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.

Die Performancevorgaben für den Konnektor werden in folgenden Punkten präzisiert:

- Die Abhängigkeit der Bearbeitungszeiten von der Dokumentengröße wird präzisiert. Diese ist bei 25 MB großen Dokumenten vom Typ der Dokumente abhängig.
- Inzwischen sind LAN-Anbindung mit 1Gbit/s Stand der Technik, so dass vom Konnekor verlangt wird, diesen Stand zu unterstützen. Damit die Konnektorhersteller motiviert sind diese Bandbreite soweit möglich auch bereitzustellen, wird als Rahmenbedingung für die Performancemessungen die LAN-Bandbreite auf 1 Gbit/s hochgesetzt. Entsprechend werden die Bearbeitungszeiten (relevant für große Nachrichten) angepasst.
- Die Karten- und Kartenterminalreferenzzeiten in Tabelle *Tab_gemSpec_Perf* werden an die aktuell in der COS-Spezifikation vorgegebenen G2-Kartenzeiten angepasst. Die Zeiten für Kartenoperationen bei QES werden nachgeschärft.
- Für QES-Signaturen war in den Vorgabezeiten die Zeit für die Prüfung des Signaturzertifikats nicht berücksichtigt. Sie wird ergänzt.
- Die Lastvorgabe für QES-Stapelsignaturen wird korrigiert entsprechend der Annahme, dass 25% der QES-Signaturen als Stapelsignaturen erfolgen. Dabei wird berücksichtigt, dass mit einem Signaturauftrag zwei dokumente signiert werden.
- Für QES-Stapelsignaturen (Stapel > 1) wird die Zeit zum Aufbau und zur Nutzung der sicheren Kanäle zwischen den Karten zur Übertragung der PIN und des zu signierenden Hashes genauer berücksichtigt.
- VerifyDocument wird präzisiert: Im typischen Fall IncludeRevocationInfo=false wird das Dokument mit Signatur nicht von Konnektor zum Clientsystem zurücktransportiert, so dass die Größe der Antwortnachricht unabhängig von der Dokumentengröße ist. Das reduziert die Antwortzeit.
- Bisher haben sich die Werte in der Spalte ”Konnektor Gesamt” aus der Summe der Werte der übrigen Spalten zuzüglich 50 msec Puffer berechnet. Dieser Puffer ist dem Konnektor zuzurechnen und wird daher in der Spalte ”Konnektor intern” ergänzt.
- Da Karten und Kartenterminalzeiten bereits in Tabelle *Tab_gemSpec_Perf_Konnektorbearbeitungszeiten_pro_Komponenten* berücksichtigt sind, ist Tabelle *Tab_gemSpec_Perf_Normierte_Karten_Kartenterminal_Bearbeitungszeiten* nicht erforderlich. Tabelle *Tab_gemSpec_Perf_Normierte_Karten_Kartenterminal_Bearbeitungszeiten* wird daher gestrichen.
- Die Antwortzeiten des Konnektor werden über Mittelwertvorgaben an die Bearbeitungszeit im Bereich der Erwartungen gehalten. Dadurch werden

insbesondere auch die Schwankungen eingegrenzt. Es hat sich herausgestellt, dass eine zusätzliche Einschränkung durch die 99%-Quantilvorgaben nicht praktikabel ist und keinen tatsächlichen Mehrwert bringt. Sie wird daher für den Konnektor gestrichen.

- encrypt_Document_Symmetric und decrypt_Document_Symmetric wird aus Tab_gemSpec_Perf_Konnektor gestrichen, weil die Operationen nicht an der Außenschnittstelle des Konnektors angeboten werden.

Änderungsbedarf in gemSpec_Perf

Kapitel 4.1.2. Produkttyp Konnektor

Skalierbarkeit

⌦ **GS-A_5327 Performance - Konnektor - Skalierbarkeit**

Der Konnektor MUSS die von 8 durchschnittlichen Anwendungen erzeugte Last im vorgegebenen Bearbeitungszeitrahmen für die vorgesehene Leistungserbringerumgebung bedienen können. Dabei wird die erzeugte Last einer durchschnittlichen Anwendung als die durch Tabelle Tab_gemSpec_Perf_Konnektor definierte Last (VSDM, KOM-LE, QES) geteilt durch 3 definiert. ⌫

Der Test von [GS-A_5327] erfolgt für den VSDM-Konnektor anhand eines QES-Produktmusters. Das QES-Produktmuster muss dafür funktional nur soweit implementiert sein, dass eine Überprüfung der Bearbeitung paralleler Requests unter der Ziellast möglich ist. Welche Tests durchgeführt werden und welche Eigenschaften dafür beim QES-Produktmuster erforderlich sind, beschreibt „Anhang D – Performancerelevante Produktmustereigenschaften des QES-Konnektors“.

Der Test von [GS-A_5327] erfolgt für den QES-Konnektor vom Verfahren her analog den Tests für den VSDM-Konnektor. Getestet wird an Hand eines breiteren Spektrums von Signatur- und Verschlüsselungsverfahren, beschrieben in „Anhang E – Testverfahren zur Prüfung der Skalierungsfähigkeit des QES-Konnektors“.

