

---

## **C\_12445\_Anlage - Krypt: u.a. Import von Root-CA-Zertifikaten über Cross-Zertifikate für FdV**

---

# **Inhaltsverzeichnis**

<b>1 Änderungsbeschreibung.....</b>	<b>2</b>
<b>2 Änderung in gemSpec_Krypt.....</b>	<b>3</b>
2.1 Neu 2.x Import von Root-CA-Schlüsseln über Cross-Zertifikate.....	3
2.2 Änderung in 1.1 Zielsetzung und Einordnung des Dokuments.....	4
2.3 Löschen 1.4 Abgrenzung des Dokuments.....	5
2.4 Umbenennen "2 Einsatzszenarioübergreifende Algorithmen".....	5
2.5 Änderung in 3.4 Masterkey-Verfahren (informativ).....	5
2.6 Änderung in 2.4.3 RSA-Schlüssel in X.509-Zertifikaten.....	5
2.7 Änderung in 3.1 Kryptographische Algorithmen für XML-Dokumente.....	6
2.8 Änderung in 3.2.2 Card-to-Server (C2S) Authentisierung und Trusted Channel G2.....	6
2.9 Änderung in 4.1 XMLDSig und PKCS1-v2.1.....	6
2.10 Änderung in 2.4 Schlüsselerzeugung und Schlüsselbestätigung.....	7
2.11 Änderung in 3.3.2 TLS-Verbindungen.....	7
2.12 Änderung in 3.11.1 Hashfunktionen und OCSP (informativ).....	7
2.13 Änderung in 9 Post-Quantum-Kryptographie (informativ).....	7
2.14 Gelöscht 10 Erläuterungen (informativ).....	7
2.15 Änderung in 11.5 Referenzierte Dokumente.....	7

---

## **1 Änderungsbeschreibung**

---

In Abstimmung mit den FdV-Herstellern wird sich eine Klärung gewünscht, wie in Bezug auf den Import von Root-CA-Zertifikaten über Cross-Zertifikate innerhalb eines E-Rezept-FdV umgegangen werden soll.

Die im Änderungseintrag definierte Vorgehensweise ist allgemeingültig und kann im FdV anwendungsübergreifend angewandt werden.

Aufgrund des Hinweises des BSI ein Copy&Paste-Fehler in "A\_17092 RSA-Schlüssel Zertifikatserstellung, keine kleinen Primteiler und e ist prim" für TSP X.509 nonQES korrigiert.

Die Referenz [BSI-TR-03116-1] wird auf [BSI-TR-02101-1]

Weiterhin werden editorische Aktualisierungen in gemSpec\_Krypt vorgenommen.

---

## **2 Änderung in gemSpec\_Krypt**

---

Es wird ein neuer Abschnitt "Import von Root-CA-Schlüsseln über Cross-Zertifikate" am Ende von Abschnitt 2 wie folgt eingefügt.

### **2.1 Neu 2.x Import von Root-CA-Schlüsseln über Cross-Zertifikate**

Bei verschiedenen Client-Systemen wird initial eine Root-CA-Version in Form eines Root-CA-Zertifikats als Vertrauensanker eingebracht (vgl. A\_24958-\*, A\_26923-\*, A\_24470-\* etc.). Root-CA-Versionen werden regelmäßig (i. d. R. alle 2 Jahre) von der X.509-Root-CA der TI neu erzeugt und diese müssen im Client sicherheitstechnisch geeignet automatisiert importiert werden können. Dafür werden Cross-Zertifikate von der X.509-Root-CA erzeugt und veröffentlicht (vgl. bspw. <https://download.tsl.ti-dienste.de/ECC/ROOT-CA/roots.json>). Aufgrund des Schalenmodells können die Cross-Zertifikate nicht die gleiche Gültigkeitsdauer wie die selbstsignierten Root-Zertifikate besitzen, die die Cross-Zertifikate bestätigen. Dies führt dazu, dass je nachdem mit welcher initiale Root-CA-Version der Client "begonnen" hat, die Root-Schlüssel im Vergleich zu anderen Clients mit unterschiedlichen Gültigkeitsdauern vorliegen. Dies ist eine technische Eigenschaft, die im vorliegenden Szenario eine ungewünschte Komplexitätserhöhung erzeugt, ohne wirklichen fachlichen Gewinn. Aus diesem Grunde wird folgende vereinfachenden Festlegung getroffen.

