

Formular Zertifikatsanforderung

1. Institution (anforderndes Krankenhaus/Rechenzentrum)

a. Name der Einrichtung		
b. Adresse		
c. Institutionskennzeichen		
d. Ansprechpartner (Schlüsselverantwortlicher)	<small>Vorname</small>	<small>Nachname</small>

Hinweis: Die obigen Angaben unter Pkt. 1 a, c und d sind Bestandteil der X.500-Adresse, unter der das Zertifikat im öffentlichen Verzeichnis der Zertifikate aufgeführt wird. Diese Angaben müssen zur eindeutigen Identifizierung unbedingt mit den Angaben im Request übereinstimmen. Bitte verwenden Sie keine Umlaute (ä,ö,ü) oder Sonderzeichen (z.B. ß=/_\).

2. Kontakt-Informationen des Ansprechpartners (Schlüsselverantwortlichen)

Telefon	
E-Mail	
Abteilung	

3. Datenschutzrechtliche Einwilligung und Authentifizierung des Schlüsselverantwortlichen

Bei Anlage des Schlüsselverantwortlichen verarbeitet die DKTIG dessen personenbezogene Daten in dem unter Ziffer 1 lit. d und Ziffer 2 ersichtlichen Umfang.

Darüber hinaus findet eine eindeutige Authentifizierung des Schlüsselverantwortlichen statt. Hierbei nutzt die DKTIG das Videoidentverfahren, bei dem per Videocall eine Prüfung der Identität anhand eines amtlichen Lichtbildausweises festgestellt wird. Das Ergebnisprotokoll wird anschließend samt der im Prüfungsprozess aufgenommenen Fotos und der Unterschrift, wie sie im amtlichen Lichtbildausweises abgebildet ist, gespeichert.

Schließlich werden im öffentlichen Schlüsselverzeichnis der Vor- und Nachname des Schlüsselverantwortlichen veröffentlicht.

Für die vorgenannten Verarbeitungen benötigt die DKTIG die Einwilligung des Schlüsselverantwortlichen. Die Einwilligung ist freiwillig. Ohne Einwilligung kann diese Person jedoch nicht als Schlüsselverantwortlicher fungieren. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Der Widerruf wirkt erst für die Zukunft. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

Weitere datenschutzrechtliche Informationen sind dem Dokument „Ausfüllhinweise für das Formular Zertifikatsanforderung“ unter Ziffer 3 zu entnehmen.

Einwilligung

Mit meiner Unterschrift willige ich in die Verarbeitung meiner Daten im Rahmen der Anlegung und Authentifizierung als Schlüsselverantwortlicher sowie der Veröffentlichung meines Vor- und Nachnamens im öffentlichen Schlüsselverzeichnis ein.

Ort, Datum

Unterschrift des Schlüsselverantwortlichen

4. Erklärung des Ansprechpartners zur Sicherheit

Ich erkläre hiermit, 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 Zertifizierungspfad 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.

Ort, Datum

Unterschrift des Schlüsselverantwortlichen

5. Software zur Schlüsselerzeugung

Folgende Verschlüsselungssoftware wird verwendet:

Software	
Version Nr. (vom)	

6. Kommunikations-Kennwort

Für die telefonische Kommunikation mit der DKTIG bei Rückfragen im Zusammenhang mit der Identifizierung (Bestätigung der Zertifikats-Anforderung) oder bei Veranlassung einer Sperrung gilt folgendes Kennwort:

Das Passwort sollte mindestens aus 8 Zeichen, Groß- und Kleinschreibung und einer Zahl bestehen.

7. Kommunikations-Parameter für Zertifikate

- E-Mail TRUST@DKTIG-TRUST.DE

- FTAM

TrustCenter: FTAM-System: IP: 194.145.83.92; Port: 3280

Telefonische Hotline: +49 341 308951-0

Krankenhaus: Technischer Ansprechpartner: _____

Telefon: _____

E-Mail: _____

Hinweis: Die FTAM-spezifischen Anmeldeparameter lauten wie folgt:

Nutzer-Account:	anonymous
Nutzer-Kennwort:	keines
CallUserData (Hex):	03 01 01 00
ACSE-Adressinformation (OSI-Standard):	13999917
P-Selector, S-Selector, T-Selector: jeweils	FTAM

8. Unterschrift Vertretungsberechtigte/r des Krankenhauses (z. B. Geschäftsführer, Vorstand, Kfm. Direktor o.a.)

Ort, Datum

Unterschrift und Stempel
(Unterzeichnender des TrustCenter-Vertrages im Krankenhaus)

Name in Druckbuchstaben

Geschäftsführer:
Dipl. Kfm. (FH) René Schubert
Verwaltungsratsvorsitzender:
Dr. Stephan Helm

Gesellschafter:
Deutsche Krankenhausgesellschaft e. V.
Landeskrankenhausgesellschaften

Sitz der GmbH: Leipzig
Amtsgericht Leipzig: HRB 31322
Steuer-ID: 231/107/17261

Bankverbindung: Deutsche Bank
Privat- und Geschäftskunden AG
IBAN DE71 5907 0070 0040 2214 00
BIC DEUTDE33