



Institut für Telematik unter Betreuung der
Fraunhofer Gesellschaft



 **Digitale Signaturen**

**Zertifizierungsdienste-
Anbieter in Deutschland**

Lutz Gollan

Thomas Engel

Christoph Meinel

Author	Lutz Gollan Dr. iur. Thomas Engel Prof. Dr. rer. nat. Christoph Meinel Univ.-Prof. Dr. sc.
Copyright	© 2002 Institut für Telematik e.V., Trier
Trademarks	All terms that are mentioned in this paper that are known to be trademarks or service marks have been appropriately capitalised. Use of a term in this paper should not be regarded as affecting the validity of any trademark and service mark. The product or brand names are trademarks of their respective owners.
Printing	05/02
Document status	Version 1.1 (05.2002) Printed in Germany All rights reserved The documentation was accomplished through the Institut für Telematik. The information contained in this document represents the current view of the authors on the issues discussed as of the date of publication. Because the present methodology must respond to changing research conditions, the results of this paper should not be interpreted to be a commitment on the part of the authors. Any information presented after the date of publication are subject to change. The right to copy this documentation is limited by copyright law. Making unauthorised copies, adaptations or compilation works without permission of the authors or institutions mentioned above is prohibited and constitutes a punishable violation of the law.

Inhaltsverzeichnis

1. Zusammenfassung	8
2. Einleitung	10
3. Allgemeines	13
3.1. Ziele der Informationssicherheit.....	13
3.2. Verschlüsselung	14
3.3. Signatur.....	15
4. Rechtliche Begriffe und Bedeutung elektronischer Signaturen	16
4.1. Gesetzliche Definitionen	16
4.1.1. Elektronische Signatur, § 2 Nr. 1 SigG	16
4.1.2. Fortgeschrittene elektronische Signaturen, § 2 Nr. 2 SigG.....	17
4.1.3. Qualifizierte elektronische Signaturen, § 2 Nr. 3 SigG	17
4.1.4. Qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung, § 15 I SigG .	18
4.2. Rechtliche Bedeutung elektronischer Signaturen	18
5. Funktionsweise digitaler Signaturen.....	20
5.1. Schlüsselpaar	20
5.2. Hash-Funktion	20
5.3. Präsentationsproblem	21
5.4. Rolle der Trust Center, Zertifikate und Registrierungsstellen.....	22
5.5. Zeitstempeldienst.....	23
6. Gesetzliche Anforderungen	24
6.1. Gemeinsame Voraussetzungen	24
6.1.1. Fachkunde des Personals.....	24
6.1.2. Umgesetztes Sicherheitskonzept	25
6.1.3. Deckungsvorsorge	25
6.1.4. Jahresbeitrag	25

6.2. Anforderungen an die Produkte.....	26
6.2.1. Interoperabilität	27
6.2.2. Schlüsselerzeugung, -speicherung und -anwendung.....	27
6.2.3. Darstellung und Überprüfung der Daten.....	28
6.2.4. PKI-Aufbau und Gültigkeitsmodell des Signaturgesetzes	29
6.2.5. Verzeichnisdienst	31
6.2.6. Zeitstempeldienst.....	31
6.3. Angezeigte Zertifizierungsdiensteanbieter	31
6.3.1. Schlüsselerzeugung, § 17 III Nr. 1 SigG.....	32
6.3.2. Schlüsselspeicherung und Signaturerstellung, § 17 I SigG	32
6.3.3. Darstellung zu signierender Daten, § 17 II 1 SigG	32
6.3.4. Überprüfung signierter Daten, § 17 II 2 SigG	32
6.3.5. Verzeichnisdienst, § 17 III Nr. 2 SigG	32
6.3.6. Zeitstempeldienst, § 17 III Nr. 3 SigG	32
6.3.7. Zusammenfassung	33
6.4. Akkreditierte Zertifizierungsdiensteanbieter	33
6.4.1. Bestätigung des Sicherheitskonzepts	33
6.4.2. Produkte für elektronische Signaturen	33
6.4.2.1. Schlüsselerzeugung, § 17 III Nr. 1 SigG.....	33
6.4.2.2. Schlüsselspeicherung und Signaturerstellung, § 17 I SigG	33
6.4.2.3. Darstellung zu signierender Daten, § 17 II 1 SigG	33
6.4.2.4. Überprüfung signierter Daten, § 17 III 2 SigG	33
6.4.2.5. Sicheres Verzeichnis, § 17 III Nr. 2	34
6.4.2.6. Zeitstempeldienst, § 17 III Nr. 3 SigG	34
6.4.3. Zusammenfassung	34
7. Zertifizierungsdiensteanbieter und deren Produkte	35
7.1. Telesec	36
7.1.1. Kontaktinformationen.....	36
7.1.2. Schlüsselerzeugung, § 17 III Nr. 1 SigG.....	36

