

Einführung der Gesundheitskarte

Spezifikation Kartenpersonalisierung HBA/SMC-B

Version: 1.0.8
Stand: 21.11.2016
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemSpec_Pers_HBA_SMC-B

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.8	21.11.16		freigegeben	

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

Inhaltsverzeichnis

Dokumentinformationen	2
Inhaltsverzeichnis	3
1 Einordnung des Dokumentes	6
1.1 Zielsetzung	6
1.2 Zielgruppe	6
1.3 Geltungsbereich	6
1.4 Abgrenzungen	6
1.5 Methodik.....	6
2 Systemüberblick	8
3 Systemkontext	10
3.1 Akteure und Rollen.....	10
3.2 Nachbarsysteme.....	12
4 Zerlegung des Produkttyps	13
5 Übergreifende Festlegungen	15
5.1 Gesetzliche Anforderungen	15
5.2 Kommunikation	15
5.3 Authentisierung und Signatur	16
5.3.1 Registrierung	21
5.3.1.1 Anforderungen.....	23
5.4 Portale	26
5.5 Datenformate	27
5.6 Löschen.....	30
5.7 Zertifikatshistorie.....	32
5.8 Produktivumgebung.....	32
5.9 Mandantenfähigkeit	34
5.10 Ansprechpartner.....	34
5.11 Betrieb	35
6 Funktionsmerkmale	36

6.1	Vorbefüllung	36
6.1.1	TUC-Beschreibung	36
6.1.2	Ablauf	39
6.1.3	Anforderungen.....	42
6.1.3.1	Anforderungen für alle Varianten der Vorbefüllung	42
6.1.3.2	Anforderungen für die Varianten [VB-1], [VB-2], [VB-4] und [VB-5] der Vorbefüllung.....	44
6.1.3.3	Anforderungen für die Varianten [VB-1], [VB-2], [VB-3] und [VB-4] der Vorbefüllung.....	44
6.1.3.4	Anforderungen für Variante [VB-1].....	45
6.1.3.5	Anforderungen für Variante [VB-2].....	45
6.1.3.6	Anforderungen für Varianten [VB-1], [VB-2] und VB[4].....	46
6.1.3.7	Anforderungen für Variante [VB-3].....	47
6.1.3.8	Anforderungen für Variante [VB-4].....	48
6.1.3.9	Anforderungen für Variante [VB-5].....	48
6.1.4	Artefakte	49
6.1.5	Testunterstützung	49
6.1.6	Hardwaremerkmale	49
6.2	Antragstellung	49
6.2.1	TUC-Beschreibung	53
6.2.2	Ablauf	56
6.2.3	Anforderungen.....	57
6.2.4	Artefakte	68
6.2.5	Testunterstützung.....	68
6.2.6	Hardwaremerkmale	68
6.3	Freigabe	69
6.3.1	TUC-Beschreibung	70
6.3.2	Ablauf	73
6.3.3	Anforderungen.....	74
6.3.4	Artefakte	78
6.3.5	Testunterstützung.....	78
6.3.6	Hardwaremerkmale	79
6.4	Lieferung	79
6.4.1	TUC-Beschreibung	79
6.4.2	Ablauf	82
6.4.3	Anforderungen.....	83
6.4.4	Artefakte	84
6.4.5	Testunterstützung.....	84
6.4.6	Hardwaremerkmale	84
6.5	Sperrung	85
6.5.1	TUC-Beschreibung	85
6.5.2	Ablauf	89
6.5.3	Anforderungen.....	91
6.5.4	Artefakte	93
6.5.5	Testunterstützung.....	93
6.5.6	Hardwaremerkmale	93
6.6	Monitoring und Benachrichtigungen	94
6.6.1	Monitoring.....	94
6.6.1.1	TUC-Beschreibung.....	94

Spezifikation Kartenpersonalisierung HBA/SMC-B

6.6.1.2	Ablauf	97
6.6.1.3	Anforderungen	98
6.6.1.4	Artefakte	105
6.6.1.5	Testunterstützung	105
6.6.1.6	Hardwaremerkmale	105
6.6.2	Benachrichtigungen	105
6.6.2.1	TUC-Beschreibung	105
6.6.2.2	Ablauf	106
6.6.2.3	Anforderungen	107
6.7	Auftrag, Freischaltung und Sperrung über Praxisregister	109
6.7.1	TUC-Beschreibung	109
6.7.2	Ablauf	114
6.7.3	Anforderungen	116
6.7.4	Artefakte	119
6.7.5	Testunterstützung	119
6.7.6	Hardwaremerkmale	119
6.8	Beantragung, Personalisierung und Lieferung von Verifikationskarten ..	119
6.8.1	TUC-Beschreibung	121
6.8.2	Ablauf	122
6.8.3	Registrierung der BVK	123
6.8.4	Anforderungen	123
6.8.5	Artefakte	124
6.8.6	Testunterstützung	124
6.8.7	Hardwaremerkmale	124
6.9	Ausgabe von Austauschweisen	125
6.9.1	TUC-Beschreibung	126
6.9.2	Ablauf	128
6.9.3	Anforderungen	128
6.9.4	Artefakte	132
6.9.5	Testunterstützung	132
6.9.6	Hardwaremerkmale	132
7	Informationsmodell	133
8	Verteilungssicht	134
Anhang A – Verzeichnisse		135
A1 – Abkürzungen		135
A2 – Glossar		137
A3 – Abbildungsverzeichnis		137
A4 – Tabellenverzeichnis		138
A5 – Referenzierte Dokumente		139
A5.1	Dokumente der gematik	139
A5.2	Weitere Dokumente	139

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb der Kartenpersonalisierung für HBA und/oder SMC-B.

1.2 Zielgruppe

Das Dokument richtet sich an das IT-Personal von Kartenherausgebern und Personalisierern, das für Prozesse zur Beantragung, Freigabe und Auslieferung verantwortlich ist.

1.3 Geltungsbereich

Das vorliegende Dokument ist informativ.

1.4 Abgrenzungen

Spezifiziert werden in dem Dokument die vom TSP bereitgestellten Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang A5).

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zum Betrieb und zu internen Abläufen in der Produktivumgebung.

Die Erzeugung der Schlüssel und Zertifikate sowie die Personalisierung der Karten und die Generierung von PIN/PUK werden nicht im Detail beschrieben. Die PIN/PUK-Generierung muss den Vorgaben von [gemSpec_PINPUK_TI] folgen.

Die Benutzerverwaltung (z. B. Löschen eines Accounts, Entsperren eines Accounts, Änderung der Zugriffsrechte) der Mitarbeiter des Kartenherausgebers ist außerhalb der Betrachtungsgrenzen dieser Spezifikation.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselwörter MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

Spezifikation Kartenpersonalisierung HBA/SMC-B

☒ **gem_AFO_xxxx <Titel der Afo>**

Text/Beschreibung☒

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Systemüberblick

Im Rahmen der Einführung der elektronischen Gesundheitskarte gibt es neben der elektronischen Gesundheitskarte weitere Karten:

- Heilberufsausweis (HBA)
- Institutionsausweis (SMC-B)
- Verifikationskarten

In diesem Dokument wird beschrieben, wie diese Karten beantragt, freigegeben und ausgeliefert werden und wie sie ggf. gesperrt werden können. Außerdem wird das Monitoring dieser Prozesse durch die Kartenherausgeber und deren Spitzenorganisationen beschrieben.

Der TSP bietet für die Kartenpersonalisierung Portale (Vorbefüllungsportal, Antragsportal und Freigabeportal) sowie weitere Schnittstellen an. Diese werden in Kapitel 4 *Zerlegung des Produkttyps* aufgelistet.

Die folgenden Abbildungen zeigen vereinfacht die wesentlichen Abläufe bei der Kartenpersonalisierung. Die hellblauen Kästchen sind außerhalb der Betrachtungsgrenzen. Nicht dargestellt sind die Benachrichtigungen, die während des Ablaufs vom TSP verschickt oder in das Praxisregister eingestellt werden, diese werden in Kapitel 6.6.2 *Benachrichtigungen* und in Kapitel 6.7 beschrieben. Ebenfalls nicht dargestellt sind die Monitoring-Funktionen.

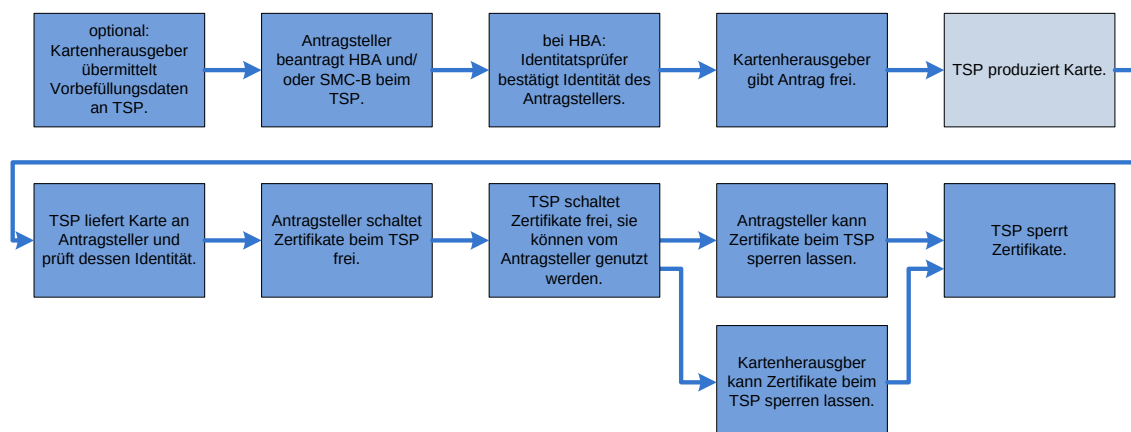


Abbildung 1: Abb_008_Ablauf_der_Kartenpersonalisierung_von_HBA_und_SMC-B

Spezifikation Kartenpersonalisierung HBA/SMC-B

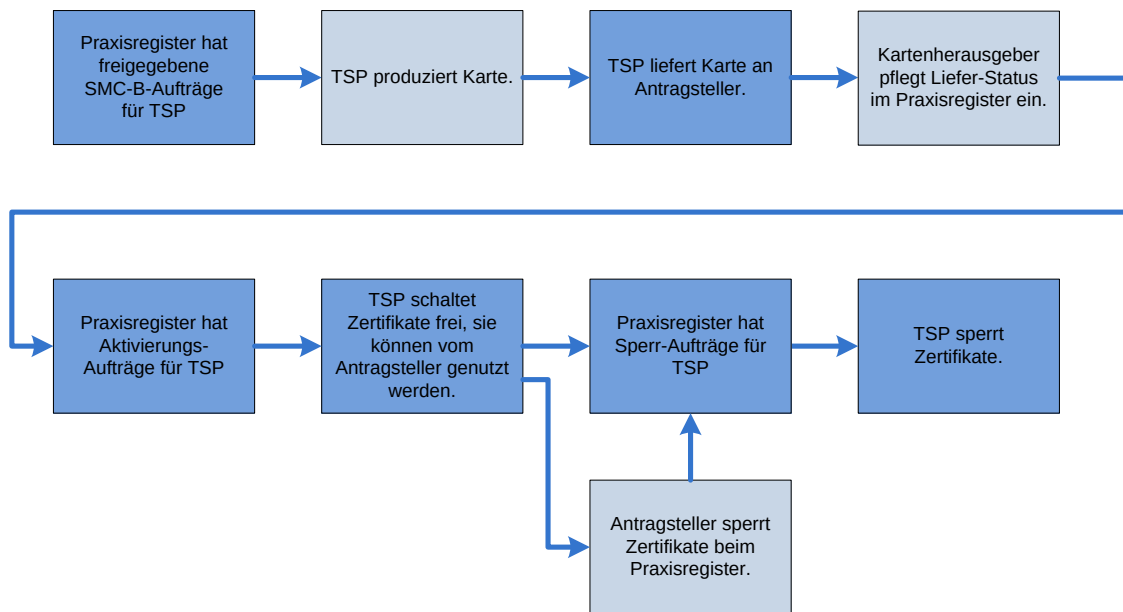


Abbildung 2: Abb_009_Ablauf_der_Kartenpersonalisierung_über_das_Praxisregister

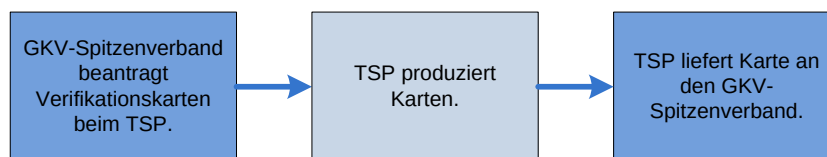


Abbildung 3: Abb_010_Ablauf_der_Kartenpersonalisierung_von_Verifikationskarten

3 Systemkontext

3.1 Akteure und Rollen

Die folgende Tabelle beschreibt die im Kontext der Kartenpersonalisierung relevanten Akteure und Rollen.

Tabelle 1: Tab_010_Akteure und Rollen

Rolle	Beschreibung
Antragsteller	Berechtigte Personen, die einen HBA oder eine SMC-B beantragen dürfen.
Berechtigte Mitarbeiter von Kartenherausgebern	Für die Nutzung der Portalfunktionalitäten für Kartenherausgeber existieren in der TSP-Schnittstelle drei getrennte Berechtigungen: Berechtigung zur Nutzung der Vorbefüllung, Berechtigung zur Freigabe, Berechtigung zur Sperrung. Die Berechtigung zum Monitoring folgt automatisch aus der Berechtigung zur Freigabe oder zum Sperren. T-Systems führt eine Registrierung berechtigter Mitarbeiter der Kartenherausgeber für die Portale durch. Jedem registrierten Mitarbeiter werden gemäß der Festlegung des Kartenherausgebers eine oder mehrere dieser o.g. Berechtigungen zugeordnet.
GKV-Spitzenverband	Der Spitzenverband der GKV beantragt die Verifikationskarten für die gesetzlichen Krankenversicherungen beim TSP und ist Kartenherausgeber der Verifikationskarten.
Beauftragter Verifikationskarte Kartenherausgeber (BVK)	Der Beauftragte Verifikationskarte Kartenherausgeber (BVK) wird vom GKV Spitzenverband benannt und ist verantwortlich für die Beantragung der Verifikationskarten beim TSP.
Identitätsprüfer	Person oder Institution, die die Identität einer Person verifizieren und bestätigen kann. Es kann die Post (im Fall des Verfahrens PostIdent) oder die zuständige Kammer (im Fall des Verfahrens KammerIdent) oder ein berechtigter Mitarbeiter des TSP sein.
Kartenherausgeber	Geben für eine Berufsgruppe HBA oder SMC-B oder Verifikationskarten heraus und sind für die ausgegebenen Karten sperrberechtigt. In diesem Dokument wird nicht zwischen Kartenherausgeber und attributbestätigender Stelle unterschieden, die die berufsspezifischen bzw. institutionspezifischen Attribute vergeben/bestätigen. Im Kontext dieser Spezifikation sind die Leistungserbringeror-

Spezifikation Kartenpersonalisierung HBA/SMC-B

Rolle	Beschreibung
	Organisationen die Kartenherausgeber von SMC-B und HBA und der GKV-Spitzenverband der Kartenherausgeber der Verifikationskarten, siehe Abbildung 4.
Kostenträger	Die Kostenträger im Gesundheitswesen sind die gesetzlichen Krankenversicherungen (GKV). Siehe auch GKV-Spitzenverband.
Praxisregister	Das Praxisregister ist ein System zur Verwaltung von SMC-B-Anträgen und -Karten. Das Praxisregister stellt dem TSP fertige Aufträge zur Produktion und Sperrung von SMC-Bs zur Verfügung. Es wird nicht von allen Sektoren eingesetzt.
Sektor	Ein Sektor repräsentiert eine Berufsgruppe wie z. B. Ärzte, Psychotherapeuten oder Zahnärzte. Zu einem Sektor können mehrere Kartenherausgeber gehören, die entweder HBAs oder SMC-Bs herausgeben.
Spitzenorganisation eines Sektors	Eine Spitzenorganisation legt für die ihr unterstellten Kartenherausgeber die sektorspezifische Ausgestaltung der TSP-Schnittstelle fest.
Berechtigte Mitarbeiter der Spitzenorganisation eines Sektors	T-Systems führt eine Registrierung berechtigter Mitarbeiter der Spitzenorganisationen der Sektoren zur Nutzung der Monitoring Funktionen durch.
TSP	Verantwortet den Betrieb der PKI (RA, CA, OCSP) und stellt die Schnittstellen für die Kartenpersonalisierung bereit. Der TSP ist zudem verantwortlich für die Personalisierung und Ausgabe der Karten. Im Rahmen dieses Dokuments wird nicht zwischen den Rollen TSP, Zertifizierungsdiensteanbieter (ZDA) und Personalisierer unterschieden. Der TSP stellt für die Antragsteller und Kartenherausgeber einen „Single Point of Contact“ (SPOC) bereit, über den per E-Mail, Telefon, Fax oder Postweg mit dem TSP kommuniziert werden kann.

Die folgende Abbildung stellt die Sektoren, deren Spitzenorganisationen und die zugeordneten Kartenherausgeber für HBA und SMC-B (Leistungserbringer) und Verifikationskarten (Kostenträger) beispielhaft¹ dar.

¹ Die Leistungserbringerorganisationen sind in der Abbildung beispielhaft als Organisationen auf Landesebene (z. B. als „LÄK“, Landesärztekammern) dargestellt, es gibt jedoch auch verschiedene Organisationen auf Bezirksebene, z. B. Bezirksärztekammern.

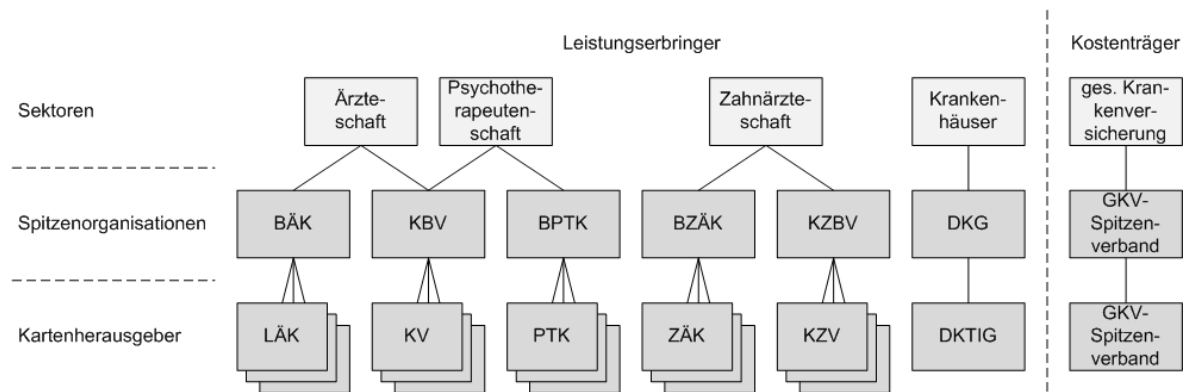


Abbildung 4: Abb_002_Leistungserbringer_und_Kostenträger

3.2 Nachbarsysteme

Eine Beschreibung des Systemkontexts ist nicht erforderlich.

4 Zerlegung des Produkttyps

Die Kartenpersonalisierung lässt sich in die folgenden Technischen Use Cases (TUC) aufteilen:

- Vorbefüllung
- Antragstellung
- Freigabe
- Lieferung
- Sperrung
- Monitoring und Benachrichtigungen
- Beauftragung und Sperrung über Praxisregister
- Beantragung, Personalisierung und Lieferung von Verifikationskarten

Bei der Kartenpersonalisierung werden die folgenden Schnittstellen verwendet.

Tabelle 2: Tab_001_Schnittstellen

Schnittstelle	Kommunikationspartner des TSP	Beschreibung findet sich in den folgenden Kapiteln
[Sch_Vorbefüllungsportal]	Kartenherausgeber	6.1 Vorbefüllung
[Sch_Antragsportal]	Antragsteller	6.2 Antragstellung 6.4 Lieferung (Freischaltung) 6.5 Sperrung
[Sch_Freigabeportal]	Kartenherausgeber Spitzenorganisationen	6.3 Freigabe 6.5 Sperrung 6.6.1 Monitoring
[Sch_Onlineschnittstelle_Vorbefüllung]	Kartenherausgeber	6.1 Vorbefüllung
[Sch_Praxisregister]	Praxisregister	6.7 Auftrag, Freischaltung und Sperrung über Praxisregister
[Sch_E-Mail_Antragsteller]	Antragsteller	6.6.2 Benachrichtigungen

Spezifikation Kartenpersonalisierung HBA/SMC-B

Schnittstelle	Kommunikationspartner des TSP	Beschreibung findet sich in den folgenden Kapiteln
[Sch_E-Mail_Kartenherausgeber]	Kartenherausgeber	6.6.2 Benachrichtigungen
[Sch_Post]	Antragsteller Kartenherausgeber Identitätsprüfer	6.2 Antragstellung 6.3 Freigabe 6.4 Lieferung 6.8 Beantragung, Personalisierung und Lieferung von Verifikationskarten
[Sch_SOAP]	Kartenherausgeber Spitzenorganisationen	6.1 Vorbefüllung 6.3 Freigabe 6.5 Sperrung 6.6.1 Monitoring
[Sch_Fax]	BVK	6.8 Beantragung, Personalisierung und Lieferung von Verifikationskarten

5 Übergreifende Festlegungen

In diesem Kapitel werden Anforderungen definiert, die sich entweder keinem oder mehreren TUCs zuordnen lassen. In Kapitel 6 *Funktionsmerkmale* werden die TUCs beschrieben und weitere Anforderungen definiert, die nur zu einzelnen TUCs gehören.

5.1 Gesetzliche Anforderungen

☒ **gem_AFO_0033 Umsetzung von Signaturgesetz und Signaturverordnung**

Der TSP MUSS die Vorgaben des Signaturgesetzes [SigG01] und der Signaturverordnung [SigV01] für den Bereich der qualifizierten Signaturzertifikate umsetzen. ☒

5.2 Kommunikation

☒ **gem_AFO_0007 Absicherung von Kommunikationsverbindungen mittels TLS**

Die unten genannten Kommunikationsverbindungen zwischen dem TSP und dem jeweiligen Kommunikationspartner MÜSSEN TLS-Verbindungen sein. Zu Beginn einer Kommunikationsverbindung MUSS sich der TSP gegenüber dem Kommunikationspartner authentisieren und beide Kommunikationspartner MÜSSEN die Kommunikation verschlüsseln.

Der TSP MUSS außerdem die Anforderungen [GS-A_4359], [GS-A_4362], [GS-A_4384], [GS-A_4385], [GS-A_4386], [GS-A_4387] und [GS-A_5035] aus [gemSpec_Krypt] erfüllen.

Die Kommunikationsverbindungen sind:

- Schnittstelle [Sch_Vorbefüllungsportal]: Mitarbeiter des Kartenherausgebers nutzt das Vorbefüllungsportal.
- Schnittstelle [Sch_Onlineschnittstelle_Vorbefüllung]: Kartenherausgeber sendet Vorbefüllungsdaten über die Online-Schnittstelle.
- Schnittstelle [Sch_Antragsportal]: Antragsteller nutzt das Antragsportal.
- Schnittstelle [Sch_Freigabeportal]: Mitarbeiter eines Kartenherausgebers oder einer Spitzenorganisation nutzt das Freigabeportal. Diese Schnittstelle umfasst auch die Kommunikation im Zusammenhang mit der qualifizierten Signatur von Freigaben oder Sperrungen im Freigabeportal.
- Schnittstelle [Sch_SOAP]: Der Kartenherausgeber kann über SOAP Vorbefüllung, Freischaltung, Sperrung und Monitoring durchführen. Die Spitzenorganisationen können über SOAP Monitoring durchführen.
- Schnittstelle [Sch_Praxisregister]: Das Praxisregister stellt SMC-B-Aufträge, Freischaltungen und Sperraufträge bereit. ☒

☒ **gem_AFO_0093 WebTrust-zertifizierte CA für TSP-Zertifikat für TLS**

Für die in [gem_AFO_0007] genannten Kommunikationsverbindungen MUSS der TSP Zertifikate einer CA verwenden, die WebTrust zertifiziert ist. ☒

Anmerkung: Als CA, die [gem_AFO_0093] erfüllt, kann zum Beispiel die ServerPass-CA von T-Systems verwendet werden.

☒ **gem_AFO_0037 Bereitstellen der Root- und CA-Zertifikate der TSP-Zertifikate für TLS**

Der TSP MUSS den Kommunikationspartnern Links bereitstellen, über die die Root- und CA-Zertifikate heruntergeladen werden können, die zu den TSP-Zertifikaten gehören, welche in TLS-Verbindungen verwendet werden.

Der TSP MUSS für sein Zertifikat eine CA auswählen, deren Root-Zertifikat in den gängigen Browsern bereits vorinstalliert ist. ☒

5.3 Authentisierung und Signatur

☒ **gem_AFO_0108 Nutzung einer Signaturanwendungskomponente für qualifizierte elektronische Signatur von Freigabeaufträgen und Sperraufträgen**

Der TSP MUSS es den Kartenherausgebern ermöglichen, im Freigabeportal die Freigabeaufträge und Sperraufträge als PDF-Dokument mit einer qualifizierten elektronischen Signatur zu signieren.

Der TSP MUSS es den Kartenherausgebern ermöglichen, die qualifizierten elektronischen Signaturen für Freigabeaufträge und Sperraufträge mit einer SigG-konformen Signaturanwendungskomponente (SAK) zu erstellen. Der TSP MUSS die Konformität durch Bestätigung oder Herstellererklärung gemäß SigG [SigG01] nachweisen.

Der TSP MUSS die SAK in das Freigabeportal integrieren, so dass keine lokale Installation beim Client des Kartenherausgebers erforderlich ist. ☒

☒ **gem_AFO_0153 Zeitgleiche Nutzung der SAK**

Der TSP SOLL eine SAK einsetzen, die eine zeitgleiche Nutzung der SAK in mehreren Sessions auf dem Client ermöglicht. Die SigG-Signaturkarte, die für die qualifizierte elektronische Signatur der Freigabeaufträge und Sperraufträge verwendet wird, SOLL auch dann für andere Anwendungen genutzt werden können, wenn das Freigabeportal geöffnet ist. ☒

☒ **gem_AFO_0184 Prüfung der qualifizierten elektronischen Signatur von Freigabeaufträgen und Sperraufträgen**

Der TSP MUSS die qualifizierten elektronischen Signaturen von Freigabeaufträgen und Sperraufträgen prüfen.

Dies gilt für:

- alle Freigabeaufträge für HBAs am Freigabeportal

- alle Freigabeaufträge für SMC-Bs am Freigabeportal, sofern sie mit einer qualifizierten elektronischen Signatur signiert wurden und nicht über einen Freigabe-Button ausgelöst wurden.
- alle Freigabeaufträge über die SOAP-Schnittstelle
- alle Sperraufträge am Freigabeportal
- alle Sperraufträge über die SOAP-Schnittstelle

Der TSP MUSS bei der Prüfung einer qualifizierten elektronischen Signatur sicherstellen, dass das zur Signaturerstellung verwendete Zertifikat eines Mitarbeiters eines Kartenherausgebers mit dem beim TSP hinterlegten Zertifikat des Mitarbeiters übereinstimmt.

Als fehlgeschlagene Prüfung wird auch der Fall angesehen, dass keine qualifizierte elektronische Signatur vorhanden ist, obwohl eine solche erforderlich ist.