Tabelle 18 Tab_gemSpec_Perf_Konnektor – Last- und Bearbeitungszeitvorgaben

Schnittstellenoperationen	Last		Bearbeitungszeit		
	LE-U	Spitzen-last [1/h]	Größe der Anfrage-nachricht [kByte]	Mittelwert [msec]	~~99%-Quantil [msec]~~
Fachanwendung					
I_VSD_Service					
ReadVSD – mit Akt.-Prüfung, mit Update	1	1		6130	~~6700~~
	2	1			
	3	4			
	4	11			
ReadVSD – mit Akt.-Prüfung, ohne	1	50		3940	~~4480~~

Schnittstellenoperationen	Last		Bearbeitungszeit		
	LE-U	Spitzen-last [1/h]	Größe der Anfrage-nachricht [kByte]	Mittelwert [msec]	~~99%-Quantil [msec]~~
Update	2	50			
	3	175			
	4	437			
ReadVSD – ohne Akt.-Prüfung				3820	~~4500~~
UpdateVSD – automat. Akt.-Prüfung, mit Update				5720	~~6260~~
UpdateVSD – automat. Akt.-Prüfung, ohne Update				3130	~~3540~~
Basisdienste					
I_Sign_Operations					
sign_Document			10	~~1460~~ 1010	~~1740~~
	1	217	100	~~1480~~ 1030	~~1760~~
	2	258			
	3	351			
	4	575			
			1000	~~1670~~ 1440	~~1970~~
		~~13~~	~~25000~~	~~6680~~	~~7280~~
sign_Document (XAdES, XML_25MB, enveloped)		13	25000	10500	
sign_Document (CAdES, TIFF_25MB, detached)			25000	7300	
sign_Document (PAdES, PDFA_2b_25MB)			25000	7300	
verify_Document			10	~~1280~~ 1570	~~1550~~
	1	217	100	~~1300~~ 1600	~~1570~~
	2	258			
	3	351			
	4	575			
			1000	~~1490~~ 1930	~~1770~~
		~~13~~	~~25000~~	~~6500~~	~~7100~~
verify_Document (XAdES, XML_25MB, enveloped, IncludeRevocationInfo=false)		13	25000	9000	
verify_Document (CAdES, TIFF_25MB, IncludeRevocationInfo=false)			25000	9000	
verify_Document (PAdES, PDFA_2b_25MB, IncludeRevocationInfo=false)			25000	10600	
external_Authenticate				885	~~1110~~
get_Certificate				220	~~330~~
I_SAK_Operations					
sign_Document_QES			10	~~1580~~	~~1890~~

Schnittstellenoperationen	Last		Bearbeitungszeit		
	LE-U	Spitzen-last [1/h]	Größe der Anfrage-nachricht [kByte]	Mittelwert [msec]	~~99%-Quantil [msec]~~
(Stapelgröße 1)				3540	
	1	17	100	~~1860~~ 3790	~~2210~~
	2	65			
	3	177			
	4	442			
			1000	~~2380~~ 4070	~~2780~~
			~~25000~~	~~7740~~	~~8410~~
sign_Document_QES (XAdES, XML_25MB, enveloped)			25000	12810	~~17070~~
sign_Document_QES (CAdES, TIFF_25MB)			25000	9610	~~11920~~
sign_Document_QES (PAdES, PDFA_2b_25MB)			25000	9610	~~12540~~
sign_Document_QES (Stapelgröße 2, 2 * 100 kB Dokumente)	1	3	~~100~~ 200	~~3480~~ 8870	~~3960~~
	2	~~33~~ 11			
	3	~~89~~ 30			
	4	~~221~~ 74			
verify_Document_QES			10	~~2300~~ 2580	~~2660~~
	1	10	100	~~2340~~ 2610	~~2710~~
	2	39			
	3	113			
	4	282			
			1000	~~2560~~ 2940	~~2940~~
			~~25000~~	~~7720~~	~~8370~~
verify_Document_QES (XAdES, XML_25MB, enveloped, IncludeRevocationInfo=false)			25000	10010	
verify_Document_QES (CAdES, TIFF_25MB, detached IncludeRevocationInfo=false)			25000	10010	
verify_Document_QES (PAdES, PDFA_2b_25MB, IncludeRevocationInfo=false)			25000	11610	
I_KV_Card_Unlocking					
authorize_Card (no Cache)				2020	~~2350~~
authorize_Card (Cache)				1830	~~2140~~
I_Crypt_Operations					
encrypt_Document			10	~~1870~~ 1860	~~2190~~
	1	217	100	~~1890~~ 1880	~~2210~~
	2	258			
	3	351			
	4	575			
			1000	~~2080~~	~~2410~~