#### **A\_28419 -FdV: Import von Root-CA-Schlüssel über Cross-Zertifikate**

Ein Client, der Root-CA-Schlüssel über Cross-Zertifikate importiert, MUSS folgendes Vorgehen umsetzen.

Im Client liegt ein Root-CA-Zertifikat als Start eines Import-Vorgangs vor, und der Client erhält ein Cross-Zertifikat für eine neue Root-CA-Version und das dazugehörige selbstsignierte Root-CA-Zertifikat der zu importierenden Root-CA-Version. Das Cross-Zertifikat wird im folgenden als C bezeichnet, das dazugehörige selbstsignierte Root-CA-Zertifikat als S.

Der Client hat das Ziel S als weiteren Vertrauensanker bei sich lokal hinzuzufügen. Dafür MUSS er

1. prüfen, ob die Signatur von C per Signaturprüfung valide rückführbar ist auf ein schon im System als ein Vertrauensanker vorhandenes Root-CA-Zertifikat.
2. prüfen, ob C zum Prüfzeitpunkt/Import-Zeitpunkt zeitlich noch gültig ist.
3. prüfen, ob der SubjectCommonName der im Cross-Zertifikat bestätigten Identität dem Namensschema "GEM.RCA<natürliche Zahl>" entspricht.
4. prüfen, ob der SubjectKeyIdentifier in C gleich dem in S ist.
5. prüfen, ob der SubjectCommonName in C und in S gleich ist.
6. prüfen, ob bestätigte öffentliche Schlüssel in C gleich dem in S ist.
7. prüfen, ob die Signatur von S valide per Signaturprüfung mit dem öffentlichen Schlüssel aus C prüfbar ist.

Ergibt eine der o. g. Prüfungen kein positives Prüfergebnis MÜSSEN C und S verworfen werden (der Import kann also nicht erfolgen).  
Anderenfalls MUSS vom Client S als weiterer Vertrauensanker im Client hinzugefügt werden.

[<=,eRp\_FdV,Sich.techn. Eignung: Produktgutachten]

## **2.2 Änderung in 1.1 Zielsetzung und Einordnung des Dokuments**

Für die TI ist die Technische Richtlinie 03116 Teil 1 [BSI-TR-03116-1] normativ, d. h. nur dort aufgeführte kryptographische Verfahren dürfen von Produkten in der TI verwendet werden. Wenn mehrere unterschiedliche Produkttypen der TI zusammenarbeiten ist es bez. der Interoperabilität nicht sinnvoll wenn jeder beteiligte Produkttyp alle dort aufgeführten Verfahren umsetzen muss, da er vermuten muss, die Gegenstelle beherrscht nur eine Teilmenge der dort aufgeführten Verfahren. Um einen gemeinsamen Nenner zu definieren, legt dieses Dokument für bestimmte Einsatzzwecke ein Mindestmaß an verpflichtend zu implementierenden Verfahren aus [BSI-TR-03116-1] fest, oftmals mit spezifischen Parametern. Ein Produkttyp ist frei, weitere Verfahren aus der [BSI-TR-03116-1] optional zu implementieren, kann sich jedoch nicht ohne Weiteres darauf verlassen, dass sein potentieller Kommunikationspartner diese auch beherrscht.

Nur die in [gemSpec\_Krypt] aufgeführten kryptographischen Verfahren dürfen in den Produkten in der TI verwendet werden. Die Vorgaben im Dokument werden in Zusammenarbeit mit dem BSI festgelegt. Neben den eigentlichen kryptographischen Verfahren werden ebenfalls erlaubte Domainparameter (Schlüssellänge, ECC-Kurvenparameter etc.) und Vorgaben zu sicherheitstechnisch geeigneten Verwendung der kryptographischen Verfahren in [gemSpec\_Krypt] festgelegt.

