Bestätigung der Eignung und praktischen Umsetzung eines Teilsicherheitskonzeptes (Moduls)

zur Verwendung in einem Sicherheitskonzept

gemäß § 15 Abs. 2 des Gesetzes über Rahmenbedingungen für elektronische Signaturen (SigG)

Gültig bis 21.06.2018

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20
45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 2 Satz 1 Signaturgesetz[1] und § 11 Abs. 2 Signaturverordnung[2],
dass das

Postident-Verfahren

der Deutsche Post AG

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter

TUVIT.94154.SW.06.2015

Essen, 22.06.2015

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 126 vom 10.07.1999, Seite 11181, und gemäß § 25 Abs. 3 SigG zur Erteilung von Bestätigungen für die Umsetzung von Sicherheitskonzepten gemäß § 15 Abs. 2 Satz 1 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 Absatz 111 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 4 Absatz 112 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

Beschreibung zum Sicherheitskonzept:

1 Bezeichnung des Betreibers:

Deutsche Post AG
Charles-de-Gaulle-Straße 20
53113 Bonn

2 Funktionsbeschreibung

Die Deutsche Post AG übernimmt für Zertifizierungsdiensteanbieter gemäß § 2 Nr. 8 SigG die Aufgaben „Identifizierung von Antragstellern“ und „persönliche Übergabe von sicheren Signaturerstellungseinheiten (SSEE) an Signaturschlüssel-Inhaber“.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Das von der Deutsche Post AG vorgelegte Sicherheitskonzept zum POSTIDENT-Verfahren, Version 10.0.3 vom 15.06.2015, erfüllt für die in Kapitel 2 genannten Aufgaben die Anforderungen nach § 2 SigV.

3.2 Einsatzbedingungen

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

a) Einsatzumgebung

Die Deutsche Post AG setzt als Identifizierungsstellen, DPAG Postfilialen, Postbank Finanzcenter und Postfilialen im Einzelhandel unter Anwendung des *POSTIDENT BASIC*-Verfahrens ein. Die für die Identifizierung eingesetzten Mitarbeiter wurden im Auftrag der Deutsche Post AG für ihre Aufgaben geschult und autorisiert. Sie sind in dieser Funktion an die Weisungen der Abteilung gebunden und in die Organisation und das Sicherheitskonzept für die Nutzung des Postident-Verfahrens durch Zertifizierungsdiensteanbieter eingebunden.

Die Deutsche Post AG setzt als Auslieferungsstellen für SSEE die Zustellstützpunkte unter Anwendung des *POSTIDENT SPECIAL*-Verfahrens ein. Wird die zu identifizierende Person bei der Zustellung nicht angetroffen, wird eine Nachricht für die Person hinterlassen, dass sie die Sendung in der dem Zustellstützpunkt zugeordneten Filiale abholen kann. In diesem Fall erfolgen die Identifizierung und Übergabe der SSEE in der Filiale analog zum *POSTIDENT BASIC*-Verfahren.

Die für die Identifizierung bei der Übergabe der SSEE eingesetzten Mitarbeiter der Zustellstützpunkte wurden im Auftrag der Deutsche Post AG für ihre Aufgaben geschult und autorisiert. Sie sind in dieser Funktion an die Weisungen der Abteilung gebunden und in die Organisation und das Sicherheitskonzept für die Nutzung des Postident-Verfahrens durch Zertifizierungsdiensteanbieter eingebunden.

Jede sicherheitserhebliche Veränderung im Gesamtkonzept, in Prozessabläufen oder den Sicherheitselementen ist einer Bestätigungsstelle anzuzeigen und erfordert ggf. eine Überprüfung und eine Erweiterung der Bestätigung. Die hiernach gültigen Änderungen im Sicherheitskonzept sind den vertraglich angebundenen Zertifizierungsdiensteanbietern zur Ermöglichung der Überprüfung ihrer eigenen Sicherheitskonzepte unverzüglich zur Kenntnis zu bringen.

b) Inbetriebnahme

Diese Bestätigung erweitert nach der Aktualisierung des Sicherheitskonzeptes die Bestätigung TUVIT.94127.SW.06.2012 vom 22.06.2012. Der Betriebsablauf des Postident-Verfahrens wurde der Bestätigungsstelle im Rahmen der Wiederholungsprüfung gemäß § 15 Abs. 2 SigG und § 11 Abs. 2 SigV demonstriert. Die weiterhin korrekte Umsetzung des Sicherheitskonzeptes wird bestätigt. Der Betrieb des Postident-Verfahrens für Zertifizierungsdiensteanbieter kann unmittelbar weitergeführt werden.