Schnittstellenoperationen			Last		Bearbeitungszeit		
			LE-U	Spitzen-last [1/h]	Größe der Anfrage-nachricht [kByte]	Mittelwert [msec]	~~99%-Quantil [msec]~~
						2200	
				~~13~~	~~25000~~	~~6970~~	~~7580~~
		encrypt_Document (XMLEnc, TIFF_25MB, ein Empfänger)		13	25000	10600	
		encrypt_Document (CMS, TIFF_25MB, ein Empfänger)			25000	7800	
		decrypt_Document			10	~~1110~~ 490	~~1350~~
			1	217	100	~~1120~~ 510	~~1370~~
			2	258			
			3	351			
			4	575			
					1000	~~1310~~ 820	~~1570~~
				~~13~~	~~25000~~	~~6200~~	~~6780~~
		decrypt_Document (XMLEnc, TIFF_25MB)		13	25000	8900	
		decrypt_Document (CMS, TIFF_25MB)			25000	8900	
		~~encrypt_Document_Symmetric~~			~~10~~	~~510~~	~~670~~
					~~1000~~	~~710~~	~~900~~
		~~decrypt_Document_Symmetric~~			~~10~~	~~160~~	~~250~~
					~~1000~~	~~360~~	~~500~~
	I_Cert_Verification						
		verify_Certificate				1150	~~1400~~
	I_Directory_Query						
		search_Directory	1	200		1220	~~1470~~
			2	300			
			3	500			
			4	1000			

[…]

- Das Leistungserbringer-LAN wird mit einer Bandbreite von 1Gbit/sec ~~100 Mbit/sec, einer TCP-Effizienz von 1309/1500 = 87% und einer Latenz (eine Strecke) von 2 msec normiert~~ angesetzt.
- Die Performancevorgaben aus Tab_gemSpec_Perf_Konnektor für die Basisdienste I_Sign_Operations und I_Crypt_Operations ~~im Fall von XML-Dokumenten~~ sind an Hand folgender Referenzdokumente nachzuweisen:
  - XML_25MB
  - XML_1MB
  - XML_100KB

- XML_10KB
- TIFF_25MB
- TIFF_1MB
- PDFA_2b_25MB_Bilder_und_Text
- PDFA_2b_1MB_Komplex
- TEXT_100KB
- TEXT_10KB

Die konkreten Dokumente zu diesen Bezeichnern legt die Dokumentenlandkarte fest.

Stapelsignatur und gSMC-Ks

Bei der Operation sign_Document_QES in Tabelle Tab_gemSpec_Perf_Konn wurde gemäß Lastmodell aus Kapitel 3.1.4 davon ausgegangen, dass 25% der Signaturen per Stapelsignatur (Annahme Lastmodell: Stapelgröße 2) erfolgen. Tabelle 1 stellt für diese Situation dar, wie groß die Wahrscheinlichkeit ist, dass n Stapelsignaturen oder mehr parallel erfolgen müssen.

Tabelle 1 Tab_gemSpec_Perf_Konnektor_Stapelsignatur – Parallelverarbeitung gemäß Lastmodell

~~Lastvorgaben~~		~~Mittelwert Bearbeitungs-zeit [msec]~~	~~Sp.Last * Mittelwert Bearbeitungs-zeit [msec]~~	~~Wahrscheinlichkeit für n oder mehr parallele Bearbeitungen~~					
~~LE-U~~	~~Spitzenlasten [1/h]~~			~~n=1~~	~~n=2~~	~~n=3~~	~~n=4~~	~~n=5~~	~~n=6~~
~~1~~	~~3~~	~~4280~~	~~0,00~~	~~0,3%~~	~~0,0%~~	~~0,0%~~	~~0,0%~~	~~0,0%~~	~~0,0%~~
~~2~~	~~32~~		~~0,04~~	~~3,8%~~	~~0,1%~~	~~0,0%~~	~~0,0%~~	~~0,0%~~	~~0,0%~~
~~3~~	~~89~~		~~0,11~~	~~10,0%~~	~~0,5%~~	~~0,0%~~	~~0,0%~~	~~0,0%~~	~~0,0%~~
~~4~~	~~221~~		~~0,26~~	~~23,1%~~	~~2,9%~~	~~0,2%~~	~~0,0%~~	~~0,0%~~	~~0,0%~~

Lastvorgaben		Mittelwert Bearbeitungs-zeit [msec]	Sp.Last * Mittelwert Bearbeitungs-zeit [msec]	Wahrscheinlichkeit in % für n oder mehr parallele Bearbeitungen					
LE-U	Spitzenlasten [1/h]			n=1	n=2	n=3	n=4	n=5	n=6
1	3	8870	0,01	1	0	0	0	0	0
2	11		0,03	3	0	0	0	0	0
3	30		0,07	7	0	0	0	0	0
4	74		0,18	17	1	0	0	0	0

In Tabelle 1 sind alle Wahrscheinlichkeiten ~~unter 1 % grün markiert, da beim 99%-Quantil 1% der Antwortzeiten von der Vorgabe abweichen dürfen. Die Wahrscheinlichkeiten~~ über 1% ~~sind~~ rot markiert, weil hier davon ausgegangen wird, dass die Vorgaben nur erreicht werden können, wenn eine vollständige parallele Verarbeitung der Anfragen erfolgt. Geht man davon

aus, dass pro gSMC-K drei logische Kanäle für die parallele Verarbeitung von Stapelsignaturen zur Verfügung stehen, dann folgt daraus, dass für das angenommene Lastszenario der Einsatz einer gSMC-K ausreichend ist.