Wenn die Prüfung einen Fehler ergibt, MUSS der TSP den Kartenherausgeber benachrichtigen: In Abhängigkeit der genutzten Funktionalität (Portal oder SOAP) wird entweder im Portal eine Fehlermeldung angezeigt oder der TSP sendet eine entsprechende SOAP-Response. ☒

☒ **gem_AFO_0038 Kryptographische Algorithmen für Signaturen**

Der TSP MUSS bei der Erstellung und Prüfung von Signaturen die Anforderungen GS-A_4357, GS-A_4358, GS-A_4370, GS-A_4371, GS-A_4372 und GS-A_5081 aus [gemSpec_Krypt] einhalten, sofern sie im konkreten Fall anwendbar sind. Dies schließt die Signatur von XML-Dokumenten, von PDF-Dokumenten und sowohl qualifizierte als auch nicht-qualifizierte elektronische Signaturen ein. ☒

☒ **gem_AFO_0023 Signatur von E-Mails vom TSP an Antragsteller und Kartenherausgeber**

Die vom TSP versendeten E-Mails MÜSSEN signiert sein. Der TSP MUSS die zugehörigen CA- und Root-Zertifikate zur Verfügung stellen, damit die Empfänger die Signatur prüfen können. ☒

☒ **gem_AFO_0139 Gegenseitige Authentisierung bei Nutzung der SOAP-Schnittstelle**

Der TSP MUSS bei jeder Nutzung der SOAP-Schnittstelle durch den Kartenherausgeber eine TLS-Verbindung zum Kartenherausgeber mit Server- und Clientseitiger Authentisierung aufbauen, bei der sich der Kartenherausgeber durch ein X.509-Zertifikat beim TSP authentisiert. Der TSP MUSS sicherstellen, dass das Zertifikat mit dem beim TSP für diesen Kartenherausgeber und diese SOAP-Schnittstelle hinterlegten Zertifikat übereinstimmt. Wenn die Client Authentisierung fehlschlägt, MUSS der TSP eine SOAP Anfrage mit einer Fehlermeldung ohne Übermittlung angefragter Daten beantworten. ☒

☒ **gem_AFO_0006 Authentisierung des Kartenherausgebers am Vorbefüllungsportal und am Freigabeportal ohne nPA**

Der TSP MUSS den Mitarbeiter des Kartenherausgebers vor dem Zugriff auf das Vorbefüllungsportal und das Freigabeportal authentifizieren, d. h., der Mitarbeiter MUSS sich beim TSP authentisieren. Der TSP MUSS mindestens die beiden folgenden Möglichkeiten zur Authentisierung zur Verfügung stellen:

- Der Mitarbeiter authentisiert sich mittels einer Standardsignaturkarte gemäß [gem_AFO_0915],
- Der Mitarbeiter authentisiert sich mittels Benutzername und Passwort. ☒

☒ **gem_AFO_0915 Authentisierung des Kartenherausgebers am Vorbefüllungsportal und am Freigabeportal mittels einer Standardsignaturkarte**

Der TSP setzt voraus, dass die Anforderungen [gem_AFO_0916] erfüllt sind.

Der TSP MUSS für die Authentisierung der Mitarbeiter von Kartenherausgebern mittels Standardsignaturkarte einen in den Webserver von Vorbefüllungs- und Freigabeportal integrierten Java Mechanismus bereitstellen, der die lokale Einbindung von Kartentreibern in die von den Mitarbeitern genutzten Browser überflüssig macht.

Der TSP MUSS die Authentisierung auf Basis des auf der Standardsignaturkarte enthaltenen AUTH-Zertifikats und seiner Schlüsselpaare vornehmen.

Der TSP MUSS sicherstellen, dass für die Nutzung des Java Mechanismus keine Lizenzkosten für die Kartenherausgeber anfallen.

Der TSP MUSS mit dem Java-Mechanismus sicherstellen, dass außer den in [gem_AFO_0916] genannten Anforderungen keine weitere lokale Installation einer Client Software (z.B. Crypto Service Provider oder PKCS#11 Modul) erforderlich ist, und dass keine weitere lokale administrative Unterstützung seitens des Mitarbeiters erforderlich ist.

Der TSP MUSS sicherstellen, dass eine Nutzung der Ressourcen (z. B. Kartenterminal oder Signaturkarte) durch andere Anwendungen vor oder nach dem Login nicht verhindert oder blockiert wird.

Die Lösung des TSP MUSS kompatibel mit den Standardsignaturkarten der Herausgeber D-TRUST, T-Systems, dgnservice und mediSign sein.

Die Lösung des TSP MUSS kompatibel mit den gängigen Kartenterminals und den von der gematik zugelassenen Kartenterminals sein.

Die Lösung des TSP MUSS die o. g. Kartenterminals und Standardsignaturkarten automatisch erkennen.

Die Lösung des TSP MUSS kompatibel mit den Browsern Internet Explorer und Firefox in den gängigen Versionen sein.

Im Fall technischer Änderungen der o. g. Standardsignaturkarten, Kartenterminals und Browserschnittstellen, die dazu führen, dass die implementierte Lösung bei einem relevanten Teil der o. g. Komponenten nicht mehr funktioniert, MUSS der TSP die Lösung innerhalb eines angemessenen Zeitraums anpassen. ☒

Hinweis: Die Mitarbeiter von Kartenherausgebern verwenden z. T. die Signaturkarte von dgnservice. Diese und die mediSign Karte sind technisch identisch.

☒ **gem_AFO_0916 Anforderung an die Arbeitsplatzumgebung zur Authentisierung mittels einer Standardsignaturkarte**

Auf dem Arbeitsplatzrechner eines Mitarbeiters eines Kartenherausgebers, der die Authentifizierung mittels Standardsignaturkarte nutzen möchte, MUSS eine Java Runtime Engine (ab Version Java 7) installiert sein. Auf dem Arbeitsplatzrechner ei-

nes Mitarbeiters eines Kartenherausgebers, der die Authentifizierung mittels Standardsignaturkarte nutzen möchte, MUSS der Treiber des genutzten Kartenterminals installiert sein. ☒

☒ **gem_AFO_0810 Authentisierung des Kartenherausgebers am Vorbefüllungsportal und am Freigabeportal mit nPA**

Der TSP SOLL zusätzlich zu den in [gem_AFO_0006] genannten Möglichkeiten den folgenden Authentisierungsmechanismus anbieten:

- Der Mitarbeiter authentisiert sich mittels des neuen Personalausweises (nPA). ☒

☒ **gem_AFO_0811 Deaktivierung von Authentisierungsmöglichkeiten des Kartenherausgebers am Vorbefüllungsportal und am Freigabeportal**

Der TSP MUSS es ermöglichen, dass auf Veranlassung eines Kartenherausgebers die von diesem nicht gewünschten Authentisierungsmechanismen für diesen Kartenherausgeber deaktiviert werden. ☒

Anmerkungen:

- Das Zertifikat für die Authentisierung am Portal ist ein anderes als das für die qualifizierte elektronische Signatur.
- Die Registrierung der Mitarbeiter wird in Kapitel 5.3.1 Registrierung beschrieben.

☒ **gem_AFO_0700 Authentisierung der Spitzenorganisationen der Sektoren für das Monitoring ohne nPA**

Der TSP MUSS Mitarbeiter der Spitzenorganisation eines Sektors vor dem Zugriff auf das Monitoring authentifizieren, d. h., der Mitarbeiter MUSS sich beim TSP authentisieren. Der TSP MUSS mindestens die beiden folgenden Möglichkeiten zur Authentisierung zur Verfügung stellen:

- Der Mitarbeiter authentisiert sich mittels einer Standardsignaturkarte.
- Der Mitarbeiter authentisiert sich mittels Benutzername und Passwort. ☒

Anmerkung:

- Die Registrierung der Mitarbeiter wird in Kapitel 5.3.1 Registrierung beschrieben.

☒ **gem_AFO_0812 Authentisierung der Spitzenorganisationen der Sektoren für das Monitoring mit nPA**

Der TSP SOLL zusätzlich zu den in [gem_AFO_0700] genannten Möglichkeiten den folgenden Authentisierungsmechanismus anbieten:

- Der Mitarbeiter authentisiert sich mittels des neuen Personalausweises (nPA). ☒

☒ **gem_AFO_0813 Deaktivierung von Authentisierungsmöglichkeiten der Spitzenorganisationen der Sektoren für das Monitoring**

Der TSP MUSS es ermöglichen, dass auf Veranlassung der Spitzenorganisationen der Sektoren die von diesen nicht gewünschten Authentisierungsmechanismen für das Monitoring deaktiviert werden. ☒

☒ gem_AFO_0036 Benennung von berechtigten Mitarbeitern durch den Kartenherausgeber für Vorbefüllungsportal und Freigabeportal

Der Kartenherausgeber MUSS dem TSP schriftlich die Mitarbeiter benennen, die berechtigten Zugriff auf das Vorbefüllungsportal und/oder das Freigabeportal haben.

Zu jedem Mitarbeiter MUSS er dem TSP die zugehörigen Zugriffsrechte mitteilen. Die Zugriffsrechte MÜSSEN eines oder mehrere aus folgender Liste sein:

- Vorbefüllung
- Freigabe
- Sperrung

Für die Funktionen „Freigabe“ und „Sperrung“ MUSS der Kartenherausgeber Mitarbeiter benennen, für die Funktion „Vorbefüllung“ KANN er Mitarbeiter benennen.

Der TSP MUSS für jeden Mitarbeiter einen individuellen Account anlegen.

Der TSP MUSS beliebige Benutzernamen akzeptieren, auch Pseudonyme oder IDs. Dies gilt nicht für Mitarbeiter des Kartenherausgebers, die eine qualifizierte elektronische Signatur durchführen, da deren Namen dem TSP bekannt sein müssen. ☒

☒ gem_AFO_0125 Benennung von berechtigten Mitarbeitern durch Spitzenorganisationen der Sektoren für Monitoring

Die Spitzenorganisationen der Sektoren KÖNNEN dem TSP Mitarbeiter benennen, die berechtigten Zugriff auf die Monitoring-Funktion im Freigabeportal haben. ☒

☒ gem_AFO_0702 Account und Benutzername von berechtigten Mitarbeitern der Spitzenorganisationen der Sektoren für Monitoring

Der TSP MUSS für jeden von den Spitzenorganisationen der Sektoren für das Monitoring benannten Mitarbeiter einen individuellen Account anlegen.

Der TSP MUSS beliebige Benutzernamen akzeptieren, auch Pseudonyme oder IDs. ☒

☒ gem_AFO_0096 Mitteilung der E-Mail-Adressen des Kartenherausgebers

Der Kartenherausgeber MUSS dem TSP die E-Mail-Adressen der berechtigten Mitarbeiter oder eines Sammelpostfachs zum Empfang der Benachrichtigungen gemäß [gem_AFO_0609] bereitstellen. ☒

☒ gem_AFO_0009 Einhaltung einer Passwortrichtlinie für die Authentisierung am Vorbefüllungsportal und Freigabeportal und für das Monitoring

Der TSP DARF NICHT Passwörter zum Einloggen von Mitarbeitern des Kartenherausgebers am Vorbefüllungsportal und Freigabeportal bzw. von Mitarbeitern der Spitzenorganisationen der Sektoren beim Monitoring akzeptieren, erzeugen oder verwenden, die nicht die folgenden Kriterien erfüllen:

- Mindestlänge: 8 Zeichen
- Zeichen aus mindestens 3 der folgenden Gruppen: Kleinbuchstabe, Großbuchstaben, Ziffern, Sonderzeichen. ☒

☒ **gem_AFO_0034 Fehlerzähler und Sperrung beim Einloggen am Vorbefüllungsportal und Freigabeportal**

Der TSP MUSS den Account eines Mitarbeiters des Kartenherausgebers nach 5 aufeinander folgenden Fehlversuchen beim Einloggen am Vorbefüllungsportal oder am Freigabeportal sperren. In diesem Fall ist der Account in beiden Portalen gesperrt. ☒

☒ **gem_AFO_0703 Fehlerzähler und Sperrung beim Einloggen zum Monitoring**

Der TSP MUSS den Account eines Mitarbeiters einer Spitzenorganisation eines Sektors nach 5 aufeinander folgenden Fehlversuchen beim Einloggen zum Monitoring sperren. ☒

☒ **gem_AFO_0130 An Portalen und beim Monitoring Ausloggen ermöglichen**

Der TSP MUSS es den Anwendern ermöglichen, sich am Freigabeportal und am Vorbefüllungsportal sowie beim Monitoring auszuloggen. ☒

☒ **gem_AFO_0064 Eingabe einer Captcha-Zeichenfolge**

Damit die Möglichkeit, falsche Anträge massenhaft zu verschicken, verhindert wird, MUSS der TSP vom Anwender die Eingabe einer Captcha-Zeichenfolge fordern, wenn dies von der Spitzenorganisation des Sektors, zu dem der zuständige Kartenherausgeber gehört, gewünscht wird:

- beim Absenden eines Antrags
- bei Aufruf eines gespeicherten Antrags (Eingabe von entweder Referenznummer und Servicepasswort oder im Fall von vorbereiteten Anträgen der Vorgangsnummer im Antragsportal)
- bei Aufruf eines Vorbefüllungsdatensatzes (Eingabe der Vorgangsnummer im Antragsportal)
- bei Sperrung einer Karte (Eingabe von Referenznummer und Sperrkennwort im Antragsportal)
- bei Freischaltung einer Karte (Eingabe von Kartennummer und Freischaltkennwort im Antragsportal)

Die in anderen Anforderungen geforderte Anzeige von Daten oder Ausführung von Aktionen nach diesen Eingaben DARF nur durchgeführt werden, wenn im Fall der Forderung der Eingabe einer Captcha-Zeichenfolge diese korrekt eingegeben wurde. ☒

5.3.1 Registrierung

Hinweis: Die folgenden Ausführungen beziehen sich nicht auf Verifikationskarten. Der Registrierungsprozess im Zusammenhang mit Verifikationskarten ist in Kapitel 6.8.3 beschrieben.

Zur Absicherung der Kommunikation zwischen Kartenherausgebern und TSP über [Sch_Vorbefüllungsportal], [Sch_Onlineschnittstelle_Vorbefüllung], [Sch_Freigabeportal] und [Sch_SOAP] im Rahmen der Vorbefüllung, Freigabe, Sperrung oder Monitoring ist es erforderlich, dass die Kartenherausgeber sich zum einen gegenüber dem TSP authenti-

sieren und zum anderen die Freigabe und Sperrung mittels QES durchführen können. Ebenso müssen sich Mitarbeiter der Spitzenorganisationen der Sektoren beim Zugriff auf Monitoring Funktionen des Freigabeportals gegenüber dem TSP authentisieren.

Die Mitarbeiter der Kartenherausgeber und der Spitzenorganisation der Sektoren müssen dazu vor Nutzung der Funktionen initial registriert werden. Im Rahmen der Registrierung werden abhängig von der zu nutzenden Schnittstelle und Funktion folgende Credentials dem Mitarbeiter zugeordnet:

- Credential [CR-1]: Benutzername/Passwort für die Authentisierung am Vorbefüllungsportal, am Freigabeportal oder bei der Vorbefüllung per http-POST.
- Credential [CR-2]: Authentisierungszertifikat für die Authentisierung am Vorbefüllungsportal oder am Freigabeportal mit einer Standard-Signaturkarte.
- Credential [CR-3]: TLS- bzw. Web-Service-Security-Zertifikate zur Signatur, Authentisierung und Verschlüsselung im Rahmen der Kommunikation über SOAP.
- Credential [CR-4]: QES-Zertifikat(e) zur qualifizierten Signatur von Freigaben oder Sperrungen (nur Mitarbeiter der Kartenherausgeber).
- Credential [CR-5]: „restrictedID“ bei Nutzung der Online-Ausweisfunktion des nPA zur Authentisierung am Vorbefüllungsportal oder am Freigabeportal.

Hinweise:

- Auch für „Maschinen-Accounts“ (z. B. Server bei automatisierter Kommunikation per SOAP oder bei der Vorbefüllung) müssen Mitarbeiter benannt werden, welche für die Credentials verantwortlich sind. Es wird daher nachfolgend nicht weiter unterschieden, ob es sich um Personen- oder Maschinen-Credentials handelt, die Registrierungsbedingungen gelten analog.
- Als Credentials [CR-2], [CR-3] und [CR-4] können Authentisierungs- oder Signaturzertifikate von Standard-Signaturkarten (QES) sowie am Markt erhältliche TLS-Zertifikate (Anforderungen analog zu [gem_AFO_0093]) genutzt werden. Optional können diese auch über den TSP ausgegeben werden, was jedoch nicht im Scope dieser Spezifikation ist und daher hier nicht weiter betrachtet wird.

Zur Registrierung der Mitarbeiter sind folgende Schritte erforderlich:

1. Benennung der Leiter bzw. Mitarbeiter:

Dem TSP wird von jedem Kartenherausgeber ein Mitarbeiter in der Rolle „Leiter der Attributbestätigenden Stelle“ benannt, sowie optional ein Stellvertreter. Bei Kartenherausgebern, die KammerIdent unterstützen, kann dies z.B. der „Leiter Ident“ sein. Dem TSP wird von der Spitzenorganisation jedes Sektors ein „Leiter Monitoring“ benannt, sowie optional ein Stellvertreter.

Der Leiter benennt gegenüber dem TSP die berechtigten Mitarbeiter und übermittelt deren Registrierungsinformationen. Ein Leiter oder stellvertretender Leiter kann gleichzeitig in der Rolle „berechtigter Mitarbeiter“ tätig sein.

Insbesondere benennt der Leiter die Berechtigung eines Mitarbeiters für Vorbefüllung, Freigabe, Sperrung oder Monitoring (siehe [gem_AFO_0036], [gem_AFO_0125] und [gem_AFO_0701]).

2. Bereitstellung der Registrierungsunterlagen durch den TSP:

Über den SPOC des TSP wird den benannten Leitern eine Prozessbeschreibung zur Weitergabe an die Mitarbeiter bereit gestellt. Es erfolgt weiterhin eine bilaterale Festlegung über das Format der Registrierungsunterlagen (PDF-Formulare) zur Angabe von Identifizierungs- und Registrierungsdaten sowie der Vereinbarung der zu verwendenden Credentials [CR-1], [CR-2], [CR-3], [CR-4] oder [CR-5].)

3. Übermittlung der ausgefüllten Registrierungsunterlagen an den TSP:

Jeder Leiter übersendet dem TSP die folgenden Unterlagen per Post:

- a. Eine vom Leiter unterschriebene Liste der berechtigten Mitarbeiter mit den ihnen zugewiesenen Berechtigungen.
- b. Pro Mitarbeiter ein vom Mitarbeiter und vom Leiter unterschriebenes Registrierungsformular mit Angabe der Identifizierungs- und Registrierungsdaten sowie den zu verwendenden Credentials des Mitarbeiters.

4. Prüfung der Unterlagen und Registrierung der Mitarbeiter:

Die Formulare werden durch den TSP geprüft. Nach erfolgreicher Prüfung werden die benannten Mitarbeiter als berechtigte Mitarbeiter des Kartenherausgebers oder einer Spitzenorganisation eines Sektors beim TSP registriert und darüber per E-Mail informiert.

5. Nur bei [CR-1]: Übergabe des Initialkennworts an den Mitarbeiter:

Nach Abschluss der Registrierung sendet der TSP dem Mitarbeiter per Post das Initialkennwort zu [CR-1], welches der Mitarbeiter am Vorbefüllungs- oder Freigabeportal bei der ersten Nutzung ändern muss.

5.3.1.1 Anforderungen

☒ **gem_AFO_0601 Bereitstellung bzw. Bilaterale Abstimmung der Registrierungsunterlagen**

Der TSP MUSS den Leitern der Attributbestätigenden Stelle der Kartenherausgeber bzw. den Leitern Monitoring der Spitzenorganisationen der Sektoren die Kontaktdaten des SPOC im Rahmen der Projektabstimmung mitteilen und ihnen die Registrierungsunterlagen über den SPOC bereitstellen bzw. diese bilateral abstimmen. ☒

☒ **gem_AFO_0602 Vollständigkeit der Registrierungsunterlagen**

Die Leiter der Kartenherausgeber und der Spitzenorganisationen der Sektoren MÜSSEN eine vom Leiter unterschriebene Liste der berechtigten Mitarbeiter mit den ihnen zugewiesenen Berechtigungen an den TSP übermitteln.

Die Leiter der Kartenherausgeber und der Spitzenorganisationen der Sektoren MÜSSEN die Registrierungsunterlagen berechtigter Mitarbeiter vollständig ausgefüllt an den TSP übermitteln. Die Registrierungsunterlagen jedes Mitarbeiters MÜSSEN folgende Angaben enthalten:

- Persönliche Daten zur Zuordnung der Credentials und Kontaktaufnahme bei Rückfragen: Name, Vorname, Kontaktdaten (persönliche E-Mail-Adresse, Telefon). Die E-Mail-Adresse eines Mitarbeiters aus den Registrierungsunterlagen wird nicht für die Übermittlung von Statusinformationen/Rückmeldungen des TSP an den Kartenherausgeber verwendet. Für die Übermittlung von Statusinformationen/Rückmeldungen MUSS

der TSP pro Kartenherausgeber eine oder mehrere von Kartenherausgeber festgelegte E-Mail-Adressen im Portal konfigurieren. Es wird empfohlen, dafür Adressen von Funktionspostfächern zu verwenden.

- Angaben zu den Credentials:
 - o [CR-1]: gewünschter Benutzername für den Account.
 - o [CR-2], [CR-3], [CR-4]:
 - Aussteller des Zertifikats,
 - Seriennummer des Zertifikats,
 - Fingerprint des Zertifikats (Hashwert).
 - o Die Festlegung der Details (z. B. Hash-Verfahren) erfolgt in den Registrierungsunterlagen. Diese können dadurch flexibel gehalten werden und auch spezifische Anforderungen der Spitzenverbände der Sektoren umsetzen.
- Unterschrift des Mitarbeiters und des Leiters. ☒

☒ **gem_AFO_0604 Übergabe der Credentials bei [CR-2], [CR-3], [CR-4]**

Ergänzend zu den Registrierungsunterlagen MUSS der Mitarbeiter die Credentials (in diesem Fall Zertifikate) unter Verwendung seiner persönlichen E-Mail-Adresse und der Nennung seines Namens an den SPOC des TSP senden. Der TSP MUSS anhand des Namens und der persönlichen E-Mail-Adresse den Bezug zu den Registrierungsunterlagen des Mitarbeiters herstellen. ☒

☒ **gem_AFO_0814 Übergabe der Credentials bei [CR-5]**

Ergänzend zu den Registrierungsunterlagen MUSS der Mitarbeiter sich auf einer Registrierungsseite des TSP mittels seines nPA registrieren. Dabei MUSS der TSP sowohl den Namen des Mitarbeiters als auch die sog. „restrictedID“ aus dem nPA auslesen. Der TSP MUSS anhand des Namens den Bezug zu den Registrierungsunterlagen des Mitarbeiters herstellen. Zur späteren Authentifizierung des Mitarbeiters genügt dann das Auslesen der „restrictedID“. ☒

☒ **gem_AFO_0605 Registrierung der Mitarbeiter und Zuordnung der Credentials**

Der TSP MUSS die Registrierungsunterlagen und bei [CR-2], [CR-3] oder [CR-4] auch die gelieferten Credentials überprüfen. Bei erfolgreicher Prüfung MUSS der TSP den entsprechenden Account im Portal anlegen und die Credentials des Mitarbeiters dem Account zuordnen. Anschließend MUSS der TSP die Registrierungsunterlagen gegenzeichnen und im Papierarchiv ablegen.

Bei nicht erfolgreicher Prüfung MUSS der TSP Kontakt zum Leiter bei Kartenherausgeber und der Spitzenorganisation eines Sektors aufnehmen und wenn möglich eine Klärung herbeiführen oder, falls keine Klärung möglich ist, den Registrierungsvorgang abbrechen. ☒

☒ **gem_AFO_0606 Erzeugung und Übergabe Initialkennwort**

Nur bei [CR-1]: Der TSP MUSS nach erfolgreicher Registrierung für jeden Account ein zufälliges Initialkennwort entsprechend den Anforderungen aus

[gem_AFO_0009] generieren und dem Mitarbeiter per Post zusenden. Der TSP DARF in der Benutzerverwaltung des Portals NICHT das Initialkennwort selbst sondern nur den Hashwert des Kennworts speichern. Gleiches gilt analog auch für die nach Erstanmeldung neu vergebenen Kennwörter.☒

☒ **gem_AFO_0607 Änderung des Initialkennworts bei erster Nutzung**

Nur bei [CR-1]: Die Mitarbeiter MÜSSEN nach der ersten Anmeldung mit dem Initialkennwort ein neues Kennwort gemäß [gem_AFO_0009] erzeugen und MÜSSEN sich danach mit dem neuen Kennwort authentisieren. Der TSP MUSS den Hashwert des Initialkennworts löschen und eine Authentisierung mit dem Initialkennwort ablehnen.☒

☒ **gem_AFO_0608 Mitteilung über Änderung von Mitarbeiterdaten**

Der Leiter bei Kartenherausgebern oder die Spitzenorganisation eines Sektors MUSS dem TSP Änderungen der Mitarbeiterdaten (Namen, E-Mail-Adresse, Telefonnummer, Zugriffsrechte, Wegfall der Berechtigung durch Wechsel oder Einstellen der Tätigkeit etc.) und bei [CR-2], [CR-3], [CR-4] oder [CR-5] auch Änderungen der Credentials schriftlich mitteilen.☒

☒ **gem_AFO_0622 Änderung von Mitarbeiterdaten**

Wenn der TSP vom Kartenherausgeber oder der Spitzenorganisation eines Sektors über Änderungen von Mitarbeiterdaten informiert wurde, MUSS er daraufhin innerhalb von 10 Tagen die Daten des Accounts ändern oder bei Wegfall der Berechtigung den Account löschen. Wenn keine vom betreffenden Mitarbeiter freigegebenen oder gesperrten Anträge mehr im Portal verfügbar sind, frühestens jedoch 4 Wochen nach dem Löschen des Accounts, MUSS der TSP die Registrierungsunterlagen aus dem Papierarchiv sicher entsorgen. Dies betrifft nur die dokumentierten Credentials des Mitarbeiters, nicht jedoch die Bestätigung der Berechtigung des Mitarbeiters durch den Leiter der Attributbestätigenden Stelle. Der TSP MUSS eine Rückmeldung über die erfolgte Änderung oder Löschung der Account Daten an die zuständige Stelle (Kartenherausgeber oder Spitzenorganisation eines Sektors) geben.☒

5.4 Portale

Anmerkungen:

Das Vorbefüllungsportal wird in Kapitel 6.1 Vorbefüllung beschrieben.

☒ gem_AFO_0046 Bereitstellung Antragsportal für Beantragung von HBA und SMC-B

Der TSP MUSS den Antragstellern ein Antragsportal in Form eines Web-Portals im Internet bereitstellen, das sie mit einem Browser aufrufen und verwenden können. Es MÜSSEN die Browser Internet Explorer und Firefox in aktuellen Versionen unterstützt werden. ☒

☒ gem_AFO_0076 Funktionen im Antragsportal

Im Antragsportal MUSS der Antragsteller die folgenden Funktionen aufrufen können:

- Antrag stellen
- Zertifikat freischalten
- Zertifikat sperren.

Wenn der Antragsteller eine dieser Aktivitäten auswählt, MUSS der TSP den entsprechenden Inhalt anzeigen unter Berücksichtigung von [gem_AFO_0161]. ☒

Anmerkung: „Antrag stellen“ wird in Kapitel 6.2 Antragstellung beschrieben, „Zertifikat freischalten“ wird in Kapitel 6.4 Lieferung beschrieben, „Zertifikat sperren“ in Kapitel 6.5 Sperrung.