7.1.3.	Schlüsselspeicherung und Signaturerstellung, § 17 I SigG	36
7.1.4.	Darstellung zu signierender Daten, § 17 II 1 SigG	36
7.1.5.	Überprüfung signierter Daten, § 17 III 2 SigG	37
7.1.6.	Sicheres Verzeichnis, § 17 III Nr. 2	37
7.1.7.	Zeitstempeldienst, § 17 III Nr. 3 SigG	37
7.1.8.	Kosten	37
7.1.9.	Weitere Leistungen	37
7.1.10.	Einsetzbare Kartenleser	38
7.2.	Signtrust	39
7.2.1.	Kontaktinformation	39
7.2.2.	Schlüsselerzeugung, § 17 III Nr. 1 SigG	39
7.2.3.	Schlüsselspeicherung und Signaturerstellung, § 17 I SigG	39
7.2.4.	Darstellung zu signierender Daten, § 17 II 1 SigG	40
7.2.5.	Überprüfung signierter Daten, § 17 III 2 SigG	40
7.2.6.	Sicheres Verzeichnis, § 17 III Nr. 2	40
7.2.7.	Zeitstempeldienst, § 17 III Nr. 3 SigG	40
7.2.8.	Kosten	40
7.2.9.	Weitere Leistungen	40
7.2.10.	Einsetzbare Kartenleser	40
7.3.	Bundesnotarkammer	41
7.4.	Kontaktinformation	41
7.4.1.	Einzelne Produkte und Verfahren	41
7.4.2.	Kosten	41
7.5.	Datev	43
7.5.1.	Kontaktinformation	43
7.5.2.	Schlüsselerzeugung, § 17 III Nr. 1 SigG	43
7.5.3.	Schlüsselspeicherung und Signaturerstellung, § 17 I SigG	43
7.5.4.	Darstellung zu signierender Daten, § 17 II 1 SigG	43
7.5.5.	Überprüfung signierter Daten, § 17 III 2 SigG	44

7.5.6.	Sicheres Verzeichnis, § 17 III Nr. 2	44
7.5.7.	Zeitstempeldienst, § 17 III Nr. 3 SigG	44
7.5.8.	Weitere Leistungen	44
7.5.9.	Verwendbare Kartenleser	44
7.6.	Medizon	45
7.6.1.	Kontaktinformation	45
7.6.2.	Einzelne Produkte und Verfahren	45
7.6.3.	Zeitstempeldienst, § 17 III Nr. 3 SigG	45
7.6.4.	Kosten	45
7.6.5.	Weitere Leistungen	46
7.7.	Steuerberater- und Rechtsanwaltskammern	46
7.8.	AuthentiDate - Zeitstempeldienst	47
7.8.1.	Kontaktinformation	47
7.8.2.	Betriebssystem	47
7.8.3.	Datenübertragung	48
7.8.4.	Interoperabilität	48
7.8.5.	Kosten	48
7.8.6.	Weitere Leistungen	48
7.9.	TC Trustcenter	49
7.9.1.	Kontaktinfo	49
7.9.2.	Schlüsselerzeugung, § 17 III Nr. 1 SigG	49
7.9.3.	Schlüsselspeicherung und Signaturerstellung, § 17 I SigG	50
7.9.4.	Darstellung zu signierender Daten, § 17 II 1 SigG	50
7.9.5.	Überprüfung signierter Daten, § 17 III 2 SigG	50
7.9.6.	Sicheres Verzeichnis, § 17 III Nr. 2	50
7.9.7.	Zeitstempeldienst, § 17 III Nr. 3 SigG	50
7.9.8.	Weitere Leistungen	50
7.9.9.	Verwendbare Kartenleser	51
7.10.	D-Trust	52



7.10.1. Kontaktinformation	52
7.10.2. Schlüsselerzeugung, § 17 III Nr. 1 SigG.....	52
7.10.3. Schlüsselspeicherung und Signaturerstellung, § 17 I SigG	52
7.10.4. Darstellung zu signierender Daten, § 17 II 1 SigG	53
7.10.5. Überprüfung signierter Daten, § 17 III 2 SigG	53
7.10.6. Verzeichnisdienst	53
7.10.7. Kosten.....	53
7.10.8. Weitere Leistungen:	53
7.10.9. Einsetzbare Kartenleser	54