgerichts, die die Urteile signiert haben, in das lokale PGP importiert sein.

Zur einfacheren Handhabung wurde eine Nutzungsanleitung für die Besucher der WWW-Seite des Bundesverfassungsgerichts in die Entscheidungssammlung des Gerichts aufgenommen:

Dort heißt es:

1. Rufen Sie mit Ihrem Browser den Key-Server der Zertifizierungsinstanz auf unter: https://www.iks-jena.de/cgi-bin/ca-iks.lookup.pl

2. Suchen Sie in dem vorgegebenen Formular für die PGP-Suche nach "bundesverfassungsgericht.de". Es wird nun eine Liste von Namen und Schlüsseln ausgeworfen.

3. In der Liste ist linker Hand die Schlüsselidentifizierungsnummer verlinkt auf den eigentlichen Schlüssel. Klicken Sie auf die Identifizierungsnummer. (Die Identifizierungsnummern sehen ungefähr so aus: 442CD201) Es erscheint nun eine Datei, die mit "BEGIN PGP PUBLIC KEY BLOCK" beginnt. Speichern Sie diese Seite in einem Verzeichnis unter einem Namen, der mit "asc" endet. Im Beispiel wäre das der Dateiname "rigo.asc". Wiederholen Sie diesen Vorgang, bis Sie alle Schlüssel des Bundesverfassungsgerichts auf die Festplatte gespeichert haben.

4. Importieren Sie nun diese Schlüssel in Ihr PGP. Falls Sie die Windows-Version benutzen, müssen Sie dazu PGP-Keys aufrufen. Unix-Benutzer müssen pgp -ka "datei mit den Schlüsseln" eingeben.

Falls Sie PGP korrekt installiert und die Schlüssel korrekt importiert haben, können Sie nun die Authentizität der Urteile überprüfen, auch wenn diese nicht direkt vom Server des Bundesverfassungsgerichts herrühren. Dazu gehen Sie wie folgt vor:

1. Wenn das Dokument in ihrem Browser geladen ist, speichern Sie es auf Ihrer Festplatte ab. (z.B. unter dem Namen Urteil.asc)

2. Rufen Sie PGP auf. Unter Unix genügt es pgp "Dateiname" einzugeben. Unter Windows müssen Sie die Datei mit einem Doppelklick aufrufen. Eine andere Möglichkeit ist es, mit PGP-TOOLS die Datei aufzurufen.

3. Wenn alles geklappt hat, erscheint eine Meldung, die folgenden Inhalt haben könnte, je nachdem, welcher Dokumentar unterschrieben hat:

BESTÄTIGTE Unterschrift von "Wolfgang Rohrhuber , EXPIRE:2001-09-01", Unterschrift erzeugt am 1999/09/18 17:18 GMT mit 2048-Bit-Schlüssel 0x2D1C9C4F

oder

BESTÄTIGTE Unterschrift von "Peter Maier , EXPIRE:2001-09-01", Unterschrift erzeugt am 1999/09/18 17:18 GMT mit 2048-Bit-Schlüssel 0xDDBB20FB

Unter Windows taucht ein Fenster auf, das einen Status der Signatur anzeigt. Neben dem erkannten Autor der Signatur muss ein grünes Licht leuchten. Bei anderen PGP-Versionen ist das grüne Licht am Anfang der Zeile.