Einführung der Gesundheitskarte

Errata zu Release 1.6.4 Online-Rollout (Stufe 1) Erprobung und Produktivbetrieb

führt zu

Release 1.6.4-1

Version:	1.0.0
Stand:	12.07.2017
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_R1.6.4-1]

Betroffene Produkttypen	Neue Produkttypversion
gemProdT_X.509_TSP_QES	1.7.1-0
gemProdT_X.509_TSP_nonQES_ SMC-B	1.8.0-0
gemProdT_Kon	1.10.1-0
gemProdT_Kon (mit QES)	2.11.1-0
gemProdT_VPN_ZugD	1.7.2-0

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6128	gemSpec_PKI		**HBA-QES-Zertifikatsprofil Anpassungen** Es gibt mehrere kleine Konsistenzfehler bzw. Unklarheiten in den kürzlich übernommenen sektorspezifischen QES-HBA-Zertifikats-Profilen. Diese sollen behoben werden. Wenn diese Änderung nicht umgesetzt wird, bleiben einige Unklarheiten bei Anbietern als auch bei der Testung bestehen.	Anlage C_6128	gemSpec_PKI gemProdT_X.509_TSP_QES
C_6127	gemSpec_Krypt	GS-A_5508	**IPsec, Re-Authentication mit make_before_break** Die Erprobung hat ergeben, dass es zu vielen Fehlern bei der Anwendung VSDM kommt, weil die IPsec-Verbindung vom Konnektor zum VPN-Konzentrator TI während der Re-Authentication für eine kurze Zeit abbricht. Um diese Fehler zu vermeiden, wird das Verfahren für die Re-Authentication angepasst.	neue Anforderung **GS-A_5508 IPsec-Kontext – Re-Authentication** Alle Produkttypen, die mittels IPsec-Daten schützen, SOLLEN die Re-Authentication durchführen, indem die neue IPsec-SA aufgebaut wird bevor die bestehende IPsec-SA gelöscht wird.	gemSpec_Krypt gemProdT_Kon
C_6126	gemSpec_Kon	TAB_KON_689	Aktuell wird der Timeout-Parameter für OCSP-Abfragen (CERT_OCSP_TIMEOUT_NONQES/QES) einheitlich auf 10s als Defaultwert in TUC_PKI_006/_018/_030 festgelegt. Ferner wird mittels TUC-Anmerkungen in gemSpec_PKI klargestellt, dass der Parameter in zertifikatsprüfenden Komponenten konfigurierbar sein muss. Der Default-Wert stammt von Default-Konfiguration verschiedener OCSP-Produkte. Die laufende Erprobung hat ergeben, dass der Default-Wert zu groß ist und eine zu lange Wartezeit erfordert, falls der OCSP-Responder nicht antwortet. Der Default-Wert sollte verkleinert werden.	Nach der Regel „ist T_OCSP die durchschnittliche OCSP-Bearbeitungszeit (OCSP response time, für NONQES 1s, für QES 2s), so ist der Default-Wert für den Timeout-Parameter höchstens mit dem Faktor 3 zu setzen“ wird folgende Änderung in der Tabelle TAB_KON_689 in den entsprechenden Zeilen mit den Werten CERT_OCSP_TIMEOUT_NONQES und CERT_OCSP_TIMEOUT_QES in der Spalte ReferenzID umgesetzt: ---------- *alt* CERT_OCSP_TIMEOUT_NONQES: Timeout für OCSP-Abfragen bei der Prüfung von nonQES-Zertifikaten. Der Wert MUSS zwischen 1 und **120** Sekunden liegen. Default-Wert = **10** Sekunden CERT_OCSP_TIMEOUT_QES Timeout für OCSP-Abfragen bei der Prüfung von QES-Zertifikaten. Der Wert MUSS zwischen 1 und **120** Sekunden liegen. Default-Wert = **10** Sekunden ---------- *neu* CERT_OCSP_TIMEOUT_NONQES: Timeout für OCSP-Abfragen bei der Prüfung von nonQES-Zertifikaten. Der Wert MUSS zwischen 1 und **30** Sekunden liegen. Default-Wert = **3** Sekunden CERT_OCSP_TIMEOUT_QES Timeout für OCSP-Abfragen bei der Prüfung von QES-Zertifikaten. Der Wert MUSS zwischen 1 und **30** Sekunden liegen. Default-Wert = **6** Sekunden	gemSpec_Kon gemProdT_Kon
C_6117	gemSpec_Perf	Kapitel 4.1.2 Produkttyp Konnektor	**Performanceanforderung für IPsec Tunnel TI und SIS** Es fehlt eine Anforderung, die verhindert, dass der Konnektor eine unnötige Einschränkung des Durchsatzes über das Transportnetz durch die IPsec-Tunnel TI und SIS verursacht.	Anlage C_6117	gemSpec_Perf gemProdT_Kon gemProdT_VPN_ZugD

