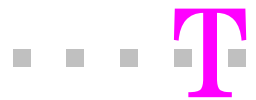
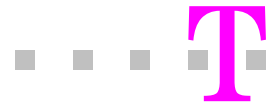


Informationen zur Teilnahme am Public Key Service (PKS[®]-SigG)



Bitte unbedingt vor Auftragsstellung lesen.



1. Inhalt

1	Die elektronische Signatur	4
1.1	Was ist eine elektronische Signatur?	4
1.2	Welche Arten von elektronischen Signaturen gibt es?	4
1.3	Wie funktioniert die elektronische Signatur?	4
1.4	Welche Rechtswirkung hat die elektronische Signatur?	5
1.5	Wie wird das Schlüsselpaar einer Person zugeordnet?	5
1.6	Kann die elektronische Signatur eingeschränkt werden?	5
1.7	Welche weiteren Attribute sind möglich?	5
2	Der Zertifizierungsdiensteanbieter	6
2.1	Welche Aufgaben übernimmt ein Zertifizierungsdiensteanbieter ?	6
2.2	Wer überwacht den Zertifizierungsdiensteanbieter?	7
2.3	Was ist eine Anbieterakkreditierung ?	7
3	Umgang mit der elektronischen Signatur	8
3.1	Handhabung der Chipkarte	8
3.2	Was ist beim Signieren und Prüfen zu beachten?	9
3.3	Wie werden die elektronischen Signaturen archiviert ?	9
3.4	Besonderheiten bei Multisignaturkarten	9
4	Weitere Informationen	11
4.1	Antworten auf häufig gestellte Fragen	11
4.2	Was uns noch wichtig ist:	11
4.3	Informationsquellen	12

Informationen zur Teilnahme am Public Key Service (PKS[®]-SigG)



Sehr geehrter Kunde, sehr geehrte Kundin,

die Gesellschaft bewegt sich zunehmend weg von der traditionellen, papiergebundenen Kommunikation, zu einer elektronischen Kommunikation. Die Nutzung von elektronischen Briefdiensten (E-Mail) ist aus unserem Privat- und Geschäftsleben fast nicht mehr wegzudenken. Unzählige Dokumente werden täglich über das Internet oder in Unternehmensnetzen übertragen.

Doch konnte bis vor kurzem nicht die gesamte Kommunikation elektronisch abgewickelt werden, da für bestimmte Dokumente eine bestimmte Form gesetzlich vorgegeben war. Dies betraf z. B. Dokumente, die zur ihrer Rechtswirksamkeit eine handschriftliche Unterschrift benötigten. Der Gesetzgeber hat mit dem Signaturgesetz, der Signaturverordnung und der Änderung weiterer Rechtsvorschriften nun die Möglichkeit geschaffen, hier als Äquivalent zur eigenhändigen Unterschrift die qualifizierte elektronische Signatur einzusetzen.

Strenge Prüfkriterien an Technik und Organisation schaffen ein hohes Sicherheitsniveau für die qualifizierte elektronische Signatur nach dem deutschen Signaturgesetz und der Europäischen Richtlinie zu elektronischen Signaturen.

Die vorliegenden Informationen sollen Ihnen den Einstieg in die Welt der elektronischen Signatur des Public Key Service der Deutschen Telekom AG erleichtern. Sie müssen die Kenntnisnahme dieser Informationen im Auftrag bestätigen. Indem Sie diese Informationen zur Kenntnis nehmen, werden Sie im Sinne des § 6 Signaturgesetz und des § 6 Signaturverordnung unterrichtet. Lesen Sie die Informationen vor der Auftragsstellung sorgfältig durch und wenden Sie sich bei Fragen an unsere Supportline.

