



## Das elektronische Nachweisverfahren - Sicher elektronisch „unterschreiben“

### Eine Information zur qualifizierten Signatur für Erzeuger, Entsorger und Beförderer von gefährlichen Abfällen

#### Einsatz der elektronischen Form

Alle Dokumente im Nachweisverfahren sind künftig als elektronische Datensätze auszutauschen und elektronisch zu „unterschreiben“. Für die Unterschrift bedeutet dies: die bisherigen handschriftlichen Unterschriften unter den Formularen sind in den elektronischen Dokumenten durch eine elektronische Signatur zu ersetzen. Diese Dokumente umfassen u. a. **Entsorgungsnachweise, Begleitscheine** und **Register** (ersetzt das bisherige Nachweisbuch) und werden am PC erzeugt und kommuniziert. Dies gilt sowohl für alle **Nachweispflichtigen** als auch für alle zuständigen **Behörden**.

#### Rechtlicher Hintergrund

Der rechtliche Rahmen ergibt sich durch die Verknüpfung der **Nachweisverordnung** (1) mit dem Verwaltungsverfahrensgesetz (2), dem **Signaturgesetz** (3) und der darauf beruhenden **Signaturverordnung** (4). Die rechtliche Gleichstellung mit der qualifizierten elektronischen Signatur im Verwaltungsverfahren hat der Gesetzgeber zunächst mit dem 3. Änderungsgesetz zum Verwaltungsverfahrensgesetz, die Anforderungen an die Signatur selbst mit dem Signaturgesetz und der Signaturverordnung bestimmt. Das Signaturgesetz kennt verschiedene Arten der elektronischen Signaturen. Als Ersatz für handschriftliche Unterschriften nicht ausreichend sind bloße „elektronische Signaturen“ oder „fortgeschrittene elektronische Signaturen“. Vielmehr ist es notwendig, dass die elektronischen Dokumente mit einer **qualifizierten elektronischen Signatur** versehen werden. Nur diese Art von Signatur bietet im elektronischen Nachweisverfahren - als eine Art „digitaler Fingerabdruck“ – die mit der herkömmlichen Unterschrift vergleichbare Rechtsverbindlichkeit (siehe [www.bsi.de](http://www.bsi.de)).

#### Die qualifizierte elektronische Signatur

Die qualifizierte elektronische Signatur muss wie die Handunterschrift an eine (natürliche) Person gebunden sein. Die Abfolge der elektronischen Signatur – also wer signiert in welcher Reihenfolge – verläuft wie im Papierverfahren.

Überall dort, wo rechtsverbindliche Willenserklärungen eine Unterschrift erfordern und es auf

- vertrauenswürdige Kommunikation (Authentizität),
- sichere Identifikation und
- Integrität elektronischer Daten ankommt,

ist die gesetzeskonforme qualifizierte elektronische Signatur einsetzbar. Für die

Kommunikation bedeutet es, dass der Urheber der Nachricht sicher zu identifizieren ist und die Nachricht unverfälscht den Empfänger erreicht.

#### Inhalt:

##### Elektronisch „unterschreiben“

- Einsatz der elektronischen Form
- Rechtlicher Hintergrund
- Die qualifizierte elektronische Signatur
- Schlüsselpaar
- Erwerb und Einsatz
- Betriebliche Voraussetzungen
- Reihenfolge der Signaturen
- Zeitplan

##### Hintergrundinformationen zu folgenden Themen:

- Rechtsquellen
- HASH-Wert
- PIN-Eingabe
- Kartenlesegeräte und Signaturkarte

#### Rechtsquellen:

- (1) Verordnung zur Vereinfachung der abfallrechtlichen Überwachung vom 20. Oktober 2006 (BGBl. I S. 2298, Artikel 1 dieser Verordnung: Nachweisverordnung)
- (2) Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), geändert durch Artikel 4 Abs. 8 des Gesetzes vom 5. Mai 2004
- (3) Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Art. 4 des Gesetzes vom 26.2.2007 (BGBl. I S. 179)
- (4) Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

## Was bedeutet „privater“ und „öffentlicher“ Schlüssel (Schlüsselpaar)

Zur Erzeugung und Überprüfung einer qualifizierten elektronischen Signatur benötigt man immer ein Schlüsselpaar aus

- einem persönlichen, geheimen (privaten) Schlüssel und
- einem passenden öffentlichen Schlüssel,

die aus geeigneten Algorithmen erzeugt werden. Vereinfacht dargestellt beruht das Verfahren auf zwei mathematischen Prüfschlüsseln, die einander zugeordnet sind, nämlich ein privater und ein öffentlicher Schlüssel. Der damit erzeugte „elektronische Fingerabdruck“, der sog. **HASH-Wert**, wird mit dem zu signierenden elektronischen Dokument verbunden. Hierdurch werden eine sichere Authentifizierung für den jeweiligen Kommunikationspartner sowie eine Vertraulichkeit hergestellt und eine Prüfung der Integrität der übermittelten Daten ermöglicht.