Der Konnektor muss jedoch auch auf ein geändertes Nutzungsverhalten vorbereitet sein, wie es durch verstärkte Nutzung oder systematische Häufung von Anfragen gegen Schichtende oder durch eine verstärkte Nutzung der Stapelsignatur hervorgerufen werden kann. Angenommen in einer Leistungserbringerumgebung wird dadurch ~~werden nur Stapelsignaturen ausgeführt und es gibt eine zusätzliche Lasterhöhung von Faktor 10~~ (zusätzlich zum angenommenen Spitzenlastfaktor) die Last um den Faktor 30 erhöht, dann stellt sich die Situation aus Tabelle 26 wie folgt dar:

Tabelle 2 Tab_gemSpec_Perf_Konnektor_Stapelsignatur_Perspektivisch - Parallelverarbeitung perspektivisch

~~Last~~				~~Wahrscheinlichkeit für n oder mehr parallele Bearbeitungen~~											
~~LE-U~~	~~Spitzen-lasten [1/h]~~	~~B.zeit [msec]~~	~~Sp.Last * B.zeit~~	~~n=1~~	~~n=2~~	~~n=3~~	~~n=4~~	~~n=5~~	~~n=6~~	~~n=7~~	~~n=8~~	~~n=9~~	~~n=10~~	~~n=11~~	~~n=12~~
~~1~~	~~170~~	~~4220~~	~~0,2~~	~~18%~~	~~2%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~
~~2~~	~~648~~		~~0,8~~	~~54%~~	~~18%~~	~~4%~~	~~1%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~
~~3~~	~~1770~~		~~2,1~~	~~88%~~	~~62%~~	~~35%~~	~~16%~~	~~6%~~	~~2%~~	~~1%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~	~~0%~~
~~4~~	~~4421~~		~~5,3~~	~~99%~~	~~97%~~	~~90%~~	~~77%~~	~~60 %~~	~~43%~~	~~28%~~	~~16%~~	~~9%~~	~~4%~~	~~2%~~	~~1%~~

Last		Mittelwert Bearbeitungs-zeit [msec]	Sp.Last * Mittelwert Bearbeitungs-zeit [msec]	Wahrscheinlichkeit in % für n oder mehr parallele Bearbeitungen											
LE-U	Spitzen-lasten [1/h]			1	2	3	4	5	6	7	8	9	10	11	12
1	90	8870	0,2	19	2	0	0	0	0	0	0	0	0	0	0
2	330		0,8	55	19	5	1	0	0	0	0	0	0	0	0
3	900		2,2	89	64	37	18	7	2,4	1	0	0	0	0	0
4	2220		5,4	100	97	91	79	63	46	31	18	10	5	2	1

Anhang B – Modelldetails

~~B1 – Normierte Karten- und Kartenterminalbearbeitungszeiten für den Messaufbau~~

~~In den Vorgaben für die Bearbeitungszeiten des Konnektors werden pro Kartenoperation normierte Bearbeitungszeiten für Kartenterminal und Karte in Summe angesetzt. Sie werden durch Tabelle 45 festgelegt.~~

~~Tabelle 3 Tab_gemSpec_Perf_Normierte_Karten_Kartenterminal_Bearbeitungszeiten~~

~~Kartenoperationen~~	~~Bearbeitungszeiten (Karte + Kartenterminal)~~	
	~~volumen-unabhängig [msec]~~	~~volumen-abhängig [msec/kByte]~~
~~VERIFY~~	~~122~~	~~0~~
~~RESET RETRY COUNTER~~	~~130~~	~~0~~
~~CHANGE REFERENCE DATA~~	~~130~~	~~0~~
~~GET PIN STATUS~~	~~60~~	~~0~~
~~Select~~	~~65~~	~~0~~
~~PSO Decipher~~	~~865~~	~~0~~
~~MSE Set~~	~~65~~	~~0~~
~~PSO Compute Digital Signature~~	~~800~~	~~0~~
~~READ BINARY~~	~~69~~	~~80~~
~~UPDATE BINARY~~	~~74~~	~~146~~
~~Text im Display des Kartenterminals anzeigen (inkl. RoundTrip)~~	~~160~~	~~0~~
~~Reset ICC~~	~~210~~	~~0~~
~~Select DF.ESIGN~~	~~42~~	~~0~~
~~Read Binary EF.C.CH.AUT mit SFID~~	~~156~~	~~0~~
~~MSE SET Puk.RCA.CS~~ ~~PSO Verify Certificate aus EF.C.CA_SMC.CS der SMC bzw. EF.C.CA_eGK.CS der eGK~~	~~330~~	~~0~~
~~MSE SET Public Key aus EF.C.CA_SMC.CS der SMC bzw. EF.C.CA_eGK.CS der eGK~~ ~~PSO Verify Certificate aus EF.C.SMC.AUTR_CVC der SMC bzw. EF.C.eGK.AUTR_CVC der eGK~~	~~330~~	~~0~~
~~MSE SET Public Key aus EF.C.SMC.AUTR_CVC der SMC bzw. aus EF.C.eGK.AUT_CVC der eGK~~ ~~Get Challenge~~ ~~MSE SET PrK.SMC.AUTR_CVC bzw. PrK.eGK.AUT_CVC~~ ~~Internal Authenticate~~ ~~External Authenticate~~	~~1070~~	~~0~~
~~MSE Set PuK.SMC.AUTR_CVC~~	~~25~~	~~0~~