Unsere Kontaktdaten für Ihre Fragen:

Telefonisch: + 49 1805 / 26 82 04

Sperrhotline: + 49 1805 / 26 82 02

Per E-Mail: Telesec_Support@T-Systems.com

**Per Brief: Deutsche Telekom AG
c/o T-Systems International GmbH
Trust Center – Notary Services
Postfach 12 51**

57236 Netphen



1 Die elektronische Signatur

1.1 Was ist eine elektronische Signatur?

Die handschriftliche Unterschrift verbindet ein Papierdokument mit dem Unterzeichner. Der Unterzeichner schließt z.B. einen Vertrag durch Unterzeichnung mit seiner eigenhändigen Unterschrift. Ebenso verbindet die elektronische Signatur einen Unterzeichner mit elektronischen Daten z.B. einem Textdokument so, dass man diese Zuordnung sicher nachprüfen kann. Im Gegensatz zur handschriftlichen Unterschrift, für die der Unterzeichner „Papier und Stift“ benötigt, nutzt er bei der elektronischen Signatur mathematische Verfahren.

1.2 Welche Arten von elektronischen Signaturen gibt es?

Das Signaturgesetz definiert vier Arten elektronischer Signaturen:

- Die einfache elektronische Signatur
- Die fortgeschrittene elektronische Signatur
- Die qualifizierte elektronische Signatur
- Die qualifizierte elektronische Signatur mit Anbieterakkreditierung

Die Nummern 3 und 4 werden im Signaturgesetz ausführlich beschrieben und sind der handschriftlichen Unterschrift weitgehend gleichgestellt.

1.3 Wie funktioniert die elektronische Signatur?

Das Public-Key-Verfahren bildet in der Regel die Grundlage für die elektronische Signatur. Für das Verfahren benötigt man ein spezielles Schlüsselpaar. Daten, die mit dem einen Schlüssel verschlüsselt werden, können nur mit dem dazugehörigen anderen Schlüssel entschlüsselt werden. Diese Eigenschaft nutzt man für die Erstellung einer elektronischen Signatur und deren Überprüfung.

Bei der elektronischen Signatur erzeugt man zuerst einen digitalen Fingerabdruck des Dokuments. Der Fingerabdruck wird nun mit dem ersten Schlüssel verschlüsselt, das ist die elektronische Signatur. Das elektronisch signierte Dokument kann nun anderen Nutzern zugänglich gemacht werden. Der Unterzeichner stellt den zweiten Schlüssel nun den anderen Nutzern zur Prüfung der elektronischen Signatur zur Verfügung. Mit dem vorliegenden Schlüssel und dem Wissen, wem dieser Schlüssel zugeordnet ist, kann nun jeder eine sichere Überprüfung vornehmen. Das Signaturgesetz bezeichnet den ersten Schlüssel als Signaturschlüssel und den zweiten Schlüssel als Signaturprüfschlüssel.



1.4 Welche Rechtswirkung hat die elektronische Signatur?

Die qualifizierte elektronische Signatur ist der handschriftlichen Unterschrift in vielen Fällen gleichgestellt. Das bedeutet, dass in vielen Rechtsgeschäften der Einsatz der qualifizierten elektronischen Signatur neben der handschriftlichen Unterschrift möglich ist.

Informieren Sie sich bitte vorher, ob dies im jeweiligen Rechtsgeschäft zugelassen ist.

Durch die Nutzung Ihres Signaturschlüssels wird Ihnen die qualifizierte elektronische Signatur zugerechnet. D.h. Sie zeichnen verantwortlich wie bei einer handschriftlichen Unterschrift.

1.5 Wie wird das Schlüsselpaar einer Person zugeordnet?

Die Zuordnung von Person und Schlüssel wird durch ein qualifiziertes Zertifikat bestätigt. Ein Zertifikat ist eine Art elektronischer Ausweis. Der Zertifizierungsdiensteanbieter (ZDA), z. B. die Deutsche Telekom AG, identifiziert die Person und bestätigt die Zuordnung zu einem Schlüssel mit einer qualifizierten elektronischen Signatur.

1.6 Kann die elektronische Signatur eingeschränkt werden?

Es ist möglich, die elektronische Signatur durch eine Angabe im qualifizierten Zertifikat (Attribut im Hauptzertifikat) oder durch ein zugehöriges qualifiziertes Attribut-Zertifikat auf bestimmte Anwendungen in Art und Umfang zu beschränken. Es kann im qualifizierten Zertifikat oder im Attribut-Zertifikat z. B. eingetragen sein: „Es dürfen nur Rechtsgeschäfte unter 500 Euro Wert mit der elektronischen Signatur abgeschlossen werden“.

