



Sicherheitsbestätigung und Bericht

T-Systems. 03174.SE.10.2006

**Zertifizierungsdienst (2048) der
Deutschen Post Com GmbH –
Geschäftsfeld Signtrust**

Bestätigung

für die Umsetzung von Sicherheitskonzepten

gemäß § 15 Abs. 2 Gesetz über Rahmenbedingungen für elektronische Signaturen¹ und §§ 11 Abs. 2 Signaturverordnung²

T-Systems GEI GmbH
- Zertifizierungsstelle -
Rabinstr.8, 53111 Bonn

**bestätigt hiermit gemäß
§§ 15 Abs. 2 S.1 SigG sowie § 11 Abs. 2 SigV,
dass der**

**Zertifizierungsdienst (2048)
der Deutschen Post Com GmbH – Geschäftsfeld Signtrust**

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.03174.SE.10.2006

Bonn, den 31.10.2006

(Dr. Heinrich Kersten)

The logo for T-Systems, featuring a stylized 'T' in a square followed by the word 'Systems' and three dots.

Die T-Systems GEI GmbH – Zertifizierungsstelle - ist gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für die Umsetzung von Sicherheitskonzepten gemäß § 15 Abs. 2 Satz 1 SigG ermächtigt.

¹ Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG), zuletzt geändert durch Art. 3 (9) des Zweiten Gesetzes zur Neuregelung des Energiewirtschaftsgesetzes (EnWG) vom 07. Juli 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 42)

² Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), zuletzt geändert durch Art. 2 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigGÄndG) vom 04. Januar 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 1)

Beschreibung zum Sicherheitskonzept:

1. Bezeichnung des Zertifizierungsdiensteanbieters:

Zertifizierungsdienst (2048) der Deutschen Post Com GmbH – Geschäftsfeld Signtrust

Anschrift:
Hilpertstr. 31
64295 Darmstadt

Anmerkung: Die Deutsche Post Com GmbH - Geschäftsfeld Signtrust betreibt bereits einen anderen (sicherheitsbestätigten) Zertifizierungsdienst. Im Hinblick auf eine eindeutige Kennzeichnung wurde für den neuen Zertifizierungsdienst der Zusatz "(2048)" gewählt. Der andere Zertifizierungsdienst wird übergangsweise parallel zum neuen Zertifizierungsdienst (2048) betrieben.

2. Funktionsbeschreibung

Die Deutsche Post Com GmbH betreibt einen zentralen Zertifizierungsdienst mit den Funktionen Registrierung, Schlüsselgenerierung, Schlüsselzertifizierung, Verzeichnisdienst und Zeitstempeldienst.

Zertifizierungsdiensteanbieter (ZDA) können Instanzen dieses Zertifizierungsdienstes ganz oder modulweise nutzen.

Die vorliegende Bestätigung betrifft ausschließlich die Nutzung dieses Zertifizierungsdienstes durch andere Zertifizierungsanbieter.

Ein ZDA als Nutzer des Zertifizierungsdienstes (2048) der Deutschen Post Com GmbH - Geschäftsfeld Signtrust gilt erst dann als sicherheitsbestätigt, wenn

1. die vom ihm genutzten Module des zentralen Zertifizierungsdienstes (2048) der Deutschen Post Com GmbH - Geschäftsfeld Signtrust unter die vorliegende Sicherheitsbestätigung für den Zertifizierungsdienst fallen,
2. das Sicherheitskonzept des ZDA gemäß SigG/SigV von einer anerkannten Prüf- und Bestätigungsstelle auf Gesetzeskonformität und korrekte praktische Umsetzung überprüft wurde.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Das Sicherheitskonzept des Zertifizierungsdienstes (2048) der Deutschen Post Com GmbH – Geschäftsfeld Signtrust erfüllt die Anforderungen nach § 2 SigV unter den im Folgenden genannten Auflagen.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

Der Zertifizierungsdienst bietet zur Identifizierung von Antragstellern die folgenden Varianten (Module) an, die von dem jeweiligen ZDA genutzt werden können:

- Nutzung von PostIdent Basic,
- Identifizierung in der RA des jeweiligen ZDAs,
- Identifizierung durch Außendienstmitarbeiter der RA des jeweiligen ZDAs oder des Zertifizierungsdienstes (2048) der Deutschen Post Com GmbH – Geschäftsfeld Signtrust.

