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 Änderungen

1) Ort Kapitel 18.5.3
   a) Die Definitionen vor und in (N109.200) bis (N109.400) werden verschoben und geändert, der nachfolgende Text wird an diese Änderungen angepasst.

Es gelten folgende Definitionen:
(N109.200) Diese Anforderung ist absichtlich leer. Ihr Inhalt wurde nach (N109.450)c verschoben.
(N109.300) Diese Anforderung ist absichtlich leer. Ihr Inhalt wurde nach (N109.450)d verschoben.
(N109.400) Diese Anforderung ist absichtlich leer. Ihr Inhalt wurde nach (N109.450)e verschoben.

(N109.450) K_Performanztest
Der Performanztest MUSS bei der Berechnung der Punktzahl P folgende Formeln verwenden: <=

$$X = \frac{1}{n}\sum_{i=1}^{n} x_i \quad = \text{Mittelwert (Erwartungswert) aller Einzelmessungen im } n\text{-Tupel } \underline{t} \quad \text{(a)}$$

$$\sigma = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(t_i - X)^2} \quad = \text{Standardabweichung aller Einzelmessungen im } n\text{-Tupel } \underline{t} \quad \text{(b)}$$

$$f_1 = e^{-\frac{\sigma}{X}} \quad \text{(c)}$$

$$f_2 = 1 - \left(\frac{X}{2 f_1 T_R}\right)^2 \quad \text{(d)}$$

$$P = f_2 \cdot T_R \quad \text{(e)}$$

Die Funktion P besteht aus dem Faktor ~~f_1 und~~ f_2 und wird durch T_R gewichtet. Im Faktor f_2 wirkt eine größere Standardabweichung über den Faktor f_1 wie eine verkleinerte Referenzzeit T_R.

Wenn die Standardabweichung null ist, dann ist der Faktor f_1 exakt eins. Größere Standardabweichungen führen zu kleineren Faktoren und damit zu geringeren Punktzahlen P.

Der Faktor f_2 setzt den Mittelwert X in Relation zur Referenzzeit T_R. Deshalb wird f_2 als Funktion von X aufgefasst, die durch T_R parametrisiert wird. Trivialerweise ist es wünschenswert, dass ein kleinerer Wert von X zu einem größeren Wert von f_2 führt. Daraus folgt, dass f_2 streng monoton fallend ist, mithin also die Ableitung von f_2 nach X kleiner null ist. Zudem ist es ratsam, auch die zweite Ableitung von f_2 nach X kleiner gleich null zu wählen, weil es dann eher lohnt, schlechte Mittelwerte zu verbessern, als gute Mittelwerte weiter zu optimieren.

Wenn der Mittelwert X der Messergebnisse gleich dem Referenzwert T_R ist, dann ist der Faktor f_2 gleich 0,75, falls die Standardabweichung vernachlässigbar klein ist.

~~Das Produkt aus f_1 und~~Der Faktor f_2 wird zur Ermittlung des Wertes P mit der Referenzzeit T_R gewichtet. Durch diese Gewichtung korreliert das Gewicht eines Prüfpunktes mit dem Beitrag des Prüfpunkt im Rahmen zusammengesetzter Kommandosequenzen.

   b) Begründung:

i) Für Mittelwert und Standardabweichung wird eine präzise Definition angegeben.
ii) Die Definition des Faktors f2 wird korrigiert. Der Faktor f2 kann auch negativ werden. In der alten Definition wurde dann eine große Standardabweichung belohnt, statt bestraft. Die neue Definition vermeidet diesen Fehler.
iii) Da f1 nun schon im Faktor f2 enthalten ist, wurde f1 in der Formel für P entfernt.