~~Kartenoperationen~~	~~Bearbeitungszeiten (Karte + Kartenterminal)~~	
	~~volumen-unabhängig [msec]~~	~~volumen-abhängig [msec/kByte]~~
~~Internal Authenticate~~	~~750~~	~~0~~
~~ReadBinary EF.ATR~~	~~144~~	~~0~~
~~Select DF.HCA~~	~~50~~	~~0~~
~~MSE SET SK.VSD~~	~~31~~	~~0~~
~~Get Challenge~~	~~24~~	~~0~~
~~MutualAuthenticate~~	~~179~~	~~0~~
~~Update Binary EF.StatusVD mit SFID~~	~~88~~	~~0~~
~~Update Binary EF.PD mit SFID~~	~~161~~	~~0~~
~~Update Binary EF.VD mit SFID~~	~~222~~	~~0~~
~~Update Binary EF.GVD mit SFID~~	~~131~~	~~0~~
~~Read Binary EF.StatusVD mit SFID~~	~~40~~	~~0~~
~~Read Binary EF.PD mit SFID~~	~~112~~	~~0~~
~~Read Binary EF.VD mit SFID~~	~~157~~	~~0~~
~~Read Binary EF.GVD mit SFID~~	~~86~~	~~0~~
~~Append Record mit SFID EF.Logging~~	~~98~~	~~0~~
~~Update Binary mit SFID EF.Prüfungsnachweis~~	~~96~~	~~0~~
~~Read Binary mit SFID EF.Prüfungsnachweis~~	~~61~~	~~0~~

Tabelle 40 Tab_gemSpec_Perf_Konnektorbearbeitungszeiten_pro_Komponente

Schnittstellenoperationen	Konnektor Gesamt [msec]	Konnektor intern mit LE-LAN [msec]	Kartenterm. + Karte [msec]	~~LE-LAN [msec]~~	OCSP + Zugangsnetz+ Zentr.Netz [msec]
Lesen VSD mit Onlineprüfung mit Aktualisierung	6140	~~1210~~ 1260	3780	~~0~~	1100
Lesen VSD mit Onlineprüfung ohne Aktualisierung	3940	~~740~~ 790	3150	~~0~~	0
Lesen VSD ohne Onlineprüfung	3820	~~560~~ 610	3210	~~0~~	0
Automatische Onlineprüfung mit Aktualisierung der VSD	5720	~~980~~ 1030	3590	~~0~~	1100
Automatische Onlineprüfung ohne Aktualisierung der VSD	3130	~~410~~ 460	2670	~~0~~	0
I_Sign_Operations::sign_Document (10 kB)	~~1460~~ 1010	300	~~1100~~ 710	~~10~~	0
I_Sign_Operations::sign_Document (100 kB)	~~1470~~ 1030	~~300~~ 320	~~1100~~ 710	~~20~~	0
I_Sign_Operations::sign_Document (1 MB) (XAdES, XML_1MB, enveloped) (CAdES, TIFF_1MB, detached)	~~1670~~ 1440	~~330~~ 730	~~1100~~ 710	~~190~~	0

Schnittstellenoperationen	Konnektor Gesamt [msec]	Konnektor intern mit LE-LAN [msec]	Kartenterm. + Karte [msec]	~~LE-LAN [msec]~~	OCSP + Zugangsnetz+ Zentr.Netz [msec]
(PAdES, PDFA_2b_1MB_Komplex)					
~~I_Sign_Operations::sign_Document (25 MB)~~	~~6680~~	~~930~~	~~1100~~	~~4600~~	~~0~~
I_Sign_Operations::sign_Document (XAdES, XML_25MB, enveloped)	10500	9790	710	0	0
I_Sign_Operations::sign_Document (CAdES, TIFF_25MB, detached)	7300	6590	710	0	0
I_Sign_Operations::sign_Document (PAdES, PDFA_2b_25MB_Bilder_und_Text)	7300	6590	710	0	0
I_Sign_Operations::verify_Document (10 kB)	~~1290~~ 1570	~~110~~ 470	~~20~~ 0	~~10~~	1100
I_Sign_Operations::verify_Document (100 kB)	~~1310~~ 1600	~~110~~ 500	~~20~~ 0	~~30~~	1100
I_Sign_Operations::verify_Document (1 MB) (XAdES, XML_1MB, enveloped) (CAdES, TIFF_1MB, detached) (PAdES, PDFA_2b_1MB_Komplex)	~~1500~~ 1930	~~140~~ 830	~~20~~ 0	~~190~~	1100
~~I_Sign_Operations::verify_Document (25 MB)~~	~~6510~~	~~740~~	~~20~~	~~4600~~	~~1100~~
I_Sign_Operations::verify_Document (XAdES, XML_25MB, enveloped, IncludeRevocationInfo=false)	9000	7900	0	~~2350~~	1100
I_Sign_Operations::verify_Document (CAdES, TIFF_25MB, IncludeRevocationInfo=false)	9000	7900	0	~~2350~~	1100
I_Sign_Operations::verify_Document (PAdES, PDFA_2b_25MB, IncludeRevocationInfo=false)	10600	9500	0	~~2350~~	1100
I_SAK_Operations::sign_Document_QES (10KB)	~~1580~~ 3540	~~470~~ 520	~~1050~~ 910	~~10~~	~~0~~ 2100
I_SAK_Operations::sign_Document_QES (100KB, Stapelgröße 1, SE#1)	~~1860~~ 3790	~~720~~ 770	~~1050~~ 910	~~40~~	~~0~~ 2100
I_SAK_Operations::sign_Document_QES (100KB, Stapelgröße 2, SE#2)	~~3480~~ 8870	~~1380~~ 1430	~~1980~~ 5330	~~70~~	~~0~~ 2110
I_SAK_Operations::sign_Document_QES (1MB)	~~2380~~ 4070	~~1000~~ 1050	~~1050~~ 910	~~280~~	~~0~~ 2110
~~I_SAK_Operations::sign_Document_QES (25MB)~~	~~7740~~	~~1850~~	~~1050~~	~~4790~~	~~0~~
I_SAK_Operations::sign_Document_QES (XAdES, XML_25MB, enveloped)	12810	9790	~~1050~~ 910	~~4700~~	2110
I_SAK_Operations::sign_Document_QES (CAdES, TIFF_25MB)	9610	6590	~~1050~~ 910	~~4700~~	2110
I_SAK_Operations::sign_Document_QES (PAdES, PDFA_2b_25MB)	9610	6590	~~1050~~ 910	~~4700~~	2110