Für die Prüfung der Antragsdaten und deren Übernahme in die Auftragsdatenbank sind die folgenden Varianten vorgesehen:

- durch die RA des jeweiligen ZDAs,
- durch die RA des Zertifizierungsdienst (2048) der Deutschen Post Com GmbH – Geschäftsfeld Signtrust.

Die weitere Antragsbearbeitung erfolgt in der zentralen RA des Zertifizierungsdienstes (2048) der Deutschen Post Com GmbH – Geschäftsfeld Signtrust.

Die für die Registrierung und Identifizierung vom Zertifizierungsdienst (2048) der Deutschen Post Com GmbH – Geschäftsfeld Signtrust eingesetzten Mitarbeiter wurden vom Betreiber für ihre Aufgaben geschult und autorisiert. Sie sind in dieser Funktion an die Weisungen des Betreibers des Zertifizierungsdienstes gebunden und in die Organisation und das Sicherheitskonzept eingebunden.

Die Auslieferung der sicheren Signaturerstellungseinheiten erfolgt mit einer der folgenden Varianten:

- mittels PostIdent Special - ausgelöst vom Zertifizierungsdienst (2048) der Deutschen Post Com GmbH - Geschäftsfeld Signtrust,
- durch Außendienstmitarbeiter der RA des jeweiligen ZDAs oder des Zertifizierungsdienstes (2048) der Deutschen Post Com GmbH – Geschäftsfeld Signtrust,
- in der RA des jeweiligen ZDAs,
- durch postalischen Versand.

Für das PostIdent-Verfahren (basierend dem Sicherheitskonzept Version 8.0) mit den Teilverfahren PostIdent Basic und PostIdent Special liegt die Sicherheitsbestätigung TUVIT.09487.SW.05.2006 vom 02.05.2006 vor. Alle hierin aufgeführten Bedingungen und Auflagen an das PostIdentverfahren werden durch die Deutsche Post Com GmbH – Geschäftsfeld Signtrust eingehalten.

Der Zertifizierungsdienst (2048) der Deutschen Post Com GmbH - Geschäftsfeld Signtrust bietet weiterhin die Funktionen Schlüsselerzeugung, Schlüsselzertifizierung, Verzeichnis- mit Sperrdienst sowie Zeitstempeldienst.

Alle genannten Funktionen sind im Sicherheitskonzept des Zertifizierungsdienstes (2048) der Deutschen Post Com GmbH - Geschäftsfeld Signtrust mit der Versionsnummer 1.0 vom 27.10.2006 (letzte Revision) und mitgeltenden Dokumenten beschrieben. Diese Beschreibung enthält auch die Schnittstellen und weitere Informationen zur Nutzung der Funktionen durch andere ZDAs.

Im Hinblick auf die Einsatzumgebung sind folgende Auflagen durch den Betreiber des Zertifizierungsdienstes zu erfüllen:

Auflage 1: Die Vereinzelungsschleuse zum Raum AZR/DV2 muss noch eingebaut werden.

Auflage 2: Vorübergehend – bis zur Außerbetriebnahme des älteren Zertifizierungsdienstes – können die vorhandenen redundanten Systeme im Raum ARZ/DV2 gemeinsam aufgebaut bleiben. Danach sind die laut Sicherheitskonzept vorgesehenen getrennten Räumlichkeiten zu nutzen.

Der Zertifizierungsdienst (2048) der Deutschen Post Com GmbH - Geschäftsfeld Signtrust wird durch für ihre Aufgaben geschulte und autorisierte Mitarbeiter innerhalb einer baulich, organisatorisch und systemtechnisch abgesicherten Umgebung betrieben.

Jede Veränderung an den Abläufen, den Sicherheitsmaßnahmen, den eingesetzten technischen Komponenten sowie am Sicherheitskonzept und seinen mitgeltenden Dokumenten ist der Prüf- und Bestätigungsstelle anzuzeigen und erfordert ggf. eine Überprüfung und eine Erweiterung der Bestätigung.

