FAQ-Zertifizierung

1. Wie lange gilt das aktuelle Zertifikat?

PKCS#7-Zertifikate die mit dem rsa4096-Algorithmus erzeugt wurden, haben eine zweijährige Gültigkeit. Das Gültigkeitsdatum können Sie dem Informationsschreiben, welches Sie von uns mit Bereitstellung des Zertifikates per E-Mail erhalten, entnehmen.

2. Was ist unter einem Nachfolgezertifikat zu verstehen?

Ein Nachfolgezertifikat liegt dann vor, wenn die DKTIG zu diesem Institutionskennzeichen bereits ein Zertifikat erstellt hat, die zweijährige Gültigkeit abgelaufen ist und keine Änderungen in den Kommunikationsparametern eingetreten sind. Die DKTIG benötiget dann

- den Ausdruck des "Fingerprints", also des öffentlichen Schlüssels zum neu generierten Schlüsselpaar - versehen mit der Unterschrift des Schlüsselverantwortlichen und dem Stempel des Krankenhauses im **Original** auf dem Postweg - und
- den elektronischen Request zur Zertifizierung Ihres Schlüssels.
- Das „Formular Zertifikatsanforderung" ist bei gleichbleibendem Schlüsselverantwortlichen für ein Nachfolgezertifikat nur dann erforderlich, sofern der Schlüsselverantwortliche noch keine Identifizierung nach den aktuellen Zertifizierungsrichtlinien durchgeführt hat.

3. Wie kann ein falscher TrustCenter-Name bei einer Zertifikatsanfrage mit der Software CoCoNet geändert werden?

Der fehlerhafte Zertifizierungsantrag entsteht aufgrund eines konkurrierenden Zugriffs, wenn innerhalb einer KKS-Sitzung zunächst die öffentlichen Schlüssel abgeholt und im Anschluss daran die Zertifizierungsanfrage gesendet wird. Um dieses Problem zu beheben genügt es, das KKS-Programm zu beenden und erneut zu starten. Anschließend direkt, ohne andere Aufträge zu starten, einen erneuten Zertifizierungsantrag an das TrustCenter senden. In alten Versionen ist der Vorgang des Holens der öffentlichen Schlüssel automatisiert. Hierzu gibt es innerhalb der KKS*.ini (wobei * für AG, LE, KH, etc. steht) einen Eintrag, der entsprechend geändert werden muss. Der Eintrag befindet sich in der Section: [SECURITY]; GetGlobalKeyFileAutomatically=-1
Dieser Eintrag muss wie folgt geändert werden: GetGlobalKeyFileAutomatically=0 (d.h. Semikolon entfernen und den Wert auf Null setzen) Anschließend erneut das KKS starten und unmittelbar die Zertifizierungsanfrage senden.

4. Wann muss das „Formular Zertifikatsanforderung" ausgefüllt werden?

- Bei der ersten Zertifizierung im TrustCenter der DKTIG.
- Bei Wechsel des Schlüsselverantwortlichen.
- Bei Wechsel des Institutionskennzeichens, z. B. durch Trägerwechsel.

5. Wie wird das Schlüsselpaar in der Verschlüsselungssoftware erzeugt?

Da jede Software spezifische Leistungsmerkmale und Menüführungen hat, wenden Sie sich bitte an Ihren Softwareanbieter oder an das Sie betreuende Beratungsunternehmen.

6. Welche Schritte sind für die Erstzertifizierung vorzunehmen?

- Füllen Sie das „Formular Zertifikatsanforderung" aus und übersenden Sie dieses unterschrieben und mit Stempel versehen an:

  DKTIG mbH
  Humboldtstr. 9
  04105 Leipzig

- Mit Ihrer Übermittlungssoftware ist das Schlüsselpaar zu erzeugen.
- Bitte übersenden Sie den öffentlichen Schlüssel mittels Datenfernübertragung (DFÜ) an das TrustCenter der DKTIG (per FTAM: IP: 194.145.83.92; Port: 3280 - per E-Mail: trust@dktig-trust.de).
- Drucken Sie den "Fingerprint" des öffentlichen Schlüssels aus und übersenden Sie ihn unterschrieben im **Original** ebenfalls an die oben angegebene Adresse der DKTIG.
- Sofern bereits ein gültiger Vertrag mit dem DKTIG-TrustCenter geschlossen wurde, erhalten Sie nach Prüfung der Daten und Bereitstellung des Zertifikates per E-Mail die Information, dass der Schlüssel zur Abholung bereitsteht.

7. Wo ist das „Formular Zertifikatsanforderung" zu finden?

Sie können das Formular im Download-Bereich des § 301-TrustCenters herunterladen oder es per E-Mail an trustcenter@dktig.de anfordern.