☒ gem_AFO_0095 Bereitstellung Freigabeportal

Der TSP MUSS den Kartenherausgebern und den Spitzenorganisationen der Sektoren ein Freigabeportal in Form eines Web-Portals im Internet bereitstellen, das sie mit einem Browser aufrufen und verwenden können. Es MÜSSEN die Browser Internet Explorer und Firefox in aktuellen Versionen unterstützt werden. ☒

☒ gem_AFO_0098 Struktur und Inhalt des Freigabeportals

Der TSP MUSS im Freigabeportal dem Kartenherausgeber ermöglichen, die folgenden Funktionen durchzuführen:

- Eingabe von Suchkriterien zur Suche nach bestimmten Anträgen
- Überblicksansicht von Anträgen, die den eingegebenen Suchkriterien entsprechen
- Detailansicht eines ausgewählten Antrags aus der Überblicksansicht
- Optionale Änderung, optionale Ergänzung eines Antrags
- Freigabe oder Ablehnung eines Antrags

- Sperrung eines Antrags (damit ist die Sperrung aller X.509-Zertifikate der beantragten Karte gemeint)
- Export einer Überblicksansicht von Anträgen
- Export von Detailansichten von Anträgen
- Export von Produktionsrückmeldungen zu Anträgen

Der TSP MUSS bzgl. der Anzeige von Informationen oder der Zulässigkeit von Funktionsaufrufen die Einschränkungen in [gem_AFO_0117] umsetzen. 

Anmerkung: Die Funktionen des Freigabeportals werden in den Kapiteln 6.3 Freigabe, 6.5 Sperrung und 6.6.1 Monitoring beschrieben. Die Spitzenorganisationen der Sektoren haben ausschließlich Zugriff auf die Monitoring Funktionen (siehe Kapitel 6.6.1).

5.5 Datenformate

gem_AFO_0040 Datenformat für die Schnittstellen zwischen Kartenherausgeber und TSP

Der TSP MUSS für die Übermittlung von Daten zwischen TSP und Kartenherausgeber die Anforderungen

- [gemSpec_Pers_HBA] Card-G2-A_3134 Datenformat an der Schnittstelle zwischen AttrBS und TSP
- [gemSpec_Pers_SMC-B] Card-G2-A_3105 Datenformat an der Übergabschnittstelle zwischen AttrBS und TSP

einhalten. 

gem_AFO_0044 Unterstützung der Feldtypen und Strukturtypen

Der TSP MUSS die Feldtypen und Strukturtypen aus [gemSpec_Pers_HBA] und [gemSpec_Pers_SMC-B] unterstützen:

- Card-G2-A_3139 Feldtypen der HBA-Übergabeschnittstelle
- Card-G2-A_3109 Feldtypen der SMC-B-Übergabeschnittstelle
- Card-G2-A_3140 Strukturtyp AdressType der HBA-Übergabeschnittstelle
- Card-G2-A_3110 Strukturtyp AdressType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3141 Aufzähltyp AntragsArt der HBA-Übergabeschnittstelle
- Card-G2-A_3178 Aufzähltyp AntragsArt der SMC-B-Übergabeschnittstelle
- Card-G2-A_3142 Strukturtyp AntragstellerType der HBA-Übergabeschnittstelle
- Card-G2-A_3111 Strukturtyp AntragstellerType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3143 Strukturtyp AntragsStatusHistoryType der HBA-Übergabeschnittstelle

- Card-G2-A_3112 Strukturtyp AntragsStatusHistoryType der SMC-Übergabeschnittstelle
- Card-G2-A_3144 Strukturtyp AntragStatusKey der HBA-Übergabeschnittstelle
- Card-G2-A_3113 Strukturtyp AntragStatusKey der SMC-B-Übergabeschnittstelle
- Card-G2-A_3145 Strukturtyp AttrBSType der HBA-Übergabeschnittstelle
- Card-G2-A_3114 Strukturtyp AttrBSType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3146 Aufzähltyp AusweisArt der HBA-Übergabeschnittstelle
- Card-G2-A_3171 Strukturtyp CertificateRefKey der HBA-Übergabeschnittstelle
- Card-G2-A_3179 Strukturtyp CertificateRefKey der SMC-B-Übergabeschnittstelle
- Card-G2-A_3147 Strukturtyp CertType der HBA-Übergabeschnittstelle
- Card-G2-A_3115 Strukturtyp CertType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3148 Strukturtyp ChangeType der HBA-Übergabeschnittstelle
- Card-G2-A_3116 Strukturtyp ChangesType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3149 Strukturtyp DruckzeilenType der HBA-Übergabeschnittstelle
- Card-G2-A_3150 Strukturtyp ExtCertType der HBA-Übergabeschnittstelle
- Card-G2-A_3117 Strukturtyp ExtCertType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3172 Strukturtyp FileTransferType der HBA-Übergabeschnittstelle
- Card-G2-A_3151 Strukturtyp GeburtsdatenType der HBA-Übergabeschnittstelle
- Card-G2-A_3118 Strukturtyp GeburtsdatenType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3153 Strukturtyp HNameType der HBA-Übergabeschnittstelle
- Card-G2-A_3119 Strukturtyp HNameType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3154 Strukturtyp InstAnschriftType der HBA-Übergabeschnittstelle
- Card-G2-A_3120 Strukturtyp InstAnschriftType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3155 Strukturtyp KartenStatusHistoryType der HBA-Übergabeschnittstelle
- Card-G2-A_3123 Strukturtyp KartenStatusHistoryType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3156 Aufzähltyp KartenStatusKey der HBA-Übergabeschnittstelle
- Card-G2-A_3124 Strukturtyp KartenStatusKey der SMC-B-Übergabeschnittstelle
- Card-G2-A_3157 Strukturtyp KommType der HBA-Übergabeschnittstelle
- Card-G2-A_3125 Strukturtyp KommType der SMC-B-Übergabeschnittstelle

Spezifikation Kartenpersonalisierung HBA/SMC-B

- Card-G2-A_3159 Strukturtyp PostfachAdressType der HBA-Übergabeschnittstelle
- Card-G2-A_3128 Strukturtyp PostfachAdressType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3160 Strukturtyp ProdResultType der HBA-Übergabeschnittstelle
- Card-G2-A_3129 Strukturtyp ProdResultType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3161 Strukturtyp ProfessionalDataType der HBA-Übergabeschnittstelle
- Card-G2-A_3162 Aufzähltyp ProfessionItemKey der HBA-Übergabeschnittstelle
- Card-G2-A_3122 Strukturtyp InstProfessionItemKey der SMC-B-Übergabeschnittstelle
- Card-G2-A_3163 Strukturtyp StrassenAdressType der HBA-Übergabeschnittstelle
- Card-G2-A_3130 Strukturtyp StrassenAdressType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3164 Strukturtyp TelematikIDType der HBA-Übergabeschnittstelle
- Card-G2-A_3121 Strukturtyp InstitutionType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3126 Strukturtyp KVBereichKey der SMC-B-Übergabeschnittstelle
- Card-G2-A_3127 Strukturtyp OrgFormKey der SMC-B-Übergabeschnittstelle
- Card-G2-A_3131 Strukturtyp SubjectDNType der SMC-B-Übergabeschnittstelle
- Card-G2-A_3132 Strukturtyp VPersonType der SMC-B-Übergabeschnittstelle ☒

☒ **gem_AFO_0042 Einhaltung der vereinbarten Datenstruktur für Exportdatensätze**

Der TSP MUSS für Exportdatensätze die Datenstrukturen aus [gemSpec_Pers_HBA] und [gemSpec_Pers_SMC-B] verwenden:

- [gemSpec_Pers_HBA] Card-G2-A_3137 Datenstruktur für den Export von HBA-Antragsdaten
- [gemSpec_Pers_HBA] Card-G2-A_3169 Datenstruktur für Sammelübertragung von HBA- Exportdatensätzen
- [gemSpec_Pers_SMC-B] Card-G2-A_3107 Datenstruktur für den Export von SMC-B-Antragsdaten
- [gemSpec_Pers_SMC-B] Card-G2-A_3176 Datenstruktur für Sammelübertragung von SMC-B-Exportdatensätzen. ☒

☒ **gem_AFO_0128 Dokumentation der SOAP-Schnittstelle**

Für die SOAP-Schnittstelle MUSS der TSP eine WSDL-Datei und eine zusätzliche aussagekräftige Nutzerdokumentation in Form einer PDF-Datei im Rahmen der

Umsetzung bereitstellen. Die Nutzerdokumentation MUSS einen Nutzungs- und Implementierungsleitfaden darstellen, in dem mindestens

- die zusammengehörigen Requests und Responses der SOAP-Schnittstelle dargestellt werden,
- die Parametrisierung der Requests und Responses im Überblick erläutert wird und auf verwendete Datenstrukturen der Übergabeschnittstellen referenziert wird,
- zu verwendende Fehlercodes beschrieben sind,
- alle Angaben zur Absicherung der SOAP-Schnittstelle (Angaben zu Authentisierung im Rahmen von TLS, Angaben zu Webservice Security sowie verwendete Algorithmen)

beschrieben sind. ☒

5.6 Löschen

☒ **gem_AFO_0065 Löschen oder Anonymisieren von Antragsdaten**

Der TSP MUSS die Antragsdaten wie in „Tab_004_Löschfristen“ angegeben löschen oder anonymisieren. ☒

Tabelle 3: Tab_004_Löschfristen

Status	Löschen oder anonymisieren
Der Kartenherausgeber hat einen Antrag mit Werten vorbefüllt. Der Antragsteller stellt keinen Antrag beim TSP.	Der TSP MUSS die Vorbefüllungsdaten nach einer konfigurierbaren Frist löschen. Die Frist wird vom Kartenherausgeber festgelegt. Der TSP MUSS für verschiedene Kartenherausgeber verschiedene Fristen umsetzen können.
Ein Antragsteller hat einen Antrag zwischen gespeichert, aber noch nicht abgesendet. Für das Wiederaufrufen des Antrags hat er vom TSP eine Referenznummer mit einem zugehörigen Servicepasswort erhalten.	Der TSP MUSS die Antragsdaten des Antrags löschen, wenn die Lebensdauer überschritten ist. Die Lebensdauer ist konfigurierbar, siehe [gem_AFO_0192].
Ein Antragsteller hat einen HBA-Antrag im Antragsportal ausgefüllt und abgesendet. Der Antragsteller reicht beim TSP keinen unterschriebenen Antrag (schriftlich per Postweg) oder Identitätsnachweis ein.	Der TSP MUSS die Antragsdaten nach einer konfigurierbaren Frist löschen. Die Frist wird vom Kartenherausgeber festgelegt. Der TSP MUSS für verschiedene Kartenherausgeber verschiedene Fristen umsetzen können.
Ein Antragsteller hat einen Antrag im Antragsportal ausgefüllt und abgesendet.	Der TSP MUSS die Antragsdaten nach einer konfigurierbaren Frist löschen. Die

Spezifikation Kartenpersonalisierung HBA/SMC-B

Status	Löschen oder anonymisieren
Bei der Prüfung (siehe [gem_AFO_0089]) hat der TSP Fehler gefunden, so dass der Antrag nicht zur Freigabe bereitgestellt werden kann. Der TSP versucht zunächst, den Fehler mit dem Antragsteller zu korrigieren (siehe [gem_AFO_0091]), aber die Korrekturversuche schlagen fehl.	Frist wird vom Kartenherausgeber festgelegt. Der TSP MUSS für verschiedene Kartenherausgeber verschiedene Fristen umsetzen können.
Der TSP hat den Antrag zur Freigabe an den Kartenherausgeber bereitgestellt. Der Kartenherausgeber lehnt den Antrag ab.	Der TSP MUSS die Antragsdaten (auch die im „Freigabeauftrag“ der Ablehnung) nach einer konfigurierbaren Frist anonymisieren. Die Frist wird vom Kartenherausgeber festgelegt. Der TSP MUSS für verschiedene Kartenherausgeber verschiedene Fristen umsetzen können. Die Daten werden nicht gelöscht, sondern nur anonymisiert, damit der Vorgang für die Trust Center Operatoren (z.B. auch bzgl. der Audit Events) nachvollziehbar ist. Die Antrags-Datenbank des TSP ist anhand der Referenznummern und Vorgangsnummern organisiert, daher müssen diese erhalten bleiben, wenngleich die zugehörigen sonstigen Antragsdaten anonymisiert werden.
Der Kartenherausgeber hat einen HBA-Antrag freigegeben.	Alle zum Antrag zugehörigen Daten werden 35 Jahre nach dem letzten zulässigen Folgeantrag ohne erneute Identifizierung (Anforderung aus [SigV01]) gelöscht. Dazu gehören auch die Freigabeaufträge und die Einträge in die Zertifikatshistorie.
Der Kartenherausgeber hat einen SMC-B-Antrag freigegeben.	Alle zum Antrag zugehörigen Daten werden 5 Jahre nach Ablauf der Gültigkeit der Zertifikate gelöscht. Dazu gehören auch die Freigabeaufträge und die Einträge in die Zertifikatshistorie.
Der Account eines Mitarbeiters eines Kartenherausgebers oder einer Spitzenorganisation wurde gelöscht.	Die Accountdaten inkl. der SigG-Zertifikate in der Benutzerverwaltung werden gelöscht, wenn der Account gelöscht wird. Die Entsorgung der Registrierungsunterlagen wird in [gem_AFO_0622] beschrieben.

5.7 Zertifikatshistorie

☒ **gem_AFO_0163 Speichern von Statusänderungen der Anträge in einer Zertifikatshistorie**

Der TSP MUSS die Statusänderungen der Anträge in einer Zertifikatshistorie speichern. Ein Eintrag MUSS mindestens aus dem neuen Status, Zeitstempel, Referenznummer und Bearbeiter bestehen. Die Einträge MÜSSEN signiert sein. Damit kann nachverfolgt werden, wann Änderungen an dem Antrag durchgeführt wurden. Das Löschen der Einträge wird in „Tab_004_Löschfristen“ beschrieben. Der TSP MUSS mindestens die in [gem_AFO_0100] genannten Status in die Zertifikatshistorie aufnehmen. ☒

5.8 Produktivumgebung

Für Informationsobjekte und Anwendungsprozesse mit maximal mittlerem Schutzbedarf gilt:

AN_UZP_TI_1²: Die Umgebungen von zentralen Produkten der Telematikinfrastruktur sind so gestaltet, dass keine weiteren durch die gematik spezifizierten Sicherheitsmaßnahmen erforderlich sind, um Informationsobjekte und Anwendungsprozesse mit einem maximalen Schutzbedarf von „mittel“ zu verarbeiten.

Da hier auch Schutzbedarf vorkommt, der höher ist als „mittel“, werden zusätzlich die folgenden Anforderungen gestellt:

☒ **gem_AFO_0011 Verhinderung von Angriffen und Fehlverhalten von Innentätern**

Der TSP MUSS ein geeignetes Konzept für Personaleinsatz und -qualifizierung in der Produktivumgebung erstellen. Es ist sicherzustellen, dass Personen in sicherheitsrelevanten Bereichen vertrauenswürdig und zuverlässig sind. ☒

☒ **gem_AFO_0012 Physische Sicherheit der Produktivumgebung**

Der TSP MUSS sicherheitsrelevante Bereiche der Produktivumgebung in einem geeigneten Rechenzentrum betreiben, welches allgemein anerkannten Standards genügt. Er MUSS weitere Maßnahmen zur Verfügbarkeit des TSP und der gesamten Produktivumgebung ergreifen, wie z. B. redundante Systeme. ☒

☒ **gem_AFO_0013 Schutz der Protokolldaten**

Der TSP MUSS Maßnahmen umsetzen, die die Vertraulichkeit und Integrität von Protokolldaten in der Produktivumgebung sicherstellen. Der TSP MUSS durch technische und organisatorische Regelungen eine unberechtigte Löschung von Protokolldaten vermeiden. Der TSP MUSS den Zugriff auf die Protokolldaten technisch schützen und die Zugriffsrechte restriktiv vergeben. Der TSP MUSS jeden Zugriff protokollieren. ☒

² aus [gemMeth_SichAnalyse]

☒ **gem_AFO_0014 Technisch bedingter Ausfall der Produktivumgebung**

Der TSP MUSS einen Komplettausfall der Produktivumgebung durch entsprechende redundante Auslegung relevanter Komponenten so gut wie technisch möglich und wirtschaftlich angemessen verhindern. ☒

☒ **gem_AFO_0016 Keine fehlerhafte Umsetzung von Rollen und Berechtigungen**

Der TSP MUSS eine Rollen- und Rechtematrix für die Produktivumgebung erstellen und prüfen, ob ggf. Konflikte entstehen und bestimmte Kombinationen von Rollen bzw. Rechten auszuschließen sind. ☒

☒ **gem_AFO_0017 Übertragung und Datenspeicherung innerhalb der Produktivumgebung**

Der TSP MUSS Maßnahmen zur sicheren Datenübertragung und Speicherung innerhalb der Produktivumgebung umsetzen. ☒

☒ **gem_AFO_0019 Maßnahmen gegen eine Manipulation des Prozessablaufs umsetzen**

Der TSP DARF NICHT ermöglichen, Prozessschritte der Kartenpersonalisierung unberechtigt auszulassen, zu wiederholen oder die Reihenfolge zu ändern. Das gilt insbesondere für Prüfungen und Freigaben. ☒

☒ **gem_AFO_0020 Maßnahmen gegen eine Manipulation des Portals umsetzen**

Der TSP MUSS das Webportal unter Beachtung anerkannter Sicherheitsstandards entwickeln. ☒

Anmerkung: Ein Beispiel für einen solchen Standard ist [OWASP].

☒ **gem_AFO_0022 Maßnahmen zur sicheren Erzeugung, Speicherung und Bereitstellung der Zertifikate und Schlüssel der CA**

Die CAs des TSP MÜSSEN die Schlüssel nach einem anerkannten Verfahren erzeugen. Der TSP MUSS die in der Produktivumgebung gespeicherten CA Schlüssel wirksam gegen unberechtigten Zugriff (Auslesen, Manipulation, Löschen, unberechtigte Verwendung) schützen. Der TSP MUSS die Zertifikate zuverlässig bereitstellen, dies beinhaltet Maßnahmen zur Verfügbarkeit und einen OCSP-Dienst. ☒

☒ **gem_AFO_0024 Rechtliche Zulässigkeit der internen Protokolldaten**

Zur Erhebung, Verarbeitung und Nutzung personenbezogener Protokolldaten MUSS der TSP sicherstellen, dass dies rechtlich zulässig ist und der Betroffene seine Einwilligung dazu gegeben hat. Der TSP MUSS die Prinzipien der Datensparsamkeit und Zweckbindung einhalten. ☒

☒ **gem_AFO_0025 Prüfung und Umsetzung von Anonymisierung bzw. Pseudonymisierung von Protokolldaten**

Der TSP MUSS so wenig personenbezogene Protokolldaten wie möglich erheben, verarbeiten oder nutzen. Insbesondere MUSS er personenbezogene Daten anonymisieren oder pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. ☒

☒ gem_AFO_0026 Maßnahmen gegen zweckfremde Verkettungen innerhalb der Produktivumgebung

Der TSP MUSS Sicherheitsmaßnahmen umsetzen, die den unberechtigten Zugriff auf Identitätsdaten erschweren (Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle), so dass Identitätsdaten aus der Fachanwendung nicht einfach mit anderen Identitätsdaten verkettet werden können. ☒

☒ gem_AFO_0027 Maßnahmen zur Datentrennung

Der TSP MUSS Speicherorte von Daten aus der Fachanwendung Kartenpersonalisierung von anderen Fachanwendungen trennen. Bei den Zugriffsrechten MUSS er das Prinzip „Separation of Duties“ einhalten. ☒

☒ gem_AFO_0028 Maßnahmen zum Datenschutz

Der TSP MUSS die technischen und organisatorischen Sicherheitsmaßnahmen aus [BDSG], Anlage zu § 9 umsetzen (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungsgebot). ☒

5.9 Mandantenfähigkeit

☒ gem_AFO_0126 Mandantenfähigkeit des TSP

Der TSP DARF beim Zugriff auf Daten von verschiedenen Kartenherausgebern, Sektoren und Spitzenorganisationen NICHT Daten anzeigen oder zur Verfügung stellen, für die der jeweilige Kartenherausgeber, Sektor und Spitzenorganisation nicht zugriffsberechtigt ist. ☒

Anmerkung: Eine Übersicht über die verschiedenen Organisationen findet sich in Abbildung 4.

5.10 Ansprechpartner

☒ gem_AFO_0720 Benennung von Ansprechpartnern des TSP

Der TSP MUSS Ansprechpartner für die Sektoren benennen und diesen schriftlich mitteilen. ☒

☒ gem_AFO_0071 Anzeige einer Hotline Nummer zum Service Desk

Der TSP MUSS im Antragsportal und im Freigabeportal eine Hotline-Nummer zu einem Service Desk (SPOC) mit Servicezeiten und Anrufrufen anzeigen. ☒

☒ gem_AFO_0072 Verfügbarkeit des Service Desk

Der TSP MUSS den zu der Hotline-Nummer zugehörigen Service Desk Montag bis Freitag jeweils 8 bis 17 Uhr zur Verfügung stellen. ☒

5.11 Betrieb

gem_AFO_0127 IT-Service-Management

Der TSP MUSS gemäß [gemKPT_Betr] ein providerspezifisches Betriebskonzept für die Produktivumgebung erstellen. Die in diesem Betriebskonzept definierten Vorgaben und Prozesse zum IT-Service-Management nach ITIL MÜSSEN auch für die TSP-Schnittstelle berücksichtigt und angewendet werden. 

6 Funktionsmerkmale

In diesem Kapitel werden die TUCs aus Kapitel 4 *Zerlegung des Produkttyps* im Detail beschrieben und TUC-spezifische Anforderungen definiert. Es werden die Schnittstellenbezeichnungen [Sch_xxx] aus diesem Kapitel verwendet.

6.1 Vorbefüllung

Bei der Vorbefüllung werden Daten vom Kartenherausgeber an den TSP übermittelt, die im Antragsprozess und den administrativen Prozessen (z. B. Freigabe, Sperrung) genutzt werden. Die Übermittlung der Daten dient u. a. der Vermeidung von Eingabefehlern sowie der Erhöhung der Effizienz bei Antragstellung und Bearbeitung.

Die Vorbefüllung wird nicht von allen Sektoren eingesetzt.

Die Vorbefüllung kann in verschiedenen Varianten realisiert werden, die im Folgenden beschrieben werden.

- Variante [VB-1]: Vorbefüllung über Datei-Upload am Vorbefüllungsportal.
- Variante [VB-2]: Vorbefüllung über Eingabe am Vorbefüllungsportal.
- Variante [VB-3] (OPTIONAL): Vorbefüllung über Online-Schnittstelle mit Authentisierung des Kartenherausgebers.
- Variante [VB-4]: Vorbefüllung über SOAP-Schnittstelle.
- Variante [VB-5]: Vorbefüllung über synchrone Online-Schnittstelle ohne Authentisierung des Kartenherausgebers

Die Varianten der Vorbefüllung, die eine Authentisierung des Kartenherausgebers erfordern ([VB-1] bis [VB-4]) setzen die Rechte zur Vorbefüllung voraus. Zugriff auf das Vorbefüllungsportal ist für Anwender mit Monitoring Rolle nicht möglich.

6.1.1 TUC-Beschreibung

Tabelle 4: Tab_002_TUC_Vorbefüllung

Element	Beschreibung
Name	Vorbefüllung
Beschreibung	Bei der Vorbefüllung werden Daten vom Kartenherausgeber an den TSP übermittelt, die im Antragsprozess genutzt werden. Die Übermittlung der Daten dient u. a. der Vermeidung von Eingabefehlern sowie der Erhöhung der Effizienz bei Antragstellung und Bearbeitung.

Element	Beschreibung
Auslöser	Der Kartenherausgeber will dem TSP Daten für die Vorbefüllung übermitteln.
Vorbedingungen	Eine TLS/SSL-Verbindung wurde gemäß [gem_AFO_0007] aufgebaut. Variante [VB-1] und [VB-2]: Der Kartenherausgeber hat sich am Vorbefüllungsportal authentisiert. Variante [VB-3]: Der Kartenherausgeber hat sich an der Online-Schnittstelle authentisiert. Variante [VB-4]: Der Kartenherausgeber hat sich an der SOAP-Schnittstelle authentisiert. Variante [VB-5]: Es wird empfohlen, dass der Kartenherausgeber den Antragsteller am Portal des Kartenherausgebers auf geeignete Weise authentifiziert, um unberechtigten Zugriff auf Vorbefüllungsdaten zu verhindern.
Eingangsdaten	• Daten zur Vorbefüllung von Anträgen. Die Vorbefüllungsdaten liegen in den Varianten [VB-1], [VB-3], [VB-4] und [VB-5] in Form einer XML-Datenstruktur vor. Innerhalb einer XML-Datei können bei [VB-1], [VB-3], [VB-4] ein oder mehrere Datensätze enthalten sein, bei [VB-5] nur ein Datensatz. Die Struktur ist in [gem_AFO_0005] beschrieben. In Variante [VB-2] werden Vorbefüllungsdaten im Portal eingegeben, die dem Inhalt der XML-Struktur entsprechen. Optional enthält diese XML-Struktur auch eine Vorgangsnummer (VorgangsNrAttrBS siehe unten). • Vorgangsnummer Mit der Vorgangsnummer kann der Antragsteller nach Abschluss der Vorbefüllung die vorbefüllten Daten beim TSP aufrufen. Dazu teilt der Kartenherausgeber diese Vorgangsnummer dem Antragsteller mit (dies ist außerhalb der Betrachtungsgrenzen dieser Spezifikation). Weiterhin kann der Antragsteller mit der Vorgangsnummer auf zwischengespeicherte und abgesendete Anträge, die auf Basis dieser Vorbefüllung erstellt wurden, zugreifen. Der Zugriff auf abgesendete Anträge ist nur solange möglich, bis der Antrag in Bearbeitung beim TSP ist. Es gibt zwei Arten von Vorgangsnummern: - o VorgangsNrAttrBS: Der Kartenherausgeber erzeugt optional zu einer Vorbefüllung eine Vorgangsnummer, die er zusammen mit den restlichen Vorbefüllungsdaten an den TSP übermittelt, d. h. die Vorgangsnummer ist ein Eingangsdatum (Übergabe im Attribut „VorgangsNrAttrBS“).

