



Sicherheitsbestätigung und Bericht

T-Systems. 03145.SE.08.2006

**Zertifizierungsdiensteanbieter
DGN Service GmbH**

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**

„Zertifizierungsdiensteanbieter DGN Service GmbH“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems. 03145.SE.08.2006

Bonn, den 24.08.2006

(Dr. Heinrich Kersten)

 T-Systems

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:

Zertifizierungsdiensteanbieter DGN Service GmbH

Richard-Oskar-Mattern-Straße 6

40547 Düsseldorf

2. Funktionsbeschreibung

Die Firma DGN Service GmbH betreibt einen Zertifizierungsdienst gemäß §§ 2 Nr. 8, 15 Abs. 1 SigG mit den Funktionen Registrierung, Schlüsselgenerierung, Schlüsselzertifizierung, Verzeichnisdienst und Sperrdienst.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Das Sicherheitskonzept des Zertifizierungsdiensteanbieter DGN Service GmbH erfüllt die Anforderungen nach § 2 SigV.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Der Zertifizierungsdiensteanbieter bietet zur Identifizierung von Antragstellern die folgenden Varianten an:

1. Identifizierung durch den ZDA.
2. Identifizierung mittels POSTIDENT BASIC.
3. Identifizierung durch beauftragte Dritte ("ZDA Ident").

Die Variante "ZDA Ident" ist im Sicherheitskonzept vorgesehen, wird aber zur Zeit noch nicht genutzt.

Mit Ausnahme des POSTIDENT-Verfahrens³ hat der Zertifizierungsdiensteanbieter alle für die Registrierung und Identifizierung eingesetzten Mitarbeiter für ihre Aufgaben geschult und autorisiert. Sie sind in dieser Funktion an die Weisungen des Zertifizierungsdiensteanbieters gebunden und in die Organisation und das Sicherheitskonzept eingebunden.

Die Personalisierung der Signaturerstellungseinheiten erfolgt beim ZDA. Im Sicherheitskonzept ist außerdem eine externe Teil-Personalisierung vorgesehen. Diese wird jedoch zur Zeit nicht genutzt.

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

1. Persönliche Übergabe durch den ZDA.
2. Übergabe mittels POSTIDENT SPECIAL.
3. Übergabe entsprechend eines mit dem Antragsteller vereinbarten Verfahrens nach §5 (2) SigV in Verbindung mit Art. 2 SigÄndG.
4. Persönliche Übergabe durch einen beauftragten Dritten.

Die Variante 4 ist im Sicherheitskonzept vorgesehen, wird aber zur Zeit noch nicht genutzt.

Die Archivierung der Dokumentation gemäß §10 SigG bzw. §8 SigV erfolgt durch den ZDA. Im Sicherheitskonzept ist außerdem eine externe Archivierung bei einem Dienstleister vorgesehen. Diese wird jedoch zur Zeit nicht genutzt.

Der Zertifizierungsdienst bietet weiterhin die Funktionen Schlüsselerzeugung, Schlüsselzertifizierung, Verzeichnis- und Sperrdienst.

Alle Funktionen sind im Sicherheitskonzept des Zertifizierungsdienstes mit der Versionsnummer 1.17 vom 07.08.2006 (letzte Revision) beschrieben.

Im Sicherheitskonzept ist weiterhin ein Zeitstempeldienst beschrieben, der jedoch zur Zeit nicht angeboten wird.

Der Zertifizierungsdienst 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

³ Siehe hierzu die Version 8.0 des betreffenden Sicherheitskonzeptes bzw. die Sicherheitsbestätigung TUVIT.09487.SW.05.2006 vom 02.05.2006.

Dokumenten ist der Prüf- und Bestätigungsstelle anzuzeigen und erfordert ggf. eine Überprüfung und eine Erweiterung der Bestätigung. Insbesondere ist eine Umsetzungsprüfung durch die Prüf- und Bestätigungsstelle erforderlich, bevor

- die Variante "ZDA Ident" bei der Identifizierung oder die Varianten 4 bei der Auslieferung der Signaturerstellungseinheiten genutzt werden kann,
- die externe Teil-Personalisierung der Signaturerstellungseinheiten genutzt werden kann,
- die Archivierung zu einem externen Dienstleister verlagert werden kann,
- Zeitstempeldienst in Betrieb genommen werden kann.

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

b) Inbetriebnahme

Der Betriebsablauf beim Zertifizierungsdienst wurde im Rahmen der Umsetzungsprüfung in allen Funktionen demonstriert. Die korrekte Umsetzung des Sicherheitskonzeptes wird bestätigt.

Vor der Inbetriebnahme sind folgende Auflagen durch den ZDA zu erfüllen:

Auflage 1: Die vom ZDA genutzten technischen Komponenten "FlexiTrust 3.5" und "FlexSecure OCSP Responder 3.5" müssen sicherheitsbestätigt sein.

Sollten sich hierdurch bisher nicht bekannte Anforderungen an die Einsatzumgebung dieser Komponenten ergeben, sind diese im Sicherheitskonzept zu berücksichtigen. Eine Prüfung der Umsetzung solcher Vorgaben durch die Prüf- und Bestätigungsstelle kann dann im Rahmen der Inbetriebnahmeprüfung (Auflage 2) erfolgen.

Auflage 2: Eine erfolgreiche Inbetriebnahmeprüfung ist erforderlich.

Die Inbetriebnahme des Zertifizierungsdienstes kann erfolgen, sobald die Auflage 1 erfüllt ist und entsprechende Zertifikate der Bundesnetzagentur für den Zertifizierungs- und Verzeichnisdienst vorliegen.

Grundsätzlich gilt darüber hinaus:

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 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 Prüf- und Bestätigungsstellen 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.

Ende der Bestätigung

Sicherheitsbestätigung:
T-Systems. 03145.SE.08.2006

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