8. Was ist bei einer Folgezertifizierung zu tun?

Bei einer Folgezertifizierung benötigt die DKTIG, sofern sich bezüglich des Schlüsselverantwortlichen oder der installierten Software keine Änderungen ergeben haben, den neu generierten elektronischen Request (.p10-Datei) und den vom Schlüsselverantwortlichen eigenhändig unterschriebenen originalen Fingerprint

9. Genügt es, die schriftlichen Unterlagen („Formular Zertifikatsanforderung" und Fingerprint) per Fax / E-Mail an die DKTIG zu übermitteln?

Leider nicht. Sie können in dringenden Fällen nach telefonischer Rücksprache unter 0341 308951 0 mit der DKTIG die Unterlagen an das TrustCenter vorab per E-Mail: trustcenter@dktig.de übermitteln. Sofern die Unterlagen nicht im Original nachgereicht werden, kann das neu erteilte Zertifikat von der DKTIG gesperrt werden.

10. Wohin wird der öffentlichen Schlüssel übermittelt?
Die Kommunikationsparameter für Zertifikate an das TrustCenter der DKTIG lauten bei Übermittlung

- per FTAM: IP: 194.145.83.92; Port: 3280
- per E-Mail: trust@dktig-trust.de

11. Welcher Namen wird bei der Schlüsselerzeugung für das TrustCenter eintragen?

Der richtige Name lautet:

DKTIG TrustCenter fuer Krankenhaeuser und Leistungserbringer PKC

12. Wie lange dauert das Zertifizierungsverfahren?

Das Zertifizierungsverfahren erfordert nach positivem Abschluss des Videoldents und bei Vorliegen der vollständigen und korrekten Zertifizierungsunterlagen ca. zwei Arbeitstage.

13. Was muss beim Ausfüllen des „Formulars Zertifikatsanforderung" beachtet werden?

Sie tragen auf der **ersten** Seite folgende Daten ein:

- Name der Einrichtung
- Adresse des Hauses
- Institutionskennzeichen
- Vorname und Nachname des Schlüsselverantwortlichen
- Telefon
- E-Mail
- Abteilung

Auf der **zweiten** Seite sind zwei Unterschriften des Schlüsselverantwortlichen erforderlich.

Für die **dritte** Seite halten Sie bitte folgende Daten bereit:

- Name des Softwareherstellers
- Softwareversion (sofern bekannt)
- Kommunikationskennwort
- Technischer Ansprechpartner – gern mit einer von Seite 1 abweichenden E-Mailadresse
- Ort, Datum und Unterschrift eines Vertretungsberechtigten laut öffentlich einsehbarem Verzeichnis (z.B. Handelsregister) und Stempel der Einrichtung
    - Einrichtungen in öffentlicher Trägerschaft reichen ersatzweise bitte ein gesiegeltes Organigramm ein, woraus die Zeichnungsberechtigung **namentlich** hervorgeht.

Bitte beachten Sie, dass wir das **Originaldokument mit allen erforderlichen Unterschriften und dem Krankenhausstempel** benötigen. Die Unterlagen per Fax oder E-Mail zuzusenden, reicht leider nicht aus.

14. Beim Einspielen der eigenen Schlüsseldatei (p7c-Datei) in die Software CoCoNet bzw. beim Abholen der eigenen Schlüsseldatei (p7c-Datei) über den Menüpunkt "Zertifikat abholen" der Software CoCoNet tritt ein Fehler auf. Die Datei kann infolgedessen nicht verarbeitet werden. Was ist zu tun?

Bitte laden Sie sich Ihre Schlüsseldatei (p7c-Datei) über unsere Homepage unter Online Status Zertifizierung nach Eingabe des Institutionskennzeichens sowie der Vorgangsnummer (laut Bereitstellungsinformation via E-Mail) herunter.

oder

lassen Sie sich die Zertifikatsdatei über unseren E-Mail-Responder zusenden: Hierzu senden Sie bitte eine E-Mail an trust@dktig-trust.de mit folgendem Befehl im Textfeld (nicht in der Betreffzeile!): send 12345678.p7c ("send" + Leerstelle + ersten acht Stellen Ihrer IK-Nr. + ".p7c").
Ergänzen Sie im Dateinamen der Schlüsseldatei (p7c-Datei) bitte die neunte Stelle des Institutionskennzeichens und lesen Sie diese Schlüsseldatei dann in ein Eingangsverzeichnis (jobin-Verzeichnis) Ihrer Software CoCoNet ein.

15. Wann sollte das neue Zertifikat eingelesen werden?

Da Ihr neues Zertifikat und die Schlüssellisten von den Annahmestellen erst am Nachmittag (ca. 15:30 Uhr) aktualisiert werden, lesen Sie Ihr Zertifikat bitte erst einen Tag nach der Bereitstellung in Ihre Verschlüsselungssoftware ein.

Zur Beantwortung weiterer Fragen stehen wir Ihnen gerne zur Verfügung:

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