Schnittstellenoperationen	Konnektor Gesamt [msec]	Konnektor intern mit LE-LAN [msec]	Kartenterm. + Karte [msec]	~~LE-LAN [msec]~~	OCSP + Zugangsnetz+ Zentr.Netz [msec]
I_SAK_Operations::verify_Document_QES (10KB)	~~2300~~ 2580	~~130~~ 470	0	~~10~~	2110
I_SAK_Operations::verify_Document_QES (100KB)	~~2340~~ 2610	~~160~~ 500	0	~~20~~	2110
I_SAK_Operations::verify_Document_QES (1 MB)	~~2560~~ 2940	~~210~~ 830	0	~~190~~	2110
~~I_SAK_Operations::verify_Document_QES (25 MB)~~	~~7720~~	~~960~~	~~0~~	~~4600~~	~~2110~~
I_SAK_Operations::verify_Document_QES (XAdES, XML_25MB, enveloped, IncludeRevocationInfo=false)	~~9600~~ 10010	~~5120~~ 7900	0	~~2350~~	2110
I_SAK_Operations::verify_Document_QES (CAdES, TIFF_25MB, IncludeRevocationInfo=false)	~~9600~~ 10010	~~2420~~ 7900	0	~~2350~~	2110
I_SAK_Operations::verify_Document_QES (PAdES, PDFA_2b_25MB, IncludeRevocationInfo=false)	~~10200~~ 11610	~~5720~~ 9500	0	~~2350~~	2110
I_KV_Card_Unlocking::authorize_Card (no Cache)	2020	~~50~~ 100	1920	~~0~~	0
I_KV_Card_Unlocking::authorize_Card (Cache)	1830	~~50~~ 100	1730	~~0~~	0
I_Crypt_Operations::encrypt_Document (10 kB)	~~1880~~ 1860	~~700~~ 760	~~20~~ 0	~~10~~	1100
I_Crypt_Operations::encrypt_Document (100 kB)	~~1900~~ 1880	~~700~~ 780	~~20~~ 0	~~30~~	1100
I_Crypt_Operations::encrypt_Document (1 MB)	~~2080~~ 2200	~~720~~ 1100	~~20~~ 0	~~190~~	1100
~~I_Crypt_Operations::encrypt_Document (25 MB)~~	~~6970~~	~~1200~~	~~20~~	~~4600~~	~~1100~~
I_Crypt_Operations::encrypt_Document (XMLEnc, XML_25MB, ein Empfänger)	10600	9500	0	~~4700~~	1100
I_Crypt_Operations::encrypt_Document (CMS, TIFF_25MB, ein Empfänger)	7800	6700	0	~~4700~~	1100
I_Crypt_Operations::decrypt_Document (10 kB)	~~1110~~ 490	~~100~~ 150	~~950~~ 340	~~10~~	0
I_Crypt_Operations::decrypt_Document (100 kB)	~~1120~~ 510	~~100~~ 170	~~950~~ 340	~~20~~	0
I_Crypt_Operations::decrypt_Document (1 MB) (XMLEnc, XML_1MB) (CMS, TIFF_1MB)	~~1310~~ 820	~~120~~ 480	~~950~~ 340	~~190~~	0
~~I_Crypt_Operations::decrypt_Document (25 MB)~~	~~6200~~	~~600~~	~~950~~	~~4600~~	~~0~~
I_Crypt_Operations::decrypt_Document (XMLEnc, XML_25MB)	8900	8560	~~930~~ 340	~~4700~~	0
I_Crypt_Operations::decrypt_Document (CMS, TIFF_25MB)	8900	8560	~~930~~ 340	~~4700~~	0
~~I_Crypt_Operations::encrypt_Document_Symmetric~~	~~510~~	~~450~~	~~0~~	~~10~~	~~0~~