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6116	gemSpec_VPN_ZugD	TIP1-A_5103: Tab_ZD_Nameserver_Int_RR TIP1-A_4373: Tab_ZD_TUC_IPsec_Tunnel_TI_aufbauen TIP1-A_4397: Tab_ZD_TUC_IPsec_Tunnel_SIS_aufbauen	**Hash & URL Server Anpassung** Sind mehrere Hash & URL Server beim VPN-Zugangsdienst installiert, ist bisher nicht vereinbart wie bei einem "Standortwechsel im Fehlerfall" zu verfahren ist. Bei unterschiedlicher Umsetzung kann es somit zu einem Interoperabilitätproblem kommen.	TIP1-A_5103: Tab_ZD_Nameserver_Int_RR alt: _hashandurl._tcp.<DNS_DOMAIN_VPN_ZUGD_INT> SRV Resource Record zur Ermittlung der URL des hash&URL-Servers HASH_AND_URL_SERVER_FQDN A Resource Records zur Namensauflösung des FQDN des hash&URL Servers in IP-Adressen neu: _hashandurl._tcp.<DNS_DOMAIN_VPN_ZUGD_INT> SRV Resource Record zur Ermittlung der URL der hash&URL-Server HASH_AND_URL_SERVER_FQDN A Resource Records zur Namensauflösung von FQDN der hash&URL Server in IP-Adressen TIP1-A_4373: Tab_ZD_TUC_IPsec_Tunnel_TI_aufbauen TIP1-A_4397: Tab_ZD_TUC_IPsec_Tunnel_SIS_aufbauen alt: Verbindungsaufbau • Der Konnektor empfängt vom VPN-Konzentrator das Zertifikat C.VPNK.VPN. Falls HASH_AND_URL = Enabled muss das Hash & URL Verfahren gemäß [RFC5996] oder [RFC7296] zum Austausch der Zertifikate zwischen Konnektor und VPN-Konzentrator verwendet werden. neu: • Der Konnektor empfängt vom VPN-Konzentrator das Zertifikat C.VPNK.VPN. Falls HASH_AND_URL = Enabled muss das Hash & URL Verfahren gemäß [RFC5996] oder [RFC7296] zum Austausch der Zertifikate zwischen Konnektor und VPN-Konzentrator verwendet werden. Sind mehrere Hash & URL Server per SRV Resource Record konfiguriert, muss bei Nichterreichbarkeit eines Hash & URL Servers der nächste verfügbare Hash & URL Server verwendet werde.	gemSpec_VPN_ZugD gemProdT_Kon
C_6090	gemSpec_PKI	Tab_SMCB_KZBV_KZV	Der Object Identifier (OID) <oid_policy_gem_or_cp_smcb_erprobung> wurde zur Bezeichnung der SMC-B-Policy für die Erprobung definiert, im Produktivbetrieb (OPB1) wird diese Policy und somit der zugerehörige OID nicht mehr verwendet. Trotzdem tauch der OID noch in der SMC-ORG-Ausprägung für KZVen (Tab_SMCB_KZBV_KZV) auch in der OPB1-Version der gemSpec_PKI noch auf.	In der [gemSpec_PKI] für das OPB1-Release wird der policyIdentifier <oid_policy_gem_or_cp_smcb_erprobung> aus der Tabelle "Tab_SMCB_KZBV_KZV SMC-B-Zertifikate für KZV (Sektor KZBV)" gestrichen: CertificatePolicies {2 5 29 32}; siehe Kap 5.3.4 ~~zusätzlich: policyIdentifier = <oid_policy_gem_or_cp_smcb_erprobung>;~~	gemSpec_PKI gemProdT_X.509_TSP_nonQES_SMC-B

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6080	gemSpec_Kon	Kapitel 4.2.1.6 Betriebsaspekte 4.3.9.3.4 TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“ 4.2.1.1.1 Netzwerksegmentierung Anhang E - Übersicht Konfigurationsparameter und Zustandswerte	Als Ergebnis der Erprobung soll eine Aktivierung der durch die Konfigurationsdatei "Bestandsnetze.xml" bereitgestellten Bestandsnetze standardmäßig erfolgen, damit sichergestellt ist, dass alle Leistungserbringerinstitutionen mit der Default-Einstellung des Konnektors Zugang zu den Bestandsnetzen haben.	Anlage C_6080	gemSpec_Kon gemProdT_Kon gemKPT_Arch_TIP
C_6136	gemKPT_Betr, gemRL_Betr	diverse Stellen + TIP1-A_6358 gestr. TIP1-A_6361 gestr. neu: TIP1-A_6456 neu: TIP1-A_6457	Im Zuge der ersten Erkenntnissen der Erprobung und in Vorbereitung auf den startenden Produktivbetrieb wurde entschieden, auf Zertifizierungen der Dienstleister-Vor-Ort (DVO) zu verzichten. Stattdessen werden die Serviceprovider Endnutzernaher Dienste (SPED) in ihrem Kooperationsvertrag mit der gematik verpflichtet, Ihre DVOs regelmäßig zu schulen.	Im Dokument **gemKPT_Betr** wird der Begriff "Zertifizierung" gelöscht; darüber hinaus werden zwei neue Anforderungen gestellt: neu: TIP1-A_6456 Regelmäßige Schulungen der DVO durch den SPED neu: TIP1-A_6457 Vorlage eines Mustervertrages durch den SPED Im Dokument **gemRL_Betr** wird der Begriff "ZDVO" durch "DVO" ersetzt. Die Änderungen wirken sich auf den **Anbietertypsteckbrief SPED** aus.	gemKPT_Betr gemRL_Betr gemAnbT_SPED
C_6170	gemKPT_PKI_TIP	Kap. 2.7.3.3 Herausgeber der SMC-B	In der beschreibenden Aufzählung zur Herausgabe der SMC-B fehlen ergänzende Hinweise bezüglich der TSP-Sektorzulassung für SMC-B Profil 2ZA Karten. Wird die Änderung nicht umgesetzt, bleiben Festlegungen zur TSP-Sektorzulassung im Bereich Vertragszahnärzteschaft ungeklärt.	Der Passus in gemKPT_PKI_TIP bzgl. der Verantwortlichkeit für die Herausgabe der SMC-B für Vertragszahn-ärzte/Vertragszahnarztpraxis wird wie folgt angepasst: **ALT:** "~~• Für den jeweiligen Vertragszahnarzt /Vertragszahnarztpraxis zuständige KZV: Zahnarztpraxis mit vertragszahnärztlicher Zulassung (die jeweils zuständige KZV ist zudem berechtigt, auch SMC-B für Zahnärzte auszugeben, die sich im Zulassungsverfahren zur vertragszahnärztlichen Zulassung befinden)~~," **NEU:** "• Für den jeweiligen Vertragszahnarzt /Vertragszahnarztpraxis zuständige KZV: Zahnarztpraxis mit vertragszahnärztlicher Zulassung (die jeweils zuständige KZV ist zudem berechtigt, auch SMC-B für Zahnärzte auszugeben, die sich im Zulassungsverfahren zur vertragszahnärztlichen Zulassung befinden). Die abschließenden Regelungen zur Antragsberechtigung werden von der jeweils zuständigen KZV festgelegt. Die TSP-Sektorzulassung im Bereich Vertragszahnärzteschaft für SMC-B Profil 2ZA wird von der KZBV durchgeführt."	gemKPT_PKI_TIP
C_6115	gemSpec_PKI	Tab_PKI_215	Im QES-CA-Zertifikat sind die Einträge zum policyIdentifier und zum QCStatement QcCompliance verpflichtend gefordert, obwohl sie lt. Standard nicht vorgeschrieben sind. Wenn diese Änderung nicht umgesetzt wird, bleiben einige Einträge verpflichtend, obwohl sie lt. Standard optional sind.	In der Extension "CertificatePolicies {2 5 29 32}": alt: Inhalt "policyIdentifier = <id-etsi-qcp-natural-qscd>", Kar. "1" neu: Inhalt "policyIdentifier = <id-etsi-qcp-natural-qscd>", Kar. "**0-1**" In der Extension "QCStatements {1.3.6.1.5.5.7.1.3}": alt: Inhalt "<id-etsi-qcs-QcCompliance> {0.4.0.1862.1.1}", Kar. "1" neu: Inhalt "<id-etsi-qcs-QcCompliance> {0.4.0.1862.1.1}", Kar. "**0-1**"	gemSpec_PKI gemProdT_X.509_TSP_QES