2) Ort CosT_1b9 = Tabelle 274 Gesamtbewertung für das Basisbetriebssystem.
   a) Folgende Änderungen:
      i) Die Tabelle wird in eine neue Afo (N109.460) integriert

(N109.460) K_Performanztest

Der Performanztest MUSS bei der Bewertung der einzelnen Prüfpunkte für das Basisbetriebssytem die in CosT_1b9 dargestellten Werte für die Referenzzeit T_{Ri} und die Gewichte g_i zugrundelegen.

Tabelle 348, CosT_1b9: Gesamtbewertung für das Basisbetriebssystem

Prüfpunkt	Use Case	Kapitel	Bezeichnung	T_{Ri} / [ms]	g_i	$g_i\ T_{Ri}$ / [ms]
Kanallaufzeit	(N024.100)	CosK.232	Bus	17	50.000	850.000

      ii) Sämtliche Gewichte g_i und damit das Produkt $g_i\ T_{Ri}$ werden geändert.
      iii) Die Referenzzeit von Karte starten wird auf 50 ms geändert.
      iv) Die Referenzzeit von LOAD APPLICATION wird auf 1000 ms geändert.
      v) Darüber hinaus werden folgende Referenzzeiten geändert (gelb hinterlegt):

READ BINARY *b*	(N051.100)	18.8.7	$P_{ReadBinary,b}$	11
READ BINARY *m*			$P_{ReadBinary,m}$	5
UPDATE BINARY *b*	(N053.200)	18.8.6	$P_{UpdateBin,b}$	60
UPDATE BINARY *m*			$P_{UpdateBin,m}$	60
WRITE BINARY *b*	(N055.205)	18.8.5	$P_{write,b}$	60
WRITE BINARY *m*			$P_{write,m}$	60
ACTIVATE RECORD	(N055.500)		$P_{ActivateRec}$	30
APPEND RECORD *b*	(N058.400)		$P_{AppendRecord,b}$	60
APPEND RECORD *m*			$P_{AppendRecord,m}$	40
DEACTIVATE RECORD	(N060.700)		$P_{DeactivateRec}$	30
DELETE RECORD	(N063.422)	18.8.8	$P_{DeleteRec}$	50
ERASE RECORD wipe *b*	(N063.600)		$P_{WipeRecord,b}$	30
ERASE RECORD wipe *m*			$P_{WipeRecord,m}$	30
READ RECORD *b*	(N065.700)		$P_{ReadRecord,b}$	8
READ RECORD *m*			$P_{ReadRecord,m}$	4
SEARCH RECORD	(N067.900)	18.8.9	$P_{SearchRec}$	120
UPDATE RECORD *b*	(N070.300)	18.8.8	$P_{UpdateRecord,b}$	30
UPDATE RECORD *m*			$P_{UpdateRecord,m}$	40
CHANGE REFERENCE DATA change	(N073.300)		$P_{ChRefData}$	90
CHANGE REFERENCE DATA set	(N073.700)		P_{SetPIN}	50
DISABLE VERIFICATION REQUIREMENT	(N075.386)		$P_{DisablePIN}$	50
ENABLE VERIFICATION REQUIREMENT	(N078.586)	18.8.1	$P_{EnablePIN}$	50
GET PIN STATUS	(N077.900)		$P_{GetPinStatus}$	10
RESET RETRY COUNTER	(N079.300)		$P_{ResetRC}$	70
VERIFY	(N082.200)		P_{VERIFY}	60

vi) Darüber hinaus werden folgende Referenzzeiten geändert und die Performanz Anforderungen für das Kommando GET RANDOM werden in diese Tabelle verschoben:

PSO Compute Digital Signature	(N085.500)	18.8.13	$P_{signPSS,2048}$	200	1.000	200.000
			$P_{signPSS,3072}$	750	10	7.500
		18.8.14	$P_{signECDSA,256}$	100	2.000	200.000
			$P_{signECDSA,384}$	150	600	90.000
			$P_{signECDSA,512}$	250	100	25.000
PSO Decipher	(N089.200)	18.8.15	$P_{dec,2048}$	200	2.000	400.000
			$P_{dec,3072}$	900	100	90.000
	(N089.800)	18.8.16	$P_{dec,256}$	150	2.000	300.000
			$P_{dec,384}$	180	600	108.000
			$P_{dec,512}$	270	100	27.000
PSO Encipher	(N090.790)	18.8.15	$P_{enc,2048}$	40	200	8.000
	(N091.400)	18.8.16	$P_{enc,256}$	200	1.000	200.000
			$P_{enc,384}$	300	500	150.000
			$P_{enc,512}$	500	100	50.000
PSO Verify Certificate	(N095.410)	18.8.11.1	$P_{Import,ELC256}$	300	500	150.000
		18.8.11.2	$P_{Import,ELC384}$	630	100	63.000
		18.8.11.3	$P_{Import,ELC512}$	900	20	18.000
PSO Verify Digital Signature	(N096.388)	18.8.14	$P_{verifyECDSA,256}$	80	12	960
			$P_{verifyECDSA,384}$	140	6	840
			$P_{verifyECDSA,512}$	220	1	220
FINGERPRINT	(N096.454)	18.8.3	$P_{fingerprint}$	8.000	1	8.000
GENERATE ASYMMETRIC KEY PAIR	(N097.266)	18.8.16	$P_{GAKP,256}$	140	500	70.000
			$P_{GAKP,384}$	200	100	20.000
			$P_{GAKP,512}$	280	30	8.400
GET CHALLENGE	(N098.625)	18.8.17	$P_{challenge}$	10	1.000	10.000
MANAGE CHANNEL reset Channel	(N099.524)		P_{reset_Ch}	5	500	2.500
MANAGE SECURITY ENVIRONMENT Restore	(N099.900)	18.8.18	$P_{MSE\_Restore}$	5	500	2.500
MANAGE SECURITY ENVIRONMENT Set	14.9.9		P_{MSE_Set}	10	10.000	100.000
GET RANDOM	(N099.322	18.8.22	$P_{Random,b}$	4	18	72
			$P_{Random,m}$	40	2	80
Spaltensummen				23.589	1.000.000	12.687.572

b) Begründung:
   i) Anpassung der Referenzzeiten und Gewichte an den Stand der Technik.
   ii) Fehlerkorrekturen für LOAD APPLICATION und VERIFY Kommando.
   iii) Verschieben des Kommandos GET RANDOM in den Basisteil des COS.

3) Ort CosT_930 = Tabelle 275 Gesamtbewertung Option_kontaktlose_Schnittstelle
   a) Die Tabelle wird in eine neue Afo (N109.465) integriert und sämtliche Gewichte g_i und damit das Produkt g_i T_{Ri} werden geändert:

(N109.465) K_Performanztest

Der Performanztest MUSS bei der Bewertung der einzelnen Prüfpunkte für die Option_kontaktlose_Schnittstelle die in CosT_930 dargestellten Werte für die Referenzzeit T_{Ri} und die Gewichte g_i zugrundelegen.

Tabelle 349, CosT_930: Gesamtbewertung für Option_kontaktlose_Schnittstelle

Prüfpunkt	Use Case	Kapitel	Bezeichnung	T_{Ri} / [ms]	g_i	g_i T_{Ri} / [ms]
GENERAL AUTHENTICATE	CosK_e2b	CosK_eb3	P_{PACE}	750	500	375.000
Spaltensummen				750	500	375.000

   b) Begründung: Anpassung der Referenzzeiten und Gewichte an den Stand der Technik.