Schnittstellenoperationen	Konnektor Gesamt [msec]	Konnektor intern mit LE-LAN [msec]	Kartenterm. + Karte [msec]	~~LE-LAN [msec]~~	OCSP + Zugangsnetz+ Zentr.Netz [msec]
~~(10 kB)~~					
~~I_Crypt_Operations::encrypt_Document_Symmetric (1 MB)~~	~~710~~	~~470~~	~~0~~	~~190~~	~~0~~
~~I_Crypt_Operations::decrypt_Document_Symmetric (10 kB)~~	~~160~~	~~100~~	~~0~~	~~10~~	~~0~~
~~I_Crypt_Operations::decrypt_Document_Symmetric (1 MB)~~	~~360~~	~~120~~	~~0~~	~~190~~	~~0~~
I_Cert_Verification::verify_Certificate	1150	50	0	0	1100
I_Directory_Query::search_Directory	1220	1220	0	0	0

Anhang E – Testverfahren zur Prüfung der Skalierungsfähigkeit des QES-Konnektors

Entsprechend der Lastvorgaben aus [GS-A_5327] für 8 Anwendungen wird das Messverfahren festgelegt. Auf Grund der unterschiedlichen Lastanforderungen für die beiden Ausprägungsformen „Einbox-Konnektor“ und „HighSpeed-Konnektor“ wird das Verfahren für beide Fälle dargestellt. Für beide Ausprägungsformen werden die Signaturverfahren CAdES, XAdES, PAdES und die Verschlüsselungsverfahren XMLEnc und CMS unterschieden.

Es gelten die Bearbeitungszeitvorgaben aus Tabelle Tab_gemSpec_Perf_QES-Konnektor_Skalierungsfähigkeit_Bearbeitungszeitvorgaben.

Tab_gemSpec_Perf_QES-Konnektor_Skalierungsfähigkeit_Bearbeitungszeitvorgaben

	Mittlere Bearbeitungszeit μ_o^{SOLL} [ms]		
	CMS, CAdES	XMLEnc, XAdES	CMS, PAdES
I_Sign_Operations::sign_Document (100 kB)	1100	1100	1100
I_Sign_Operations::sign_Document (25 MB)	7300	10500	7300
I_Sign_Operations::verify_Document (100 kB)	500	500	500
I_Sign_Operations::verify_Document (25 MB)	7900	7900	9500
I_Crypt_Operations::encrypt_Document (100 kB)	780	780	780
I_Crypt_Operations::encrypt_Document (25 MB)	6700	9500	6700
I_Crypt_Operations::decrypt_Document (100 kB)	510	510	510

I_Crypt_Operations::decrypt_Document (25 MB)	8900	8900	8900

Einbox-Konnektor

In der Lastsituation für 8 Anwendungen ergeben sich verschiedene Situationen in Bezug auf die parallele Bearbeitung von Anfragen, dargestellt in Tabelle Tab_gemSpec_Perf_Einbox_QES-Konnektor_Lastsituationen. In Situation 1 bearbeitet der Konnektor weder Operationen mit 25-MB-Dokumenten noch solche mit 100-kB-Dokumenten. In den Situationen 2 und 5 bearbeitet der Konnektor genau jeweils ein Dokument. In den übrigen Situationen liegt parallele Verarbeitung vor.

Die Situationen sind getrennt für die folgenden drei Verfahrensgruppen zu betrachten:

- Verschlüsselungsverfahren CMS und Signaturverfahren CAdES,
- Verschlüsselungsverfahren XMLEnc und Signaturverfahren XAdES,
- Verschlüsselungsverfahren CMS und Signaturverfahren PAdES.

Tab_gemSpec_Perf_Einbox_QES-Konnektor_Lastsituationen

Situationen i					
i	25 MB [Anzahl]	100 kB [Anzahl]	Wahrscheinlichkeiten p_i		
			CMS, CAdES	XMLEnc, XAdES	CMS, PAdES
1	0	0	39	37	38
2	0	1	25	24	25
3	0	2	8	8	8
4	0	3	2	2	2
5	1	0	12	13	12
6	1	1	7	8	8
7	1	2	2	3	2

Für jede der Lastsituationen i in Tab_gemSpec_Perf_Einbox_QES-Konnektor_Lastsituationen ist eine Messreihe zu erstellen. In jeder Messreihe sind vom Clientsystem jeweils ein Aufruferthread pro parallele Bearbeitung zu starten, der 100mal sign_Document, encrypt_Document, decrypt_Document und verify_Document sequentiell, direkt nacheinander aufruft. In Lastsituation 8 sind es beispielsweise 1 Thread, der 25 MB große Dokumente bearbeitet, und 3 Threads, die 100 kB große Dokumente bearbeiten.

Für jede der Lastsituationen i und der Operationen o sind die Mittelwerte ${\mu_{i,o}}^{IST}$ der Bearbeitungszeiten für die beiden Klassen 25-MB-Dokumente und 100-kB-Dokumente zu bestimmen.