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	o VorgangsNrTSP: Der TSP erzeugt für jede Vorbefüllung eine losübergreifend eindeutige Vorgangsnummer und teilt sie dem Kartenherausgeber mit. (Übergabe im Attribut „VorgangsNr“ der Rückmeldung des TSP) Alle Funktionen, die die Eingabe einer Vorgangsnummer erfordern, akzeptieren sowohl die VorgangsNrAttrBS (falls vorhanden) als auch die VorgangsNrTSP.
Komponenten	Kartenpersonalisierung.
Ausgangsdaten	[VB-1], [VB-2], [VB-3], [VB-4] : Gesamter Vorbefüllungsdatensatz inkl. einer oder zwei Vorgangsnummern (optional die vom Kartenherausgeber erzeugte Vorgangsnummer, immer die vom TSP erzeugte Vorgangsnummer). [VB-5] : zwischengespeicherter oder abgesendeter Antrag des Antragstellers (sofern der Antragsteller die Bearbeitung nicht abgebrochen hat)
Nachbedingungen	[VB-1], [VB-2], [VB-3], [VB-4] : Beim TSP liegen die Daten aus der Vorbefüllung inkl. der zugehörigen Vorgangsnummern vor und können zur Antragstellung genutzt werden. Teile der übermittelten Daten können vom Antragsteller geändert werden, sie haben daher nur vorläufigen Charakter. Daher werden die Vorbefüllungsdaten separat von den übrigen Daten in einer Vorbefüllungs-Datenbank des TSP abgelegt. [VB-5]: beim TSP liegt ein zwischengespeicherter oder abgesendeter Antrag vor (sofern der Antragsteller die Bearbeitung nicht abgebrochen hat)
Standardablauf	[VB-1], [VB-2], [VB-3], [VB-4] : Siehe Abbildung 5 „Abb_001_Vorbefüllung_mit_KH_Authentisierung“ [VB-5]: Abbildung 6 „Abb_003_Vorbefüllung_ohne_KH_Authentisierung“
Varianten/Alternativen	• Der Kartenherausgeber kann die Daten über verschiedene Schnittstellen an den TSP übermitteln. Diese Varianten

Element	Beschreibung
	sind beim Standardablauf beschrieben ([VB-1], [VB-2], [VB-3], [VB-4], [VB-5]). Die Vorgangsnummer VorgangsNrAttrBS kann optional vom Kartenherausgeber erzeugt werden.
Fehlerfälle	- Wenn die Authentisierung des Kartenherausgebers fehlschlägt, lässt der TSP keine Übertragung der Vorbefüllungsdaten zu (nur [VB-1], [VB-2], [VB-3], [VB-4]) - Wenn der Kartenherausgeber im Fall von [VB-1], [VB-2], [VB-3], [VB-4] die geforderten TLS-Versionen oder Ciphersuites nicht unterstützt, lässt der TSP keine Übertragung der Vorbefüllungsdaten zu. - Wenn der Browser des Antragstellers im Fall von [VB-5] die geforderten TLS-Versionen oder Ciphersuites nicht unterstützt, lässt der TSP keine Übertragung der Vorbefüllungsdaten zu. - Wenn die Vorbefüllungsdaten nicht im vereinbarten XML-Format vorliegen, sendet der TSP dem Kartenherausgeber eine Fehlermeldung.
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Siehe Abbildung 5 „Abb_001_Vorbefüllung_mit_KH_Authentisierung“ Siehe Abbildung 6 „Abb_003_Vorbefüllung_ohne_KH_Authentisierung“

6.1.2 Ablauf

Die Kommunikation zwischen Kartenherausgeber und TSP erfolgt über folgende Schnittstellen:

- Variante [VB-1]: [Sch_Vorbefüllungsportal].
- Variante [VB-2]: [Sch_Vorbefüllungsportal].
- Variante [VB-3] (OPTIONAL): [Sch_Onlineschnittstelle_Vorbefüllung].
- Variante [VB-4]: [Sch_SOAP]
- Variante [VB-5]: [Sch_Onlineschnittstelle_Vorbefüllung].

Der Ablauf für [VB-1] bis [VB-4] ergibt sich aus der folgenden Abbildung:

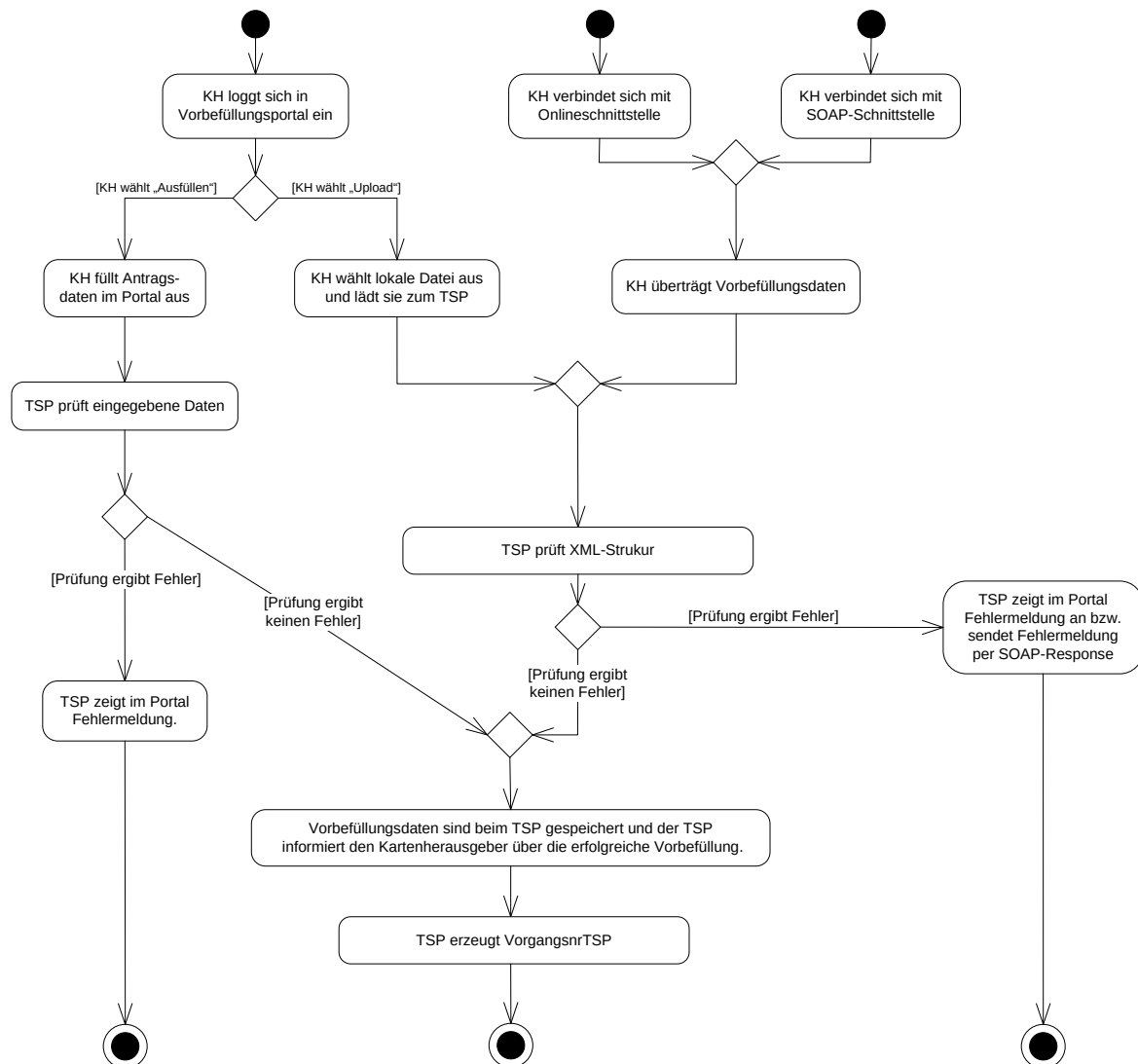


Abbildung 5: Abb_001_Vorbefüllung_mit_KH_Authentisierung

Der Ablauf für [VB-5] ergibt sich aus der folgenden Abbildung:

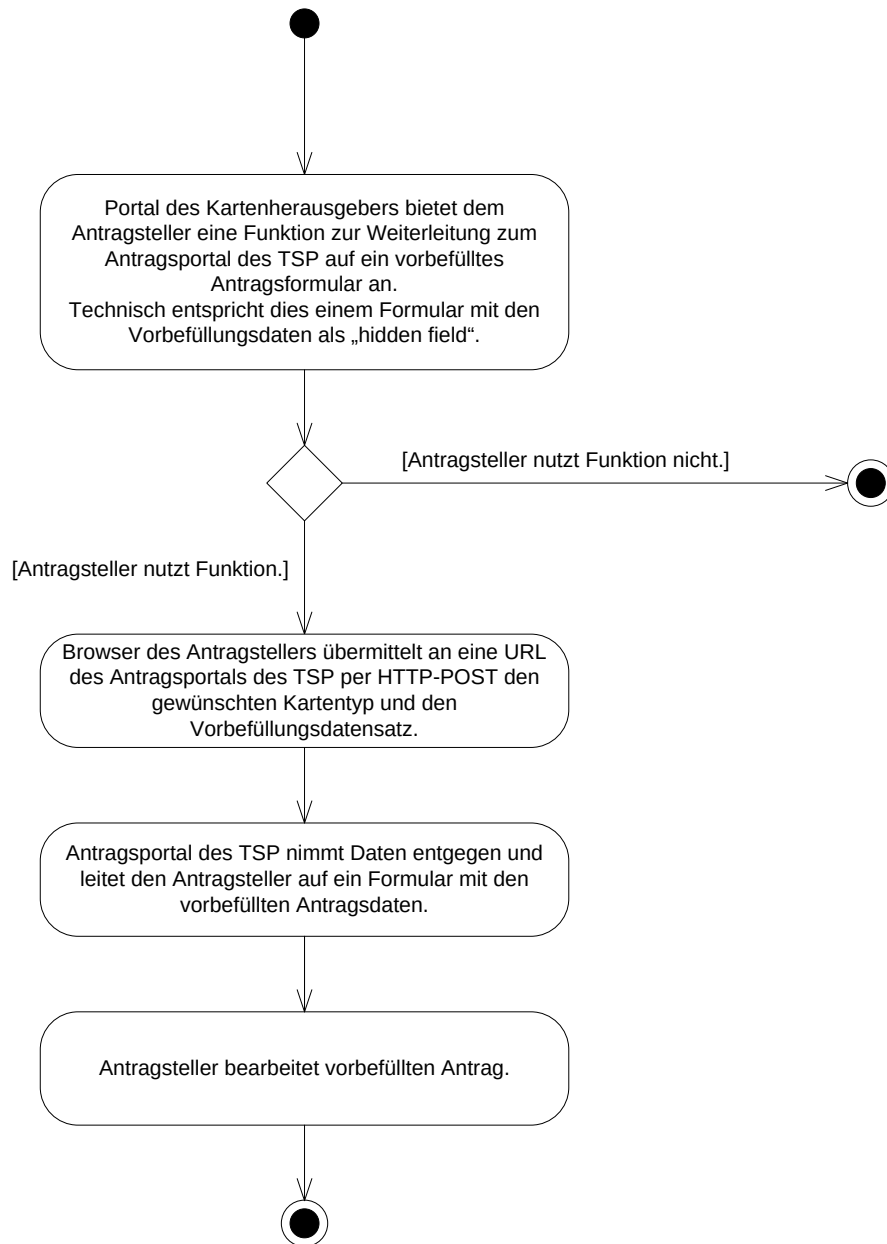


Abbildung 6: Abb_003_Vorbefüllung_ohne_KH_Authentisierung

6.1.3 Anforderungen

6.1.3.1 Anforderungen für alle Varianten der Vorbefüllung

☒ **gem_AFO_0005 Einhaltung der vereinbarten XML-Struktur für die Vorbefüllungsdaten**

Der Kartenherausgeber MUSS die Vorbefüllungsdaten in der vereinbarten XML-Struktur anordnen. Die XML-Struktur ist in den folgenden Anforderungen aus [gemSpec_Pers_HBA] und [gemSpec_Pers_SMC-B] definiert:

- [gemSpec_Pers_HBA] Card-G2-A_3135 Struktur der Vorbefüllungsdaten HBA
- [gemSpec_Pers_SMC-B] Card-G2-A_3106 Struktur der Vorbefüllungsdaten SMC-B
- [gemSpec_Pers_HBA] Card-G2-A_3167 Datenstruktur für die Sammelübertragung von HBA-Vorbefüllungen
- [gemSpec_Pers_SMC-B] Card-G2-A_3173 Datenstruktur für die Sammelübertragung von SMC-B-Vorbefüllungen

Eine Ausnahme ist die Variante [VB-2], bei der der Kartenherausgeber die Daten von Hand in das Vorbefüllungsportal eingibt. ☒

☒ **gem_AFO_0141 Erzeugung einer eindeutigen Vorgangsnummer für Vorbefüllung**

Der TSP MUSS dem Kartenherausgeber ermöglichen, bei der Vorbefüllung optional eine Vorgangsnummer zu erzeugen und im Vorbefüllungsdatensatz mitzuliefern.

Wenn der Kartenherausgeber bei der Vorbefüllung eine Vorgangsnummer erzeugt und im Vorbefüllungsdatensatz mitliefert, dann MUSS diese Vorgangsnummer innerhalb des jeweiligen Kartenherausgebers eindeutig sein.

Der TSP MUSS eine losübergreifend einheitliche VorgangsNrTSP erzeugen und an den Kartenherausgeber zurückliefern.

Die folgende Bildungsregel MUSS vom TSP und von den Kartenherausgebern bei der Erzeugung von Vorgangsnummern umgesetzt werden:

- Die Vorgangsnummer hat 18 Stellen.
- 10 Stellen als „Klartext-Referenz“ zum Antrag, die sich wiederum aus zwei Blöcken zusammen setzen:
 - o 5-Stellen-Kennung des Kartenherausgebers oder TSP:
 - eindeutige Identifizierung des Kartenherausgebers im Fall der Erzeugung der Vorgangsnummer durch den Kartenherausgeber, welche sich aus dem einstelligen Präfix der TelematikID des Sektors, dem Kartentyp (HBA oder SMC-B, einstellig) und einem dreistelligen Kartenherausgeber-spezifischen Nummernraum zusammensetzt (z.B. Kammercode oder vergleichbare bereits vorhandene Kennungen)
 - ZDA Kennung im Fall der Erzeugung der Vorgangsnummer durch den TSP: T< Kartentyp (HBA oder SMC-B, einstellig)>TSI.

Spezifikation Kartenpersonalisierung HBA/SMC-B

- o 5 Stellen: eindeutiges Identifizierungsmerkmal des Kartenherausgebers oder des TSP für die Vorgangsnummer z.B. eine fortlaufende Nummer oder eine Zuordnungssnummer aus den Bestandssystemen oder eine sonstige Nummer
- 8-stelliger Zufallswert vom Typ „string“ gemäß [gemSpec_Pers_SMC-B] bzw. [gemSpec_Pers_HBA], um einen gezielten Zugriff auf Vorbefüllungsdaten durch Unberechtigte auszuschließen. Die Erzeugung der Zufallswerte obliegt dem jeweiligen Kartenherausgeber bzw. TSP.

Die folgende Übersicht illustriert die Bildungsregel (am Beispiel einer vom Kartenherausgeber gebildeten Vorgangsnummer):

Stelle	1	2	3-5	6-10	11-18
Wert	Sektorkennzeichen: Präfix der Telematik-ID gemäß gem-KPT_PKI_TIP#Tab_PKI_101	Kartentyp: „1“ für HBA, „2“ für SMC-B	Kartenherausgeber-spezifischer Nummernraum, z. B. Kammercode oder vergleichbare ggf. bereits vergebene Kennungen	Identifizierungsmerkmal für den Vorgang	8-stelliger Zufallswert



gem_AFO_0805 Überschreibung von Vorbefüllungsdaten

Der TSP MUSS dem Kartenherausgeber ermöglichen, eine vom Kartenherausgeber erzeugte VorgangsNrAttrBS erneut zur Vorbefüllung zu verwenden. Der TSP MUSS in diesem Fall den zur VorgangsNrAttrBS gespeicherten Vorbefüllungsdatensatz überschreiben. 

gem_AFO_0806 Kopplung eines Antrags an den Stand der Vorbefüllungsdaten zum Zeitpunkt der ersten Antragsbearbeitung

Der TSP MUSS im Fall des ersten Zwischenspeicherns oder ersten Absendens eines vorbefüllten Antrags den Stand der Vorbefüllungsdaten zum Zeitpunkt des Öffnens des Antragsformulars durch den Antragsteller an den Antrag koppeln und speichern. Der TSP MUSS bei der Anzeige von Änderungen im Antrag gegenüber den Vorbefüllungsdaten diesen zum Antrag gespeicherten Stand der Vorbefüllungsdaten heranziehen. 

☒ **gem_AFO_0807 Anzahl von Anträgen auf Basis einer Vorbefüllung**

Solange ein Antrag auf Basis einer Vorbefüllung noch nicht vom TSP in Bearbeitung genommen wurde, MUSS der TSP den Antragsteller bei Zugriff auf einen Antrag mittels der zu dieser Vorbefüllung gehörenden Vorgangsnummer immer auf den zwischengespeicherten oder abgesendeten Antrag leiten. Der TSP MUSS in diesem Fall dem Antragsteller die Bearbeitung des Antrags und erneute Speicherung bzw. erneutes Absenden ermöglichen. Sobald ein Antrag auf Basis einer Vorbefüllung abgesendet und vom TSP in Bearbeitung genommen wurde, MUSS der TSP den Antragsteller bei Zugriff auf einen Antrag mittels dieser Vorgangsnummer auf einen neuen vorbereiteten Antrag basierend auf dem aktuellen Stand der Vorbefüllungsdaten leiten. Der TSP MUSS sicherstellen, dass es zu einem Zeitpunkt nur jeweils einen Antrag in für den Antragsteller bearbeitbarem Zustand zu einer Vorgangsnummer gibt. ☒

6.1.3.2 Anforderungen für die Varianten [VB-1], [VB-2], [VB-4] und [VB-5] der Vorbefüllung

☒ **gem_AFO_0001 Ablauf der Vorbefüllung wie in Beschreibung**

Der TSP MUSS die Varianten [VB-1], [VB-2], [VB-4] und [VB-5] ermöglichen. Der TSP MUSS es den Kartenherausgebern ermöglichen, die Vorbefüllung wie in

- „Abb_001_Vorbefüllung_mit_KH_Authentisierung“ (für [VB-1], [VB-2], [VB-4]),
- „Abb_003_Vorbefüllung_ohne_KH_Authentisierung“ (für [VB-5]), und
- „Tab_002_TUC_Vorbefüllung“

dargestellt durchzuführen. ☒

6.1.3.3 Anforderungen für die Varianten [VB-1], [VB-2], [VB-3] und [VB-4] der Vorbefüllung

☒ **gem_AFO_0035 Keine Vorbefüllung ohne Authentisierung des Kartenherausgebers**

Der TSP DARF NICHT ermöglichen, dass Vorbefüllungsdaten ohne vorherige Authentisierung des Kartenherausgebers übertragen werden. Dabei kann es sich abhängig von der Variante entweder um eine Authentisierung eines Mitarbeiters des Kartenherausgebers am Vorbefüllungsportal oder um eine Authentisierung einer Anwendung des Kartenherausgebers handeln. ☒

☒ **gem_AFO_0145 Nicht-Anzeige von Anträgen bei Vorbefüllung**

Der TSP DARF es NICHT ermöglichen, dass sich ein berechtigter Mitarbeiter eines Kartenherausgebers andere Antragsdaten als die von berechtigten Mitarbeitern des gleichen Kartenherausgebers eingegebenen bzw. von berechtigten Anwendungen des gleichen Kartenherausgebers übertragenen Antragsdaten am Vorbefüllungsportal anzeigen lassen kann oder downloaden kann oder über die Onlineschnittstelle erhalten kann. ☒

☒ **gem_AFO_0190 Anzeige oder Benachrichtigung nach erfolgreicher Vorbefüllung**

Wenn die Vorbefüllung erfolgreich war, MUSS der TSP den Kartenherausgeber darüber informieren: In Variante [VB-1] und [VB-2] zeigt er dies im Vorbefüllungsportal an, in Variante [VB-3] und [VB-4] sendet er eine entsprechende Response. ☒

6.1.3.4 Anforderungen für Variante [VB-1]

☒ **gem_AFO_0104 Keine Vorbefüllung per Dateiupload ohne Zugriffsrechte des Kartenherausgebers**

Der TSP DARF NICHT ermöglichen, dass Vorbefüllungsdaten per Dateiupload ([VB-1]) übertragen oder angenommen werden, wenn der Anwender nicht die Zugriffsrechte für eine Vorbefüllung hat. ☒

☒ **gem_AFO_0133 Reaktion auf falsche XML-Struktur bei Upload von Vorbefüllungsdaten**

Wenn beim Upload der Vorbefüllungsdaten im Vorbefüllungsportal ([VB-1]) die XML-Struktur nicht korrekt ist, MUSS der TSP im Portal eine Fehlermeldung anzeigen. Der TSP MUSS die fehlerhaften Daten verwerfen, ohne sie zu speichern. ☒

☒ **gem_AFO_0140 Übermittlung der Vorgangsnummer bei Vorbefüllung über Upload**

Der TSP MUSS eine Vorgangsnummer erzeugen (VorgangsNrTSP), in die Datenstruktur einfügen und dem Kartenherausgeber die neue Datei zum Download anbieten. ☒

6.1.3.5 Anforderungen für Variante [VB-2]

☒ **gem_AFO_0150 Eingabe von Vorbefüllungsdaten ermöglichen**

Der TSP MUSS es ermöglichen, am Vorbefüllungsportal Vorbefüllungsdaten einzugeben ([VB-2]). Dabei MUSS der TSP ausschließlich die Eingabe von Daten ermöglichen, die zu der in der Übergabeschnittstelle gemäß [gemSpec_Pers_HBA] Card-G2-A_3135 bzw. [gemSpec_Pers_SMCB] Card-G2-A_3106 definierten Vorbefüllungsdatenstruktur gehören, und die gemäß der Sektor-spezifischen Konfiguration vorgesehen sind. ☒

☒ **gem_AFO_0191 Keine Eingabe von Vorbefüllungsdaten ohne Zugriffsrechte des Kartenherausgebers**

Der TSP DARF NICHT ermöglichen, dass Vorbefüllungsdaten am Vorbefüllungsportal ([VB-2]) eingegeben werden, wenn der eingeloggte Anwender nicht die Zugriffsrechte für eine Vorbefüllung hat. ☒

☒ **gem_AFO_0134 Reaktion auf falsche Vorbefüllungsdaten bei Eingabe im Vorbefüllungsportal**

Wenn bei der Eingabe der Vorbefüllungsdaten im Vorbefüllungsportal ([VB-2]) die Daten nicht syntaktisch korrekt sind, MUSS der TSP im Portal eine Fehlermeldung anzeigen. Der TSP MUSS die fehlerhaften Daten verwerfen, ohne sie zu speichern. ☒

☒ **gem_AFO_0142 Übermittlung der Vorgangsnummer bei Vorbefüllung über Eingabe im Vorbefüllungsportal**

Der TSP MUSS eine Vorgangsnummer erzeugen (VorgangsNrTSP) und sie dem Kartenherausgeber im Vorbefüllungsportal anzeigen. ☒

6.1.3.6 Anforderungen für Varianten [VB-1], [VB-2] und VB[4]

☒ **gem_AFO_0917 Anzeige und Aktionen in einer Übersichtsansicht im Vorbefüllungsportal**

In einer Übersichtsansicht unter dem Menüpunkt „Vorbefüllungsdaten einsehen“ MUSS der TSP die Vorbefüllungsdatensätze in einer Tabelle darstellen, die aus den in [Tab_009_Anzeige_und_Aktionen_im_Vorbefüllungsportal] genannten Tabellenspalten besteht. Jeder Vorbefüllungsdatensatz wird in einer Zeile dargestellt.

Falls der TSP die Tabelle aufgrund ihrer Größe auf mehreren Seiten verteilt, MUSS er es ermöglichen, vor- und zurückzublättern.

Der TSP MUSS die in „[Tab_009_Anzeige_und_Aktionen_im_Vorbefüllungsportal]“ genannten Aktionen in der Übersichtsansicht zur Verfügung stellen. ☒

☒ **gem_AFO_0918 Anzeige und Aktionen in einer Detailansicht im Vorbefüllungsportal**

Der TSP MUSS es einem Anwender ermöglichen, durch Aufruf eines Links direkt die Detailansicht eines Vorbefüllungsdatensatzes aufzurufen. In der Detailansicht MUSS der TSP alle Daten einer ausgewählten Vorbefüllung darstellen. Der TSP MUSS die in „[Tab_009_Anzeige_und_Aktionen_im_Vorbefüllungsportal]“ genannten Aktionen in der Detailansicht zur Verfügung stellen. ☒

Tabelle 5: Tab_009_Anzeige_und_Aktionen im_Vorbefüllungsportal

Zugriffrechte des eingeloggten Anwenders	Spalten in Übersichtsansicht	Aktionen in Übersichtsansicht	Daten in Detailansicht	Aktionen in Detailansicht
Vorbefüllung	- Vorgangsnummer des Kartenherausgebers (falls vorhanden) - Vorgangsnummer TSP - Name des Antragstellers	- Alle Datensätze/keine Datensatz markieren - markierte Datensätze löschen - markierte Datensätze in XML exportieren - Antrag	alle vorbefüllten Antrags- und Freigabedaten	- Löschen des Datensatzes - XML-Export des Datensatzes

Zugriffrechte des eingeloggten Anwenders	Spalten in Überblicks-ansicht	Aktionen in Überblicks-ansicht	Daten in Detailansicht	Aktionen in Detailansicht
	Datensatz angelegt am (Datum)	für einen markierten Datensatz stellen		

6.1.3.7 Anforderungen für Variante [VB-3]

☒ **gem_AFO_0800 Ablauf der Vorbefüllung wie in Beschreibung für [VB-3]**

Der TSP KANN die Variante [VB-3] wie in

- „Abb_001_Vorbefüllung_mit_KH_Authentisierung“ und
- „Tab_002_TUC_Vorbefüllung“

dargestellt durchführen. ☒

☒ **gem_AFO_0136 Aufruf der Onlineschnittstelle für Vorbefüllung gemäß [VB-3]**

Der TSP KANN es dem Kartenherausgeber ermöglichen, die Onlineschnittstelle zur Vorbefüllung mit einem http-POST-Request aufzurufen. ☒

☒ **gem_AFO_0008 Authentisierung des Kartenherausgebers bei Nutzung der Onlineschnittstelle**

Wenn die Vorbefüllung über die Onlineschnittstelle [VB-3] erfolgt, MUSS der TSP den Kartenherausgeber vor der Übertragung von Vorbefüllungsdaten authentisieren. Dies MUSS auf folgende Weise erfolgen:

Der Kartenherausgeber sendet beim Aufruf der Onlineschnittstelle des http-POST-Requests Benutzername und Passwort mit. Der TSP prüft Benutzername und Passwort. Er lässt eine Übertragung nur bei korrekter Authentisierung zu. ☒

☒ **gem_AFO_0135 Reaktion auf falsche XML-Struktur bei Übertragung von Vorbefüllungsdaten über die Onlineschnittstelle**

Wenn bei der Übertragung der Vorbefüllungsdaten über die Onlineschnittstelle ([VB-3]) die XML-Struktur nicht korrekt ist, MUSS der TSP dem Kartenherausgeber als http-Response eine Fehlermeldung senden. Der TSP MUSS die fehlerhaften Daten verwerfen, ohne sie zu speichern. ☒

☒ **gem_AFO_0143 Übermittlung der Vorgangsnummer bei Vorbefüllung über die Onlineschnittstelle**

Der TSP MUSS eine Vorgangsnummer (VorgangsNrTSP) erzeugen, in die XML-Struktur einfügen und die neue Datei über http-POST-Response an den Kartenherausgeber übertragen. ☒

6.1.3.8 Anforderungen für Variante [VB-4]

☒ **gem_AFO_0137 Aufruf der SOAP-Schnittstelle für Vorbefüllung**

Der TSP MUSS es dem Kartenherausgeber ermöglichen, die Vorbefüllung mit einem SOAP-Request ([VB-4]) aufzurufen. ☒

Anmerkung: Die zwingende gegenseitige Authentisierung bei Nutzung der SOAP-Schnittstelle wird in [gem_AFO_0139] beschrieben.