Beide Schlüssel sind einer natürlichen Person fest zugeordnet. Der private Schlüssel darf Unbefugten nicht zugänglich gemacht werden. Er ist aufgrund der Sicherheitsanforderungen in einer Chipkarte eingebracht und sicher gegen Auslesung geschützt. Die qualifizierte elektronische Signatur wird mit dem zu signierenden elektronischen Dokument verknüpft, indem die Chipkarte des jeweiligen Zertifizierungsdiensteanbieters (Trust-Center) in dem dazugehörigen Lesegerät und die Signaturanwendungskomponente der entsprechenden Software aktiviert werden (siehe [www.bundesnetzagentur.de](http://www.bundesnetzagentur.de)).

Der Empfänger kann mit dem zum privaten Schlüssel passenden öffentlichen Schlüssel die Nachricht wieder entschlüsseln und die Identität des Absenders feststellen. Zugleich kann er das elektronische Dokument in Klarschrift lesen.

## Erwerb und Einsatz der qualifizierten elektronischen Signatur

Zu Ihrem PC und dem Internetanschluss benötigen Sie zusätzlich eine Signaturkarte und ein Chipkartenlesegerät mit entsprechender Treibersoftware. Beides erhalten Sie üblicherweise von einem Trust-Center. Informationen hierüber können Sie z. B. bei den IHKs und Ihren Verbänden einholen.

### Was passiert bei der PIN-

#### Eingabe:

Beim Signieren werden durch die PIN-Eingabe die Chip-Daten über ein Kartenlesegerät aktiviert und mit dem Dokument virtuell verbunden und somit "versiegelt". Die "Versiegelung" gewährleistet die Sicherheit der Daten. Durch die besonderen Verschlüsselungsverfahren, die mit Hilfe dieser Chip-Karte durchlaufen werden, ist die Signatur später dem Unterzeichner eindeutig zuzuordnen (Datenauthentizität). Zudem kann zu jeder Zeit festgestellt werden, ob ein Dokument inhaltlich verändert wurde (Datenintegrität).

Nach erfolgreicher Installation legen Sie die Signaturkarte in das Lesegerät ein. Nach dem Start Ihrer „Abfallwirtschaftssoftware“ oder der Internetanwendung Länder-eANV (elektronisches Abfallnachweisverfahren der Länder) auf der Seite [www.zks-abfall.de](http://www.zks-abfall.de) rufen Sie das entsprechende Nachweisformular auf und füllen es aus. Zur rechtsverbindlichen Signierung muss nun Ihre Software aktiviert werden, um mit dem Signiervorgang das Nachweisformular letztendlich zu vervollständigen. Sie tippen Ihre PIN ein und der Vorgang ist zum Versand an die Zentrale Koordinierungsstelle Abfall (ZKS-Abfall) bereit (vereinfachte Darstellung!).

Das Lesegerät muss nach dem SigG geprüft und bestätigt sein sowie eine sichere PIN-Eingabe ermöglichen. Eine Übersicht der anerkannten Kartenlesegeräte ist unter dem Stichwort „qualifizierte elektronische Signatur“ zu erhalten ([www.bundesnetzagentur.de](http://www.bundesnetzagentur.de)). Der aktuelle Standard sieht mittlerweile eine 2048 Bit-Karte sowie die Ansteuerung

von Kartenlesern ab der Sicherheitsklasse 2 über ct-api (d.h. sichere Eingabe der PIN übers Pinpad - Card Terminal Application Programming Interface vor; mit der CT-API kann man die

### Was bedeutet der Hashwert:

Hashwert bezeichnet einen alphanumerischen Wert, der durch eine so genannte Hashfunktion erzeugt wird. Diese mathematische Funktion wird auf „Daten“ angewendet und liefert bei gleichen Daten stets den gleichen Hashwert. Mit einem Hashcode werden z. B. Binärdokumente gekennzeichnet, um deren Authentizität beim Empfänger prüfbar zu machen, ohne den Inhalt des Dokuments selbst offenzulegen.

