Zertifizierungsablauf für Zertifikate für Softwarehersteller

1. Beantragung eines gesonderten Institutionskennzeichen

Der Softwarehersteller hat bei der ARGE IK ein IK beantragt. Als Klassifikation ist „Softwarehersteller im Sozialversicherungswesen für zertifikatsbasierte Testverfahren“ anzugeben.

2. TrustCenter Vertrag zwischen der Organisation und der DKTIG

Voraussetzung für die Beantragung eines Zertifikates für Testverfahren der Softwarehersteller ist, dass zwischen dem Softwarehersteller (der Organisation) und der DKTIG ein TrustCenter Vertrag besteht.

Bei Fragen zur Vertragsstruktur beraten wir Sie gerne.

Unsere Ansprechpartner im TrustCenter 301 erreichen Sie unter:
Telefonnummer: +49 341 308951-0
E-Mail: trustcenter@dktig.de

3. Registrierung im Serviceportal

Die Registrierung im Serviceportal der DKTIG unter www.dktig-serviceportal.de ermöglicht Ihnen

- eine sichere Identifikation direkt im Portal,
- die Zuordnung Ihrer Identität zu einer oder mehreren Organisationen und
- die Beantragung und Verwaltung von Zertifikaten.

Der Vertretungsberechtigte Ihrer Organisation berechtigt Sie mit dem Formular „Ernennung zum Schlüsselverantwortlichen“, welches im Serviceportal hochgeladen werden muss, Zertifikate für den Datenaustausch gem. §§ 301, 302 SGB V und/oder Datenübermittlung für QS-Meldeverfahren oder für Testverfahren bei Softwareherstellern bei der DKTIG zu beantragen.

Die bei der Registrierung eingegebenen persönlichen Daten werden zur Identifizierung mittels Video- oder Postident benötigt und müssen mit Ihrem zur Identifikation genutzten Ausweisdokument übereinstimmen.

3.1 Verifizierung Ihrer E-Mail-Adresse

Bitte geben Sie zur Verifizierung Ihrer E-Mail-Adresse eine personalisierte E-Mail-Adresse (Beispiel: max.mustermann@krankenhaus.de) an.

3.2 Zweiten Faktor einrichten

Der zweite Faktor ist eine erforderliche Maßnahme, um die Sicherheit Ihres Kontos zu erhöhen. Wir empfehlen als zweiten Faktor das sichere und zukunftsfähige TOTP-Verfahren. Aktuell bieten wir als Alternative für den zweiten Faktor noch das SMS-Verfahren an. Dieses Verfahren wird jedoch nicht mehr empfohlen und wird zukünftig abgelöst.

a) TOTP-Verfahren
Installieren Sie eine dieser Apps auf Ihr mobiles Endgerät.
- Google Authentikator
- FreeOTP
- Microsoft-Authenticator

Öffnen Sie die App und scannen Sie den QR-Code. Den angezeigten Code geben Sie bitte im Portal ein. Innerhalb von 30 Sekunden wird automatisch ein neuer Code generiert.

b) SMS-Verfahren
Bitte kontrollieren Sie die bei der Registrierung angegebene Mobilfunknummer auf Richtigkeit. Klicken Sie auf Code anfordern. Der Code ist innerhalb von 60 Sekunden als Einmalpasswort nutzbar.

4. POSTIDENT-Identifizierungsverfahren

Bitte prüfen Sie nochmals, ob die angegebenen Daten mit Ihrem Ausweisdokument identisch sind und wählen Sie dann eines der drei genannten "POSTIDENT"-Identifizierungsverfahren aus.

- POSTIDENT durch Postfiliale
- POSTIDENT durch Videochat
- POSTIDENT durch Online-Ausweisfunktion

Alle drei Identifikationsverfahren werden durch die Deutsche Post AG durchgeführt.

5. Ernennung zum Schlüsselverantwortlichen

Nach erfolgreichem POSTIDENT können Sie sich im Serviceportal der DKTIG einer oder mehrerer Organisationen zuordnen. Bitte geben Sie dafür das neunstellige Institutionskennzeichen Ihrer Organisation ein. Das Formular zur **Ernennung zum Schlüsselverantwortlichen** finden Sie im Serviceportal der DKTIG. Wichtig ist die Unterschrift des Vertretungsberechtigten. Er bevollmächtigt Sie als sog. Schlüsselverantwortlichen Zertifizierungsanträge für den Datenaustausch gem. §§ 301, 302 SGB V Datenübermittlung für QS-Meldeverfahren oder für Testverfahren bei Softwareherstellern bei der DKTIG zu stellen.

Bitte bestätigen Sie durch die Eingabe des zuvor gewählten zweiten Faktors (entweder TOTP oder SMS Code) zur Nutzung des Portals berechtigt zu sein und klicken Sie auf Verifizieren.

Die DKTIG prüft den Antrag und führt ggf. eine Telefonvalidierung durch. Dies bedeutet, dass die DKTIG in Einzelfällen, den Vertretungsberechtigten der Organisation kontaktiert und sich davon überzeugt, dass Sie zum Beantragen von Zertifikaten bevollmächtigt wurden. Erst wenn der Antrag durch die DKTIG geprüft und „umgesetzt“ wurde, können Sie einen Zertifizierungsantrag stellen. Mit Ihren Zugangsdaten können Sie jederzeit den Bearbeitungsstand Ihrer Anträge im Serviceportal einsehen.

