Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

1 Farbliche Markierung von Änderungen

Dieses Kapitel erläutert den Farbcode der farblichen Hinterlegung von Änderungen beim Vergleich von [gemSpec_COS] in der Version 3.12.0 vom 15.05.2019 gegenüber der aktuellen Version.

1) **blaue Hinterlegung:** Editorielle Änderungen, die sich weder auf Implementierungen durch Hersteller, noch auf Testimplementierungen auswirken.
2) **gelbe Hinterlegung:** Änderungen, die sich nicht auf die Implementierung durch Hersteller, wohl aber auf gematik Artefakte (Spezifikationen, Testimplementierung, …) auswirken.
3) **orange Hinterlegung:** Änderungen, die sich auf die Implementierung durch Hersteller und / oder die gematik Artefakte auswirken.

Es ergibt sich eine Kritikalität von niedrig=ohne über blau, gelb nach orange. Im Zweifelsfall wird eine höhere Kritikalität, also eine stärkere Warnfarbe gewählt.

2 Technischer Hintergrund zum Anlass der Änderung

Bis zur Version 3.19 von [TR–03116-1:2015] wurde dort bezüglich der RSA Schlüsselgenerierung auf Anforderungen an das Verhältnis der beiden Primzahlen p und q auf [BKryA] verwiesen, wo folgende Bedingungen formuliert wurden: $\varepsilon_1 < |\log_2(p) - \log_2(q)| < \varepsilon_2$, mit $\varepsilon_1 \approx 0{,}1$ und $\varepsilon_2 \approx 30$.

In der Version 3.20 von [TR-03116-1:2018] wird stattdessen gefordert: $|p-q| \geq 2^{n/2-100}$. Zudem gibt es den Hinweis, dass p und q "nicht zu weit voneinander entfernt sein sollen.

Die alte Fassung von (N002.400) enthält für das COS die Erlaubnis, auch solche RSA Schlüssel verarbeiten zu dürfen, welche die Anforderungen aus [TR–03116-1:2015] nicht erfüllen.

Die neue Fassung von (N002.400) enthält nun einen Wertebereich für die Primzahlen p und q, der zwingend zu unterstützen ist. Dieser Bereich orientiert sich an [TR–03116-1:2015] und wurde so mit allen relevanten COS-Herstellern zwecks Testkartenpersonalisierung abgesprochen.

Falls diese Änderung nicht durchgeführt wird, dann ist es denkbar, dass in Zukunft für die Personalisierung von Echt- oder Testkarten RSA Schlüssel nach herstellerspezifischen Vorgaben zu erzeugen sind.

3 Änderung

Statt RSA Schlüssel mit beliebigem Wert für ε zuzulassen wird nun vorgeschrieben, dass das COS RSA Schlüssel mit einem ε aus einem bestimmten Bereich unterstützen muss. Als Seiteneffekt wird in der Liste der referenzierten Dokumente [BKryA] entfernt.

(N002.400) COS

~~Private RSA-Schlüssel, welche die in [BKryA#3.1] empfohlenen Schranken ε 1 und ε 2 verletzen, für die mithin NICHT gilt 0,1 < |log 2 (p) – log 2 (q)| < 30,~~

~~a. KÖNNEN vom COS akzeptiert werden.~~

~~b. KÖNNEN vom COS abgelehnt werden.~~

Das COS MUSS für die beiden Primfaktoren p und q des Modulus Intervalle unterstützen, die für die Zahl $epsilon = log_2(q) - log_2(p)$ mindestens Werte aus dem Intervall [1/10, 1/2] umfassen.

Hinweis CosH_e24: Gemäß (N002.400) sind andere, beliebige Verhältnisse von p und q funktional zulässig. Insbesondere auch solche, die zu $p > q$ gehören. Zudem handelt es sich mitnichten um eine funktionale Vorgabe für p und q im Rahmen der Onboard-Schlüsselgenerierung. Die Anfordreung (N002.400) hat lediglich die Aufgabe herstellerübergreifend einen Bereich für p und q festzulegen, der im Rahmen einer externen Schlüsselgenerierung mit dem COS interoperabel ist (etwa für Testlaborkartenspezifikation, Personalisierung und ähnliches.

~~[BKryA]~~	~~Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, veröffentlicht am 18. Januar 2012 im Bundesanzeiger, Nr. 10, S. 243 (auch online verfügbar: http://www.bundesnetzagentur.de)~~

4 Literaturstellen

[BKryA]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, veröffentlicht am 15. Dezember 2014 im Bundesanzeiger
[TR–03116-1:2015]	Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Version: 3.19, Datum: 3.12.2015
[TR-03116-1:2018]	Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur Version: 3.20, Datum: 21.09.2018
[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS), Elektrische Schnittstelle