Schnittstelle der Chipkarten ansprechen). Eine auf dem Bildschirm eines PC integrierte Eingabe entspricht nicht den Datensicherheitsmerkmalen. Wichtig ist, dass die eingesetzte Hardware (Lesegerät) mit der Software kompatibel ist.

**Betriebliche Voraussetzungen**



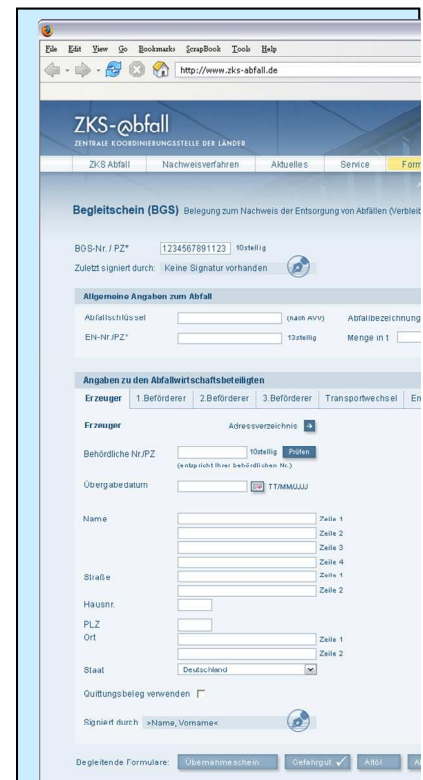
Während des Betriebes ist das Ablaufdatum der Gültigkeit eines Zertifikates zu beachten. Der Gültigkeitszeitraum beträgt je nach Zertifikatsanbieter (Trust-Center) bis zu vier Jahren. Es muss sichergestellt sein, dass die Tauglichkeit des Zertifikats zum Signieren und Verschlüsseln während des Betriebs gegeben ist. Es ist darauf zu achten, dass im Falle von Verlust oder Diebstahl die Sperrung der Karte erfolgt. Ebenso sollte eine Stornomeldung erfolgen, wenn ein Rücktritt vom Zertifizierungsantrag beabsichtigt wird. Es ist im Vorfeld abzuklären, wie der Ablauf infolge einer notwendigen Folgekarte oder Ersatzkarte aussieht. Die Software sollte verschiedene Funktionalitäten

unterstützen können, wie z.B. Mehrfachsignatur, Nutzung des Zeitstempels zur sekundengenauen Authentifizierung, Verschlüsselung von Dateien für beliebig viele Empfänger, Einbindung von Adressbüchern (z.B. Outlook), E-Mail Versand, Up und Download – Fähigkeit, Unterstützung verschiedener Formate, etc.

**Reihenfolge der Signaturen**

Nach der NachwV (§19 Absatz 1) wird gefordert, dass die qualifizierte elektronische Signatur der jeweiligen Erklärungen oder sonstigen Dokumente zu den Zeitpunkten zu setzen ist, zu denen auch im Formularverfahren die Formblätter zu unterschreiben sind; hierbei ist die Reihenfolge im Sinne des Entsorgungsablaufes einzuhalten. Das gilt auch für Änderungen. Zum Nachweis der **Reihenfolge der Signaturen** wird in den Datensätzen der Signaturzeitpunkt sekundengenau festgehalten. Zudem sind die qualifizierten elektronischen Signaturen in den Datensätzen derart integriert, dass die Abfolge der Signaturen auch an den Dokumenten selbst erkennbar ist.

Um die Handhabung der elektronischen Signatur während der **Beförderung** zu erleichtern, besteht eine Option für den Beförderer darin, dass der Begleitschein nicht nur „bei“ (Erzeugerstandort), sondern auch „nach“ Übernahme der Abfälle durch den Abfallbeförderer, spätestens aber vor Signatur des Entsorgers (Entsorgerstandort), qualifiziert elektronisch signiert werden kann, soweit dies schriftlich zwischen Abfallerzeuger und Abfallbeförderer vereinbart wird. Die Vereinbarung kann sich auf eine Vielzahl von Transporten beziehen, muss also nicht einzelfallbezogen formuliert sein. Nach Sinn und Zweck muss diese **Vereinbarung** während des Transports mitgeführt werden. Der Abfallbeförderer darf nach