☒ **gem_AFO_0138 Reaktion auf falsche XML-Struktur bei Übertragung von Vorbefüllungsdaten über die SOAP-Schnittstelle**

Wenn bei der Übertragung der Vorbefüllungsdaten über die SOAP-Schnittstelle ([VB-4]) die XML-Struktur nicht korrekt ist, MUSS der TSP dem Kartenherausgeber als SOAP-Response eine Fehlermeldung senden. Der TSP MUSS die fehlerhaften Daten verwerfen, ohne sie zu speichern. ☒

☒ **gem_AFO_0144 Übermittlung der Vorgangsnummer bei Vorbefüllung über die SOAP-Schnittstelle**

Der TSP MUSS eine Vorgangsnummer erzeugen (VorgangsNrTSP), in die XML-Struktur einfügen und die neue Datei über SOAP-Response an den Kartenherausgeber übertragen. ☒

6.1.3.9 Anforderungen für Variante [VB-5]

☒ **gem_AFO_0801 Aufruf der synchronen Online-Schnittstelle zur Vorbefüllung ohne Authentisierung des Kartenherausgebers**

Der TSP muss es ermöglichen, die synchrone Onlineschnittstelle zur Vorbefüllung ohne Authentisierung des Kartenherausgebers mit einem http-POST-Request anzusprechen.

Der http-POST-Request MUSS zwei Parameter haben. Der erste Parameter MUSS der zu beantragende Kartentyp (HBA oder SMC-B) sein, der zweite Parameter MUSS die XML-Struktur mit den Vorbefüllungsdaten des Antragstellers sein. ☒

☒ **gem_AFO_0802 Reaktion auf falsche XML-Struktur bei Übertragung von Vorbefüllungsdaten gemäß [VB-5]**

Wenn bei der Übertragung der Vorbefüllungsdaten über die Onlineschnittstelle ([VB-5]) kein gültiger Kartentyp übermittelt wurde, oder die XML-Struktur nicht korrekt ist, MUSS der TSP als http-Response dem Antragsteller mit HTTP Status code 400 eine menschenlesbare Fehlermeldung senden. Der TSP MUSS die fehlerhaften Daten verwerfen, ohne den Antragsteller auf ein vorbereitetes Antragsformular weiterzuleiten. ☒

☒ **gem_AFO_0803 Weiterleitung zum vorbereiteten Antrag**

Der TSP MUSS die übertragenen Parameter des http-POST-Requests auswerten, und bei korrekten Parametern den Antragsteller auf das mit den Werten aus der XML Struktur vorbereitete Antragsformular weiterleiten. Der TSP MUSS den Kartenherausgeber aus dem Wert „AttrBestStelle“ des übermittelten Vorbefüllungsdaten-

satzes ermitteln. Der TSP MUSS es dem Antragsteller ermöglichen, den vorbefüllten Antrag zu bearbeiten, zwischenspeichern oder abzusenden. ☒

☒ **gem_AFO_0925 Verarbeitung der Vorbefüllungsdaten bei [VB-5]**

Sofern der Antragsteller die Bearbeitung nicht abgebrochen hat, MUSS beim TSP als Resultat von [VB-5] ein zwischengespeicherter oder abgesendeter Antrag vorliegen. ☒

☒ **gem_AFO_0804 Wiederholter Aufruf der Schnittstelle [VB-5]**

Der TSP MUSS bei Zugriff mittels [VB-5] auf einen existierenden zwischengespeicherten oder bereits abgesendeten vorbefüllten Antrag die in [VB-5] übertragenen Vorbefüllungsdaten ignorieren. Des weiteren gelten die Aussagen von [gem_AFO_0807]. Der Zugriff auf einen bereits abgesendeten Antrag ist nicht mehr möglich, sobald dieser in Bearbeitung beim TSP ist. In diesem Fall MUSS der TSP den Antragsteller auf das mit den Daten von [VB-5] vorbefüllte Formular für einen neuen Antrag leiten. ☒

6.1.4 Artefakte

Zu Artefakten im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.1.5 Testunterstützung

Zur Unterstützung von Tests im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.1.6 Hardwaremerkmale

Das Funktionsmerkmal setzt keine besonderen Hardwaremerkmale voraus.

6.2 Antragstellung

Ein Antragsteller kann am Antragsportal des TSP einen Antrag für einen HBA und/oder eine HBA Ersatzkarte oder für eine oder mehrere SMC-B stellen.

Nach der Antragstellung müssen die Anträge vom Kartenherausgeber freigegeben werden, bevor die zugehörigen Karten produziert werden. Dies wird in Kapitel 6.3 *Freigabe* beschrieben.

Es ist auch möglich, dass das Praxisregister bereits freigegebene Aufträge für den TSP bereitstellt. Dies wird in Kapitel 6.7 beschrieben.

Anträge können mit und ohne Vorbefüllung gestellt werden, wenn der Kartenherausgeber diese Varianten zulässt. Im Falle einer Vorbefüllung erhält der Antragsteller die Vorgangsnummer vorher vom Kartenherausgeber. Dies ist außerhalb der Betrachtungsgrenzen dieser Spezifikation. Abgesendete Anträge können erneut bearbeitet und gesendet werden, solange die Papiergebundenen Antragsunterlagen noch nicht beim TSP eingegangen sind (d.h. solange der Status beim TSP den Wert „vom Antragsteller bearbeitet“ hat).

Spezifikation Kartenpersonalisierung HBA/SMC-B

Beim HBA-Antrag werden als Identitätsprüfungen PostIdent und (ggf. vorab durchgeführtes) KammerIdent eingesetzt.

- Bei PostIdent lässt sich der Antragsteller in der Postfiliale identifizieren. Der Postmitarbeiter sendet den Zertifikats-Antrag, den Ausweis-Antrag und den Identitätsnachweis an den TSP.
- Bei KammerIdent lässt sich der Antragsteller beim Kartenherausgeber identifizieren. Der Kammermitarbeiter sendet den Zertifikats-Antrag und den Identitätsnachweis an den TSP. Optional kann er auch die Freigabe oder Ablehnung des Antrags mitsenden.
- Bei vorab durchgeführtem KammerIdent hat sich der Antragsteller in der Vergangenheit (innerhalb eines zulässigen Zeitfensters) bereits beim Kartenherausgeber identifizieren lassen. Der Kammermitarbeiter sendet den Zertifikats-Antrag und den Identitätsnachweis an den TSP. Optional kann er auch die Freigabe oder Ablehnung des Antrags mitsenden.

Die Kommunikation zwischen Antragsteller und TSP erfolgt über die Schnittstellen [Sch_Antragsportal] und [Sch_Post], die Kommunikation zwischen Kartenherausgeber und TSP erfolgt im Fall von KammerIdent über [Sch_Post], ebenso die Kommunikation zwischen PostIdent und TSP.

Es sind zwei Antragsdokumente zu unterscheiden. Im Allgemeinen ist es aus dem Zusammenhang klar, welcher Antrag gemeint ist. Wenn die Unterscheidung relevant ist, werden die exakten Bezeichnungen verwendet

- Mit dem Zertifikats-Antrag werden beim TSP die Zertifikate beantragt.
- Mit dem Ausweis-Antrag werden beim Kartenherausgeber die Karten beantragt.

Bei der SMC-B werden keine papiergebundenen Anträge versandt, sondern die Anträge werden rein elektronisch abgebildet.

Zur Verdeutlichung ist in Abbildung 7 vereinfacht dargestellt, wie die verschiedenen Papieranträge im Fall des HBA bei Nutzung von PostIdent oder KammerIdent versendet werden, nachdem der Antragsteller den Antrag im Antragsportal abgesendet hat. Zusätzlich ist zur Information auch dargestellt, wie diese Daten bei der Freigabe übertragen werden (siehe Kapitel 6.3 *Freigabe*).

Bei vorab durchgeführtem KammerIdent unterscheidet sich der dargestellte Prozess nur dadurch, dass der Identitätsnachweis des Antragstellers von der Kammer bereits in der Vergangenheit dokumentiert wurde. Der Versand der Dokumente in Richtung TSP bleibt unverändert.

Alternativ zum Identitätsnachweis per PostIdent oder KammerIdent kann der TSP auch eine Online-Identifikation des Antragstellers mittels des nPA durchführen. Dadurch entfällt der Versand von schriftlichen Identitätsnachweisen zwischen den verschiedenen Rollen.

Da bei der SMC-B KEINE papiergebundenen Anträge versandt werden, gibt es keine vergleichbare vereinfachte Abbildung für Papieranträge für die SMC-B.

Der vollständige Ablauf für beide Karten ist im Abschnitt 6.2.2 dargestellt.

Spezifikation Kartenpersonalisierung HBA/SMC-B

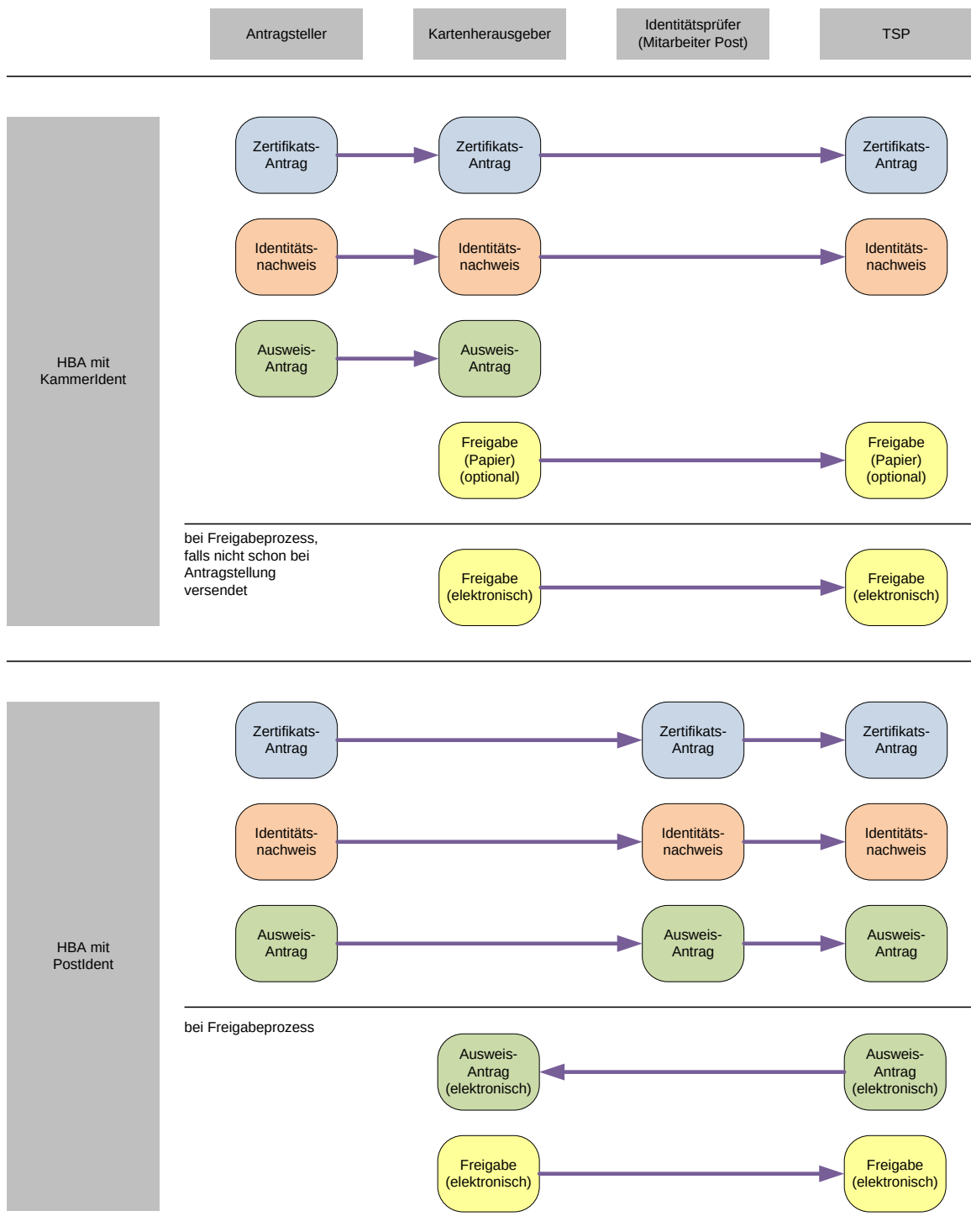


Abbildung 7: Abb_102_Vereinfachter_Ablauf_bei_Antragstellung_HBA

Die eindeutige Identifikation von Anträgen erfolgt durch eindeutige vom TSP vergebene Referenznummern. Wenn ein Antrag gestellt wird, um genau eine Karte (HBA oder SMC-B) zu beantragen, erhält der Antragsteller vom TSP eine eindeutige Referenznummer sowie ein Servicepasswort, ein Sperrkennwort und ein Freischaltkennwort zurück (siehe [gem_AFO_0070], im folgenden erläuternden Textabschnitt als „drei Passworte“ bezeichnet).

net). Die Referenznummer sowie die Vorgangsnummer (falls vorhanden die VorgangsNrAttrBS, andernfalls die VorgangsNrTSP) werden im Rahmen der Freigabe auch an den Kartenherausgeber übermittelt, entweder in der E-Mail Information über zur Freigabe vorliegende Anträge oder per Übergabeschnittstelle im Fall einer SOAP Kommunikation. Die Referenznummer oder die Vorgangsnummer kann vom Kartenherausgeber als Suchkriterium über den Datenbestand verwendet werden.

Referenznummer und Sperrkennwort müssen vom Antragsteller bei einer Sperrung zur eindeutigen Identifizierung der betroffenen Karte an den TSP übermittelt werden. Referenznummer und Freischaltekenntwort müssen vom Antragsteller bei einer Freischaltung zur eindeutigen Identifizierung der betroffenen Karte an den TSP übermittelt werden. Die Referenznummer muss vom Kartenherausgeber bei einer Sperrung zur eindeutigen Identifizierung der betroffenen Karte an den TSP übermittelt werden.

Die durch einen Kartenherausgeber vergebene Vorgangsnummer ist nicht eindeutig für einen Antrag, sondern kann wieder verwendet werden. Daher ist sie als Merkmal zur Identifizierung eines Antrags, der vom Kartenherausgeber gesperrt werden soll, nicht geeignet.

Wenn im Rahmen eines Antragsvorgangs mehrere Karten in einem Schritt beantragt werden (zum Beispiel Karte und Ersatzkarte), so erzeugt der TSP für jede einzelne Karte eine Referenznummer und die zugeordneten drei Passworte, und generiert TSP-intern mehrere Einzelanträge, die miteinander verlinkt sind. Dem Antragsteller werden alle Referenznummern und Passworte in der Antwort auf die Absendung oder Zwischenspeicherung des Antrags übermittelt.

Dem Kartenherausgeber wird vom TSP der erste dieser verlinkten Einzelanträge zusammen mit dessen Referenznummer und Vorgangsnummer während der Freigabe bereitgestellt. Der TSP muss dem Kartenherausgeber die Möglichkeit bieten, den Vorgang (inkl. der sich daraus ergebenden Einzelanträge) mit der ersten Referenznummer oder alternativ mit der Vorgangsnummer in einem Schritt zu prüfen, ggf. anzupassen und freizugeben. Auch bei der Freigabe mittels QES ist nur eine signierte Freigabe erforderlich.

Ab dem Moment der Freigabe führt der TSP die einzelnen Anträge und daraus resultierenden Karten separat weiter. Bei einer Sperrung einer der Karten muss zum Beispiel die jeweils richtige Referenznummer (und bei Sperrung durch den Antragsteller auch das richtige Sperrkennwort) für genau diese Karte verwendet werden.

Wenn ein zwischengespeicherter oder abgesendeter Antrag (für eine oder mehrere Karten) vom Antragsteller erneut geladen und weiter bearbeitet wird, werden bei jedem neuerlichen Zwischenspeichern oder Absenden neue Passworte erzeugt. Die resultierenden Passwortdatei(en) ersetzen jeweils alle vorherigen.

6.2.1 TUC-Beschreibung

Tabelle 6: Tab_003_TUC_Antragstellung

Element	Beschreibung
Name	Antragstellung
Beschreibung	Der Antragsteller erstellt am Antragsportal einen Antrag für einen HBA und/oder eine SMC-B.
Auslöser	Der Antragsteller benötigt einen HBA und/oder eine SMC-B.
Vorbedingungen	Die Konfigurationen des Kartenherausgebers (z. B. welche Felder werden angezeigt, welche Felder sind änderbar) müssen beim TSP vorliegen. Eine TLS/SSL-Verbindung wurde gemäß [gem_AFO_0007] aufgebaut. Vorbedingungen für Varianten: • zwischengespeicherten oder bereits versendeten Antrag bearbeiten: der Antragsteller muss Referenznummer und Servicepasswort kennen • bereits versendeten Antrag bearbeiten: Status des Antrags muss beim TSP den Wert „vom Antragsteller bearbeitet“ haben (d. h., papiergebundene Antragsdokumente liegen beim TSP noch nicht vor) • vorbefüllten Antrag bearbeiten (erstmalig oder zwischengespeichert oder abgesendet): der Antragsteller muss die Vorgangsnummer kennen oder durch einen Link im Portal des Kartenherausgebers zum vorbefüllten Antrag geleitet werden (siehe hierzu auch [gem_AFO_0143])
Eingangsdaten	Antragsdaten (beim HBA inkl. Foto des Antragstellers) Eingangsdaten bei Varianten: • mit leerem Antragsformular beginnen: Kartentyp und Kartenherausgeber • zwischengespeicherten oder bereits versendeten Antrag bearbeiten: Referenznummer und Servicepasswort vorbefüllten Antrag bearbeiten: Vorgangsnummer • bei einer weiteren Beantragung: falls vom Antragsteller gewünscht und durch die Sektorkonfiguration erlaubt, werden vom TSP passende Daten bereits in den neuen Antrag eingefüllt und angezeigt • OPTIONAL: bei Nutzung der Online-Identitätsfunktion des nPA durch den TSP aus dem nPA ausgelesene Daten

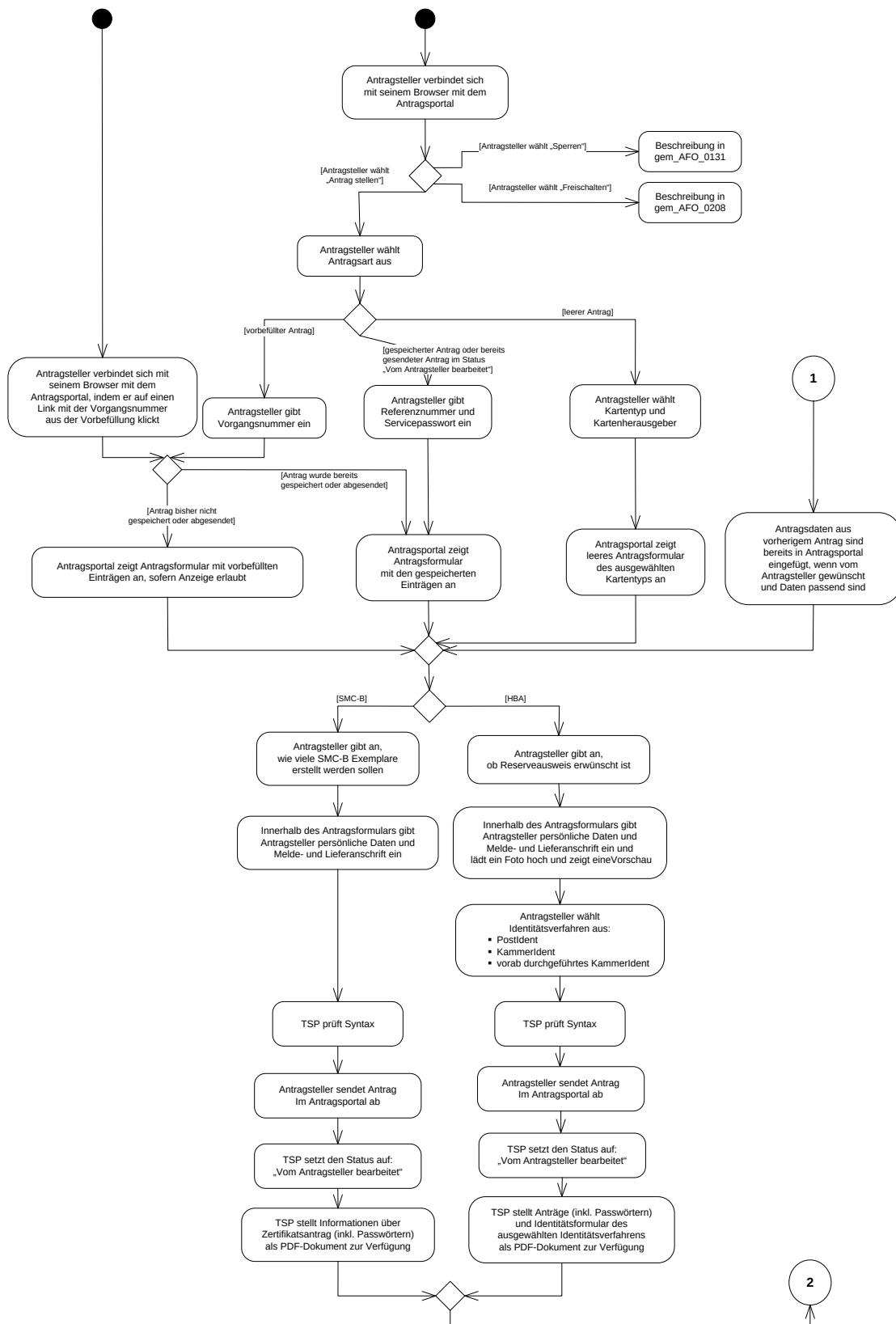
Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	des Antragstellers als Identitätsnachweis
Komponenten	Kartenpersonalisierung
Ausgangsdaten	Zertifikats-Antrag als PDF mit Antragsdaten, Referenznummer, Vorgangsnummer, Servicepasswort, Freischaltekeyword und Sperrkeyword Beim HBA zusätzlich: Ausweis-Antrag und Identitätsnachweis. Bei (zeitversetztem) KammerIdent bei HBA optional zusätzlich: Freigabe oder Ablehnung per Post
Nachbedingungen	Der Antrag ist im Status „zur Freigabe“. Zertifikats-Antrag und beim HBA zusätzlich Ausweis-Antrag und Identitätsnachweis liegen dem Antragsteller vor. Beim HBA liegen unterschriebener Zertifikats-Antrag und Identitätsnachweis sowie optional Freigabe/Ablehnung (nur bei KammerIdent) beim TSP vor. Beim HBA liegt der Ausweis-Antrag entweder beim Kartenherausgeber vor (KammerIdent) oder beim TSP (PostIdent). Im Fall der Nutzung der Online-Identitätsfunktion des nPA durch den TSP (OPTIONAL) entfallen die schriftlichen Identitätsnachweise beim HBA.
Standardablauf	Siehe Abbildung 8 „Abb_004_Antragstellung_ohne_nPA“ und Abbildung 7 „Abb_102_Vereinfachter_Ablauf_bei_Antragstellung“
Varianten/Alternativen	• HBA und/oder SMC-B beantragen • bei HBA: Reserveausweis mitbestellen oder nicht • bei SMC-B: ein oder mehrere SMC-Bs mit gleicher Personalisierung (d. h. gleiche Antragsdaten, aber verschiedene Schlüssel, Zertifikate und PIN/PUK) • neuen Antrag stellen, einen gespeicherten oder abgesendeten Antrag weiterbearbeiten oder einen vorbefüllten Antrag bearbeiten • beim HBA sind ein schriftlicher Zertifikats-Antrag und eine Identifizierung notwendig, beim SMC-B nicht • beim HBA: Identifizierung mit PostIdent oder mit (ggf. vorab durchgeführtem) KammerIdent oder optional mit der Online-Identitätsfunktion des nPA • beim HBA: Bei Identifizierung mit (ggf. vorab durchgeführtem) KammerIdent kann die Freigabe bzw. Ablehnung vom Kartenherausgeber per Post an den TSP gesendet

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	werden oder nicht.
Fehlerfälle	• Wenn der Browser des Antragstellers die geforderten TLS-Versionen oder Ciphersuites nicht unterstützt, lässt der TSP keine Verbindung zum Antragsportal zu. • Wenn die Referenznummer und das Servicepasswort abgelaufen sind oder nicht zusammenpassen oder zu keinem gespeicherten Antrag passen, wird kein zwischengespeicherter Antrag angezeigt. • Wenn die Vorgangsnummer zu keinem vorbefüllten Antrag passt, wird kein vorbefüllter Antrag angezeigt. • Wenn ein bereits versendeter Antrag bearbeitet werden soll und der Status des Antrags beim TSP nicht den Wert „vom Antragsteller bearbeitet“ hat, wird kein Antrag angezeigt. • Wenn die Prüfung der Antragsdaten, des schriftlichen Zertifikats-Antrags oder des Identitätsnachweises Fehler oder Abweichungen ergibt, kann der Antrag nicht zur Freigabe bereitgestellt werden. • Wenn der Antragsteller nicht alle geforderten Schritte der Antragstellung ausführt, kann kein Antrag zur Freigabe bereitgestellt werden.
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Siehe Abbildung 8 „Abb_004_Antragstellung_ohne_nPA“ und Abbildung 7 „Abb_102_Vereinfachter_Ablauf_bei_Antragstellung“

6.2.2 Ablauf



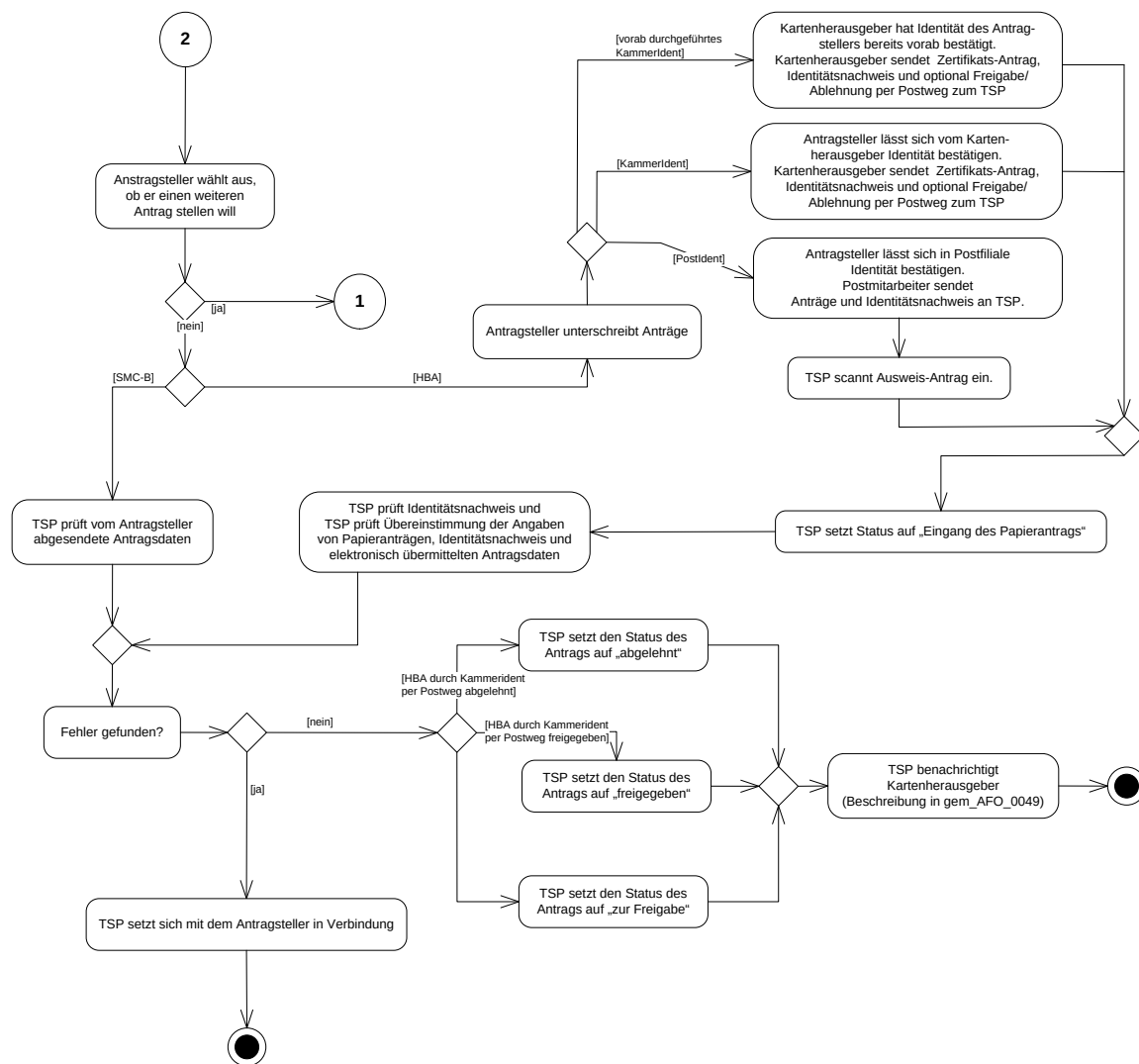


Abbildung 8: Abb_004_Antragstellung_ohne_nPA

6.2.3 Anforderungen

☒ **gem_AFO_0045 Ablauf der Antragsstellung wie in Beschreibung**

Der TSP MUSS es den Antragstellern ermöglichen, die Antragstellung wie in „Abb_004_Antragstellung“ und „Tab_003_TUC_Antragstellung“ dargestellt durchzuführen. ☒

☒ **gem_AFO_0815 Ablauf der Antragsstellung unter Nutzung des nPA**

Der TSP KANN anstelle von KammerIdent oder PostIdent im Antragsformular die Online-Identitätsfunktion des nPA als Identitätsnachweis des Antragstellers eines HBA nutzen. In diesem Fall entfallen die in „Abb_004_Antragstellung_ohne_nPA“ dargestellten Prozesse der Bearbeitung und des Versands des schriftlichen Identitätsnachweises. ☒

☒ **gem_AFO_0067 Anzeige von Hilfetexten im Antragsportal**

Der TSP MUSS dem Antragsteller im Antragsportal Hilfetexte zum Ausfüllen der Eingabefelder anzeigen, sofern für ein Eingabefeld ein Hilfetext vorliegt. ☒

☒ **gem_AFO_0068 Anzeige von Informationen im Antragsportal**

Der TSP MUSS dem Antragsteller im Antragsportal eine Auswahl an Informationen (z. B. Vereinbarungstexte, Anleitungen, Antragsbedingungen) der Sektoren anzeigen, sofern diese Informationen vorhanden sind. Der TSP MUSS diese Informationen anzeigen oder zum Download bereitstellen, wenn der Antragsteller sie aufruft. Der TSP MUSS dem Antragsteller im Antragsportal einen Link oder Button anzeigen, mit dem der Antragsteller die Informationen aufrufen kann. ☒

☒ **gem_AFO_0069 Sektorspezifische Hilfetexte und Informationen im Antragsportal**

Der TSP MUSS Hilfetexte und weitere Informationen (z. B. Vereinbarungstexte, Anleitungen) sektorspezifisch anzeigen können. ☒

☒ **gem_AFO_0052 Regional-körperschaftsspezifische Seitengestaltung des Antragsportals**

Der TSP MUSS Name und Logo der jeweiligen regional-körperschaftsspezifischen Organisation im Antragsportal anzeigen. Der TSP MUSS eine regional-körperschaftsspezifische (z. B. LÄK Nordrhein, LÄK Westfalen und LZÄK Nordrhein, LZÄK Westfalen...) Seitengestaltung hinsichtlich Benennung der Organisation und Logo unterstützen. Dazu MUSS er bei der Programmierung des Antragsportals die Benennung der Organisation und das Logo als Variable verwenden, sodass diese leicht auszutauschen sind. Bei Bedarf und mit Zustimmung des zuständigen Sektors MUSS der TSP auch Antragsfelder regional-körperschaftsspezifisch gestalten. ☒

☒ **gem_AFO_0086 Konfigurierbarkeit der Eingabefelder im Antragsformular**

Ein Antragsformular besteht aus mehreren Eingabefeldern. Diese unterscheiden sich nach HBA und SMC-B (siehe [gem_AFO_0044]). Es MÜSSEN sektorspezifische Konfigurationen pro Eingabefeld möglich sein.