Durch den Test ist pro Verfahrengruppe nachzuweisen, dass die über die Lastsituationen gemittelte Bearbeitungszeit ${\mu_o}^{IST}$ für jede Operation o kleiner als die vorgegebene Bearbeitungszeit ${\mu_o}^{SOLL}$ gemäß Tab_gemSpec_Perf_QES-Konnektor_Skalierungsfähigkeit_Bearbeitungszeitvorgaben ist:

$$ {\mu_o}^{IST} < {\mu_o}^{SOLL} $$

${\mu_o}^{IST}$ wird für 100-kB-Dokumente wie folgt gemittelt:

$$ {\mu_o}^{IST} = \frac{p_2 {\mu_{2,o}}^{IST} + p_3 {\mu_{3,o}}^{IST} + p_4 {\mu_{4,o}}^{IST} + p_6 {\mu_{6,o}}^{IST} + p_7 {\mu_{7,o}}^{IST}}{p_2 + p_3 + p_4 + p_6 + p_7} $$

${\mu_o}^{IST}$ wird für 25-MB-Dokumente wie folgt gemittelt:

$$ {\mu_o}^{IST} = \frac{p_5 {\mu_{5,o}}^{IST} + p_6 {\mu_{6,o}}^{IST} + p_7 {\mu_{7,o}}^{IST}}{p_5 + p_6 + p_7} $$

HighSpeed-Konnektor

In der Lastsituation für 8 Anwendungen ergeben sich verschiedene Situationen in Bezug auf die parallele Bearbeitung von Anfragen, dargestellt in Tabelle Tab_gemSpec_Perf_HighSpeed_QES-Konnektor_Lastsituationen.

Tab_gemSpec_Perf_HighSpeed_QES-Konnektor_Lastsituationen

Situationen i					
i	25 MB [Anzahl]	100 kB [Anzahl]	Wahrscheinlichkeiten p_i		
			CMS, CAdES	XMLEnc, XAdES	CMS, PAdES
1	0	0	12	11	14
2	0	1	22	21	23
3	0	2	20	20	19
4	0	3	12	12	11
5	0	4	6	6	5
6	0	5	2	2	2
7	1	0	3	4	4
8	1	1	6	7	7
9	1	2	6	6	6

10	1	3	4	4	3
11	1	4	2	2	1
12	2	2	3	4	4

Für jede der Lastsituationen i in Tab_gemSpec_Perf_HighSpeed_QES-Konnektor_Lastsituationen ist eine Messreihe zu erstellen. In jeder Messreihe sind vom Clientsystem jeweils ein Aufruferthread pro parallele Bearbeitung zu starten, der 100 mal sign_Document, encrypt_Document, decrypt_Document und verify_Document sequentiell, direkt nacheinander aufruft. In Lastsituation 12 sind es beispielsweise 2 Threads, die 25 MB große Dokumente bearbeiten, und 2 Threads, die 100 kB große Dokumente bearbeiten.

Für jede der Lastsituationen i und die Operationen o sind die Mittelwerte ${\mu_{i,o}}^{IST}$ der Bearbeitungszeiten für die beiden Klassen 25 MB-Dokumente und 100 kB-Dokumente zu bestimmen.

Durch den Test ist nachzuweisen, dass die über die Lastsituationen gemittelte Bearbeitungszeit ${\mu_o}^{IST}$ für jede Operation o kleiner als die vorgegebene Bearbeitungszeit ${\mu_o}^{SOLL}$ gemäß Tab_gemSpec_Perf_QES-Konnektor_Skalierungsfähigkeit_Bearbeitungszeitvorgaben ist:

$$ {\mu_o}^{IST} < {\mu_o}^{SOLL} $$

${\mu_o}^{IST}$ wird für 100 kB Dokumente wie folgt gemittelt:

$$ {\mu_o}^{IST} = \frac{\sum_{i=2,3,4,5,6,8,9,10,11,12} p_i {\mu_{i,o}}^{IST}}{\sum_{i=2,3,4,5,6,8,9,10,11,12} p_i} $$

${\mu_0}^{IST}$ wird für 25 MB Dokumente wie folgt gemittelt:

$$ {\mu_o}^{IST} = \frac{\sum_{i=7}^{12} p_i {\mu_{i,o}}^{IST}}{\sum_{i=7}^{12} p_i} $$

<u>Rahmenbedingungen</u>

Folgende konkretisierende Rahmenbedingungen gelten für Einbox-Konnektoren und HighSpeed-Konnektoren gleichermaßen zusätzlich zu den generellen Rahmenbedingungen für die Messungen aus Kapitel 4.1.2:

- Die Messungen werden mit den Referenzdokumenten TIFF_25MB und TEXT_100KB durchgeführt.
- Es wird im Offline-Modus (MGM_LU_ONLINE = Disabled) getestet.
- Pro Aufruferthread wird eine Karte und ein Kartenterminal für Signatur und Entschlüsselung eingesetzt.
- Für die einzelnen Operationen wird konkretisiert:
    - sign_Document: nonQES
    - verify_Document: Signatur verifizieren, die in sign_Document erzeugt wurde, IncludeRevocationInfo=false

- encrypt_Document: ein Empfänger
- decrypt_Document: Dokument entschlüsseln, das mit encrypt_Document verschlüsselt wurde.