Deutsche Krankenhaus TrustCenter
und Informationsverarbeitung GmbH

Zertifizierungsablauf für den Datenaustausch nach § 301 SGB V

Stand: 01.10.2021

Wichtig: Aufgrund neuer gesetzlicher Vorgaben an das Verfahren zur Ausgabe von Zertifikaten nach § 301 SGB V ist es erforderlich, dass die DKTIG sich davon überzeugt, dass der Schlüsselverantwortliche tatsächlich derjenige ist, der er vorgibt zu sein. Wir bitten daher um Beachtung des nachfolgend beschriebenen Zertifizierungsablaufes.

1. TrustCenter Vertrag zwischen dem Krankenhaus und der DKTIG

Für Neukunden: Das Krankenhaus schließt mit der DKTIG einen TrustCenter-Vertrag ab.

2. Überprüfung der Daten in der Verschlüsselungssoftware durch das Krankenhaus

- Korrektes **Institutionskennzeichen** (IK)
- Korrekter **Krankenhausname** (ohne Umlaute und Sonderzeichen)
- Korrekter **Ansprechpartner = Schlüsselverantwortlicher**
  (Vor- und Nachname, ohne Umlaute und Sonderzeichen)
- Korrekter **TrustCenter-Name**
  - PKCS#7: TrustCenter für Krankenhäuser und Leistungserbringer PKC
- Ausfüllen des Formulars Zertifikatsanforderung (auch wenn der Schlüsselverantwortliche sich nicht ändert)

  Neu: Das Formular Zertifikatsanforderung hat die DKTIG an die gesetzlichen Vorgaben angepasst. Die DKTIG benötigt die datenschutzrechtliche Einwilligung und Authentifizierung des Schlüsselverantwortlichen.

3. Erzeugung eines neuen Schlüsselpaars durch das Krankenhaus

- In der Verschlüsselungssoftware sendet das Krankenhaus die P10-Datei (PKCS#7) an das TrustCenter.

  Es können unsere Kommunikationsparameter genutzt werden, um aus der CoCoNet-Software die p.10-Datei (Request) zu übermitteln.
  - **IP-Nr.: 194.145.83.92**
  - **Port-Nr.: 3280**

  oder

  Per E-Mail (im Anhang): **trust@dktig-trust.de**

- Ausdrucken des Fingerprints (Begleitschreiben)

4. Einreichung der Unterlagen durch das Krankenhaus

Die DKTIG benötigt für die Antragsbearbeitung folgende Unterlagen:

- vom Schlüsselverantwortlichen unterschriebenen und mit Stempel versehenen Fingerprint **im Original**
- Formular Zertifikatsanforderung **im Original**
- Für Rehabilitationseinrichtungen wird zusätzlich benötigt:
  Vergabe-Bescheid der ARGE-IK (Vergabe des Institutionskennzeichens) **in Kopie**

Bitte senden Sie diese Dokumente an die
DKTIG mbH, Humboldtstraße 9, 04105 Leipzig

Die o. g. Dokumente können bei drohenden Fristabläufen der DKTIG vorab elektronisch per E-Mail an trustcenter@dktig.de übermittelt werden.

5. Authentifizierung des Schlüsselverantwortlichen

Nach Eingang des Formulars Zertifikatsanforderung erhält der Schlüsselverantwortliche weitere Informationen zum Videoidentverfahren per E-Mail. Es erfolgt die Identifizierung des Schlüsselverantwortlichen.
Das Ergebnisprotokoll wird anschließend samt der im Prüfungsprozess aufgenommenen Fotos und der Unterschrift, wie sie im amtlichen Lichtbildausweises abgebildet ist, der DKTIG übermittelt.

6. Registrierung: Prüfung der Unterlagen durch das TrustCenter der DKTIG

- Plausibilitätsprüfung des elektronisch übermittelten Request (maschinell)
- Prüfung der antragstellenden Institution mittels IK-Verzeichnis der ARGE-IK in Verbindung mit den öffentlichen Zertifikatsdaten der SMC-B, die für die Anbindung an die Telematikinfrastruktur genutzt wird.
- Die DKTIG prüft das Ergebnisprotokoll der Authentisierung (vgl. Punkt 5).
- Überprüfung des eindeutigen Hash-Wertes des elektronisch übermittelten Request mit dem Hash-Wert des Fingerprints auf Übereinstimmung

6 a) Bei korrektem Antrag und positivem Ergebnis des identityTM-Videoverfahrens

- Zusendung der Vorgangsnummer zur Beobachtung des Online-Status der Zertifizierung durch das TrustCenter der DKTIG (nur bei E-Mail-Aufträgen)

Nachverfolgung unter:
https://www.dktig-trust.de/dktig/osa.php
(Login mittels Eingabe der Vorgangs-Nr. und des Institutionskennzeichen)

6 b) Bei fehlerhaftem Antrag oder negativem Ergebnis des identityTM-Videoverfahrens

- Benachrichtigung durch die DKTIG mit genauer Fehlermeldung
- Korrektur durch Ansprechpartner und erneute Beantragung (vgl. Punkt 2 bis 6)

7. Zertifizierung des öffentlichen Teilnehmerschlüssels durch das TrustCenter der DKTIG

- Benachrichtigung des Ansprechpartners über erfolgreiche Zertifizierung
  - FTAM-Anträge: Bereitstellung des Zertifikats per FTAM
  - E-Mail-Anträge: Zusendung des Zertifikates an die E-Mail-Adresse des Absenders
- Bereitstellung des Zertifikates über den E-Mail-Responder:
  Senden Sie eine E-Mail an: **trust@dktig-trust.de** mit folgendem Befehl im Textfeld (nicht in der Betreffzeile!)**:**

  send 12345678.p7c („**send**“ + **die ersten acht Ziffern des IK** + „**.p7c**“)
- Bereitstellung des Zertifikates auf der DKTIG-Homepage zum Download (vgl. Punkt 6 a).

8. Veröffentlichung des Zertifikates in den öffentlichen Schlüsselverzeichnissen

- Die Veröffentlichung des zertifizierten öffentlichen Schlüssels in den folgenden Schlüsselverzeichnissen erfolgt am Nachmittag der Bereitstellung
  - **gesamt-pkcs.key**
- Die öffentlichen Schlüssel der Annahmestellen stehen über folgende Wege zur Abholung bereit:
  - über die Verschlüsselungssoftware
  - über den E-Mail-Responder:
    Senden Sie eine E-Mail an: **trust@dktig-trust.de** mit folgendem Befehl im Textfeld (nicht in der Betreffzeile!):
    send annahme-rsa4096.key (rsa4096 für GKV) und **send pkv-rsa4096.key** (rsa4096 für PKV)
  - als Download über die Homepage der DKTIG (https://www.dktig.de/de/trustcenter/downloads)

9. Weitere Fragen zur Zertifizierung

Zur Beantwortung ggf. weiterer Fragen stehen wir gerne zur Verfügung:

DKTIG
Humboldtstr. 9
04105 Leipzig
E-Mail: trustcenter@dktig.de
Telefon: + 49 341 308951-0
Homepage: www.dktig.de