Die Inbetriebnahme des Postident-Verfahrens für die Nutzung durch weitere Zertifizierungsdiensteanbieter zur Identifizierung der Antragsteller und zur Auslieferung der SSEE kann unmittelbar nach Vertragsabschluss mit dem Zertifizierungsdiensteanbieter erfolgen. Darin verpflichtet sich die Deutsche Post AG gegenüber den Zertifizierungsdiensteanbietern verbindlich, das Postident-Verfahren für die Nutzung durch Zertifizierungsdiensteanbieter uneingeschränkt auf der Grundlage des bestätigten Sicherheitskonzeptes einzusetzen

c) Betrieb des Postident-Verfahrens für Zertifizierungsdiensteanbieter

Während des Betriebes sind von den Zertifizierungsdiensteanbietern die folgenden Hinweise für die sachgemäße Nutzung des Postident-Verfahrens zu beachten:

- Beim Zertifizierungsdiensteanbieter müssen beim Einsatz des Postident-Verfahrens die in Kapitel 11.1 des Sicherheitskonzeptes beschriebenen Aufgaben gelöst werden.
- Die Eignung des Ausweisdokumentes gemäß § 3 Abs. 1 Satz 1 SigV ist durch den Zertifizierungsdiensteanbieter zu überprüfen.
- Der Zertifizierungsdiensteanbieter hat alle beim Postident-Verfahren festgestellten Reklamationen, z. B. inkorrekt ausgefülltes Postident-Formular, an das Reklamationsmanagement (Backoffice) der Deutsche Post AG zu melden und mit dem Grund und Datum der Reklamation zu dokumentieren. Die Dokumentation ist für 3 Jahre aufzubewahren und auf begründetes Verlangen einer Bestätigungsstelle vorzulegen.
- Das Sicherheitskonzept zum Postident-Verfahren kann als Modul des Sicherheitskonzeptes eines Zertifizierungsdiensteanbieters referenziert werden, wenn die dort in Kapitel 12 beschriebenen Schnittstellenanforderungen, soweit anwendbar, eingehalten werden.
- Die Zertifizierungsdiensteanbieter sind insbesondere darauf hinzuweisen, die Vertrauensanker bei der Übermittlung der Antragsteller-Identifizierung mittels *POSTIDENT BASIC* (*POSTIDENT BASIC*-Formular, ZORA-Aufdruck mit Unterschrift des Identifizierungsmitarbeiters) jeweils in der Registrierungsstelle sorgfältig zu prüfen.

- Das Postident-Verfahren darf nur im Rahmen der Gültigkeit dieser Bestätigung gemäß Abschnitt 3.3 eingesetzt werden. Die Zertifizierungsdiensteanbieter müssen daher die Gültigkeit dieser Bestätigung überwachen und dürfen das Postident-Verfahren nach Gültigkeitsablauf nicht mehr einsetzen.

d) Allgemeine Hinweise

Jede sicherheitserhebliche Veränderung ist der zuständigen Behörde unverzüglich anzuzeigen.

Diese Urkunde gilt nur zusammen mit dem Bestätigungsbericht zum Bestätigungsvorgang TUVIT.94154.SW.06.2015.

3.3 Gültigkeit der Bestätigung

Diese Bestätigung erweitert die Bestätigung TUVIT.94127.SW.06.2012 vom 22.06.2012 und ist nach sicherheitserheblichen Veränderungen, jedoch spätestens am 21.06.2018 zu erneuern.

Die Gültigkeit der Bestätigung kann jedoch verlängert werden, wenn vor diesem Zeitpunkt die Eignung und praktische Umsetzung des Sicherheitskonzeptes durch eine Bestätigungsstelle erneut geprüft und bestätigt worden ist, oder verkürzt werden, wenn der Bestätigungsstelle Erkenntnisse vorliegen, dass die gesetzlichen Anforderungen nicht mehr im vollen Umfang erfüllt sind.

Ende der Bestätigung