Änderungsbedarf in gemSpec_Kon

Kapitel 4.2.1.6 Betriebsaspekte

Tabelle 270: TAB_KON_624 - Konfigurationsparameter der Anbindung LAN/WAN"

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
ANLW_ANBINDUNGS_MODUS	InReihe	Der Konnektor ist in Reihe zu dem IAG der Einsatzumgebung geschaltet. Wenn ANLW_WAN_ADAPTER_MODUS= ENABLED befindet sich der Konnektor in diesem Anbindungsmodus. Der Administrator MUSS diesen Wert einsehen und DARF ihn NICHT ändern können.
	Parallel	Der Konnektor ist parallel (zu allen bestehenden Systemen) ins Netzwerk der Einsatzumgebung angebunden. Wenn ANLW_WAN_ADAPTER_MODUS= DISABLED befindet sich der Konnektor in diesem Anbindungsmodus. Der Administrator MUSS diesen Wert einsehen und DARF ihn NICHT ändern können.
ANLW_INTERNET_MODUS	SIS	Der (am Konnektor LAN-seitig ankommende) Internet-Traffic wird per VPN an den SIS geschickt.
	IAG	Bei Anfragen ins Internet wird der Aufrufer per ICMP-Redirect (Type 5) auf die Route zum IAG verwiesen. Wenn (ANLW_ANBINDUNGS_MODUS = InReihe) DARF dieser Wert NICHT auswählbar sein - statt dessen MUSS dann der Wert SIS verwendet werden.
	KEINER	Es wird kein Traffic ins Internet geroutet
ANLW_INTRANET_ROUTES_MODUS	REDIRECT	Der Konnektor MUSS sicherstellen, dass dieser Wert nur gesetzt werden kann, wenn der Administrator zuvor ein oder mehrere Intranet (ANLW_LEKTR_INTRANET_ROUTES) definiert hat.

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
	BLOCK	Der Konnektor MUSS alle IP-Pakete für ein Intranet (gemäß ANLW_LEKTR_INTRANET_ROUTES) ablehnen.
ANLW_WAN_ADAPTER_MODUS	ENABLED	Dieser Parameter ändert den Interface-Status des WAN-Adapters. Der Administrator MUSS diesen Wert einsehen können. Der Administrator MUSS diesen Wert ändern können.
	DISABLED	Dieser Parameter ändert den Interface-Status des WAN-Adapters. Der Administrator MUSS diesen Wert einsehen können. Der Administrator MUSS diesen Wert ändern können.
ANLW_LEKTR_INTRANET_ROUTES	Tupel aus Netzwerksegment und dazugehörigem Next-Hop	Der Administrator MUSS in diese Liste Einträge hinzufügen, editieren und löschen können. Liste von Routen zur Erreichung der Clientsysteme und Kartenterminals vom Konnektor; jeweils mit IP-Netzwerk dazugehörigem Next Hop. Die Netzwerksegmente DÜRFEN NICHT mit den Netzbereichen - NET_SIS - NET_TI_DEZENTRAL NET_TI_ZENTRAL - NET_TI_OFFENE_FD - NET_TI_GESICHERTE_FD - ANLW_BESTANDSNETZE kollidieren.
ANLW_SERVICE_TIMEOUT	X Sekunden	Der Administrator MUSS die maximale Zeit konfigurieren können, in der ein Service antworten muss, bevor das System einen Timout-Fehler meldet. Default-Wert: 60 Sekunden
ANLW_IAG_ADDRESS	IP Adresse	ANLW_IAG_ADDRESS ist die Adresse des Default Gateways. Diese IP-Adresse MUSS

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
		innerhalb des ANLW_WAN_NETWORK_SEGMENT liegen. Die Adresse wird entweder über DHCP automatisch (DHCP_CLIENT_WAN_STATE=ENABLED oder DHCP_CLIENT_LAN_STATE=ENABLED) oder anderenfalls manuell durch den Administrator konfiguriert. Bei automatischer Konfiguration per DHCP MUSS der Administrator den Wert von ANLW_IAG_ADDRESS ausschließlich einsehen können.
ANLW_AKTIVE_BESTANDSNETZE	Liste von IP-Address-Segmenten	Der Administrator MUSS manuell aus der empfangenen Liste der zur Verfügung stehenden Bestandsnetzen (gemäß TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“) einzelne deaktivieren, bzw. nach vorheriger Deaktivierung, freischalten können. Nur die freigegeben Bestandsnetze werden in dieser Variablen erfasst. Nur die freigegebenen Bestandsnetze sind aus den Netzwerken der Einsatzumgebung erreichbar. Wird eine Änderung an der Liste der freigegebenen Bestandsnetze vorgenommen, so MUSS der Konnektor für jedes freigegebene Bestandsnetz in DNS_SERVERS_BESTANDSNETZE ein DNS-Referer-Eintrag für jede der dazugehörigen Domains mit allen zugehörigen DNS-Servern im Konnektor hinterlegen. Die Werte hierzu werden der via TUC_KON_283 aktualisierten Bestandsnetze.xml entnommen. Für „nicht freigegebene“ oder zwischenzeitlich gelöschte Bestandsnetze DARF der Konnektor NICHT Referer-Einträge in DNS_SERVERS_BESTANDSNETZE enthalten. Die Einträge in DHCP_AKTIVE_BESTANDSNETZE_ROUTES sind entsprechend zu aktualisieren. Der Konnektor MUSS nach jeder Änderung dieser Variablen durch den Administrator den TUC_KON_304 „Netzwerk-Routen einrichten“ aufrufen.
ANLW_IA_BESTANDSNETZE	AN	Der Konnektor MUSS alle über TUC_KON_283 übermittelten Bestandsnetze aktivieren. Eine spätere manuelle

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
		Deaktivierung über das Management-Interface durch den Administrator ist möglich. Dieses Verhalten ist als Standartverhalten zu konfigurieren.
	AUS	Der Konnektor MUSS alle über TUC_KON_283 übermittelten Bestandsnetze anbieten, diese aber nicht aktivieren. Eine spätere manuelle Aktivierung erfolgt über das Mangement-Interface durch den Administrator.

4.3.9.3.4 TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“

⌦ TIP1-A_5153 TUC_Kon_283 „Infrastruktur Konfiguration aktualisieren“

Der Konnektor MUSS den technischen Use Case TUC_Kon_283 „Infrastruktur Konfiguration aktualisieren“ umsetzen.

