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 für eine höhere Kritikalität, also eine stärkere Warnfarbe gewählt.

2 Technischer Hintergrund zum Anlass der Änderung

Die Prüfung auf den unendlich fernen Punkt wurde in der [TR–03111] beim Übergang von der Version 1.11 zur Version 2.0 hinzugefügt. Zudem fordert [PP-COS] im Punkt FCS_COP.1/COS.ECDSA.V bezüglich der Signaturprüfung ebenfalls Konformität zu [TR–03111] Version 2.0. Deshalb wird diese Prüfung nun auch hier aufgenommen.

3 Änderung

Schritt 4 wird um eine Prüfung auf "unendlich fernen Punkt" ergänzt.

(N003.800)e K_COS

Schritt 4: $Q = [u_1]\,G + [u_2]\,P_a$ mit $Q = (x_Q, y_Q)$.

Wenn Q gleich dem unendlich fernen Punkt O entspricht,

dann gibt die Funktion *out* = *False* zurück und bricht diesen Algorithmus ab.

4 Literaturstellen

[PP-COS]	Common Criteria Protection Profile Card Operating System Generation 2, BSI-CC-PP-0082, Version 2.0, 19th June 2018
[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS), Elektrische Schnittstelle
[TR–03111]	Technical Guideline TR-03111, Elliptic Curve Cryptography Version 1.11 – 2009-04-17 Version 2.0 – 2012-06-28 Version 2.10 – 2018-06-01