1.7 Welche weiteren Attribute sind möglich?

Neben der Beschränkung siehe Ziffer 1.6 können Sie in Ihr Attribut auch eine Vertretungsmacht für Dritte (z. B. Prokura) oder eine berufsbezogene oder sonstige Angabe zur Person, z. B. Arzt, eintragen lassen. In diesem Falle hat der betroffene Dritte (Firma, berufsständische Kammer etc.), der den Eintrag eines solchen Attributes genehmigen bzw. bestätigen muss auch das Recht, dieses Attribut zu sperren.

Attribute können Bestandteile Ihres Hauptzertifikates („Attribut im Hauptzertifikat“) sein oder als gesondertes Zertifikat ausgestellt werden („qualifiziertes Attribut-Zertifikat“).

Der Unterschied zwischen diesen beiden Möglichkeiten besteht darin, dass Ihr „Attribut im Hauptzertifikat“ fester unabänderlicher Bestandteil des Hauptzertifikates ist und bei jedem Signiervorgang beigefügt wird. Dagegen ist das qualifizierte Attribut-Zertifikat ein eigenes Zertifikat, das eine eindeutige Referenz auf Ihr Hauptzertifikat besitzt. Sie können bei einem Signiervorgang entscheiden, ob Sie das Attributszertifikat beifügen oder nicht.

Ob Sie sich für ein „Attribut im Hauptzertifikat“ oder ein „qualifiziertes Attribut-Zertifikat“ entscheiden, hängt vom geplanten Einsatz der Signatur und der verwendeten Software ab.



2 Der Zertifizierungsdiensteanbieter

2.1 Welche Aufgaben übernimmt ein Zertifizierungsdiensteanbieter ?

Der Zertifizierungsdiensteanbieter (auch Trust Center oder kurz ZDA genannt) stellt die benötigten Komponenten und Dienstleistungen für die elektronische Signatur zur Verfügung.

Dies sind im Einzelnen:

2.1.1 Identifizierung des Kunden

Der ZDA prüft bei der Auftragsstellung Ihre Identität anhand von Personalausweis oder Reisepass + Meldebestätigung.

2.1.2 Beschlüsselung der Chipkarte

Der ZDA erzeugt Ihre Schlüssel in einer besonders gesicherten Umgebung. Der Signaturschlüssel wird beim ZDA nicht gespeichert oder archiviert. Der Signaturschlüssel wird auf die Chipkarte unauslesbar gespeichert und die Chipkarte wird mit einer elektronischen Transportsicherung versehen.

2.1.3 Sperrung der PKS-Karte

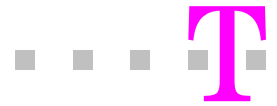
Der ZDA betreibt einen 24-Stunden-Sperrservice. Sie können Ihre Sperrung telefonisch durchgeben, dann benötigt der ZDA zur Bearbeitung Ihr Telepasswort.

**Telefonische Sperrung unter der Rufnummer: + 49 1805/26 82 02
Sie benötigen zur telefonischen Sperrung das Telepasswort.**

Sie können aber auch schriftlich eine Sperrung durchführen, dazu verwenden Sie bitte folgende Adresse:

**Deutsche Telekom AG
c/o T-Systems International GmbH
Trust Center – Notary Services
Postfach 12 51**

57236 Netphen



Die Sperrung einer PKS-Karte wird mit Angabe des Datums und der Zeit im Zertifikatsverzeichnis eingetragen. Eine rückwirkende Sperrung ist nicht möglich. Bitte beachten Sie, dass bei der Aufnahme von drittbezogenen Angaben (z.B. Vertretungsmacht) oder bei berufsbezogenen Angaben, der betroffenen Dritte (z.B. der Vertretene oder die berufsständische Kammer) zur Sperrung berechtigt sein kann. Eine Sperrung kann nicht rückgängig gemacht werden.