Tabelle 321: TAB_KON_799 - TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“

Element	Beschreibung
Name	TUC_KON_283 Infrastruktur Konfiguration aktualisieren
Beschreibung	Dieser TUC liest die Infrastrukturdaten vom KSR ein.
Auslöser	Automatisch einmal täglich; BOOTUP, Administrator
Vorbedingungen	Der TUC_KON_304 „Netzwerk-Routen einrichten“ MUSS fehlerfrei durchgelaufen sein. Der TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“ MUSS fehlerfrei durchgelaufen sein.
Eingangsdaten	Keine
Komponenten	Konnektor, Konfigurationsdienst
Ausgangsdaten	Keine
Standardablauf	Der Konnektor MUSS folgende Schritte durchlaufen: 1. „Einlesen des Konfigurations-XML“: a) Der Konnektor MUSS eine TLS-Verbindung zum Konfigurationsdienst anhand des in MGM_KSR_KONFIG_URL angegebenen Parameters aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels TUC_KON_037 "Zertifikat prüfen" {C.ZD.TSL-S; not_required; ; true; oid_zd_tls_s; digitalSignature&keyEncipherment; id-kp-serverAuth; ; OCSP} auf Gültigkeit prüfen. Das Server-Zertifikat C.ZD.TLS-S MUSS für den Konfigurationsdienst ausgestellt sein. b) Herunterladen der Konfigurationsdaten mittels I_KSRS_Download::get_Ext_Net_Config (MGM_KSR_KONFIG_URL, „Bestandsnetze.xml“) c) Beenden der TLS-Verbindung 2. „Prüfen der Versionskennung auf Änderungen“: Wenn das Element /Infrastructure/Version der heruntergeladenen Datei keine höhere Versionsnummer als die aktuell im Konnektor hinterlegte Version trägt, muss der TUC ohne Fehler beendet werden. 3. Aktualisieren der Gesamtnetzliste. Alle in der Datei enthaltenen Netzsegmente sind nach

Element	Beschreibung
	ANLW_BESTANDSNETZE zu übernehmen. In Abhängigkeit von ANLW_IA_BESTANDSNETZE sind neue Bestandsnetze nach ANLW_AKTIVE_BESTANDSNETZE zu übernehmen. War der Aktivierungsstatus eines Bestandsnetzes bereits durch den Administrator manuell konfiguriert, so muss dieser Status erhalten bleiben. 4. „Aktualisieren von Konfigurationsinformationen“ Haben sich Konfigurationsdaten zu einem in ANLW_AKTIVE_BESTANDSNETZE gelisteten Netz verändert, so a) sind die Änderungen entsprechend zu übernehmen und zu aktivieren (Anpassung ANLW_AKTIVE_BESTANDSNETZE, DHCP_AKTIVE_BESTANDSNETZE_ROUTES, DNS_SERVERS_BESTANDSNETZE). b) ist anschließend TUC_KON_304 „Netzwerk-Routen einrichten“ aufzurufen ~~War ein Bestandsnetz bereits durch den Administrator freigegeben, so muss diese Freigabe erhalten bleiben.~~ 5. „Entfernen von nicht mehr gültigen Bestandsnetzen“ Ist ein Netz in der neuen Datei gegenüber der alten Datei nicht mehr vorhanden, so: a) sind alle diesbezüglichen Daten zu entfernen und die Änderungen direkt aktiv zu schalten (Anpassung ANLW_AKTIVE_BESTANDSNETZE, DHCP_AKTIVE_BESTANDSNETZE_ROUTES, DNS_SERVERS_BESTANDSNETZE). b) ist anschließend TUC_KON_304 „Netzwerk-Routen einrichten“ aufzurufen.
Varianten / Alternativen	Keine
Fehlerfälle	(→ 1-5) Es ist ein unerwarteter Fehler aufgetreten; Fehlercode: 4198
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 322: Tab_Kon_726 Übersicht Fehler TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4198	Technical	Error	Beim Übernehmen der Bestandsnetze ist ein Fehler aufgetreten.

⌫

4.2.1.1.1 Netzwerksegmentierung

In Anlehnung an die in der [gemSpec_Net#2.3.3] definierten Netzwerksegmente werden in der Konnektorspezifikation die folgenden Bezeichner verwendet:

Tabelle 257: TAB_KON_680 Mapping der Netzwerksegmente

ReferenzID im Konnektor	Adressbereich für die TI-Produktivumgebung	Adressbereich für die TI-Testumgebung	Adressbereich für die TI-Referenz-umgebung
NET_SIS	TI_Dezentral_SIS - Konnektoren	TI_Test_Dezentral_SIS - Konnektoren	Ist durch den Testbetriebs-verantwortlichen zu definieren.
NET_TI_DEZENTRAL	TI_Dezentral - Konnektoren	TI_Test_Dezentral - - Konnektoren	Ist durch den Testbetriebs-verantwortlichen zu definieren.
NET_TI_ZENTRAL	TI_Zentral - Zentrale Dienste	TI_Test_Zentral - Zentrale Dienste	Ist durch den Testbetriebs-verantwortlichen zu definieren.
NET_TI_OFFENE_FD	TI_Fachdienste - Offene Fachdienste	TI_Test_Fachdienste - Offene Fachdienste	Ist durch den Testbetriebs-verantwortlichen zu definieren.
NET_TI_GESICHERTE_FD	TI_Fachdienste - Gesicherte Fachdienste	TI_Test_Fachdienste - Gesicherte Fachdienste	Ist durch den Testbetriebs-verantwortlichen zu definieren.
NET_LEKTR	Liste der Netzwerke die in der Einsatzumgebung über den Konnektor erreichbar sind. Ein Eintrag der Liste enthält die Netzwerkadresse und den Netzwerkprefix.		
ANLW_BESTANDSNETZE	Liste der an die TI angeschlossenen Bestandsnetze (u. a. das Sichere Netz der KVen). Ein Eintrag der Liste enthält die Netzwerkadresse und den Netzwerkprefix.		
ANLW_AKTIVE_BESTANDSNETZE	Liste der an die TI angeschlossenen und ~~vom Administrator freigegebenen~~ aktivierten Bestandsnetze		

Anhang E - Übersicht Konfigurationsparameter und Zustandswerte

ACHTUNG: nur Auszug !!!