Übernahme der Abfälle den Begleitschein somit auch bei Übergabe der Abfälle an den Abfallentsorger qualifiziert signieren. Eine solche Signatur kann direkt am Fahrzeug, vom Firmenstandort (Officelösung) oder an der Anlage des Abfallentsorgers (aber zeitlich vor dem Abfallentsorger!) erfolgen. D.h. der Abfallbeförderer darf nach Übernahme der Abfälle den Begleitschein somit auch erst bei Übergabe der Abfälle an den Abfallentsorger qualifiziert signieren. Er kann insbesondere die hierfür geeigneten Einrichtungen im Annahmehbereich des Entsorgungsunternehmens nutzen.

## Was ist zu beachten

Die Verfahrensbeteiligten sollten

- die eigenen Geschäftsprozesse durchleuchten und ggf. an das elektronische Nachweisverfahren anpassen,
- festlegen, welches Kommunikationsmodell sie nutzen möchten,
- festlegen, an welcher Stelle eine qualifizierte elektronische Signatur notwendig ist,
- die Unterschriftenregelungen anpassen,
- die entsprechenden Mitarbeiter mit der persönlichen Signaturkarte ausstatten,
- die erforderlichen internen EDV-Entscheidungen direkt herbeiführen,
- die Implementierung des Verfahrens mit der geplanten technischen Lösung umsetzen,
- die Einhaltung der Datenformate und Kommunikationsbedingungen rechtzeitig mit der Zentralen Koordinierungsstelle Abfall ([www.zks-abfall.de](http://www.zks-abfall.de)) erproben,
- die Anforderungen des BSI an einen IT-Grundschutz für die EDV-Anwendungen berücksichtigen.

### Kartenlesegeräte und Signaturkarte:

Zur Signatur Ihrer Daten benötigen Sie eine Signaturkarte und ein Kartenlesegerät. Um die außerdem notwendige Software brauchen Sie sich bei Nutzung des Länder-eANV nicht zu kümmern, da Sie diese automatisch erhalten.

Für eine qualifizierte Signatur ist eine Signaturkarte erforderlich, die von einem akkreditierten Trust-Center ausgegeben sein muss.

Trust-Center, die gemäß dem deutschen Signaturrecht berechtigt sind, qualifizierte Signaturkarten auszustellen, finden Sie unter [www.bundesnetzagentur.de](http://www.bundesnetzagentur.de). Z. Zt. werden von der ZKS-Abfall alle akkreditierten Trust-Center unterstützt.

Dort finden Sie ebenfalls eine Auflistung der von der Bundesnetzagentur zertifizierten Kartenlesegeräte.

## Zeitplan

Ab sofort: freiwilliger Einsatz der Mini-ZKS, wenn die Entsorgerbehörde zustimmt.

Ab 1.2.2009: Erprobung und Übergang zum Echtbetrieb der zentralen Koordinierungsstelle der Länder bei bereit gestellter Infrastruktur, wenn die Entsorgerbehörde zustimmt.

Ab 1.4.2010: elektronische Nachweisführung ist verbindlich; Entsorger und Behörde müssen elektronisch signieren. Wenn Erzeuger und/oder Beförderer noch nicht elektronisch signieren, muss zusätzlich ein Nachweis und Begleitschein in Papierform geführt werden (Quittungsbeleg).

Ab 1.2.2011: auch Erzeuger und Beförderer müssen elektronisch signieren.

### Weitere Informationen erhalten Sie

- bei der IKA ([www.zks-abfall.de](http://www.zks-abfall.de) und [www.asysnet.de](http://www.asysnet.de))
- auf der BMU-Homepage ([www.bmu.de](http://www.bmu.de))
- bei zuständigen (Abfall-)Behörden, Landesabfallgesellschaften

### Informationen zum elektronischen Signaturverfahren und zur Datensicherheit finden Sie auf den Seiten

- des BSI ([www.bsi.de](http://www.bsi.de))
- der Bundesnetzagentur ([www.bundesnetzagentur.de](http://www.bundesnetzagentur.de))

Bitte beachten Sie auch unsere Informationsveranstaltungen zur ZKS-Abfall in Hannover beim Niedersächsischen Landesamt für Bergbau, Energie und Geologie (LBEG) am: **22.04.2009** und **12.11.2009**.

Stand der Information: Februar 2009