4) Ort CosT_005 = Tabelle 276 Gesamtbewertung Option_Kryptobox
   a) Die Tabelle wird in eine neue Afo (N109.470) integriert und sämtliche Gewichte g_i und damit das Produkt g_i T_{Ri} werden geändert:

Tabelle 351: CosT_005: Gesamtbewertung für Option_Kryptobox

Prüfpunkt	Use Case	Kapitel	Bezeichnung	T_{Ri} / [ms]	g_i	g_i T_{Ri} / [ms]
Sessionkeyaushandlung für Trusted Channel (Blattanforderung: ML-92294)	15.4.1	18.8.20	$P_{SK4TC,AES128}$	70	1.400	98.000
			$P_{SK4TC,AES192}$	90	500	450.000
			$P_{SK4TC,AES256}$	100	100	10.000
PSO Compute Cryptographic Checksum	(N087.228)	18.8.21	$P_{compute128,b}$	10	10.000	100.000
			$P_{compute128,m}$	5	22.000	110.000
			$P_{compute192,b}$	10	6.000	60.000
			$P_{compute192,m}$	6	10.000	60.000
			$P_{compute256,b}$	10	500	5.000
			$P_{compute256,m}$	7	1.000	7.000
PSO Decipher	(N089.845)		$P_{dec128,b}$	10	10.000	100.000
			$P_{dec128,m}$	10	22.000	220.000
			$P_{dec192,b}$	10	6.000	60.000
			$P_{dec192,m}$	12	10.000	120.000
			$P_{dec256,b}$	10	500	5.000
			$P_{dec256,m}$	14	1.000	14.000
PSO Encipher	(N091.446)		$P_{enc128,b}$	10	10.000	100.000
			$P_{enc128,m}$	10	22.000	220.000
			$P_{enc192,b}$	10	6.000	60.000
			$P_{enc192,m}$	12	10.000	120.000
			$P_{enc256,b}$	10	500	5.000
			$P_{enc256,m}$	14	1.000	14.000
PSO Verify Cryptographic Checksum	(N096.346)		$P_{verify128,b}$	10	10.000	100.000
			$P_{verify128,m}$	5	22.000	110.000
			$P_{verify192,b}$	10	6.000	60.000
			$P_{verify192,m}$	6	10.000	60.000
			$P_{verify256,b}$	10	500	5.000
			$P_{verify256,m}$	7	1.000	7.000
Spaltensummen				488	200.000	1.875.000

   b) Begründung: Anpassung der Referenzzeiten und Gewichte an den Stand der Technik.

5) Ort CosT_51e = Tabelle 277 Gesamtbewertung Option_logische_Kanäle
   a) Die Tabelle wird in eine neue Afo (N109.475) integriert und sämtliche Gewichte g_i und damit das Produkt g_i T_{Ri} werden geändert, GET RANDOM wurde entfernt, siehe Punkt 2)b)iii):

(N109.475) K_Performanztest

Der Performanztest MUSS bei der Bewertung der einzelnen Prüfpunkte für die Option_logische_Kanäle die in CosT_51e dargestellten Werte für die Referenzzeit T_{Ri} und die Gewichte g_i zugrundelegen.

Tabelle 352: CosT_51e: Gesamtbewertung für Option_logische_Kanäle

Prüfpunkt	Use Case	Kapitel	Bezeichnung	T_{Ri} / [ms]	g_i	g_i T_{Ri} / [ms]
~~GET RANDOM~~	~~(N099.322)~~	~~18.8.22~~	~~$P_{Random,s}$~~	4	~~1.800~~	~~7.200~~
			~~$P_{Random,m}$~~	~~40~~	~~200~~	~~8.000~~
MANAGE CHANNEL open	(N099.508)	18.8.23	P_{Open}	5	50.000	250.000
MANAGE CHANNEL close	(N099.514)		P_{Close}	3	40.000	120.000
MANAGE CHANNEL reset ICC	(N099.532)		P_{RST}	3	10.000	30.000
Spaltensummen				11	100.000	400.000

   b) Begründung: Anpassung der Referenzzeiten und Gewichte an den Stand der Technik.

6) Ort CosT_439 = Tabelle 278 Gesamtbewertung je nach Kombination der Optionen
   a) Die Tabelle wird in eine neue Afo (N109.480) integriert und gemäß den vorstehenden Änderungen aktualisiert:

(N109.480) K_Performanztest

Der Performanztest MUSS bei der Bewertung eines Prüflings die in CosT_439 dargestellten Werte für die Zulasungsgrenze zugrundelegen.