	ANLW_AKTIVE_BESTANDSNETZE	Liste von IP-Address-Segmenten	Der Administrator MUSS manuell aus der empfangenen Liste der zur Verfügung stehenden Bestandsnetzen (gemäß TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“) einzelne freischalten können. Nur die freigegeben Bestandsnetze werden in dieser Variablen erfasst. Nur die freigegebenen Bestandsnetze sind aus den Netzwerken der Einsatzumgebung erreichbar. Wird eine Änderung an der Liste der freigegebenen Bestandsnetze vorgenommen, so MUSS der Konnektor für jedes freigegebene Bestandsnetz in DNS_SERVERS_BESTANDSNETZE ein DNS-Referer-Eintrag für jede der dazugehörigen Domains mit allen zugehörigen DNS-Servern im Konnektor hinterlegen. Die Werte hierzu werden der via TUC_KON_283 aktualisierten Bestandsnetze.xml entnommen. Für „nicht freigegebene“ oder zwischenzeitlich gelöschte Bestandsnetze DARF der Konnektor NICHT Referer-Einträge in DNS_SERVERS_BESTANDSNETZE enthalten. Die Einträge in DHCP_AKTIVE_BESTANDSNETZE_ROUTES sind entsprechend zu aktualisieren. Der Konnektor MUSS nach jeder Änderung dieser Variablen durch den Administrator den TUC_KON_304 „Netzwerk-Routen einrichten“ aufrufen.
	ANLW_IA_BESTANDSNETZE	AN	Der Konnektor MUSS alle über TUC_KON_283 übermittelten Bestandsnetze aktivieren. Eine spätere manuelle

			Deaktivierung über das Management-Interface durch den Administrator ist möglich. Dieses Verhalten ist als Standartverhalten zu konfigurieren.
		AUS	Der Konnektor MUSS alle über TUC_KON_283 übermittelten Bestandsnetze anbieten, diese aber nicht aktivieren. Eine spätere manuelle Aktivierung erfolgt über das Mangement-Interface durch den Administrator.

Änderungsbedarf in gemKPT_Arch_TIP

2.1.4 Kontrolle der Kommunikationswege

…

In der TI-Plattform zentral ist die Kommunikation in Richtung aller zugelassenen Dienste und angeschlossenen Bestandsnetze im Rahmen des Test- und Zulassungsverfahrens freizuschalten. Im dezentralen Bereich ist die Kommunikation zu Pflichtanwendungen gemäß §291a SGB V [SGB V] immer erlaubt. ~~Die Kommunikation in Richtung eines Bestandsnetzes muss durch den Administrator explizit freigeschaltet werden.~~ Die Kommunikation in Richtung aller Bestandsnetze ist grundsätzlich freigeschaltet, kann durch den Administrator aber für jedes einzelne Bestandsnetz explizit unterbunden werden. Dabei wird immer das Bestandsnetz als Ganzes und nicht einzelne Dienste im Bestandsnetz freigeschaltet.

7.2.4.3 Ablauf Bestandsnetzkonfigurationen aktualisieren

TIP1-A_5116 Ablauf Bestandsnetzkonfigurationen aktualisieren

Alle am Ablauf „Bestandsnetzkonfigurationen aktualisieren“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

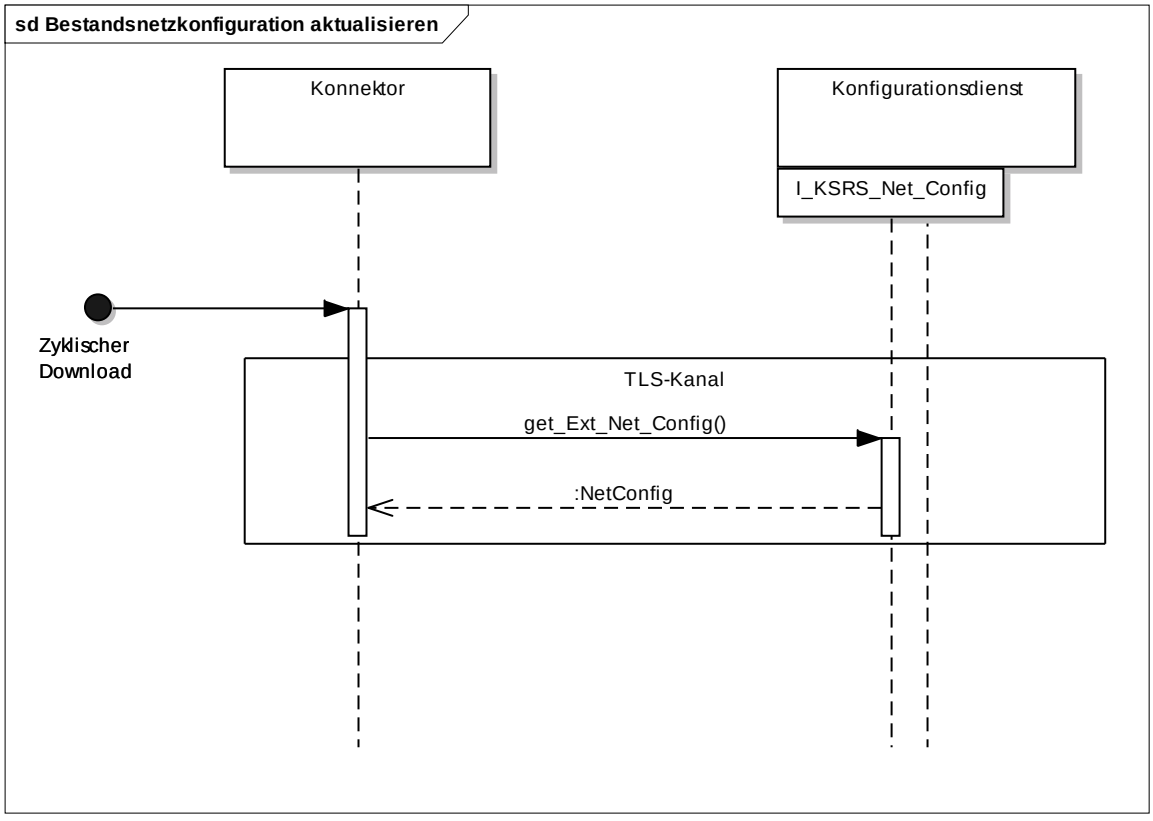

Abbildung 29: Ablauf: Bestandsnetzkonfigurationen aktualisieren

Der Konnektor lädt zyklisch die aktuelle Konfigurationsdatei mit den nötigen Bestandsnetzparametern vom Konfigurationsdienst. Im Fall einer Änderung der Parameter passt der Konnektor seine Konfigurationsmöglichkeiten dementsprechend an.

~~Neu angeschlossene Bestandsnetze müssen im Konnektor durch den Administrator freigeschaltet werden bevor die entsprechende Konfiguration angewendet wird und die Bestandsnetze für angeschlossenen Clientsysteme erreichbar sind.~~

Neu angeschlossene Bestandsnetze sind im Konnektor grundsätzlich freigeschaltet und ihre Konfiguration wird umgehend angewendet. Die Freischaltung eines Bestandsnetzes kann durch den Administrator aber widerrufen werden. In diesem Fall wird die entsprechende Konfiguration gelöscht und das Bestandsnetz ist durch angeschlossene Clientsysteme nicht mehr erreichbar.

