Zertifikate und Schlüssel Ihrer TK-Gesundheitskarte

Ihre Gesundheitskarte besitzt einen modernen Prozessorchip. Darauf liegen geschützt wichtige Zertifikate und Schlüssel.

Was ist ein digitales Zertifikat?

Ein Zertifikat ist ein Ausweis in der digitalen Welt. Mit ihm können Sie sich **identifizieren** und Gesundheitsdaten individuell **verschlüsseln**. Es garantiert, dass die Informationen richtig und unverändert sind.

Nur eine nach dem Signaturgesetz zugelassene **Zertifizierungsstelle** kann die Zertifikate auf der elektronischen Gesundheitskarte (eGK) herausgeben.

Was steht in einem Zertifikat?

Ein Zertifikat enthält folgende Angaben (mit Beispiel):

- Ausstellende Stelle (Techniker Krankenkasse)
- Zeitraum, in dem das Zertifikat gültig ist (01.01.2018-31.12.2022)
- Vorname und Nachname des Versicherten (Eva Wohlbefinden)
- Versichertennummer (A123456789)
- Kennnummer der Krankenkasse (101575519)
- Herausgeber (Techniker Krankenkasse)
- Ländercode (DE)
- Wert des öffentlichen Schlüssels (Erklärung folgt)
- elektronische Signatur der ausstellenden Zertifizierungsstelle (Atos)

Auf Ihrer eGK sind **mehrere Zertifikate**. Diese haben folgende Funktionen:

Ausweisen und Dokumentieren	**Ver- und Entschlüsseln von Daten**
Je 2 AUT-Zertifikate prüfen die Gültigkeit der TK-Gesundheitskarte.	**Je 2 ENC-Zertifikate** ver- und entschlüsseln persönliche Gesundheitsdaten.
Je 2 AUTN-Zertifikate dokumentieren, wann die TK-Gesundheitskarte eingelesen wurde.	**Je 2 ENCV-Zertifikate** verschlüsseln elektronische Rezepte.
Das CV-Zertifikat erkennt den Heilberufsausweis im 2-Karten-Prinzip.	

Nähere Infos zum CV-Zertifikat:

Zum Lesen und Speichern Ihrer Daten braucht man nicht nur Ihre Karte. Auch die Karte der Person oder der Institution, die die Daten liest oder speichert, ist zwingend notwendig (**2-Karten-Prinzip**). Der **Heilberufsausweis** identifiziert eindeutig eine Person, wie z. B. Ihre Ärztin oder Ihren Arzt.

Was ist ein elektronischer Schlüssel?

Ein elektronischer Schlüssel ist eine Zeichenfolge. Mithilfe dieses **Codes** werden Daten beim Speichern so verändert, dass Dritte sie nicht mehr lesen können.

Wie funktioniert ein Schlüsselpaar?

Zu einem Schlüsselpaar gehören je ein **öffentlicher** und ein **privater** Schlüssel. Der private Schlüssel ist eine nur für diese eGK hergestellte Zahlenfolge. Um den öffentlichen Schlüssel zu erhalten, wird diese Zahlenfolge mit einer weiteren zufällig generierten Zahlenfolge multipliziert.

Das Ergebnis dieser Multiplikation, der öffentliche Schlüssel, wird im Zertifikat auf Ihrer Karte gespeichert. Er wird von einer unabhängigen Stelle für den Besitzer des Zertifikats registriert und beglaubigt. Damit können z. B. Ärztinnen und Ärzte Ihre Gesundheitsdaten **verschlüsseln**.

Die verschlüsselte Information kann nicht mehr entschlüsselt werden. Dafür ist zwingend der private Schlüssel notwendig. Dieser bleibt jedoch **geheim** und ist dazu doppelt geschützt.

Zum einen wird die 2., zum Multiplizieren zufällig gewählte, Zahlenfolge **gelöscht**. Damit kann der private Schlüssel nicht mehr aus dem öffentlichen Schlüssel abgeleitet werden. Darüber hinaus ist der private Schlüssel in einem technisch besonders **gesicherten Bereich** der Karte gespeichert und damit konstruktionsbedingt an die Karte gebunden. Das heißt, er kann nicht von der Karte losgelöst und einzeln verwendet werden. So wird sichergestellt, dass niemand ohne Ihr ausdrückliches Einverständnis Ihre Daten aufrufen und lesen kann.

0007805595 - 35142800000000

Welche Verschlüsselungen werden genutzt?

Aktuell kommen 2 verschiedene Verschlüsselungs-Verfahren zum Einsatz. Sie heißen **RSA-2048** und **ECC 256**. Das Verfahren RSA-2048 verschlüsselt mit einem **2048 Bit-Schlüssel**. Das neuere Verfahren ECC 256 hingegen arbeitet mit einem 256 Bit-Schlüssel auf **elliptischen Kurven** und gilt als noch sicherer.

Wie kommen die Zertifikate und Schlüssel auf die Karte?

Die Zertifikate und Schlüssel werden bereits bei der **Produktion** der Karte auf dem Chip verankert.

Jede Karte erhält bei der Produktion eine individuelle **Seriennummer**, die sie unverwechselbar macht. Der Fachbegriff für diese Nummer lautet "Integrated Circuit Card Serial Number", kurz ICCSN.

Für die jeweilige Kartennummer wird bei uns nach dem Zufallsprinzip ein **Schlüsselpaar** mit privatem und öffentlichem Schlüssel erzeugt und bereitgestellt. Dieser Prozess läuft in besonders gesicherten Modulen ab (den Hardware Security Modules, kurz HSM).

Der öffentliche Schlüssel wird zusammen mit den anderen Informationen, die die Zertifikate der Karte enthalten, sicher an die **Zertifizierungsstelle** übermittelt. Diese stellt die Zertifikate her und authentifiziert sie. Dann werden diese an uns übermittelt.

Die Zertifikate und der private Schlüssel werden danach in der **Produktion** auf die TK-Gesundheitskarte aufgebracht. Während des gesamten Produktionsprozesses ist der private Schlüssel für keinen der Beteiligten einzusehen.

Wie lange sind Zertifikate und Schlüssel gültig?

Die Zertifikate und Schlüssel der TK-Gesundheitskarte sind aktuell nicht länger als **5 Jahre** gültig. Die maximale Gültigkeit wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgegeben. Sie kann an sich ändernde Sicherheitsstandards angepasst werden. Wir schicken Ihnen rechtzeitig vor Ablauf der Gültigkeit eine neue Karte zu.

Was passiert, wenn die Karte verloren geht oder nicht mehr funktioniert?

Sobald Sie uns den **Verlust** Ihrer eGK melden, erhalten Sie eine neue TK-Gesundheitskarte. Die Zertifikate der alten Karte werden gesperrt – so ist die Karte vor Missbrauch geschützt.

Hier erfahren Sie mehr:

Weitere **Informationen** zum Thema Zertifizierung und Zertifikate finden Sie online:

- **gematik.de**
- **bsi.de**

Weitere technische Informationen zur Gesundheitskarte finden Sie in unserem Beratungsblatt **"Datenschutz und Datensicherheit"**.

0007805595 - 35142800000000