Tabelle 352, CosT_439: Gesamtbewertung je nach Kombination der Optionen

Basis / [ms]	Dual / [ms]	Krypto / [ms]	Kanal / [ms]	Summe / [s]	Zulassungsgrenze / [s]
12.687.572	375.000	1.875.000	400.000	15.337,572	6.710
12.687.572	375.000	1.875.000	0	14.937,572	6.535
12.687.572	375.000	0	400.000	13.462,672	5.890
12.687.572	375.000	0	0	13.062,572	5.715
12.687.572	0	1.875.000	400.000	14.962,572	6.546
12.687.572	0	1.875.000	0	14.562,572	6.371
12.687.572	0	0	400.000	13.087.672	5.726
12.687.572	0	0	0	12.687,572	5.551

   b) Begründung: Konsistenz zu den übrigen Tabellen mit Performanzvorgaben.

7) Ort (N109.500) und nachfolgender Text
   a) Die Formel und konkrete Werte werden aktualisiert:

(N109.500) K_Performanztest

Der Performanztest MUSS für die Gesamtbewertung folgende Formel verwenden, wobei nur die Prüfpunkte zu berücksichtigen sind, die gemäß der vom COS unterstützten Optionen vorhanden sind.

$$P_{gesamt} = \sum_i g_i \cdot P_i = \sum_i g_i \cdot f_{2i} \cdot T_{Ri}$$ <=

Unter den vereinfachenden Annahmen, dass die Messwerte innerhalb einer Reihe identisch sind (Standardabweichung ist null) und das Verhältnis X_i / T_{Ri} in allen Messreihen konstant ist, folgt dann für das Basisbetriebssystem, mit f_2 als Funktion von X_i / T_{Ri}.

$$P_{gesamtEinfach} = f_2 \sum_i g_i \cdot T_{Ri} = 12687,572 \cdot f_2$$

CosA_3de zeigt diesen Zusammenhang graphisch mit dem Verhältnis X_i / T_{Ri} als Abszisse und $P_{gesamtEinfach}$ als Ordinate. Demnach erreicht ein unendlich schnelles Basisbetriebssystem 12.687,572s Punkte. Eine Karte, die in allen Prüfpunkten die Referenzzeit benötigt, erreicht 9515,679s Punkte. Eine Karte, die überall die doppelte Referenzzeit benötigt, null Punkte.

   b) Begründung: Formel wegen Punkt 1)b)ii), konkrete Werte wegen Punkt 6)

8) Ort 18.7 Startsequenz
   a) Die Testvorbereitung wird geändert:

Testvorbereitung:

(N200.190) K_Performanztest
Schritt 1: Der Prüfling MUSS gemäß 18.5.2.1 aktiviert werden.

(N200.195) K_Performanztest
Schritt 2: Der Prüfling MUSS gemäß (N023.920)f deaktiviert werden.

~~Keine.~~

   b) Begründung: Die Messprotokolle zeigen, dass die erste Startsequenz erheblich länger dauert, als alle übrigen Startsequenzen. Vermutlich führt der Prüfling hier Restarbeiten aus einer vorherigen Kartensession aus, was das Messergebnis verfälscht.

9) Ort (N205.240)
   a) Die Afo wird geändert:

(N205.240) K_Performanztest
Schritt 4: Das Attribute EF.transparent *positionLogicalEndOfFile* wird mittels Use Case aus (N052.932) auf den Wert null gesetzt. Die Laufzeit dieses Kommandos ist für diesen Prüfpunkt irrelevant. ~~Die Laufzeit t_{Set} dieses Kommandos MUSS gemäß CosK_056 gemessen und der Menge M_{SetEOF} hinzugefügt werden.~~ <=

   b) Begründung: In Schritt 4 ist die Datei EF.transparent nur teilweise gefüllt, weshalb das letzte SET LOGICAL EOF Kommando im Allgemeinen eine deutlich andere Laufzeit aufweist, was sich negativ auf die Standardabweichung auswirkt und damit zu einem ungewollten Punktabzug führte.