In Bezug auf die Formulierung der Ende-Daten der Zulässigkeit eines kryptographischen Verfahrens wird die Konvention aus der TR-02102-Familie und der TR-03116-Familie verwendet, d. h., eine Aussage „Algorithmus X ist geeignet bis Ende 2029+“ bedeutet generell nicht, dass Algorithmus X nach Ende 2029 nicht mehr geeignet ist, sondern lediglich, dass über die Eignung nach Ende 2029 keine explizite Aussage gemacht wird und dass aus heutiger Sicht die weitere Eignung nicht ausgeschlossen ist. Aussagen über den Betrachtungszeitraum hinaus sind mit einem höheren Maß an Spekulation verbunden. Sollte bei den Angaben zum Ende der zeitlichen Zulässigkeit kein "+" aufgeführt sein (bspw. "Ende 2025") , so bedeutet dies, dass eine Verlängerung der Zulässigkeit über den aufgeführten Zeitpunkt hinaus nicht geplant ist.

Bei neuen Erkenntnissen über die verwendeten kryptographischen Algorithmen, die zu einer Änderung der TR-03116-1 führen, wird eine Anpassung dieses Dokumentes erfolgen. Für Verwendungszwecke, bei denen bereits eine Migration zu stärkeren Algorithmen in Planung ist oder die Verwendung von Algorithmen unterschiedlicher Stärke zulässig ist, wird ein Ausblick gegeben, bis wann welche Algorithmen ausgetauscht sein müssen. Bei den Migrationsstrategien für kryptographische Algorithmen ist darauf zu achten, dass hinterlegte Objekte umzuschlüsseln sind bzw. die älteren Algorithmen (unter der Bedingung, dass sie sicherheitstechnisch noch geeignet sind) für eine gewisse Übergangsphase weiter unterstützt werden müssen und danach zuverlässig in den Komponenten deaktiviert werden müssen.

## **2.3 Löschen 1.4 Abgrenzung des Dokuments**

Der Abschnitt "1.4 Abgrenzung des Dokuments" wird gelöscht.

## **2.4 Umbenennen "2 Einsatzszenarioübergreifende Algorithmen"**

Der Abschnitt wird umbenannt zu "2 Kryptographische Verfahren und deren Schlüssel"

## **2.5 Änderung in 3.4 Masterkey-Verfahren (informativ)**

Der Abschnitt 3.4 wird nach Abschnitt 2 verschoben.

## **2.6 Änderung in 2.4.3 RSA-Schlüssel in X.509-Zertifikaten**

Ein Copy&Paste-Fehler in A\_17092 wird wie folgt korrigiert:

alt:

### **A\_17092 -RSA-Schlüssel Zertifikatserstellung, keine kleinen Primteiler und e ist prim**

Ein TSP KANN im Rahmen der Zertifikatsbeantragung, bei denen öffentliche RSA-Schlüssel bestätigt werden, folgende Tests auf die RSA-Schlüssel anwenden. Wenn ein u. g. Test das Ergebnis FAIL als Ergebnis liefert, so ist der Schlüssel fehlerhaft und der TSP muss die Zertifikatserstellung für diesen Schlüssel ablehnen.

1. Ist der öffentliche Exponent e (des untersuchten RSA-Schlüssels) prim und gilt  $2^{16} < e < 2^{256}$  (vgl. [BSI-TR-03116-1#3.2 RSA])?  
Falls nein, ist das Ergebnis FAIL.
2. Ist der Modulus des untersuchten RSA-Schlüssels kleiner als  $2^{2048}$ ?  
Falls nein, ist das Ergebnis FAIL.
3. Ist der Modulus des untersuchten RSA-Schlüssels relativ prim zu allen Primzahlen kleiner als 100?  
Falls nein, ist das Ergebnis FAIL.

**[<=,TSP X.509 nonQES - HBA, TSP X.509 nonQES - eGK, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC,funkt. Eignung: Herstellererklärung]**

neu:

### **A\_17092-01 -RSA-Schlüssel Zertifikatserstellung, keine kleinen Primteiler und e ist prim**

Ein TSP KANN im Rahmen der Zertifikatsbeantragung, bei denen öffentliche RSA-Schlüssel bestätigt werden, folgende Tests auf die RSA-Schlüssel anwenden. Wenn ein u.

g. Test das Ergebnis FAIL als Ergebnis liefert, so ist der Schlüssel fehlerhaft und der TSP muss die Zertifikatserstellung für diesen Schlüssel ablehnen.