Die Konfiguration entfallener Bestandsnetze wird im Konnektor automatisch gelöscht.

Zwischen Konnektor und Konfigurationsdienst wird eine TLS-Verbindung mit einseitiger Authentisierung aufgebaut. Zur Serverauthentisierung wird das X.509-Zertifikat mit der TLS-Server-Identität des Konfigurationsdienstes (ID.ZD.TLS_S) genutzt.⌫

Änderungsbedarf in gemSpec_Perf

Kapitel 4.1.2. Produkttyp Konnektor

Am Ende des Abschnitts "Netzwerkebene" wird folgendes ergänzt:

⌦ GS-A_5509 Performance – Konnektor (Ausbaustufe VSDM) – IPSec-Tunnel TI und SIS

Der Produkttyp Konnektor MUSS einen IPSec Durchsatz von mindestens 25 Mbit/s bidirektional und kontinuierlich erreichen. Der Wert gilt in Summe für IPSec-Tunnel TI und SIS.⌫

Die Anforderung GS-A_5509 gilt ausschließlich für den Konnektor (Ausbaustufe VSDM).

⌦ GS-A_5543 Performance - Konnektor – IPSec-Tunnel TI und SIS

Der Produkttyp Konnektor MUSS einen IPSec Durchsatz von mindestens 30 Mbit/s bidirektional und kontinuierlich erreichen. Der Wert gilt in Summe für IPSec-Tunnel TI und SIS.⌫

Die folgende Abbildung erläutert die Durchsatzmessung.

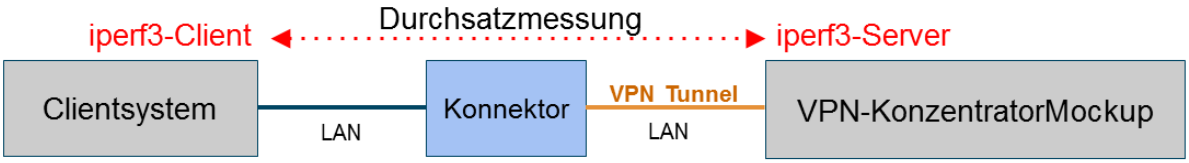

Abbildung x: Messaufbau zum IPSec Durchsatzmessung

Der geforderte IPSec Durchsatz wird unter folgenden Bedingungen ermittelt:

- Über Clientsystem<->Konnektor<->VPNKonzentratorMockup wird zwischen Clientsystem und VPNKonzentratorMockup mittels iperf3 der Durchsatz im Transport über TCP ermittelt.
- IPCompression ist durch Konfiguration am VPNKonzentratorMockup ausgeschaltet

Änderungen in gemProdT_Kon_PTV1

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_Kon_PTV1]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 1: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5509	Performance - Konnektor – IPSec-Tunnel TI und SIS	gemSpec_Perf

Hinweis: GS-A_5543 wird NICHT in gemProdT_Kon_PTV1 aufgenommen

Änderungen in gemProdT_Kon_PTV2

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_Kon_PTV2]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5543	Performance - Konnektor – IPSec-Tunnel TI und SIS	gemSpec_Perf

Hinweis: GS-A_5509 wird NICHT in gemProdT_Kon_PTV2 aufgenommen

Änderungen in [gemSpec_PKI]

Kapitel 5.2 HBA – Heilberufeausweis

[…]

5.2.1.3 C.HP.QES – Qualifizierte Signatur HBA

⌦ **GS-A_5533 Umsetzung Zertifikatsprofil C.HP.QES**
Der TSP-X.509 QES MUSS C.HP.QES gemäß Tab_PKI_270 umsetzen.⌫

Tabelle 29: Tab_PKI_270 C.HP.QES Qualifizierte Signatur HBA

Element	Inhalt *)	Kar.	
certificate	C.HP.QES		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
issuer	Distinguished Name (DN) der Aussteller-CA gemäß [gemSpec_PKI# GS-A_4948]		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName **)	Vor- und Nachname des Inhabers (bei Kürzung ev. Suffix :PN)	1	
title **)	nicht gesetzt	0	
givenName **)	Vorname des Inhabers	1	
surName **)	Nachname des Inhabers	1	
serialNumber **)	Eindeutige Identifikationsnummer (dieselbe wie in AUT und ENC)	1	
organizationalUnitName	nicht gesetzt	0	
organizationName	nicht gesetzt	0	
countryName	DE	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4358] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Inhabers	1	FALSE
KeyUsage {2 5 29 15}	nonRepudiation (laut RFC5280 alternative Bezeichnung „contentCommitment“)	1	**TRUE**
SubjectAltNames {2 5 29 17}	nicht gesetzt	0	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**

Element				Inhalt *)	Kar.	
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = <URL zur Publikation der Zertifikatsrichtlinie(n)> policyIdentifier = <oid_hba_qes> gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie ggf. weitere sektorspezifische policyIdentifier und policyQualifierInfo	1 0-1 1 1 0-1 0-1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst URL des CA-Zertifikats (vgl. EN 319 412-2 Kap. 4.4.1)	1 0-1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = gemäß [gemSpec_OID#GS-A_4442] professionOID = gemäß [gemSpec_OID#GS-A_4442] registrationNumber : Details dazu jeweils in den sektorspezifischen Profilen in Anhang C	1 1 1 0-1	FALSE
			ExtendedKeyUsage {2 5 29 37}	nicht gesetzt	0	FALSE
			ValidityModel {1 3 6 1 4 1 8301 3 5}	id-validity-Model-chain {1 3 6 1 4 1 8301 3 5 1}	1	FALSE
			QCStatements {1 3 6 1 5 5 7 1 3}	esi4-qcStatement-1 mit id-etsi-qcs-QcCompliance {0 4 0 1862 1 1}, statementInfo nicht gesetzt esi4-qcStatement-2 mit id-etsi-qcs-QcLimitValue {0 4 0 1862 1 2}, statementInfo (currency = “EUR”, amount (INT), exponent (INT)) esi4-qcStatement-3 mit id-etsi-qcs-QcRetentionPeriod {0 4 0 1862 1 3} esi4-qcStatement-4 mit id-etsi-qcs-QcSSCD {0 4 0 1862 1 4}, statementInfo nicht gesetzt esi4-qcStatement-5 mit id-etsi-qcs-QcPDS {0 4 0 1862 1 5} esi4-qcStatement-6 mit id-etsi-qct-esign {0 4 0 1862 1 6 1}	1 0-1 0-1 1 0-1 0-1	FALSE
			additionalInformation {1 3 36 8 3 15}	nicht gesetzt	0~~-1~~	FALSE
			Restriction {1 3 36 8 3 8}	Falls das optionale esi4-qcStatement-2 gesetzt und/ oder hier ein ~~weiterer~~ Freitext enthalten ist, muss diese Erweiterung mindestens die folgende Ergänzung enthalten: *Jegliche Beschränkungen gelten nicht für*	0-1	FALSE