Soweit es sich um sicherheitserhebliche Veränderungen handelt, sind diese Veränderungen zusätzlich unmittelbar der Bundesnetzagentur anzuzeigen.

b) Inbetriebnahme

Der Betriebsablauf beim Zertifizierungsdienst (2048) der Deutschen Post Com GmbH - Geschäftsfeld Signtrust wurde im Rahmen der Umsetzungsprüfung in allen Funktionen demonstriert.

Auflage 3: Die Inbetriebnahme des Zertifizierungsdienstes muss unter Aufsicht der Prüf- und Bestätigungsstelle nach Erhalt der Schlüssel für den Zertifizierungs-, Verzeichnis- und Zeitstempeldienst von der Bundesnetzagentur erfolgen.

Jede Inbetriebnahme und jede Wiederinbetriebnahme, die eine Neuinstallation erfordert, müssen durch fachkundiges Personal des ZDA erfolgen.

Jeder Austausch oder jede Veränderung im Gesamtkonzept und in den System- oder Sicherheitskomponenten ist der Prüf- und Bestätigungsstelle anzuzeigen und erfordert ggf. eine Überprüfung und eine Erweiterung der Bestätigung.

Die Inbetriebnahme neuer technischer Komponenten ist durch die Prüf- und Bestätigungsstelle zu beaufsichtigen.

Soweit es sich um sicherheitserhebliche Veränderungen handelt, ist die Veränderung zusätzlich unmittelbar der Bundesnetzagentur anzuzeigen.

c) Betrieb des Zertifizierungsdienstes

Während des Betriebes sind die folgenden Bedingungen zu beachten:

- Alle an den Prozessen des zentralen Zertifizierungsdienstes (2048) der Deutschen Post Com GmbH - Geschäftsfeld Signtrust mitwirkenden Mitarbeiter sind nachdrücklich auf die Einhaltung aller Arbeits- und Sicherheitsmaßnahmen hinzuweisen. Entsprechende Kontrollen sind vorzusehen.
- Bei sicherheitserheblichen Änderungen sowie bei Manipulationsverdacht, der sich nicht mit den dafür vorgesehenen Mechanismen und weiteren vorgesehenen Maßnahmen des Betreibers des Zertifizierungsdienstes klären bzw. beheben lässt, sind anerkannte Prüfstellen einzuschalten.
- Alle Betriebsauflagen und Umgebungsbedingungen aus den Bestätigungen für die eingesetzten technischen Komponenten sind zu beachten. Soll von den vorgegebenen Auflagen und Bedingungen abgewichen werden, ist vorab das Votum der Prüf- und Bestätigungsstelle einzuholen.
- Die Durchführung jeder organisatorischen sicherheitsrelevanten Maßnahme ist durch einen von den Zuständigen handschriftlich unterzeichneten Papierbeleg nachzuweisen.

- Jede sicherheitserhebliche Veränderung ist der Bundesnetzagentur unverzüglich anzuzeigen.

d) Nutzung des Zertifizierungsdienstes durch andere ZDA

Für die Nutzung des Zertifizierungsdienstes (2048) der Deutschen Post Com GmbH - Geschäftsfeld Signtrust durch andere ZDA ist folgende Auflage einzuhalten:

Auflage 4: Für die Nutzung eines Moduls des Zertifizierungsdienstes (2048) durch einen ZDA sind diesem vom Betreiber des Dienstes folgende Informationen in geeigneter Weise zur Verfügung zu stellen:

- ▶ Beschreibung des Moduls,
- ▶ Beschreibung der Schnittstellen Modul ↔ ZDA,
- ▶ Auswahl zulässiger Parameter und zulässiger Kombinationen von Teilmodulen (soweit zutreffend),
- ▶ Referenz auf die aktuelle Sicherheitsbestätigung des Zertifizierungsdienstes (2048) der Deutschen Post Com GmbH - Geschäftsfeld Signtrust.

Ende der Bestätigung

Sicherheitsbestätigung:
T-Systems. 03174.SE.10.2006

Hrsg.: T-Systems GEI GmbH
Adresse: Rabinstr.8, 53111 Bonn
Telefon: +49-(0)228-9841-0
Fax: +49-(0)228-9841-60
Web: www.t-systems-itc.de
www.t-systems-zert.com