2.1.7 Zeitstempeldienst

Der ZDA stellt als kostenpflichtige Zusatzdienstleistung elektronische Bescheinigungen aus, dass ein Dokument zur einer bestimmten Zeit vorgelegen hat. Dazu senden Sie dem ZDA ein elektronisches Dokument oder den elektronischen Fingerabdruck eines Dokumentes. Der ZDA fügt dann zu den vorliegenden Daten die gesetzliche Zeit hinzu und signiert dies elektronisch. Sie erhalten dann ein „zeitgestempeltes“ Dokument zurück.

2.2 Wer überwacht den Zertifizierungsdiensteanbieter?

Der ZDA ist gesetzlich zur Einhaltung von umfangreichen Sicherheitsmaßnahmen verpflichtet. Dies soll ein einheitlich hohes Sicherheitsniveau für die elektronische Signatur sicherstellen. Die Überwachung der ZDA ist der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) als zuständige Behörde für das Signaturgesetz übertragen.

2.3 Was ist eine Anbieterakkreditierung ?

Das Signaturgesetz bietet dem ZDA die Möglichkeit, sich freiwillig einer aufwändigen Prüfung zu unterziehen. Mit dieser Prüfung weist er die Einhaltung der Anforderungen des Signaturgesetzes nach und erhält nach positivem Prüfergebnis ein Gütesiegel der Bundesnetzagentur. Die elektronischen Signaturen erhalten dann den Zusatz „mit Anbieterakkreditierung“.



3 Umgang mit der elektronischen Signatur

3.1 Handhabung der Chipkarte

Die Signaturen, die mit Ihrer Chipkarte erzeugt werden, werden Ihnen unmittelbar zugerechnet, daher halten Sie bitte die nachfolgenden Hinweise unbedingt ein:

1. Halten Sie die Chipkarte immer in Ihrem persönlichen Gewahrsam. Tragen Sie diese möglichst diebstahlsicher am Körper
2. Haben Sie Ihre Chipkarte verloren, lassen Sie das Zertifikat sofort sperren.
3. Ist Ihre Chipkarte beschädigt, kann dies auf einen Manipulationsversuch hinweisen. Wenn Sie Beschädigungen nicht zuordnen können, lassen Sie sicherheitshalber das zugehörige Zertifikat sperren.
4. Verwenden Sie die Chipkarte niemals bei Anwendungen, Maschinen, Terminals, deren Funktionen Ihnen unbekannt, verdächtig oder unzuverlässig erscheinen.
5. Wir empfehlen, die Chipkarte nur in Applikationen zu benutzen, die gemäß Signaturgesetz bestätigt sind.
6. Beachten Sie auf jeden Fall die Nutzungs- und Sicherheitshinweise aller Anwendungsbereiche, in denen Sie die Chipkarte nutzen wollen.
7. Wenn Sie Ihre Chipkarte nicht mehr nutzen wollen, zerstören Sie den Chip mit einem handelsüblichen Locher. Sperren Sie in diesem Fall das zugehörige Zertifikat.
8. Halten Sie Ihre PIN und Ihr Telepasswort, wie bei Ihrer EC-Karte geheim.
9. Wechseln Sie in gewissen Zeitabständen Ihre PIN und vermeiden Sie es, sich die PIN zu notieren.
10. Bei dem Verdacht, dass jemand von Ihrer PIN Kenntnis erlangt hat, ändern Sie die PIN sofort.

Die Chipkarte kann nach drei falschen Pineingaben nicht mehr genutzt werden. Sie benötigen in diesem Fall ein neues Zertifikat und eine neue Karte.