Die Konfigurationen KÖNNEN enthalten:

- Eingabefeld sichtbar oder nicht sichtbar
- Eingabefeld änderbar oder nicht änderbar
- Eingabefeld optional oder Pflichtfeld

Der TSP MUSS die Eingabefelder entsprechend der Konfiguration anzeigen und behandeln. Der TSP MUSS es dem Kartenherausgeber ermöglichen, im Antragsformular Informationen einzugeben, die für die Freigabe erforderlich sind (zum Beispiel die Telematik-ID). Diese Möglichkeit MUSS pro Sektor auswählbar sein. ☒

Anmerkung: Dass die Informationen für die Freigabe bereits im Antragsformular eingegeben werden können, ist dann sinnvoll, wenn der Kartenherausgeber für einen Antragsteller oder mit ihm zusammen das Antragsformular ausfüllt. Dann kann der Kartenherausgeber bereits bei der Antragstellung diese Informationen eingeben und nicht erst bei der Freigabe.

☒ **gem_AFO_0066 Anzeige von Auswahlfeldern im Antragsportal**

Bei Eingabefeldern mit einem begrenzten Wertebereich SOLL der TSP kein Freitextfeld, sondern ein Drop-Down-Menü mit den möglichen Werten anbieten. ☒

☒ **gem_AFO_0055 Nutzung des Antragsportals ohne vorherige Authentisierung des Antragstellers**

Der TSP MUSS den Antragstellern im Antragsportal die Möglichkeit bieten, das Portal ohne vorherige Authentisierung zu nutzen. Der TSP MUSS sicherstellen, dass ein nicht authentisierter Antragsteller nur solche Daten anzeigen oder Funktionen ausführen kann, bei denen keine Authentisierung gefordert ist. Diese sind in den jeweiligen Anforderungen genannt. ☒

Anmerkung: Eine Authentisierung wird gefordert bei:

- Zugriff auf Vorbefüllungsdaten: nur mit Vorgangsnummer
- Zugriff auf zwischengespeicherten Antrag: nur mit Referenznummer und Servicepasswort oder alternativ mit Vorgangsnummer

☒ **gem_AFO_0161 Nutzung des Antragsportals zur Antragstellung nur nach Auswahl eines Kartenherausgebers**

Der TSP DARF dem Antragsteller im Antragsportal NICHT Daten anzeigen oder Funktionen zur Ausführung anbieten bzw. die Ausführung zulassen, solange der Antragsteller keinen Kartenherausgeber ausgewählt hat. Dies bezieht sich nur auf die Daten und Funktionen zur Antragstellung nach der Auswahl der Antragsart. Details sind in „Abb_004_Antragstellung“ zu finden. ☒

☒ **gem_AFO_0750 Leeren Antrag durch eine Körperschaft unterbinden**

Der TSP MUSS es ermöglichen, das Antragsportal so zu konfigurieren, dass gemäß Definition der jeweiligen Körperschaft ein Antragsteller nicht mit einem leeren Antrag beginnen kann. ☒

☒ **gem_AFO_0078 Auswahlmöglichkeit für Antragsart**

Der TSP MUSS dem Antragsteller im Antragsportal die Möglichkeit bieten auszuwählen, welche Art Antrag er stellen will.

Zur Auswahl stehen:

- mit leerem Antrag beginnen (sofern zulässig gemäß [gem_AFO_0750])
- gespeicherten oder abgesendeten Antrag weiterbearbeiten
- vorbefüllten Antrag weiterbearbeiten (erstmalig oder nach Speicherung/Absenden).

Nachdem der Antragsteller eine Antragsart ausgewählt hat, MUSS der TSP die zugehörigen Informationen anzeigen:

- Mit leerem Antrag beginnen: Der TSP lässt den Antragsteller Kartentyp und Kartenherausgeber auswählen (siehe [gem_AFO_0160]) und zeigt dann ein leeres Antragsformular angepasst an den Kartentyp und Kartenherausgeber an.
- Vorbefüllten Antrag weiterbearbeiten: Der TSP lässt den Antragsteller die Vorgangsnummer eingeben (siehe [gem_AFO_0057]) und zeigt bei erstmaligem Aufruf das Antragsformular mit vorbefüllten Daten an, bei Aufruf eines

zwischengespeicherten oder abgesendeten Antrags das Antragsformular mit den gespeicherten Daten.

- Gespeicherten/abgesendeten Antrag weiterbearbeiten: Der TSP lässt den Antragsteller Referenznummer und Servicepasswort (siehe [gem_AFO_0062]) eingeben und zeigt das Antragsformular mit den gespeicherten Daten an. ☒

☒ **gem_AFO_0160 Auswahl des Kartentyps und Kartenherausgebers**

Der TSP MUSS dem Antragsteller im Antragsportal die Möglichkeit bieten auszuwählen, welchen Kartentyp er beantragen möchte, und zu welchem Kartenherausgeber er gehört.

Der TSP MUSS als Kartentypen zur Auswahl stellen:

- Praxisausweis für eine Zahnarztpraxis
- Institutionskarte für ein Krankenhaus
- elektronischer Arztausweis
- elektronischer Zahnarzttausweis
- elektronischer Psychotherapeutenausweis ☒

☒ **gem_AFO_0710 Eingabe des Kartenherausgebers**

Der TSP DARF nach der Auswahl des Kartentyps keine anderen Kartenherausgeber zur Auswahl anbieten als diejenigen, bei denen dieser Kartentyp über das Antragsportal beantragt wird und die zu dem durch den Kartentyp ausgewählten Sektor gehören. Der TSP KANN dem Antragsteller die Möglichkeit geben, einen bereits ausgewählten Kartentyp und Kartenherausgeber zu wechseln. ☒

☒ **gem_AFO_0057 Eingabe der Vorgangsnummer im Antragsportal**

Der TSP MUSS dem Antragsteller die Möglichkeit bieten, die Vorgangsnummer im Antragsportal einzugeben. ☒

☒ **gem_AFO_0162 Aufruf eines vorbefüllten Antrags per Link**

Der TSP MUSS dem Antragsteller ermöglichen, dass er durch Klicken auf einen Link mit einer Vorgangsnummer direkt das Antragsformular mit den vorbefüllten bzw. gespeicherten Daten angezeigt bekommt. ☒

Anmerkung:

Den Link kann der Kartenherausgeber dem Antragsteller zum Beispiel auf der Web-Seite des Kartenherausgebers zur Verfügung stellen. Dies ist außerhalb der Betrachtungsgrenzen dieser Spezifikation.

☒ **gem_AFO_0058 Anzeige von Vorbefüllungsdaten und Anträgen nach Eingabe der Vorgangsnummer**

Wenn der Antragsteller dem TSP eine Vorgangsnummer übermittelt, MUSS der TSP im Antragsformular im Antragsportal

- beim erstmaligen Aufruf diejenigen Vorbefüllungsdaten anzeigen, die zu dieser Vorgangsnummer gehören und die lt. Spitzenorganisation des Sektors sichtbar sein dürfen, wenn dies nicht [gem_AFO_0049] widerspricht
- beim wiederholten Aufruf (nach zwischenspeichern oder absenden) die gespeicherten Antragsdaten anzeigen. ☒

☒ **gem_AFO_0049 Nicht-Anzeige von Vorbefüllungsdaten**

Der TSP DARF dem Antragsteller NICHT diejenigen Vorbefüllungsdaten anzeigen, die lt. Spitzenorganisation des Sektors nicht sichtbar sein dürfen. Der TSP DARF dem Antragsteller NICHT Vorbefüllungsdaten anzeigen, wenn der Antragsteller keine Vorgangsnummer an den TSP übermittelt hat. Der TSP DARF dem Antragsteller NICHT Vorbefüllungsdaten anzeigen, die nicht zu der vom Antragsteller übermittelten Vorgangsnummer gehören. ☒

☒ **gem_AFO_0062 Eingabe von Referenznummer und Servicepasswort im Antragsportal**

Der TSP MUSS dem Antragsteller die Möglichkeit bieten, Referenznummer und Servicepasswort zu einem zwischengespeicherten oder abgesendeten Antrag im Antragsportal einzugeben. ☒

☒ **gem_AFO_0060 Anzeige von zwischengespeicherten oder abgesendeten Anträgen bei Eingabe von Referenznummer und Servicepasswort**

Wenn der Antragsteller dem TSP eine Referenznummer und ein Servicepasswort übermittelt, MUSS der TSP im Antragsformular im Antragsportal diejenigen Antragsdaten anzeigen, die zu dieser Kombination aus Referenznummer und Servicepasswort gehören, wenn dies nicht [gem_AFO_0061] widerspricht. ☒

☒ **gem_AFO_0061 Nicht-Anzeige von zwischengespeicherten oder abgesendeten Anträgen bei Eingabe von Referenznummer und Servicepasswort**

Der TSP DARF dem Antragsteller NICHT zwischengespeicherte oder abgesendete Antragsdaten anzeigen, wenn der Antragsteller keine Referenznummer oder kein Servicepasswort oder keins von beiden an den TSP übermittelt hat. Der TSP DARF dem Antragsteller NICHT zwischengespeicherte oder abgesendete Antragsdaten anzeigen, die nicht zu dem vom Antragsteller übermittelten Kombination von Referenznummer und Servicepasswort gehören. Der TSP DARF dem Antragsteller NICHT zwischengespeicherte oder abgesendete Antragsdaten anzeigen, wenn die übermittelten Kombination von Referenznummer und Servicepasswort nicht zusammenpasst. Der TSP DARF dem Antragsteller NICHT zwischengespeicherte Antragsdaten anzeigen, wenn die Lebensdauer des Antrags überschritten ist (siehe [gem_AFO_0192]). Der TSP DARF dem Antragsteller NICHT abgesendete Antragsdaten anzeigen, wenn der zugehörige Antrag den Zustand „vom Antragsteller bearbeitet“ verlassen hat (sich also bereits in der Bearbeitung durch das Trust Center befindet). ☒

☒ **gem_AFO_0048 Mehrere Karten in einem Antragsvorgang**

Der TSP MUSS es den Antragstellern ermöglichen, in einem Vorgang mehrere Karten und/oder Anträge zu stellen, wie im Folgenden beschrieben:

- Bei Beantragung eines HBA: in einem Antrag einen HBA und optional zu dem HBA einen Reserveausweis.
- Bei Beantragung von SMC-B: in einem Antrag eine oder mehrere SMC-Bs mit gleichen Antragsdaten.
- Nach Beantragung eines HBA oder einer SMC-B kann der Antragsteller einen weiteren Antrag für die jeweils andere Kartenart stellen. Die Daten aus dem vorigen Antrag werden übernommen, sofern vorhanden und passend (jeder Antrag hat eine eigene Referenznummer und die Antragsdaten können sich unterscheiden). ☒

Anmerkung:

Die ersten beiden Optionen sind in [gem_AFO_0080] beschrieben, die dritte in [gem_AFO_0166].

☒ **gem_AFO_0080 Auswahl der Anzahl der Ausweise**

Der TSP MUSS dem Antragsteller die Möglichkeit bieten, die Anzahl der Ausweise auszuwählen. Wenn der Antragsteller einen HBA beantragt, dann MUSS der TSP die Möglichkeit bieten, dass der Antragsteller einen Reserveausweis im gleichen Schritt direkt mit beantragt. Wenn der Antragsteller eine SMC-B beantragt, dann MUSS der TSP die Möglichkeit bieten, dass der Antragsteller die Anzahl der gewünschten SMC-Bs angibt. Werden in einem Schritt mehrere Karten beantragt, MUSS der TSP für jeden darin enthaltenen Einzelantrag eine eindeutige Referenznummer und Servicepasswort erzeugen und dem Antragsteller mitteilen. ☒

☒ **gem_AFO_0050 Nicht-Änderbarkeit von Vorbefüllungsdaten**

Der TSP DARF es dem Antragsteller NICHT ermöglichen, als „nicht-änderbar“ festgelegte Vorbefüllungsdaten zu ändern. ☒

☒ **gem_AFO_0051 Änderbarkeit von Vorbefüllungsdaten**

Der TSP MUSS es dem Antragsteller ermöglichen, als „änderbar“ festgelegte Vorbefüllungsdaten zu ändern, sofern diese Vorbefüllungsdaten vorhanden sind. ☒

☒ **gem_AFO_0047 Farbige Kennzeichnung von geänderten Vorbefüllungsdaten im Antragsportal**

Wenn der Antragsteller im Antragsformular vorberefüllte Daten ändert, MUSS der TSP diese im Antragsformular in einer anderen Farbe darstellen als die nicht-geänderten Vorbefüllungsdaten. Die beiden Farben müssen sich deutlich unterscheiden und die Texte in beiden Farben gut lesbar sein. Der TSP MUSS sich dabei auf den Stand der Vorbefüllungsdaten beim erstmaligen Öffnen des vorberefüllten Antrags beziehen. ☒

Erläuterung: Vorbefüllungsdaten zu einer Vorgangsnummer können vom Kartenherausgeber jederzeit geändert werden. Diese Änderungen dürfen keinen Einfluss auf bereits begonnene Anträge haben.

☒ **gem_AFO_0082 Hochladen eines Fotos beim HBA-Antrag**

Bei Beantragung eines HBA MUSS der TSP dem Antragsteller im Antragsportal die Möglichkeit zum Hochladen des Fotos des Antragstellers anbieten. Wenn der Antragsteller die Funktion „Foto hochladen“ auswählt, MUSS der TSP ein Dateiauswahlfenster öffnen, mit dem der Antragsteller auf seinem Computer eine Datei auswählen kann. Im Dateiauswahlfenster MUSS der TSP die Dateitypen anzeigen, die für die Bilddatei zulässig sind (z. B. JPEG und PNG) Wenn der Antragsteller eine Datei ausgewählt hat, MUSS der TSP diese hochladen. Der TSP MUSS dem Antragsteller im Antragsportal als Hilfetext eine Anleitung zum Hochladen von Fotos zur Verfügung stellen. In der Anleitung MUSS der TSP die zulässige Größe der Bilddatei und die zulässigen Dateitypen angeben. Der TSP MUSS die hochgeladene Bilddatei entsprechend der für die Kartenpersonalisierung benötigten Eigenschaften konvertieren, sollte sie diesen Eigenschaften nicht entsprechen (z. B. Größe).☒

☒ **gem_AFO_0063 Anzeige von Referenznummer und Servicepasswort bei Zwischenspeicherung von Anträgen**

Der TSP MUSS dem Antragsteller die Möglichkeit bieten, einen Antrag zwischenzuspeichern und später weiterzubearbeiten. Wenn der Antragsteller die Funktion zum Zwischenspeichern aufruft, MUSS der TSP dem Antragsteller im Antragsportal eine Referenznummer und ein Servicepasswort anzeigen, mit dem später wieder auf den zwischengespeicherten Antrag zugegriffen werden kann. Werden in einem Schritt mehrere Karten gemäß [gem_AFO_0048] beantragt, MUSS der TSP für jeden darin enthaltenen Einzelantrag eine eindeutige Referenznummer und Servicepasswort erzeugen und dem Antragsteller mitteilen. Die Einzelanträge MUSS der TSP in der Art verlinken, dass der Antragsteller bis zur Freigabe mit dem ersten Paar Referenznummer/Servicepasswort auf den zwischengespeicherten Antrag (und implizit die damit verlinkten Einzelanträge) zugreifen und die Beantragung fortsetzen kann.☒

☒ **gem_AFO_0192 Konfigurierbare Lebensdauer von nicht abgesendeten Anträgen**

Der TSP MUSS konfigurieren können, wie lange ein Antrag, der noch nicht abgesendet wurde, zwischengespeichert wird. Die Definition der konkreten Löschfrist obliegt den jeweiligen Kartenherausgebern.☒

Anmerkung: Das Löschen von Anträgen, bei denen die Lebensdauer überschritten ist, ist in [gem_AFO_0065] beschrieben.

☒ **gem_AFO_0053 Überprüfung der Antragsdaten durch den TSP**

Wenn der Antragsteller im Antragsformular auf einen „Weiter“-Button oder -Link klickt, MUSS der TSP die Daten in den Eingabefeldern auf dieser Seite prüfen. Dabei prüft er, ob die Pflichtfelder ausgefüllt sind und ob die Syntax stimmt.☒

☒ **gem_AFO_0088 Auswahl eines Identitätsverfahrens beim HBA-Antrag**

Im Falle eines HBA-Antrags MUSS es der TSP dem Antragsteller ermöglichen, ein Identitätsverfahren auszuwählen. Zur Auswahl MÜSSEN mindestens PostIdent und KammerIdent stehen, sofern die zuständige Kammer KammerIdent anbietet.☒

☒ **gem_AFO_0816 Auswahl des nPA Identitätsverfahrens beim HBA-Antrag**

Der TSP KANN dem Antragsteller die Online-Identitätsfunktion des nPA als Identitätsverfahren anbieten. Wenn der Antragsteller dieses Identitätsverfahren auswählt, MUSS der TSP die Identitätsdaten über eine Funktion im Antragsformular (unter Verwendung eines eID Servers) aus dem nPA auslesen. Der Antragsteller MUSS dabei auf Client Seite dem Auslesen seines Ausweises durch Eingabe seiner nPA PIN zustimmen. Der TSP MUSS nach Auslesen der Identitätsdaten diese speichern und gegen die im Antrag enthaltenen Daten prüfen. ☒

☒ **gem_AFO_0081 Vorschau auf einen personalisierten Ausweis**

Der TSP MUSS dem Antragsteller im Antragsportal eine Vorschau auf den beantragten, personalisierten HBA-Ausweis anzeigen. Falls ausschließlich ein HBA oder ein HBA plus Ersatz-/Reserveausweis beantragt wurde, MUSS der TSP eine Vorschau des HBA anzeigen. Falls ausschließlich ein Ersatz-/Reserveausweis beantragt wurde, MUSS der TSP eine Vorschau auf den Ersatz-/Reserveausweis anzeigen. Dazu MUSS der TSP im Antragsportal ein Bild mit dem beantragten, personalisierten Ausweis anzeigen mit

- sektor-/bzw. kartenherausgeberspezifischen Merkmalen
- und den Antragsdaten, die auf der Karte angezeigt werden
- und dem Foto bzw. der Beschriftung „Ersatzausweis“ oder „Reserveausweis“ je nach den Vorgaben des zuständigen HBA Sektors. ☒

☒ **gem_AFO_0087 Absenden des Auftrags durch den Antragsteller**

Der TSP MUSS dem Antragsteller die Möglichkeit bieten, seinen Antrag im Antragsportal abzusenden. Der TSP MUSS den Absendevorgang so gestalten, dass der Antragsteller mit dem Absenden den Antragsbedingungen explizit zustimmen MUSS. In diesem Fall MUSS der TSP den Antrag in den Status „vom Antragsteller bearbeitet“ setzen.

Der TSP MUSS dem Antragsteller die Antragsbedingungen anzeigen, wenn dieser sie aufruft. ☒

☒ **gem_AFO_0166 Beantragung eines weiteren Ausweises**

Nachdem der Antragsteller einen Antrag für eine Kartenart (z. B. HBA) gestellt hat, MUSS der TSP, sofern die betroffenen Spitzenorganisationen dies wünschen, dem Antragsteller die Möglichkeit bieten, einen Antrag für die andere Kartenart (im Beispiel SMC-B) zu stellen, wobei das neue Antragsformular mit den Daten aus dem vorigen Antrag befüllt ist. Wenn der Antragsteller diese Befüllung auswählt, MUSS der TSP den neuen Antrag mit den Daten aus dem vorigen Antrag befüllen, soweit sie in die Datenstruktur passen. Für den neuen Antrag MUSS der TSP eine eindeutige Referenznummer und Servicepasswort sowie eine VorgangsNrTSP erzeugen und dem Antragsteller mitteilen. Die Weiterverwendung der VorgangsNrAttrBS bei einer andern Ausweisart ist nicht sinnvoll. Diese sollte nicht übernommen werden. ☒

☒ **gem_AFO_0070 Bereitstellung von PDF-Dokumenten nach Absenden des Antrags**

Spezifikation Kartenpersonalisierung HBA/SMC-B

Nachdem der Antragsteller den Antrag im Antragsportal an den TSP abgesendet hat [gem_AFO_0087], MUSS der TSP dem Antragsteller ein PDF-Dokument mit folgenden Teilen zur Verfügung stellen:

- SMC-B:
 - o ein oder mehrere Passwortblätter
 - o Zertifikats-Antrag (informativ)
- HBA:
 - o ein oder mehrere Passwortblätter
 - o Ausweis-Antrag
 - o Zertifikats-Antrag
 - o Identitätsformular für PostIdent oder KammerIdent oder Information über Vorgehensweise bei zeitversetztem KammerIdent (je nach Auswahl des Antragstellers)

Im Passwortblatt MÜSSEN die folgenden Zugangsinformationen enthalten sein:

- Referenznummer
- Vorgangsnummer
- Servicepasswort
- Freischaltekey
- Sperrkey

Der TSP MUSS es dem Antragsteller ermöglichen, zusammen mit dem PDF-Dokument unterstützende Anleitungen auszudrucken, sofern diese vorhanden sind.

Werden in einem Schritt mehrere Karten beantragt, MUSS der TSP für jeden darin enthaltenen Einzelantrag ein separates Passwortblatt mit den oben genannten Zugangsinformationen generieren und bereitstellen. ☒

Anmerkungen:

Die Zugangsinformationen werden für die folgenden Aktionen verwendet:

- Referenznummer + Servicepasswort:
 - o Während der Antragstellung: Zum Zugriff auf zwischengespeicherte Anträge oder bereits versendete Anträge, die sich noch im Status „vom Antragsteller bearbeitet“ befinden.
- Kartennummer + Freischaltekey: Nach der Lieferung der Karte schaltet der Antragsteller das Zertifikat frei (siehe Kapitel 6.4 *Lieferung*).
- Referenznummer + Sperrkey: Der Antragsteller kann seine Zertifikate sperren lassen (siehe Kapitel 6.5 *Sperrung*).

☒ **gem_AFO_0182 Weiterverarbeitung der ausgedruckten Anträge**

Nachdem der TSP dem Antragsteller das PDF-Dokument aus [gem_AFO_0070] zur Verfügung gestellt hat, MÜSSEN der Antragsteller, der Identitätsprüfer und der Kartenherausgeber die folgenden Schritte ausführen:

Bei der SMC-B dient das PDF-Dokument nur als Information für den Antragsteller.

Beim HBA verwendet der Antragsteller das PDF-Dokument zur Beauftragung, wie im Folgenden und in „Abb_004_Antragstellung“ beschrieben:

- Der Antragsteller druckt beide Anträge und im Fall von KammerIdent oder PostIdent das Identitätsformular aus.
- Der Antragsteller unterschreibt die Anträge.
- Der Antragsteller lässt sich im Fall von KammerIdent oder PostIdent seine Identität bestätigen: bei PostIdent in der Postfiliale bzw. bei KammerIdent beim Kartenherausgeber. Im Fall des vorab durchgeführten KammerIdent ist die Identitätsprüfung durch die Kammer bereits in der Vergangenheit (innerhalb eines zulässigen Zeitfensters) erfolgt.
- Der Identitätsprüfer sendet im Fall von KammerIdent oder PostIdent den Identitätsnachweis per Post an den TSP. Beigelegt sind:
 - o bei PostIdent beide unterschriebenen Anträge.
 - o bei KammerIdent verpflichtend nur der unterschriebene Zertifikats-Antrag, optional kann der Kartenherausgeber zusätzlich eine Freigabe oder Ablehnung per Post an den TSP senden. ☒

Anmerkung:

Für den weiteren Ablauf der Antragstellung ist es unerheblich, ob der Kartenherausgeber bei KammerIdent einen Freigabeauftrag mit sendet oder nicht, der Ablauf bleibt gleich. Dies ist erst bei der Freigabe in Kapitel 6.3 *Freigabe* von Bedeutung.

