Sicherheitsbestätigung und Bericht

T-Systems.03232.SW.08.2009

DGN Deutsches Gesundheitsnetz Service GmbH

Bestätigung
für die Umsetzung von Sicherheitskonzepten

gemäß § 15 Abs. 2 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und §§ 11 Abs. 2 Signaturverordnung[2]

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 Deutsches Gesundheitsnetz Service GmbH“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.03232.SW.08.2009

Bonn, den 13.08.2009

(Dr. Heinrich Kersten)

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 Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. Jahrgang 2007, Teil I S. 179)

2 Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

Beschreibung zum Sicherheitskonzept:

1. Bezeichnung des Zertifizierungsdiensteanbieters:

DGN Deutsches Gesundheitsnetz Service GmbH
Niederkasseler Lohweg 181-183
40547 Düsseldorf

2. Funktionsbeschreibung

Die Firma DGN Service GmbH betreibt einen Zertifizierungsdienst gemäß §§ 2 Nr. 8, 15 Abs. 1 SigG mit den Funktionen Registrierung inkl. Identifizierung, Schlüsselgenerierung, Schlüsselzertifizierung, SSEE-Auslieferung, Verzeichnis- und Auskunftsdienst sowie Sperrdienst.

Abgesehen von den Teilprozessen, die durch beauftragte Dritte durchgeführt werden, werden alle vom ZDA im Sicherheitskonzept beschriebenen Abläufe an folgenden Standorten in Düsseldorf abgewickelt:

- Büro- und Produktionsstandort: Niederkasseler Lohweg 181-183
- Haupt-RZ-Standort: Richard-Oskar-Mattern-Str. 6
- Backup-RZ-Standort: Am Seestern 8

Der Zertifizierungsdienst wird durch für ihre Aufgaben geschulte und autorisierte Mitarbeiter innerhalb einer baulich, organisatorisch und systemtechnisch abgesicherten Umgebung betrieben.

Das Rollenkonzept trennt zwischen administrativen und operativen Rollen, nutzt das 4-Augenprinzip (wo notwendig) und verhindert den Durchlauf mit einer Person bei kritischen Prozessen durch entsprechende Rollenausschlüsse.

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

- Identifizierung durch den ZDA.
- Identifizierung durch beauftragte Dritte ("ZDA-Ident").
- Identifizierung durch die Deutsche Post AG mit dem PostIdent-Verfahren (als Modul bestätigt unter TUVIT.94102.SW.07.2009 vom 10.07.2009 mit Nachtrag 1 vom 15.07.2009).

- Identifizierung durch die Ärztekammer Nordrhein mit dem Verfahren Kammer-Ident[3] (separat als Modul bestätigt unter TUVIT.09498.SE.09.2008 vom 19.09.2008 mit Nachtrag 1 vom 23.07.2009).

Für die ersten beiden Varianten 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 sicheren Signaturerstellungseinheiten (SSEE) erfolgt beim ZDA. Im Sicherheitskonzept ist außerdem eine externe Teil-Personalisierung vorgesehen, die jedoch zur Zeit nicht genutzt wird.

Die Auslieferung der SSEE erfolgt mit einer der folgenden Varianten:

1. Persönliche Übergabe durch den ZDA.
2. Persönliche Übergabe durch einen beauftragten Dritten (hier : POSTIDENT SPECIAL, ggf. auch andere beauftragte Dritte).
3. Übergabe entsprechend eines mit dem Antragsteller individuell vereinbarten Verfahrens nach §5 (2) SigV.

Die Sperrhotline wird von der Fa. Invitel GmbH (Helmstedt) betrieben, deren Abläufe in das Sicherheitskonzept des ZDA eingebunden sind. Weiterhin sind eine schriftliche Sperrung und eine Sperrung durch persönliches Erscheinen beim ZDA möglich.

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, die jedoch zur Zeit noch nicht genutzt wird.

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

Alle Funktionen – insbesondere die weiteren technischen Dienste Schlüsselgenerierung, Schlüsselzertifizierung, Verzeichnis- und Auskunftsdienst – sind im Sicherheitskonzept des Zertifizierungsdienstes mit der Versionsnummer 1.24 vom 10.08.2009 (letzte Revision) und mitgeltenden Unterlagen beschrieben.

---

[3] Dieses Verfahren nutzt intern ebenfalls das o. a. PostIdent-Verfahren.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Das Sicherheitskonzept des DGN Deutsches Gesundheitsnetz Service GmbH erfüllt die Anforderungen nach §4 (2) Satz 4 SigG i.V. mit § 2 SigV unter folgender Auflage:

- Es ist eine erfolgreiche Umsetzungsprüfung nachzuweisen; diese Umsetzungsprüfung muss folgende beauftragte Dritte einschließen: Fa. Invitel GmbH (Sperrhotline), Deutsche Apotheker- und Ärztebank (ZDA-Ident, Infrastruktur-Sicherheitsdienst).

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

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 solche Veränderungen zusätzlich unmittelbar der Bundesnetzagentur anzuzeigen.

Insbesondere ist eine Umsetzungsprüfung durch die Prüf- und Bestätigungsstelle erforderlich, bevor

- die externe Teil-Personalisierung der Signaturerstellungseinheiten genutzt werden kann,
- die Archivierung zu einem externen Dienstleister verlagert werden kann,
- der Zeitstempeldienst in Betrieb genommen werden kann.

b) Inbetriebnahme

Im Rahmen der Wiederholungsprüfung ist eine gesonderte Inbetriebnahme nicht durchzuführen. Grundsätzlich gilt aber:

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.03232.SW.08.2009

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.de/ict-security
	www.t-systems-zert.com