3.2 Was ist beim Signieren und Prüfen zu beachten?

Das Signaturgesetz schreibt Ihnen nicht vor, welche Signaturanwendungskomponente (Kartenleser, Software...) Sie mit Ihrer Chipkarte zum Signieren oder Prüfen nutzen. Das liegt allein in Ihrem Ermessen. Folgende Empfehlungen sollten Sie jedoch berücksichtigen:

- Verwenden Sie einen Kartenleser mit PIN-Pad, Ihre PIN ist dadurch besser vor Missbrauch geschützt.
- Halten Sie Ihren Computer immer auf dem aktuellen Sicherheitsstand. Wenn Sicherheitslücken auftreten, dann stellt der Hersteller Ihres Betriebssystems (z. B. Windows) meist einen Patch als Download zur Verfügung.
- Nutzen Sie Antiviren- und Firewallsoftware und laden Sie jeweils regelmäßig die aktuellen Versionen auf Ihren Computer.
- Sichern Sie Ihren Computer durch Passwörter für BIOS, Bildschirmschoner usw. oder mittels Chipkarte vor unberechtigtem Zugriff.
- Beachten Sie die Hinweise im Handbuch Ihrer Signatursoftware.
- Signieren Sie grundsätzlich nur Informationen, deren Inhalt Sie vorher geprüft haben.
- Haben Sie Zweifel an der Erstellung Ihrer elektronischen Signatur, dann überprüfen Sie die Signatur und den Inhalt vor dem Versand selbst noch einmal nach.
- Falls Sie Ihr qualifiziertes Zertifikat in der Nutzung beschränkt haben, fügen Sie das zugehörige Attribut-Zertifikat dem entsprechenden Vorgang bei, sofern es sich um ein qualifiziertes (s.o.) Attribut-Zertifikat handelt.
- Nutzen Sie die Möglichkeit, das qualifizierte Zertifikat im Verzeichnisdienst online zu überprüfen.

3.3 Wie werden die elektronischen Signaturen archiviert ?

Elektronische Signaturen verlieren aufgrund der mathematischen Verfahren mit der Zeit ihre Sicherheit. Besonders die Weiterentwicklung der Computer bezüglich Leistungsfähigkeit und Schnelligkeit, lässt den Sicherheitswert sinken (s. § 6 Ziffer 5 SigV). Daher ist es erforderlich, auch archivierte elektronische Signaturen wieder auf den neuesten Stand zu bringen, indem sie mit einer aktuell gültigen Signatur übersigniert werden. Zur Überprüfung des Alters einer Signatur, muss diese einen Zeitstempel enthalten.

3.4 Besonderheiten bei Multisignaturkarten

Der Einsatz von Multisignaturkarten erfordert eine besondere Sicherheitsumgebung.

Die Einsatzumgebung muss durch Sie unter Berücksichtigung der vorliegenden Gegebenheiten und des geplanten Einsatzzweckes physisch und logisch so abgesichert werden, dass ein

Informationen zur Teilnahme am Public Key Service (PKS[®]-SigG)



Missbrauch der Signaturfunktionalität der Multisignaturkarte und die Ausspähung der zugehörigen Identifikationsdaten (Signatur-PIN) durch Angreifer mit hohem Angriffspotential praktisch ausgeschlossen sind und damit Ihre alleinige Kontrolle über den Prozess der Signaturerzeugung gegeben ist.

Unabhängig von der genauen Ausgestaltung der Einsatzumgebung achten Sie vor und während des Betriebes Ihrer Multisignaturkarte auf folgende Punkte:

- Ordnungsgemäße Installation und Einhaltung der vorgesehenen Einsatzumgebung gemäß der Sicherheitshinweise aus den zugehörigen Handbüchern und den Bestätigungen,
- Verwendung von Komponenten, die bestätigt sind oder für die eine Herstellererklärung vorliegt.
- regelmäßige Überprüfung der Integrität und der zugrunde liegenden Plattform (Hardware und Betriebssystem),
- Schutz der IT-Plattform vor Schadsoftware,
- vertrauenswürdige Sicherheitsadministration,
- vertrauenswürdige Netzinfrastruktur, falls der Einsatz der Multisignaturkarte in einem IT-Netz erfolgt,
- vertrauenswürdige Anbindung an externe Kommunikationsnetze, falls die Multisignaturkarte in einem IT-Netz mit Anbindung an externe Kommunikationsschnittstellen eingesetzt wird.