☒ **gem_AFO_0165 Eindeutige Zugangsinformationen für Antragsteller im PDF-Dokument**

Der TSP MUSS für jeden Antrag eine eindeutige Referenznummer, ein eindeutiges Servicepasswort, ein eindeutiges Freischaltekeyword und ein eindeutiges Sperrkeyword vergeben. Das Servicepasswort und das Freischaltekeyword MÜSSEN die folgenden Kriterien erfüllen:

- Mindestlänge: 16 Zeichen
- und (ggf. eingeschränkte Menge von) Zeichen aus allen der folgenden Gruppen: Kleinbuchstabe, Großbuchstaben, Ziffern, Sonderzeichen

Das Sperrkeyword MUSS die folgenden Kriterien erfüllen:

- Länge genau 8 Zeichen
- nur Ziffern ☒

Anmerkung: Diese Bildungsregel des Sperrkeywords wurde von TÜVIT für den SigG Kontext zugelassen, damit die Sperrhotline des TSP als Telefoncomputer fungieren kann.

☒ **gem_AFO_0124 Ergänzung der Vorgangsnummer als Barcode im PDF-Ausweis-Antrag**

Der TSP SOLL die VorgangsNrAttrBS bzw. falls diese nicht vergeben wurde, die VorgangsNrTSP als Barcode in das PDF-Dokument des Ausweis-Antrags einfügen. ☒

☒ **gem_AFO_0167 Statuswechsel und Scannen bei Eingang des Papierantrags**

Wenn beim TSP der oder die Papieranträge und im Fall von KammerIdent oder PostIdent der Identitätsnachweis eines HBA per Post eintrifft, dann MUSS der TSP den Status des Antrags auf „Eingang des Papierantrags“ setzen. Wenn der Ausweis-Antrag per Post eintrifft, MUSS der TSP diesen Ausweis-Antrag einscannen. ☒

☒ **gem_AFO_0089 TSP-interne Prüfung von gesendeten Anträgen**

Wenn der Antragsteller einen SMC-B-Antrag abgesendet hat oder wenn ein HBA-Zertifikats-Antrag mit Identitätsnachweis (dieser nur im Fall von KammerIdent oder PostIdent per Post) per Post eintrifft, dann MUSS beim TSP eine manuelle Prüfung durch eine Person durchgeführt werden.

Dabei MUSS er die folgenden Eingabefelder prüfen:

- Mindestens die Pflichtfelder aus den Antragsdaten. Diese sind in [gem_AFO_0042] definiert.
- Optionale Felder, sofern sie ausgefüllt sind.
- Beim HBA zusätzlich die SigG-relevanten Antragsdaten.

Er MUSS diese Eingabefelder nach folgenden Prüfkriterien prüfen:

- Vollständigkeit (Sind die Pflichtfelder ausgefüllt?)
- Plausibilität
- Ausschluss von „Spam“
- Nimmt der Antragsteller an der Erprobung teil?

Beim HBA MUSS der TSP zusätzlich

- diese eingegebenen Daten mit den Daten im schriftlichen Zertifikats-Antrag vergleichen,
- die Identität im Zertifikats-Antrag mit der im Identitätsnachweis vergleichen,
- die Unterschrift auf dem Zertifikats-Antrag prüfen sowie
- den Identitätsnachweis prüfen (nur bei KammerIdent oder PostIdent, bei Nutzung der Online-Identifizierung per nPA wird dies durch das technische Verfahren sichergestellt). ☒

☒ **gem_AFO_0090 Fehlerfreien Antrag zur Freigabe bereitstellen**

Wenn der TSP bei der Prüfung eines Antrags wie in [gem_AFO_0089] beschrieben keinen Fehler oder Abweichungen findet, MUSS er den Antrag zur Freigabe dem

zugehörigen Kartenherausgeber zur Verfügung stellen. Der TSP MUSS den Status des Antrags auf „zur Freigabe“ setzen. Der TSP MUSS den Kartenherausgeber darüber informieren, siehe [gem_AFO_0609].

gem_AFO_0091 Fehler bei TSP-interner Prüfung von gesendeten Anträgen

Wenn der TSP bei der Prüfung eines Antrags wie in [gem_AFO_0089] beschrieben einen oder mehrere Fehler oder Abweichungen findet, DARF er den Antrag NICHT zur Freigabe dem zugehörigen Kartenherausgeber zur Verfügung stellen. Er DARF den Status des Antrags NICHT auf „zur Freigabe“ setzen.

gem_AFO_0740 Kontakt zum Antragsteller bei Fehler bei TSP-interner Prüfung von gesendeten Anträgen

Wenn der TSP bei der Prüfung eines Antrags wie in [gem_AFO_0089] beschrieben einen oder mehrere Fehler oder Abweichungen findet, MUSS er sich mit dem Antragsteller (unter Verwendung von Telefon, E-Mail oder Post) in Verbindung setzen, sofern Kontaktinformationen vorliegen. Dies ist ein manueller Prozess.

Erläuterung: Das Vorliegen von Kontaktdaten des Antragstellers ist von der Sektorspezifischen Konfiguration abhängig.

gem_AFO_0092 Bearbeitungsfrist vorliegender Anträge

Der TSP MUSS einen SMC-B-Antrag innerhalb von 10 Werktagen nach Absenden des Antrags durch den Antragsteller prüfen. Der TSP MUSS einen HBA-Antrag innerhalb von 10 Werktagen nach Eingang des schriftlichen Antrags und des Identitätsnachweises prüfen.

gem_AFO_0195 Archivierung von Zertifikats-Aufträgen und Identitätsnachweisen

Der TSP MUSS beim HBA die Zertifikats-Anträge und Identitätsnachweise (nur im Fall von KammerIdent oder PostIdent) im Papierarchiv ablegen. Der TSP MUSS beim HBA auch die Kartenanträge an die Kartenherausgeber archivieren.

6.2.4 Artefakte

Zu Artefakten im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.2.5 Testunterstützung

Zur Unterstützung von Tests im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.2.6 Hardwaremerkmale

Das Funktionsmerkmal setzt keine besonderen Hardwaremerkmale voraus.

6.3 Freigabe

Ein Freigabeauftrag kann auf die folgenden Weisen erteilt werden:

- [FG-1]: im Freigabeportal
- [FG-2]: über SOAP
- [FG-3]: schriftliche Freigabe per Post (nur bei KammerIdent)

Bei [FG-1] gilt: Die Kartenherausgeber können über das Freigabeportal Anträge freigeben oder ablehnen sowie zuvor Antragsdaten ändern oder ergänzen.

Über das Freigabeportal können die Kartenherausgeber auch Sperren und Monitoring durchführen, das wird in Kapitel 6.5 Sperrung und 6.6.1 Monitoring betrachtet. Eine allgemeine Beschreibung des Freigabeportals findet sich in 6.6.1 Monitoring und in gem_AFO_0098.

Während des Ablaufs der Freigabe erhält der Kartenherausgeber vom TSP E-Mails über Produktionsrückmeldungen. Dies wird in 6.6.2 *Benachrichtigungen* beschrieben.

Nach der Freigabe werden die Karten produziert und ausgeliefert. Die Auslieferung wird in Kapitel 6.4 *Lieferung* betrachtet.

Die Kommunikation zwischen Kartenherausgeber und TSP erfolgt über die folgenden Schnittstellen:

- [FG-1]: [Sch_Freigabeportal]
- [FG-2]: [Sch_SOAP]
- [FG-3]: [Sch_Post].

Um Missverständnisse zu vermeiden, werden hier die folgenden Bezeichnungen erklärt:

- Freigeben und freischalten:
 - o Kartenherausgeber können Anträge **freigeben**. Sie stoßen damit die Produktion beim TSP an. Dies wird in diesem Kapitel beschrieben.
 - o Antragsteller können Zertifikate **freischalten**, wenn sie ihre Karte bekommen haben. Dies wird in Kapitel 6.4 *Lieferung* beschrieben.
- Ein „Freigabeauftrag“ bezeichnet die Daten, die für eine Freigabe verwendet werden, unabhängig davon, ob sie als XML-Struktur, als PDF-Datei oder als Anzeige im Portal auftreten, und unabhängig davon, ob der Antrag freigegeben oder abgelehnt wird.

6.3.1 TUC-Beschreibung

Tabelle 7: Tab_005_TUC_Freigabe

Element	Beschreibung
Name	Freigabe
Beschreibung	[FG-1]: Der Kartenherausgeber kann am Freigabeportal Anträge im Status „zur Freigabe“ ändern, ergänzen, ablehnen oder freigeben. Die Ablehnung oder Freigabe erfolgt unter Verwendung einer SAK im Freigabeportal mit einer qualifizierten elektronischen Signatur. Bei einer SMC-B ist auch eine Ablehnung oder Freigabe ohne qualifizierte elektronische Signatur möglich (abhängig von der Konfiguration auf Sektorebene). [FG-2]: Als andere Möglichkeit kann der Kartenherausgeber über einen SOAP-Request Freigabeaufträge an den TSP senden. Diese sind bereits mit einer qualifizierten elektronischen Signatur signiert. [FG-3]: Als weitere Möglichkeit sendet der Kartenherausgeber die Freigabeaufträge zusammen mit dem unterschriebenen Antrag per Post an den TSP. Diese Variante gibt es nur, wenn bei der Antragstellung eines HBA (ggf. vorab durchgeführtes) KammerIdent als Identifizierungsverfahren gewählt wurde. Nach einer Freigabe produziert der TSP die zugehörigen Zertifikate, Schlüssel, PIN/PUK und personalisiert die Karten.
Auslöser	Der TSP informiert den Kartenherausgeber per E-Mail, dass neue Anträge im Status „zur Freigabe“ bereitstehen. Dies wird in [gem_AFO_0609] beschrieben.
Vorbedingungen	[FG-1]: Der Mitarbeiter des Kartenherausgebers hat sich am Freigabeportal authentisiert. Dem Mitarbeiter am Freigabeportal sind die Zugriffsrechte für „Freigabe“ zugewiesen und er hat sein SigG-Zertifikat beim TSP hinterlegt. Er hat einen Antrag in der Detailansicht geöffnet. Der Antrag hat den Status „zur Freigabe“. [FG-2]: Authentisierung des SOAP-Clients des Kartenherausgebers beim SOAP-Request. [FG-3]: Bei der HBA-Antragstellung hat der Antragsteller (ggf. vorab durchgeführtes) KammerIdent ausgewählt. Der Kartenherausgeber hat den Antragsteller identifiziert, den Antrag abgelehnt oder freigegeben und den Freigabeauftrag per Post an den TSP gesendet (zusammen mit dem Antrag und dem Identitätsnachweis). Dies wird in [gem_AFO_0045] beschrieben.
Eingangsdaten	[FG-1]: Daten, um den freizugebenden Antrag zu identifizieren.

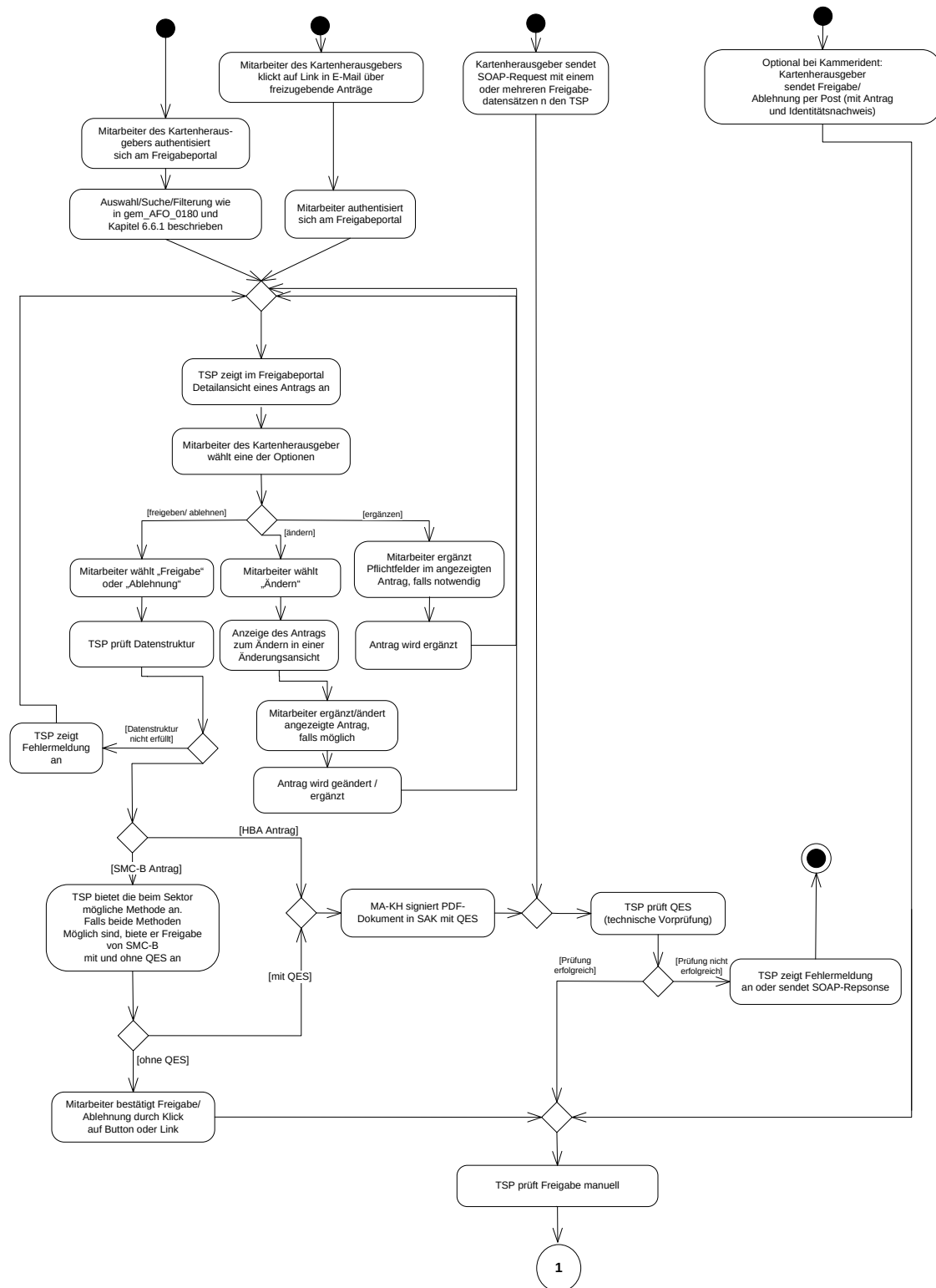
Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	[FG-2]: Freigabeauftrag mit qualifizierter elektronischer Signatur. [FG-3]: Freigabeauftrag per Post.
Komponenten	Kartenpersonalisierung.
Ausgangsdaten	• Vom Kartenherausgeber ggf. geänderte oder ergänzte Antragsdaten • Freigabeauftrag (beim HBA signiert, bei der SMC-B optional signiert) • Personalisierte Karten mit Schlüsseln, Zertifikaten und PIN/PUK • Benachrichtigungen an den Kartenherausgeber
Nachbedingungen	Der Antrag ist freigeschaltet oder abgelehnt und hat entsprechend den Status „Freigegeben“ oder „Antrag abgelehnt“. Im Fall des Status „Freigegeben“ sind die Schlüssel, Zertifikate und die PIN/PUK erzeugt, die Karten personalisiert.
Standardablauf	Siehe Abbildung 9 „Abb_005_Freigabe“.
Varianten/Alternativen	• [FG-1], [FG-2] und [FG-3]. • Der Kartenherausgeber kann einen Antrag ablehnen oder freigeben. • [FG-1], [FG-2]: Bei der SMC-B ist die qualifizierte elektronische Signatur optional. • [FG-1]: Der Kartenherausgeber kann das Freigabeportal in seinem Browser aufrufen oder er klickt auf einen Link in der Benachrichtigungs-E-Mail.
Fehlerfälle	• Wenn die Authentisierung des Kartenherausgebers (am Freigabeportal oder per SOAP) fehlschlägt, lässt der TSP keine Freigabe zu. • Wenn der Kartenherausgeber die geforderten TLS-Versionen oder Ciphersuites nicht unterstützt, lässt der TSP keinen Aufbau der TLS/SSL-Verbindung zu. • Freigabeauftrag ist nicht vollständig oder korrekt befüllt. Reaktion: - o [FG-1]: Der TSP zeigt im Freigabeportal eine Fehlermeldung an und lässt keine Signatur des Freigabeauftrags zu. - o [FG-2]: Der TSP sendet eine entsprechende Feh-

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	meldung an den Kartenherausgeber. - o [FG-3]: Der TSP setzt sich mit dem Kartenherausgeber in Verbindung. • Signatur des Freigabeauftrags ist ungültig ([FG-1] und [FG-2]). Reaktion: Der TSP informiert den Kartenherausgeber. • Manuelle Prüfung ergibt Fehler oder Abweichungen. Reaktion: Der TSP informiert den Kartenherausgeber und setzt Status des Antrags auf „Antrag verworfen“. • Es gibt keinen passenden, freizugebenden Antrag ([FG-2]). Reaktion: Der TSP sendet eine entsprechende Fehlermeldung an den Kartenherausgeber. • Der Antrag wird abgelehnt. Reaktion: Dies ist eine im Prozess vorgesehene Variante und wird nicht als Fehler angesehen. Der TSP informiert den Antragsteller über die Ablehnung, sofern Kontaktdaten des Antragstellers verfügbar sind.
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Siehe Abbildung 9 „Abb_005_Freigabe“.

6.3.2 Ablauf



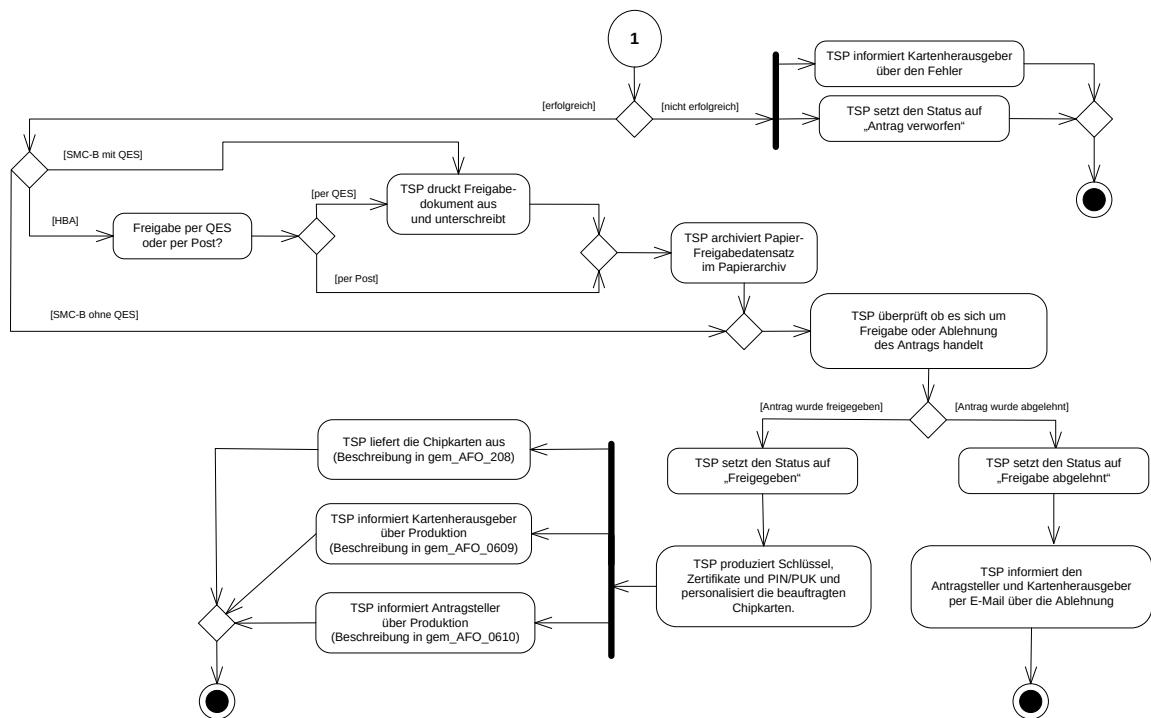


Abbildung 9: Abb_005_Freigabe

Anmerkung: Die beiden getrennten Pfade für „ändern“ und „ergänzen“ sind in [gem_AFO_0107] erläutert.

6.3.3 Anforderungen

☒ **gem_AFO_0094 Ablauf der Freigabe wie in Beschreibung**

Der TSP MUSS es den Kartenherausgebern ermöglichen, die Freigabe wie in „Abb_005_Freigabe“ und „Tab_005_TUC_Freigabe“ dargestellt durchzuführen. ☒

☒ **gem_AFO_0180 Anzeige der Detailansicht eines freizugebenden Antrags**

Der TSP MUSS es den Kartenherausgebern ermöglichen, die Detailansicht eines freizugebenen Antrags auf folgende Weise aufzurufen:

- Der Kartenherausgeber nutzt die Such-/Filterfunktionen des Freigabeportals.
- Der Kartenherausgeber klickt auf einen Link in der E-Mail mit der Benachrichtigung, dass ein freizugebender Antrag vorliegt. ☒

Anmerkung: Die Such-/Filterfunktionen des Freigabeportals werden im Kapitel 6.6.1 Monitoring beschrieben.

☒ **gem_AFO_0107 Anzeige, Änderung und Ergänzung der Antragsdaten**

Der TSP MUSS es den Kartenherausgebern im Freigabeportal ermöglichen, sich die Antragsdaten anzeigen zu lassen, vorhandene Werte zu ändern und fehlende Werte zu ergänzen. Der TSP MUSS sicherstellen, dass für die Spitzenorganisationen individuell konfigurierbar ist, welche Daten im Rahmen der Freigabe geändert und ergänzt werden dürfen. Diese Konfiguration MUSS bilateral zwischen TSP und jeder Spitzenorganisation festgelegt werden. Dabei MÜSSEN im Fall des HBA die

Anforderungen von [SigG01] und [SigV01] bezüglich der Änderbarkeit von Antragsdaten beachtet werden. Der TSP MUSS ermöglichen, dass die Änderungen und Ergänzungen manuell in ein Formular der Weboberfläche des Freigabeportals eingegeben werden. Der TSP MUSS weiterhin ermöglichen, dass die Änderungen und Ergänzungen in der Weise übermittelt werden können, dass eine durch das interne System des Kartenherausgebers generierte Datei mit einem XML-Datensatz über eine Option im Formular zum TSP hochgeladen wird. Die Datei MUSS die in den Übergabeschnittstellen [gemSpec_Pers_HBA] Card-G2-A_3137 bzw. [gemSpec_Pers_SMCB] Card-G2-A_3107 definierte Vorbefüllungsdatenstruktur (abhängig vom Kartentyp des Antrags) mit ihren definierten Pflichtfeldern und denjenigen Werten enthalten, die ergänzt oder geändert werden sollen. Der TSP MUSS diejenigen in der Struktur enthaltenen Werte übernehmen, die gemäß Konfiguration geändert/ergänzt werden dürfen, die ggf. in den Antragsdaten enthaltenen Werte damit überschreiben und das Formular mit den geänderten/ergänzten Daten anzeigen. Der TSP MUSS den Kartenherausgebern danach manuelle Änderungen, zum Beispiel der Daten für die optische Personalisierung, erlauben. Der TSP MUSS dabei die Einschränkungen in [gem_AFO_0117] umsetzen. ☒

Anmerkung 1:

Die in den Übergabeschnittstellen [gemSpec_Pers_HBA] Card-G2-A_3137 und [gemSpec_Pers_SMCB] Card-G2-A_3107 definierten Freigabedatenstrukturen können im Fall der Übermittlung von XML-Strukturen aus dem internen System des Kartenherausgebers nicht verwendet werden, weil sie für den HBA zwingend eine qualifizierte Signatur als Teil der Daten verlangen. Diese müsste innerhalb des internen Systems des Kartenherausgebers generiert werden, wozu dieser eine Signaturgesetz konforme lokale Anwendung benötigen würde. Dies kann jedoch gemäß [gemSpec_SST_TSP] nicht vorausgesetzt werden. Daher werden die Vorbefüllungsdatensätze verwendet.

Anmerkung 2:

- Vorbefüllungsdaten, die vom Antragsteller geändert wurden, werden markiert. Dies wird in [gem_AFO_0151] beschrieben.
- Der TSP kann die Funktion „Änderung/Ergänzung“ in zwei Stufen anbieten:
 - o Pflichtfelder für den Freigabeauftrag können bereits in der ersten Ansicht des Antrags ergänzt werden.
 - o Weitere Antragsdaten können geändert oder ergänzt werden, nachdem der Kartenherausgeber eine „Ändern“-Funktion aufgerufen hat. Der Antrag wird dazu in einer Änderungsansicht angezeigt.

Dies ist in Abbildung 9 „Abb_005_Freigabe“ so dargestellt.

☒ **gem_AFO_0105 Freigabe oder Ablehnung von Anträgen im Freigabeportal**

Der TSP MUSS es den Kartenherausgebern ermöglichen, im Freigabeportal einen Antrag freizugeben. Der TSP MUSS es den Kartenherausgebern ermöglichen, im Freigabeportal einen Antrag abzulehnen. ☒

☒ gem_AFO_0183 Sektorspezifische Auswahl von SMC-B-Freigaben und -Ablehnungen mit und ohne qualifizierte elektronische Signatur

Der TSP MUSS es jedem Sektor ermöglichen auszuwählen, ob die SMC-B-Freigaben oder -Ablehnungen im Freigabeportal mit oder ohne qualifizierte elektronische Signatur erfolgen sollen. Auch beide Varianten MÜSSEN möglich sein. Der TSP MUSS diese für einen Sektor festgelegte Nutzung im Portal konfigurieren. Wenn ein Sektor beide Varianten erlaubt, MUSS der TSP beim Aufruf der Funktion „Freigabe“ oder „Ablehnung“ im Freigabeportal die Auswahl anbieten, ob die Freigabe oder Ablehnung mit oder ohne qualifizierte elektronische Signatur erfolgen soll. ☒

☒ gem_AFO_0155 Freigaben und Ablehnungen von SMC-B-Anträgen ohne qualifizierte elektronische Signatur im Freigabeportal

Wenn die Konfiguration des Sektors gemäß [gem_AFO_0183] eine Freigabe oder Ablehnung ohne qualifizierte elektronische Signatur vorsieht, MUSS die Freigabe oder Ablehnung durch einen Klick auf einen Bestätigungs-Button oder -Link erfolgen. Der TSP MUSS Freigaben und Ablehnungen eines SMC-B-Antrags, die über einen Button oder Link im Freigabeportal erteilt wurden, akzeptieren, wenn im Antrag alle Pflichtfelder gefüllt sind und der vorgegebenen Datenstruktur entsprechen. ☒

☒ gem_AFO_0154 Prüfung der Datenstruktur der Freigabeaufträge

Der TSP MUSS im Freigabeportal die Datenstruktur der Freigabeaufträge prüfen, bevor er eine qualifizierte elektronische Signatur ermöglicht. Er MUSS prüfen, ob alle Pflichtfelder gefüllt sind. Wenn die Prüfung einen Fehler ergibt, MUSS der TSP die qualifizierte elektronische Signatur der Freigabeaufträge technisch unterbinden. Wenn die Prüfung einen Fehler ergibt, MUSS der TSP die Freigabe dieses SMC-B-Antrags durch einen Klick auf einen Button oder Link im Freigabeportal technisch unterbinden. ☒

Anmerkung:

Die Signatur der Freigabeaufträge im Freigabeportal mit einer qualifizierten elektronischen Signatur wird in [gem_AFO_0108] beschrieben, die Prüfung der Signatur in [gem_AFO_0184].