1. Ist der öffentliche Exponent  $e$  (des untersuchten RSA-Schlüssels) prim und gilt  $2^{16} < e < 2^{256}$  (vgl. [BSI-TR-02102-1#2.3.2 RSA-Verschlüsselung])?  
Falls nein, ist das Ergebnis FAIL.
2. Ist der Modulus des untersuchten RSA-Schlüssels kleiner als  $2^{2048}$ ?  
Falls ja, ist das Ergebnis FAIL.
3. Ist der Modulus des untersuchten RSA-Schlüssels relativ prim zu allen Primzahlen kleiner als 100?  
Falls nein, ist das Ergebnis FAIL.

[<=, TSP X.509 nonQES - HBA, TSP X.509 nonQES - eGK, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC, funkt. Eignung: Herstellererklärung]

## **2.7 Änderung in 3.1 Kryptographische Algorithmen für XML-Dokumente**

In Abschnitt "3.1 Kryptographische Algorithmen für XML-Dokumente" wird der (größtenteils) obsoletere informative Text beginnend mit "Zur vollständigen Spezifikation" bis inkl. der informative Tabelle Tab\_KYPT\_008 gelöscht.

## **2.8 Änderung in 3.2.2 Card-to-Server (C2S) Authentisierung und Trusted Channel G2**

In Abschnitt 3.2.2 wird der informative Satz "Der Algorithmus AES ist nach [BSI-TR-03116-1] in der TI bis Ende 2029+ (meint bis Ende des Betrachtungsraums der TR) zulässig." gelöscht.

## **2.9 Änderung in 4.1 XMLDSig und PKCS1-v2.1**

Die Anforderung GS-A\_5091 und der darunter stehende informative Begleittext wird nach Abschnitt "3.1 Kryptographische Algorithmen für XML-Dokumente" verschoben.

Der nach Verschiebung von GS-A\_5091 nun ausschließlich informative Text von Abschnitt 4 wird gelöscht, damit wird der Abschnitt "Migration 120-Bit-Sicherheitsniveau" zum neuen Abschnitt 4.

## **2.10 Änderung in 2.4 Schlüsselerzeugung und Schlüsselbestätigung**

Im Abschnitt "2.4" wird die Referenz auf BSI-TR-03116-1 auf BSI-TR-02101-1 geändert.

## **2.11 Änderung in 3.3.2 TLS-Verbindungen**

Im Abschnitt "3.3.2" wird die Referenz auf BSI-TR-03116-1 auf BSI-TR-02101-1 geändert.

## **2.12 Änderung in 3.11.1 Hashfunktionen und OCSP (informativ)**

Im informativen Abschnitt "3.11.1" wird die Referenz auf BSI-TR-03116-1 auf BSI-TR-02101-1 geändert.

## **2.13 Änderung in 9 Post-Quantum-Kryptographie (informativ)**

Der Abschnitt "9 Post-Quanten-Kryptographie (informativ)" wird etwas nach vorne verschoben zu neuen Abschnitt "5 Post-Quanten-Kryptographie (informativ)".

Änderung:

Dies bedeutet, dass insbesondere Authentisierungsvorgänge, die im "Jetzt" mit klassischen asymmetrischen kryptographischen Verfahren mit ausreichend großen Schlüssellängen durchgeführt werden (vgl. [SOG-IS] und ~~[BSI-TR-03116-1]~~ **[BSI-TR-02102-1]**), nicht in Frage stehen.

## **2.14 Gelöscht 10 Erläuterungen (informativ)**

Der informative Abschnitt "10 Erläuterungen (informativ)" wird gelöscht.

## **2.15 Änderung in 11.5 Referenzierte Dokumente**

Im Literaturverzeichnis werden bei [BSI-TR-02101-1] bis -3 die Referenzen von 2024-01 auf 2025-01 aktualisiert. Es entstehen dadurch keine fachlichen Änderungen an den Produkten, aber es erleichtert Gutachtern die Arbeit wenn die aktuellen Versionen referenziert werden.