6. Außerhalb des Serviceportals – Überprüfung der in der Verschlüsselungssoftware hinterlegten Daten

Bitte prüfen Sie oder Ihr Softwareunternehmen folgende Daten auf Richtigkeit, bevor das Schlüsselpaar generiert wird.

- ✓ Korrektes **Institutionskennzeichen** (IK)
- ✓ Korrekter **Krankenhausname** (ohne Umlaute und Sonderzeichen)
- ✓ Korrekter **Schlüsselverantwortlicher**
  (Vor- und Nachname, ohne Umlaute und Sonderzeichen)
- ✓ Korrekter **TrustCenter-Name**
  - ➢ PKCS#7: DKTIG TrustCenter fuer Krankenhaeuser und Leistungserbringer PKC

7. Außerhalb des Serviceportals – Erzeugung eines neuen Schlüsselpaars durch die Organisation

In der Schlüsselgenerierungssoftware sendet die Organisation die **P10-Datei (PKCS#7)** an das TrustCenter entweder

per E-Mail	oder	**per FTAM**	
trust@dktig-trust.de		IP-Nr.:	194.145.83.92
		Port-Nr.:	3280

8. Antrag Zertifikat §§ 301, 302 SGB V bzw. Datenübermittlung für QS-Meldeverfahren

1. Bitte wählen Sie Ihre Organisation aus, für die Sie ein Zertifikat benötigen.
2. Laden Sie den Fingerprint als PDF hoch. Diesen erhalten Sie in Ihrer Schlüsselgenerierungs-software bzw. von Ihrem Softwareanbieter.
3. Bitte bestätigen Sie durch die Eingabe des zuvor gewählten zweiten Faktors (entweder TOTP oder SMS Code) zur Nutzung des Portals berechtigt zu sein und klicken Sie auf Verifizieren.

Mit dem Antrag Zertifikat erklären Sie im Serviceportal, dass:

- die notwendigen Maßnahmen zur Sicherung des privaten Schlüssels gegen Zugriffe oder Verwendung von Unbefugten getroffen sind,
- Passwörter und/oder PIN's (Persönliche Identifikations-Nummer) zum Schutz des privaten Schlüssels streng vertraulich gehalten werden,
- bei Verdacht der Offenlegung, Preisgabe oder Hinweis auf einen möglichen Missbrauch von Passwort und/oder PIN diese unverzüglich ausgetauscht werden,
- ich bei Kenntnis einer möglichen Kompromittierung des privaten Schlüssels unverzüglich die Sperrung des Zertifikats durch die DKTIG veranlassen werde,
- die DKTIG ermächtigt ist, Ihrerseits das Zertifikat zu sperren, wenn der Verdacht begründet ist, dass der private Schlüssel kompromittiert ist und eine vorhergehende Information nicht möglich ist. (In diesem Fall informiert die DKTIG unverzüglich.)
- ich bei der Prüfung von Zertifikaten in eigenem Ermessen feststelle, ob der Zertifizierungs-pfad bzw. das Zertifikat entsprechend der aktuellen Sperrliste gültig ist. Ein Verzicht auf die Prüfung erfolgt auf eigenes Risiko.
- ich der Veröffentlichung des Zertifikats im öffentlichen Verzeichnis zustimme.

9. Prüfung des Zertifizierungsantrages 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 Zertifikatsdaten der SMC-B, die für die Anbindung an die Telematikinfrastruktur genutzt wird.
- ✓ Überprüfung des eindeutigen Hash-Wertes des elektronisch übermittelten Requests mit dem Hash-Wert des Fingerprints auf Übereinstimmung

10. Zertifizierung des öffentlichen Teilnehmerschlüssels durch das TrustCenter der DKTIG

Sie werden per E-Mail über die erfolgreiche Zertifizierung informiert und empfangen das Zertifikat entsprechend des Übermittlungswegs.

- ➢ FTAM-Anträge: Bereitstellung des Zertifikats per FTAM
- ➢ E-Mail-Anträge: Zusendung des Zertifikates an die E-Mail-Adresse des Absenders

Sie können optional das Zertifikat über den E-Mail-Responder erhalten:
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**“)

Den Bearbeitungsstand Ihres Zertifikates können Sie auf der DKTIG-Homepage einsehen und eine Kopie des Zertifikates herunterladen unter: Anmeldung Webserver Online-Status-Zertifikat

11. Veröffentlichung des Zertifikates in den öffentlichen Schlüsselverzeichnissen

Die Veröffentlichung des zertifizierten öffentlichen Schlüssels in den Schlüsselverzeichnissen erfolgt am Nachmittag der Bereitstellung.

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!):
  für GKV: send annahme-rsa4096.key
  für PKV: send pkv-rsa4096.key
- ➢ als Download über die Homepage der DKTIG unter: https://dktig.de/downloads-zertifikate/

Für Fragen rund um das Zertifizierungsverfahren stehen wir Ihnen gerne zur Verfügung.

Ihre DKTIG