Beachten Sie jedoch bitte, dass die Darstellung nicht für alle Einsatzumgebungen anwendbar ist und immer die Besonderheiten des Einzelfalles betrachtet werden müssen. Sollten Sie bezüglich Ihrer Einsatzumgebung unsicher sein, können Sie eine gemäß Signaturgesetz anerkannte Prüf- und Bestätigungsstelle kontaktieren. Eine Liste dieser Stellen finden Sie unter: http://www.bundesnetzagentur.de/enid/05aaef2a5f81c3ea1d0016ece496b188,0/Qualifizierte_elektronische_Signatur/Pruef-_und_Bestaetigungsstellen_vd.html

Auch bei dem Einsatz von Multisignaturkarten wird jede qualifizierte elektronische Signatur Ihnen zugerechnet. Die Ziffer 1.4 dieser Unterrichtung gilt auch in diesen Fällen.

Die ausführliche Bestätigungsurkunde des TÜV IT für die Multisignaturkarte (Urkundennummer TUVIT.93146.TE.12.2006) ist unter folgendem Link abrufbar: <http://www.tuvit.de/certuvit/pdf/93146UD.pdf>.



4 Weitere Informationen

4.1 Antworten auf häufig gestellte Fragen

Wie sicher sind die mathematischen Verfahren?

Die Verfahren, die im Public Key Service eingesetzt werden, unterliegen einer ständigen Kontrolle der Wissenschaft und Forschung. Die Algorithmen werden durch die BNetzA jährlich auf ihre Eignung geprüft. Hierbei wird auch festgelegt, bis wann die mathematischen Verfahren als geeignet gelten. Die Deutsche Telekom AG gibt keine PKS-Karten heraus, die länger gültig sind, als deren mathematische Verfahren als sicher gelten.

Schützt die Signatur die Nachricht vor fremden Blicken?

Elektronische Signaturen dienen nicht der Verschleierung oder Verschlüsselung von Informationen. Wenn Sie Ihre Nachrichten schützen wollen, müssen Sie diese verschlüsseln.

Was ist bei einem Umzug zu beachten bzw. zu tun?

Bitte teilen Sie uns alle Änderungen unbedingt umgehend mit. Besonders wichtig für die Kommunikation mit dem ZDA ist die Mitteilung über eine Änderung der E-Mailadresse. Bitte kontrollieren Sie regelmäßig Ihr elektronisches Postfach; nur so kann sichergestellt werden, dass Sie rechtzeitig Informationen oder Warnmeldungen erhalten. Sie benötigen kein neues Zertifikat.

Muss das qualifizierte Zertifikat und ggf. das qualifizierte Attributzertifikat mitsigniert werden oder kann das Zertifikat als Anlage hinzugefügt werden?

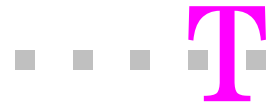
Wir empfehlen Ihnen alle Daten, die mit dem Vorgang in Verbindung stehen, in die qualifizierte Signatur einzubinden.

4.2 Was uns noch wichtig ist:

Sie haben das Gefühl, dass einer unserer Mitarbeiter oder Beauftragten nicht sorgfältig arbeitet?

Bitte melden Sie uns diese Vorfälle an die genannte Adresse. Es kann trotz aufwändiger Kontrollen und Maßnahmen zu Problemen kommen. Damit wir sofort reagieren können, ist uns Ihre Meinung sehr wichtig.

Informationen zur Teilnahme am Public Key Service (PKS[®]-SigG)



Sie haben Verbesserungsvorschläge?

In puncto Qualität setzen wir hohe Maßstäbe. Unser Ziel ist ein informierter Kunde, der sich im Thema „Elektronische Signatur“ sicher fühlt. Teilen Sie uns bitte Ihre Vorschläge und Fragen mit. Wir freuen uns auf Ihre Meinung.

4.3 Informationsquellen

Bitte informieren Sie sich regelmäßig auf folgenden Websites:

<http://www.telesec.de>

Informationen des ZDA Deutsche Telekom AG, sowie Online PKS-Auftrag, Sperrservice, Verzeichnisdienst sowie alle Informationen und Formulare zum Public Key Service.

<http://www.bundesnetzagentur.de>

Informationen der zuständigen Aufsichtsbehörde