10) Ort (N206.240)
   a) Die Afo wird geändert:

(N206.240) K_Performanztest
Schritt 4: Der Inhalt von EF.transparent wird mittels Use Case aus (N049.100) gelöscht, wobei der Kommandoparameter *offset* = 0 gesetzt wird. Die Laufzeit dieses Kommandos ist für diesen Prüfpunkt irrelevant. ~~Die Laufzeit t_{wipe} dieses Kommandos MUSS gemäß CosK_056 gemessen und der Menge M_{wipe} hinzugefügt werden.~~ <=

   b) Begründung: In Schritt 4 ist die Datei EF.transparent nur teilweise gefüllt, weshalb das letzte ERASE BINARY Kommando im Allgemeinen eine deutlich andere Laufzeit aufweist, was sich negativ auf die Standardabweichung auswirkt und damit zu einem ungewollten Punktabzug führte.

11) Ort (N211.610) und (N211.640) und (N211.730)
   a) Die Afo-Texte werden geändert:

(N211.610) K_Performanztest
Schritt 1: Aus den einhundert CV–Zertifikaten mit Authentisierungsschlüssel wird ein bislang noch nicht verwendetes gezogen (ziehen ohne zurücklegen). Durch die Ziehung wird folgende CV–Zertifikatskette gebildet:
PuK.RCA -> CVC_Test_CAx -> CVC_ICCy.
Die erste Ziehung ist beliebig. Bei allen weiteren Ziehungen MUSS die Nebenbedingung beachtet werden, dass CVC_Test_CAx verschieden ist vom unmittelbar vorher verwendeten Zertifikat CVC_Test_CAx. ~~Dann MUSS mit Schritt 4 fortgefahren werden.~~
Dann MANAGE SECURITY ENVIRONMENT Set Kommando gemäß (N103.300), wobei als *keyRef* der Wert CAR aus CVC_ICCy verwendet wird. Die Laufzeit dieses Kommandos in der *i*–ten Schleifeniteration MUSS gemäß 18.5.1.1 gemessen werden und wird mit $t_{Run1,i}$ bezeichnet. Wenn dieses Kommando mit NoError beendet wird, fahre mit Schritt 5 fort, sonst mit Schritt 2. <=

(N211.640) K_Performanztest
Schritt 4: MANAGE SECURITY ENVIRONMENT Set Kommando gemäß (N103.300), wobei als *keyRef* der Wert CAR aus CVC_ICCy verwendet wird. Die Laufzeit dieses Kommandos in der *i*–ten Schleifeniteration MUSS gemäß CosK_056 gemessen werden und wird mit $t_{Run4,i}$ bezeichnet. ~~Wenn dieses Kommando nicht mit NoError beendet wird, dann fahre mit Schritt 2 fort, sonst mit Schritt 5.~~

(N211.730) K_Performanztest
Der Performanztest MUSS die in hier ermittelten Laufzeiten wie folgt in Performanzpunkte umrechnen:
Bei der Bearbeitung einer Schleifeniteration sind folgende Fälle denkbar:

a. Der öffentliche Schlüssel der CA ist bereits in der Karte gespeichert, weil er bei der Kartenproduktion in *persistentPublicKeyList* oder durch einen früheren Zertifikatsimport in *persistentCache* gespeichert wurde. In diesem Fall besteht der *i*–te Schleifendurchlauf aus der Schrittfolge 1, 5, 6, 7, ... Die Laufzeiten der Schritte 1 und 5 werden summiert zu $t_{Import,i}$.
b. Der öffentliche Schlüssel der CA ist nicht in der Karte gespeichert ~~und dies wird bereits während der Schlüsselselektion bemerkt~~. Dann besteht der *i*–te Schleifendurchlauf aus der Schrittfolge 1, 2, 3, 4, 5, 6, 7, ... Die Laufzeiten der Schritte 1, 2, 3, 4 und 5 werden summiert zu $t_{Import,i}$.
c. Die Laufzeiten der Schritte 6, 7 und 8 werden summiert zu $t_{RoleCheck,i}$.
d. Die Laufzeiten der Schritte 11 und 12 werden aufsummiert zu $t_{SK,i}$.
e. Die gemessenen Zeiten werden zu folgenden Tupeln zusammengefasst:

$$M_{Import} = (t_{Import,1}, t_{Import,2}, \ldots, t_{Import,100})$$
$$M_{RoleCheck} = (t_{RoleCheck,1}, t_{RoleCheck,2}, \ldots, t_{RoleCheck,100})$$
$$M_{SesKey} = (t_{SesKey,1}, t_{SesKey,2}, \ldots, t_{SesKey,100})$$
$$M_{GetSecStat} = (t_{GetSecStat,1}, t_{GetSecStat,2}, \ldots, t_{GetSecStat,100})$$

   b) Begründung: Zuvor wurde der Import von CV-Zertifikaten in Form einer Schleife beschrieben. Dadurch ergeben sich Ungenauigkeiten bei der Verwendung der Schrittnummern. Die Beschreibung wird deshalb von einer Schleife in einen linearen Ablauf umgewandelt.

12) Ort (N213.130) und (N213.140) und (N215.230)
   a) Diese Anforderungen werden ersatzlos gestrichen, als Seiteneffekt werden (N215.250) (N215.270) entsprechend angepasst.
   b) Begründung: Wegen der „Option_RSA_KeyGeneration“ ist es nicht möglich vorauszusetzen, dass im Rahmen des Performanztests die Funktionalität "RSA Schlüsselgenerierung" zur Verfügung steht.

13) Ort 18.8.22 GET RANDOM
   a) Im Kapitel mit Performanzvorgaben für GET RANDOM wird der Hinweis auf "Option_logische_Kanäle" entfernt:

18.8.22 GET RANDOM

~~Dieser Prüfpunkt ist nur relevant, wenn Option_logische_Kanäle vorhanden ist.~~

   b) Begründung: GET RANDOM gehört nun zur Basisfunktionalität.

14) Ort (N108.600)
   a) Die Afo wird in zwei Afos aufgeteilt:

(N108.600) K_Performanztest {IFD}
Das IFD MUSS
a. für eine Kommandonachricht 4096 ~~und SOLL~~ 32.768 als APDU Länge unterstützen.
b. für eine Antwortnachricht 65.638 als APDU Länge unterstützen.

(N108.602) K_Performanztest {IFD}
Das IFD SOLL für eine Kommandonachricht 32.768 als APDU Länge unterstützen.

   b) Begründung: Aufspaltung je nach RFC-Wort.

15) Ort (N109.600), (N109.700)
   a) Adressat und Afo-Text werden präzisiert. die Abbildung aktualisiert:

(N109.600) K_Performanztest
Der Performanztest MUSS es als zulassungsverhindernd werten, falls ein Prüfling in wenigstens einem Prüfpunkt das Verhältnis X_i / T_{Ri} größer als vier ist. <=

(N109.700) K_Performanztest
Der Performanztest MUSS es als zulassungsverhindernd werten, falls für einen Prüfling die gemäß (N109.500) ermittelte Punktzahl kleiner ist als in CosT_439 für die Kombination von Optionen angegebene. Dies entspricht einer relativen Ausführungszeit, die 1,5-mal so groß ist wie die Referenzzeit. <=