Element				Inhalt *)	Kar.	
				Anwendungen gemäß § 291a SGB V.		
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
	signature			Wert der Signatur		

**) Sektorspezifische Ausprägungen der HBA-Zertifikate sind dem Anhang C zu entnehmen.*

***) Kodierung in einem SET als einziges Multivalued Relative Distinguished Name Element (multivaluedRDN) (siehe Hinweis unten unter Zusatzinformationen)*

[…]

Anhang C – Sektorspezifische Ausprägungen der HBA Zertifikate

Die nachfolgenden Profiltabellen der Sektoren referenzieren auf die Festlegungen aus Kap. 5.2.1 für alle sektorübergreifenden Attribute und ergänzen/ersetzen diese um sektorspezifische Ausprägungen.

Die Profiltabellen gelten einheitlich für die Zertifikate:

- C.HP.AUT
- C.HP.ENC
- C.HP.QES

C1 – BÄK

Tabelle 120: Tab_HBA_BÄK HBA-Zertifikate (AUT, ENC, QES) für BÄK

Element				Inhalt	Kar.	
certificate				C.HP.AUT, C.HP.ENC, C.HP.QES		
	tbsCertificate					
		version		*siehe Kap. 5.2.1*		
		serialNumber		*siehe Kap. 5.2.1*		
		signature		*siehe Kap. 5.2.1*		
		issuer		*siehe Kap. 5.2.1*		
		validity		*siehe Kap. 5.2.1*		
		subject				
			commonName	*siehe Kap. 5.2.1*		
			title	*siehe Kap. 5.2.1*		
			givenName	*siehe Kap. 5.2.1*		

Element				Inhalt	Kar.	
			surName	*siehe Kap. 5.2.1*		
			serialNumber	*siehe Kap. 5.2.1*		
			organizationalUnitName	*siehe Kap. 5.2.1*		
			organizationName	*siehe Kap. 5.2.1*		
			countryName	*siehe Kap. 5.2.1*		
			andere Attribute	*siehe Kap. 5.2.1*		
		subjectPublicKeyInfo		*siehe Kap. 5.2.1*		
		extensions				critical
			SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.2.1*		FALSE
			KeyUsage {2 5 29 15}	*siehe Kap. 5.2.1*		**TRUE**
			SubjectAltNames {2 5 29 17}	*siehe Kap. 5.2.1*		FALSE
			BasicConstraints {2 5 29 19}	*siehe Kap. 5.2.1*		**TRUE**
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://www.e-arztausweis.de/policies/EE_policy.html policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier = 1.3.6.1.4.1.42675.1.1: CPME European eID-Policy for Physicans policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 1 0-1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	*siehe Kap. 5.2.1*		FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.2.1*		FALSE
			AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.2.1*		FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige bestätigende Ärztekammer>,C=DE} professionItem = „Ärztin/Arzt“ (siehe [gemSpec_OID#GS-A_4442]) professionOID = <oid_arzt> (siehe [gemSpec_OID#GS-A_4442]) registrationNumber = Telematik-ID des Inhabers… ~~(nur~~ … für AUT und ENC zwingend, … für QES optional	1 1 1 ~~1~~ 1 0-1	FALSE
			ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.2.1*		FALSE
			ValidityModel {1 3 6 1 4 1 8301 3 5}	*siehe Kap. 5.2.1*		FALSE
			QCStatements {1 3 6 1 5 5 7 1 3}	*siehe Kap. 5.2.1*		FALSE

Element				Inhalt	Kar.	
			additionalInformation {1 3 36 8 3 15}	*siehe Kap. 5.2.1*		FALSE
			Restriction {1 3 36 8 3 8}	*siehe Kap. 5.2.1*		FALSE
			andere Erweiterungen	*siehe Kap. 5.2.1*		
	signatureAlgorithm			*siehe Kap. 5.2.1*		
	signature			*siehe Kap. 5.2.1*		

C2 – BZÄK

Tabelle 121: Tab_HBA_BZÄK HBA-Zertifikate (AUT, ENC, QES) für BZÄK

Element				Inhalt *)	Kar.	
certificate				C.HP.AUT, C.HP.ENC, C.HP.QES		
	tbsCertificate					
		version		*siehe Kap. 5.2.1*		
		serialNumber		*siehe Kap. 5.2.1*		
		signature		*siehe Kap. 5.2.1*		
		issuer		*siehe Kap. 5.2.1*		
		validity		*siehe Kap. 5.2.1*		
		subject				
			commonName	*siehe Kap. 5.2.1*		
			title	*siehe Kap. 5.2.1*		
			givenName	*siehe Kap. 5.2.1*		
			surName	*siehe Kap. 5.2.1*		
			serialNumber	*siehe Kap. 5.2.1*		
			organizationalUnitName	*siehe Kap. 5.2.1*		
			organizationName	*siehe Kap. 5.2.1*		
			countryName	*siehe Kap. 5.2.1*		
			andere Attribute	*siehe Kap. 5.2.1*		
		subjectPublicKeyInfo		*siehe Kap. 5.2.1*		
		extensions				critical
			SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.2.1*		FALSE
			KeyUsage {2 5 29 15}	*siehe Kap. 5.2.1*		**TRUE**
			SubjectAltNames {2 5 29 17}	*siehe Kap. 5.2.1*		FALSE
			BasicConstraints {2 5 29 19}	*siehe Kap. 5.2.1*		**TRUE**
			CertificatePolicies	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444]	1	FALSE

Element	Inhalt *)	Kar.	
{2 5 29 32}	policyQualifierInfo = http://policies.bzaek.de policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie	0-1 1 (1) 1 0-1 0-1	
CRLDistributionPoints {2 5 29 31}	CDP der ausstellenden CA … ~~- zwingend~~ … für AUT und ENC zwingend, … für QES optional	~~0~~ 1 0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.2.1*		FALSE
AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.2.1*		FALSE
Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Landeszahnärztekammer>,C=DE} professionItem = „Zahnärztin/Zahnarzt“ (siehe [gemSpec_OID#GS-A_4442]) professionOID = <oid_zahnarzt> (siehe [gemSpec_OID#GS-A_4442]) registrationNumber = Telematik-ID des Inhabers	0-1 1 1 1	FALSE
ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.2.1*		FALSE
ValidityModel {1 3 6 1 4 1 8301 3 5}	*siehe Kap. 5.2.1*		FALSE
QCStatements {1 3 6 1 5 5 7 1 3}	*siehe Kap. 5.2.1*		FALSE
additionalInformation {1 3 36 8 3 15}	*siehe Kap. 5.2.1*		FALSE
Restriction {1 3 36 8 3 8}	*siehe Kap. 5.2.1*		FALSE
andere Erweiterungen	*siehe Kap. 5.2.1*		
signatureAlgorithm	*siehe Kap. 5.2.1*		
signature	*siehe Kap. 5.2.1*		

C3 – BPtK

Tabelle 1: Tab_HBA_BPtK HBA-Zertifikate (AUT, ENC, QES) für BPtK

Element	Inhalt *)	Kar.	
certificate	C.HP.AUT, C.HP.ENC, C.HP.QES		
tbsCertificate			
version	*siehe Kap. 5.2.1*		
serialNumber	*siehe Kap. 5.2.1*		
signature	*siehe Kap. 5.2.1*		
issuer	*siehe Kap. 5.2.1*		

Element			Inhalt *)	Kar.	
		validity	*siehe Kap. 5.2.1*		
		subject			
		commonName	*siehe Kap. 5.2.1*		
		title	*siehe Kap. 5.2.1*		
		givenName	*siehe Kap. 5.2.1*		
		surName	*siehe Kap. 5.2.1*		
		serialNumber	*siehe Kap. 5.2.1*		
		organizationalUnitName	*siehe Kap. 5.2.1*		
		organizationName	*siehe Kap. 5.2.1*		
		countryName	*siehe Kap. 5.2.1*		
		andere Attribute	*siehe Kap. 5.2.1*		
		subjectPublicKeyInfo	*siehe Kap. 5.2.1*		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.2.1*		FALSE
		KeyUsage {2 5 29 15}	*siehe Kap. 5.2.1*		**TRUE**
		SubjectAltNames {2 5 29 17}	*siehe Kap. 5.2.1*		FALSE
		BasicConstraints {2 5 29 19}	*siehe Kap. 5.2.1*		**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://www.e-psychotherapeutenausweis.de/policies/EE_policy.html policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 0-1 0-1	FALSE
		CRLDistributionPoints {2 5 29 31}	*siehe Kap. 5.2.1*		FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.2.1*		FALSE
		AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.2.1*		FALSE
		Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Landespsychotherapeutenkammer>,C=DE} Eine oder zwei professionInfo-Elemente bestehend aus: professionItem = „Psychologische/-r Psychotherapeut/-in“ und/oder professionItem = „Kinder- und Jugendlichenpsychotherapeut/-in“ (siehe [gemSpec_OID#GS-A_4442]) professionOID = <oid_ps_psychotherapeut> und/oder professionOID = <oid_kuj_psychotherapeut> (siehe [gemSpec_OID#GS-A_4442]) registrationNumber = Telematik-ID des Inhabers…	0-1 1-2 ~~1-2~~ ~~1-2~~	FALSE

Element	Inhalt *)	Kar.	
	… für AUT und ENC zwingend, … für QES optional (Diese muss dann in mindestens einem professionInfo-Element aufgeführt sein)	~~1~~ 1 0-1	
ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.2.1*		FALSE
ValidityModel {1 3 6 1 4 1 8301 3 5}	*siehe Kap. 5.2.1*		FALSE
QCStatements {1 3 6 1 5 5 7 1 3}	*siehe Kap. 5.2.1*		FALSE
additionalInformation {1 3 36 8 3 15}	*siehe Kap. 5.2.1*		FALSE
Restriction {1 3 36 8 3 8}	*siehe Kap. 5.2.1*		FALSE
andere Erweiterungen	*siehe Kap. 5.2.1*		
signatureAlgorithm	*siehe Kap. 5.2.1*		
signature	*siehe Kap. 5.2.1*		

C4 – Apothekerschaft

Tabelle 123: Tab_HBA_BAK HBA-Zertifikate (AUT, ENC, QES) für Apotheker

Element	Inhalt	Kar.	
certificate	C.HP.AUT, C.HP.ENC, C.HP.QES		
tbsCertificate			
version	*siehe Kap. 5.2.1*		
serialNumber	*siehe Kap. 5.2.1*		
signature	*siehe Kap. 5.2.1*		
issuer	*siehe Kap. 5.2.1*		
validity	*siehe Kap. 5.2.1*		
subject			
commonName	*siehe Kap. 5.2.1*		
title	*siehe Kap. 5.2.1*		
givenName	*siehe Kap. 5.2.1*		
surName	*siehe Kap. 5.2.1*		
serialNumber	*siehe Kap. 5.2.1*		
organizationalUnitName	*siehe Kap. 5.2.1*		
organizationName	*siehe Kap. 5.2.1*		
countryName	*siehe Kap. 5.2.1*		
andere Attribute	*siehe Kap. 5.2.1*		
subjectPublicKeyInfo	*siehe Kap. 5.2.1*		
extensions			critical

Element		Inhalt	Kar.	
	SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.2.1*		FALSE
	KeyUsage {2 5 29 15}	*siehe Kap. 5.2.1*		**TRUE**
	SubjectAltNames {2 5 29 17}	*siehe Kap. 5.2.1*		FALSE
	BasicConstraints {2 5 29 19}	*siehe Kap. 5.2.1*		**TRUE**
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = <URL der Apotheker, unter der die o.a. CP aufzurufen ist> policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 0-1 0-1	FALSE
	CRLDistributionPoints {2 5 29 31}	*siehe Kap. 5.2.1*		FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.2.1*		FALSE
	AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.2.1*		FALSE
	Admission {1 3 36 8 3 3}	admissionAuthority = (O= <Apothekerkammer Bezeichnung>, C=DE) professionItem = Genau eine Beschreibung zu <oid_apotheker> bzw. <oid_apothekerassistent> bzw. ...<oid_pharmazieingenieur> bzw. <oid_apothekenassistent>. gemäß [gemSpec_OID#GS-A_4442] professionOID = Genau eine OID der Berufsgruppe <oid_apotheker> bzw. <oid_apothekerassistent> bzw. ...<oid_pharmazieingenieur> bzw. <oid_apothekenassistent> gemäß [gemSpec_OID#GS-A_4442] registrationNumber = Telematik-ID des Inhabers ... ... für AUT und ENC zwingend, ... für QES optional	1 1 1 ~~1~~ 1 0-1	FALSE
	ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.2.1*		FALSE
	additionalInformation	*siehe Kap. 5.2.1*		FALSE
	Restriction	*siehe Kap. 5.2.1*		FALSE
	andere Erweiterungen	*siehe Kap. 5.2.1*		
signatureAlgorithm		*siehe Kap. 5.2.1*		
signature		*siehe Kap. 5.2.1*		