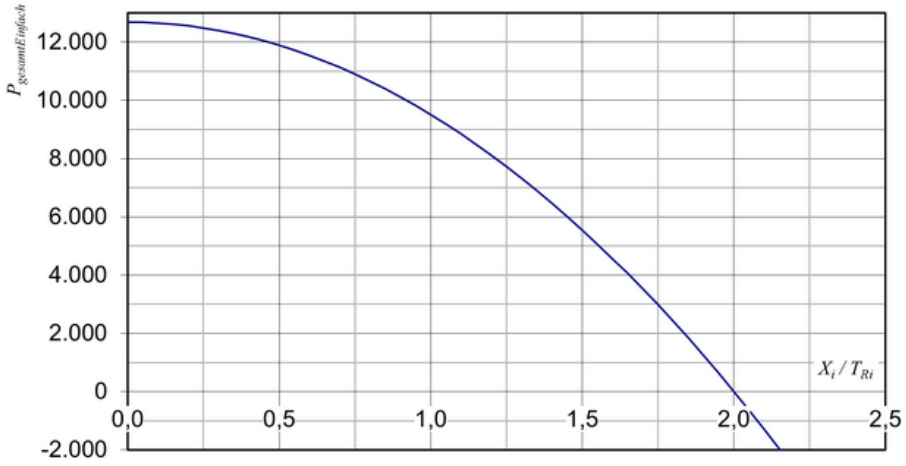

Abbildung 12, CosA_3de: Graphische Darstellung von $P_{gesamtEinfach}$

   b) Begründung: Präzisierung, Konsistenz.

16) Ort 18.6.1
   a) Die Formel zur Berechnung von P_{IO} wird in eine neue Afo (N200.100) integriert:

(N200.100) K_Performanztest
Der Performanztest MUSS die Performanzpunkte P_{IO} wie folgt ermitteln:
Für die (rechnerische) Übertragungszeit von 1.000 Oktett zur Karte gilt:

$$t_T = \frac{1000 \cdot CGT}{C}$$

Mit C aus CosT_719 für den Fall PPS1 = TA_1 und CGT in Abhängigkeit von TC_1 im ATR gemäß CosT_4ba:

Tabelle 353 , CosT_4ba: Character Guard Time (CGT) gemäß [ISO/IEC 7816-3#11.2]

TC_1	'FF'	'00'	'01'	'02'	...	'FD'	'FE'
CGT	11	12	13	14	...	265	266

P_{IO} = points((t_T, t_T), T_{IO}).

   b) Begründung: Referenzierbarkeit.

17) Afo-Texte werden mit einem RFC-Wort versehen oder Formeln für Performanz Punkte werden in eine Afo integriert. Dies betrifft:

(N200.200), (N200.250), (N201.310), (N202.220), (N202.230), (N203.200), (N203.230), (N204.200), (N204.220), (N204.230), (N205.200), (N205.250), (N206.200), (N206.250), (N207.200), (N207.230), (N208.200), (N208.280), (N209.200), (N209.240), (N210.200), (N210.220), (N210.280), (N211.110), (N211.120), (N211.130), (N211.210), (N211.220), (N211.230), (N211.310), (N211.320), (N211.330), (N211.600), (N211.730), (N212.200), (N213.200), (N213.260), (N214.200), (N215.200), (N215.270), (N216.200), (N216.270), (N217.200), (N217.240), (N218.200), (N218.250), (N219.200), (N219.230), (N220.200), (N220.210), (N220.270), (N221.200), (N221.300), (N222.200), (N222.220), (N223.200), (N223.250)

18) Ort (N253.210)
   a) Der AID im Rekord 1 des EF.DIR wird an den Wert der AID des Ordners *root* aus (N253.050) angepasst.

recordList	
Rekord 1	'61 – L_{61} – { 4F – 05 – F000000030 50 – 00 53 – L_{53} – COS_Identifier }'
Rekord 2	'61 – L_{61} – {4F – L_{4F} – AID}'
...	...

   b) Begründung: Korrektur, Konsistenz

3 Literaturstellen

[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS), Elektrische Schnittstelle