☒ gem_AFO_0156 Freigabeaufträge über SOAP-Schnittstelle

Der TSP MUSS es den Kartenherausgebern ermöglichen, einen oder mehrere Freigabeaufträge mittels eines SOAP-Requests an den TSP zu übermitteln. ☒

☒ gem_AFO_0158 Freigabeaufträge per Post bei KammerIdent

Wurde als Identifizierungsverfahren (ggf. vorab durchgeführtes) KammerIdent gewählt, MUSS es der TSP den Kartenherausgebern ermöglichen, Freigabeaufträge per Post an den TSP zu übermitteln. ☒

☒ gem_AFO_0110 Anpassung des Status nach Prüfung der qualifizierten elektronischen Signatur bzw. nach manueller Prüfung eines per Post eingegangenen Freigabeauftrags

Der TSP MUSS den Status eines Antrags in den folgenden Fällen ändern:

- Wenn die Prüfung der qualifizierten elektronischen Signatur in [gem_AFO_0184] erfolgreich war
- oder wenn ein SMC-B-Freigabeauftrag im Freigabeportal per Klick bestätigt wurde
- oder wenn die manuelle Prüfung eines Freigabeauftrags, der im Rahmen von KammerIdent per Post übermittelt wurde (siehe [gem_AFO_0106]) erfolgreich war.

Für die Änderung gilt:

- Bei einer Freigabe durch den Kartenherausgeber MUSS der TSP den Status des Antrags auf „freigegeben“ setzen.
- Bei einer Ablehnung durch den Kartenherausgeber MUSS der TSP den Status des Antrags auf „Freigabe abgelehnt“ setzen. ☒

☒ **gem_AFO_0106 Manuelle Prüfung von Freigabeaufträgen**

Der TSP MUSS Freigabeaufträge manuell prüfen. Dabei MUSS er prüfen, ob die Datenstruktur erfüllt wird und alle Pflichtfelder korrekt gefüllt sind.

Der TSP MUSS sicherstellen, dass diese Prüfung nach dem Vier-Augen-Prinzip erfolgt, d. h., diese Prüfung MUSS von einem anderen Mitarbeiter durchgeführt werden als die manuelle Prüfung des Antrags in [gem_AFO_0089].

Wenn die Prüfung einen Fehler ergibt, MUSS der TSP

- den Kartenherausgeber benachrichtigen, dies erfolgt in einem nicht-technischen Prozess.
- und er MUSS den Status des Antrags auf „Antrag verworfen“ setzen. ☒

☒ **gem_AFO_0760 Ausdruck und Unterschrift von per QES erfolgten Freigabeaufträgen eines HBA**

Wenn der TSP nicht über ein elektronisches Langzeitarchiv verfügt, MUSS ein mittels QES freigegebener HBA-Antrag vom TSP ausgedruckt, von einem berechtigten Mitarbeiter unterschrieben und im Papierarchiv archiviert werden, um den Vorgaben von [SigG01] und [SigV01] zu genügen. ☒

☒ **gem_AFO_0185 Verarbeitung von Freigabeaufträgen**

Der TSP MUSS die Freigabeaufträge eines Antrags verarbeiten, wenn

- sowohl die manuelle Prüfung in [gem_AFO_0106]
- als auch die Prüfung der qualifizierten elektronischen Signatur erfolgreich war, sofern diese Prüfung notwendig ist. Dies ist in [gem_AFO_0184] beschrieben.

Der TSP MUSS einen Freigabeauftrag ablehnen und nicht verarbeiten, wenn mindestens eine der beiden genannten Prüfungen nicht erfolgreich war. ☒

☒ **gem_AFO_0123 Produktion der freigegebenen Karten**

Wenn der TSP den Status eines Antrags gemäß [gem_AFO_0110] auf „freigegeben“ gesetzt hat, MUSS er die zugehörigen Zertifikate, Schlüssel und PIN/PUK er-

stellen und die Karten personalisieren. Die Zertifikate werden signiert. Dabei MÜSSEN GS-A_4393 und GS-A_5079 aus [gemSpec_Krypt] eingehalten werden. Die PIN/PUK Generierung MUSS den Vorgaben von [gemSpec_PINPUK_TI] folgen. ☒

Anmerkung: Die Auslieferung der Karten wird in Kapitel 6.4 *Lieferung* beschrieben. Der Kartenherausgeber wird über die Produktion informiert, dies wird in 6.6.2 *Benachrichtigungen* beschrieben.

☒ **gem_AFO_0157 Revisionssichere Archivierung von HBA-Freigabeaufträgen**

Wenn der TSP einen HBA-Freigabeauftrag erfolgreich gemäß [gem_AFO_0110] geprüft hat, MUSS er

- im Fall eines elektronischen Freigabeauftrags den Freigabeauftrag ausdrucken und unterschreiben
- und den Freigabeauftrag im Papierarchiv ablegen.

Der TSP MUSS die Freigabeaufträge so archivieren wie im Sicherheitskonzept für die Akkreditierung als ZDA beschrieben. ☒

☒ **gem_AFO_0041 Einhaltung der vereinbarten Datenstruktur für Freigabeaufträge**

Der TSP MUSS für Freigabeaufträge von HBA und SMC-B die Datenstrukturen aus [gemSpec_Pers_HBA] und [gemSpec_Pers_SMC-B] verwenden:

- [gemSpec_Pers_HBA] Card-G2-A_3136 Struktur der Freigabedaten für einen HBA-Antrag
- [gemSpec_Pers_SMC-B] Card-G2-A_3174 Struktur der Freigabedaten für einen SMC-B-Antrag
- [gemSpec_Pers_HBA] Card-G2-A_3168 Datenstruktur für HBA-Sammelfreigaben
- [gemSpec_Pers_SMC-B] Card-G2-A_3175 Datenstruktur für SMC-B-Sammelfreigaben

Bei einer Freigabe via SOAP-Request müssen diese Datenstrukturen als XML-Struktur verwendet werden. Zur Authentisierung der Freigabe bzw. Ablehnung durch den Kartenherausgeber MUSS der TSP ein zusätzlich zu den XML-Daten vorhandenes signiertes PDF akzeptieren. ☒

6.3.4 Artefakte

Zu Artefakten im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.3.5 Testunterstützung

Zur Unterstützung von Tests im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.3.6 Hardwaremerkmale

Das Funktionsmerkmal setzt keine besonderen Hardwaremerkmale voraus.

6.4 Lieferung

Nach Fertigstellung des HBA bzw. der SMC-B liefert der TSP die Karte an den Empfänger aus. Im Anschreiben nennt der TSP die für den Karteninhaber zuständige Organisation. Der Empfänger muss seine Identität bei Erhalt der Karte gegenüber dem Lieferanten mit einem gängigen Identifikationsverfahren (z. B. PostIdent) bestätigen. Im Fall des HBA ist der Empfänger immer der Antragsteller selbst, im Fall der SMC-B legen die zuständigen Sektoren fest, ob der Antragsteller bei der Beantragung einen berechtigten Empfänger benennen darf. Diese Information muss im Portal des TSP konfiguriert werden. Zeitversetzt zur Auslieferung einer Karte versendet der TSP den PIN/PUK-Brief an den Antragsteller per normaler Briefpost.

Falls ein SMC-B-Antrag durch ein Praxisregister verwaltet wird, erfolgt die Freischaltung nach erfolgreicher Auslieferung der Karte an den Empfänger durch das Praxisregister.

In allen anderen Fällen bestätigt der Antragsteller den Erhalt der Karte im Antragsportal über die Funktion „Freischaltung“, welche in [gem_AFO_0076] beschrieben ist. Der Antragsteller ruft das Antragsportal auf. Nach Auswahl der Option „Freischaltung“ wird der Antragsteller aufgefordert, die Kartennummer und das Freischaltewort einzugeben. Nach Prüfung der Kartennummer und des Freischalteworts gibt der TSP die Zertifikate frei und veröffentlicht die X.50-Verschlüsselungszertifikate in einem Verzeichnisdienst, sofern der Antragsteller der Veröffentlichung bei der Antragstellung zugestimmt hat.

Die Benachrichtigung an den Kartenherausgeber und Antragsteller werden in [gem_AFO_0609] und [gem_AFO_0610] beschrieben.

Die Kommunikation zwischen dem TSP und dem Antragsteller erfolgt über die Schnittstellen [Sch_Post] und [Sch_Antragsportal].

6.4.1 TUC-Beschreibung

Tabelle 8: Tab_202_TUC_Lieferung

Element	Beschreibung
Name	Lieferung
Beschreibung	Bei der Lieferung werden fertiggestellte Karten vom TSP an die angegebene Lieferanschrift des Antragstellers versendet. Der Empfänger identifiziert sich bei Erhalt der Karte gegenüber den Lieferanten, z. B. mittels PostIdent. Der Lieferant wiederum informiert den TSP, dass der Empfänger die Karten entgegengenommen hat. Der TSP leitet die Information an den Kartenherausgeber weiter. Ein anderer Ablauf ergibt sich, wenn SMC-B-Anträge durch ein Praxisregister verwaltet werden. In diesem Fall erhält der Kartenherausgeber die Rückmeldung vom Lieferanten, dass die Karte

Element	Beschreibung
	erfolgreich ausgeliefert wurde. Zeitversetzt zum Kartenversand (mindestens 3 Tage danach) versendet der TSP den PIN/PUK-Brief an den Antragsteller per normaler Briefpost. Zur Freischaltung der Zertifikate der Karte ruft der Antragsteller das Antragsportal auf und gibt das während der Antragstellung angezeigte Freischaltekeywort ein. Der TSP schaltet die Zertifikate frei und informiert den Kartenherausgeber darüber. Im Fall des Praxisregisters erfolgt die Freischaltung im Praxisregister. Der TSP fragt regelmäßig beim Praxisregister nach, ob Freischalttaufträge vorliegen, und führt diese durch. Sofern die Zustimmung des Antragstellers bei der Beantragung einer Karte erteilt wurde, veröffentlicht der TSP die Verschlüsselungszertifikate dieser Karte in seinem Verzeichnisdienst. Im Fall der Freischaltung im Praxisregister veröffentlicht der TSP die Verschlüsselungszertifikate immer. Die Zustimmung des Antragstellers wurde vor der Freischaltung gegenüber dem zuständigen Kartenherausgeber erteilt.
Auslöser	Der TSP will dem Antragsteller die beantragte(n) Karte(n) ausliefern.
Vorbedingungen	Der TSP hat die Karte produziert. Der TSP hat einen PIN/PUK-Brief erstellt. Der Antragsteller kennt die Kartennummer und das Freischaltekeywort (nur falls Antrag nicht durch ein Praxisregister verwaltet wird).
Eingangsdaten	• Persönliche Daten und Lieferanschrift des Antragstellers • Karte • Kartennummer • PIN/PUK-Brief • Freischaltekeywort (nur falls Antrag nicht durch ein Praxisregister verwaltet wird)
Komponenten	Kartenpersonalisierung.
Ausgangsdaten	E-Mail an den Kartenherausgeber mit dem Status der Auslieferung der Karte bzw. der Freischaltung der Karte (nur falls Antrag nicht durch ein Praxisregister verwaltet wird); Andernfalls: Freischalttauftrag wurde vom TSP im Praxisregister abgeholt und durchgeführt.

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	Jeweils Statusänderung des Antrags im Freigabeportal bei erfolgreicher Auslieferung und Freischaltung;
Nachbedingungen	Sofern die Zustimmung des Antragstellers bei der Beantragung einer Karte erteilt wurde, werden zeitnah nach erfolgter Freischaltung die Verschlüsselungszertifikate im Verzeichnisdienst des TSP veröffentlicht.
Standardablauf	Siehe: Abbildung 10 „Abb_206_Lieferung“ Abbildung 11 „Abb_207_Lieferung_Praxisregister“
Varianten/Alternativen	persönliche Übergabe der Karten und PIN/PUK-Briefe an den Antragsteller durch den TSP
Fehlerfälle	- Die Identifizierung bei Auslieferung schlägt fehl. Im Fall des Praxisregisters erfolgt daraufhin die Rücksendung der nicht ausgelieferten Karte an den Kartenherausgeber, der als Absender des Kartenversands ausgewiesen ist. Anderenfalls erfolgt eine Rücksendung an den TSP. - Der Antragsteller bestätigt den Empfang der Karte nicht, d. h., er schaltet seine Karte nicht frei (nur falls Antrag nicht durch Praxisregister verwaltet wird).
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Siehe: Abbildung 10 „Abb_206_Lieferung“ Abbildung 11 „Abb_207_Lieferung_Praxisregister“

6.4.2 Ablauf

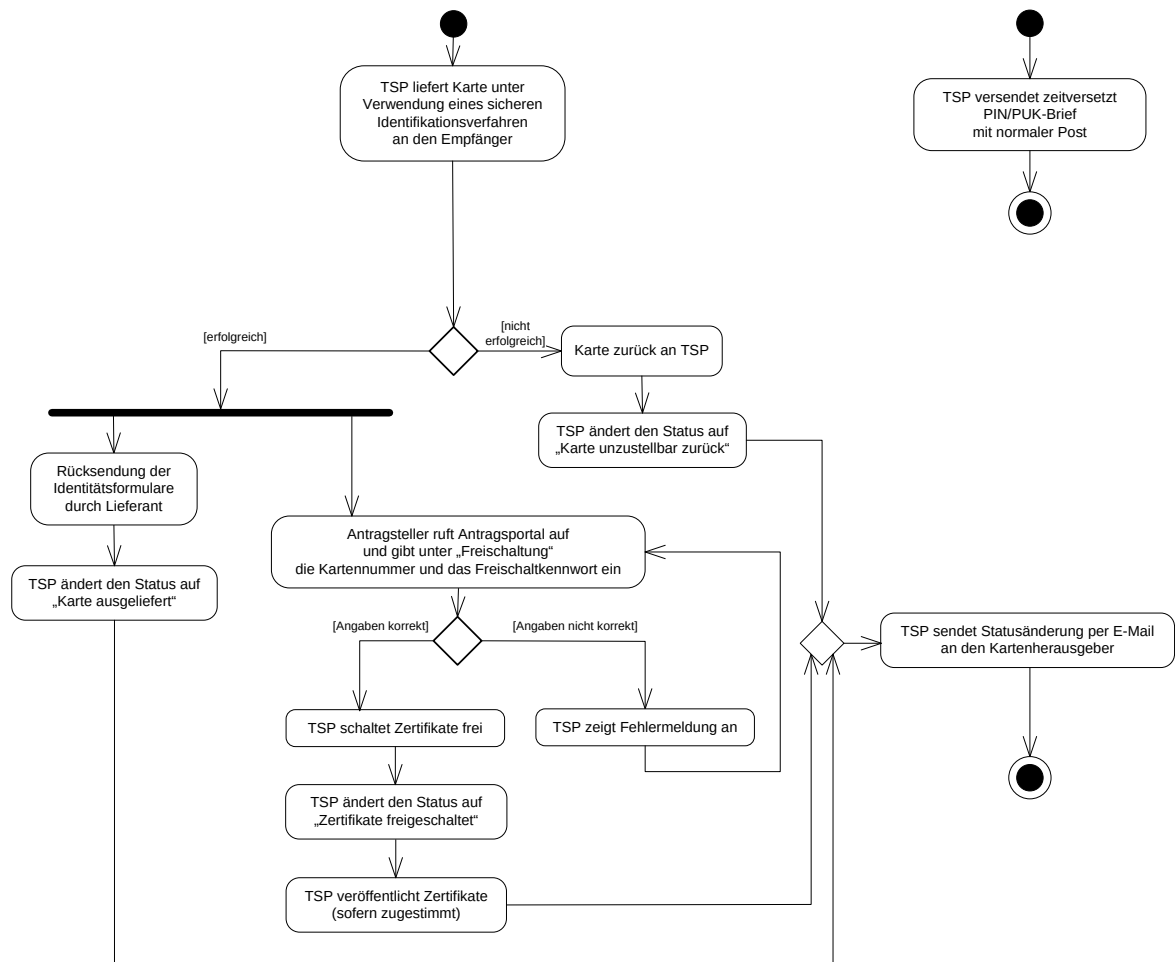


Abbildung 10: Abb_206_Lieferung

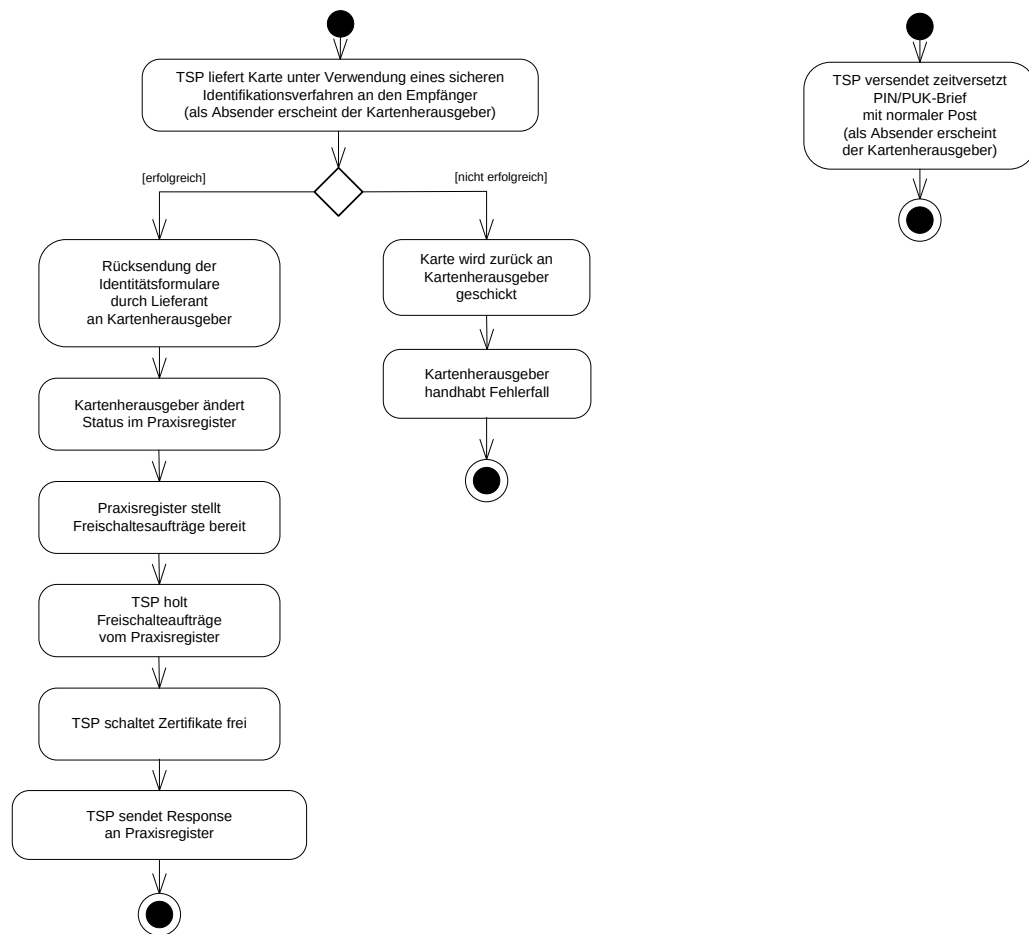


Abbildung 11: Abb_207_Lieferung_Praxisregister

6.4.3 Anforderungen

☒ **gem_AFO_0208 Ablauf der Lieferung wie in Beschreibung**

Der TSP MUSS die Lieferung wie in „Abb_206_Lieferung“ und „Tab_202_TUC_Lieferung“ dargestellt durchführen. ☒

☒ **gem_AFO_0200 Getrennter und zeitversetzter Versand der Briefe**

Der TSP MUSS den PIN/PUK-Brief mindestens um drei Tage und längstens um 10 Tage zeitversetzt zu dem Brief mit der Karte an den Antragsteller versenden. ☒

☒ **gem_AFO_0715 Benennung des zuständigen Kartenherausgebers im Anschreiben**

Im Anschreiben zur Kartenlieferung MUSS der TSP den für den Karteninhaber zuständigen Kartenherausgeber benennen. ☒

☒ gem_AFO_0201 Informierung des Kartenherausgeber nach erfolgreicher Auslieferung

Der TSP MUSS bei erfolgreicher Auslieferung der Karte den Status des Antrags im Freigabeportal auf „Karte ausgeliefert“ setzen und den Kartenherausgeber informieren. Die Benachrichtigung an den Kartenherausgeber wird in [gem_AFO_0609] beschrieben. ☒

☒ gem_AFO_0206 Sicheres Identifikationsverfahren bei Übergabe der Karte

Der TSP MUSS die Karte unter Verwendung eines sicheren Identifikationsverfahrens des berechtigten Empfängers, z. B. mittels PostIdent-Verfahren, ausliefern. ☒

☒ gem_AFO_0203 Informierung des Kartenherausgebers nach fehlgeschlagener Auslieferung

Der TSP MUSS bei fehlgeschlagener Auslieferung der Karte den Status des Antrags im Freigabeportal auf „Karte unzustellbar zurück“ setzen und den Kartenherausgeber informieren. Die Benachrichtigung an den Kartenherausgeber wird in [gem_AFO_0609] beschrieben. ☒

☒ gem_AFO_0204 Freischaltung Karte und Zertifikate durch den Antragsteller

Der Antragsteller MUSS für die Freischaltung das Antragsportal aufrufen und das während der Antragstellung im PDF-Dokument erhaltene Freischalteknwort sowie die Kartennummer der empfangenen Karte eingeben. Bei Eingabe des korrekten Freischalteknwortes und der korrekten Kartennummer MUSS der TSP die Zertifikate freischalten und den Status des Antrags im Freigabeportal auf „Zertifikate freigeschaltet“ setzen. Bei Eingabe falscher Daten MUSS der TSP eine Fehlermeldung anzeigen. ☒

☒ gem_AFO_0716 Veröffentlichung von Zertifikaten durch den TSP

Nach erfolgter Freischaltung gemäß [gem_AFO_0204] und vorliegender Zustimmung des Antragstellers MUSS der TSP die Verschlüsselungszertifikate dieser Karte in seinem Verzeichnisdienst veröffentlichen. Der Verzeichnisdienst MUSS über das Internet und die Telematik Infrastruktur abrufbar sein. ☒

6.4.4 Artefakte

Zu Artefakten im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.4.5 Testunterstützung

Zur Unterstützung von Tests im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.4.6 Hardwaremerkmale

Das Funktionsmerkmal setzt keine besonderen Hardwaremerkmale voraus.

6.5 Sperrung

Zertifikate können beim TSP gesperrt werden. Dafür gibt es die folgenden Varianten:

- [SP-1]: Antragsteller sperrt Zertifikate im Antragsportal
- [SP-2]: Kartenherausgeber sperrt Zertifikate im Freigabeportal
- [SP-3]: Kartenherausgeber sperrt Zertifikate über die SOAP-Schnittstelle
- [SP-4]: Antragsteller sperrt Zertifikate über die telefonische Sperrhotline des Trust Centers
- [SP-5]: Kartenherausgeber sperrt Zertifikate schriftlich
- [SP-6]: Antragsteller sperrt Zertifikate schriftlich

Hinweis: Die nicht-technischen Prozesse [SP-4], [SP-5] und [SP-6] laufen losgelöst von der TSP-Schnittstelle ab und werden daher in diesem Dokument nicht weiter betrachtet.

Es ist hervorzuheben, dass der TSP gemäß der Anforderungen einer Spitzenorganisation in der TSP-Schnittstelle konfigurieren können muss, ob alle Kartenherausgeber unterhalb dieser Spitzenorganisation sperrberechtigt für eine, mehrere oder alle Karten eines Antragstellers sind, auch wenn sie für diesen nicht bestätigende Stelle waren (z.B. im Fall eines Umzugs und damit verbundenem Wechsel des zuständigen Kartenherausgebers). Diese Regelung bezieht sich immer nur auf den Kartentyp, für den die jeweilige Spitzenorganisation zuständig ist (HBA oder SMC-B). Falls alle Kartenherausgeber unter einer Spitzenorganisation als sperrberechtigt konfiguriert sind, können alle registrierten sperrberechtigten Mitarbeiter aller Kartenherausgeber in diesem Fall elektronische Sperrungen durchführen, darüber hinaus können sie auch schriftlich sperren. In diesem Fall muss der TSP ihre Unterschriften gegen die beim TSP hinterlegten prüfen (siehe hierzu auch [gem_AFO_0168]). Falls eine solche Regelung nicht konfiguriert ist, darf nur der ausgebende Kartenherausgeber sperren. Dies ist z.B. im Bereich der KZBV der Fall: hier darf nur die ausgebende KZV eine SMC-B eines Zahnarztes sperren.

Zur Vereinfachung wird im Folgenden nicht zwischen „Kartenherausgeber“ und „Mitarbeiter des Kartenherausgebers“ unterschieden.

Die Benachrichtigungen an Kartenherausgeber und Antragsteller werden in Kapitel 6.6.2 Benachrichtigungen beschrieben.

6.5.1 TUC-Beschreibung

Tabelle 9: Tab_100_TUC_Sperrung

Element	Beschreibung
Name	Sperrung
Beschreibung	• [SP-1]: Ein Antragsteller gibt im Antragsportal Referenznummer und Sperrkennwort der Karte der zu sperrenden Zertifikate ein. • [SP-2]: Ein Kartenherausgeber sucht im Freigabeportal

Element	Beschreibung
	die Karten der zu sperrenden Zertifikate. Er signiert den Sperrauftrag mit einer qualifizierten elektronischen Signatur. [SP-3]: Ein Kartenherausgeber sendet einen oder mehrere Sperraufträge mit qualifizierter elektronischer Signatur über die SOAP-Schnittstelle an den TSP. Nach einer Prüfung sperrt der TSP alle Zertifikate der Karte. Im Falle von [SP-2] und [SP-3] kann er auf Wunsch des Kartenherausgebers auch alle Zertifikate weiterer Karten des Antragstellers sperren.
Auslöser	Die Zertifikate einer Karte sollen gesperrt werden, zum Beispiel weil der Antragsteller die Karte verloren hat oder sich Angaben im Zertifikat geändert haben etc.
Vorbedingungen	Eine TLS/SSL-Verbindung wurde gemäß [gem_AFO_0007] aufgebaut. Die zu sperrenden Zertifikate befinden sich in einem sperrbaren Status. [SP-1]: - Der Antragsteller kennt Referenznummer und Sperrkennwort der Karte der zu sperrenden Zertifikate. [SP-2]: - Der Kartenherausgeber ist am Freigabeportal authentisiert. - Der authentisierte Mitarbeiter des Kartenherausgebers besitzt das Zugriffsrecht für „Sperrung“. Für die qualifizierte elektronische Signatur muss der Kartenherausgeber mit seinem SigG-Zertifikat beim TSP registriert sein - Der Kartenherausgeber kennt die Referenznummer oder andere Daten, mit denen er den Antrag des zu sperrenden Zertifikats finden kann. [SP-3]: - Authentisierung beim SOAP-Request. - Identifikationsdaten der Karte der zu sperrenden Zertifikate sind bekannt.
Eingangsdaten	[SP-1]: Referenznummer und Sperrkennwort der Karte der zu sperrenden Zertifikate.

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	[SP-2]: Referenznummer oder Vorgangsnummer oder andere Suchkriterien, um die Karte der zu sperrenden Zertifikate zu finden (gemäß [gem_AFO_0121]). [SP-3]: Sperrauftrag mit Identifikationsdaten der Karte der zu sperrenden Zertifikate und qualifizierter elektronischer Signatur.
Komponenten	Kartenpersonalisierung.
Ausgangsdaten	Sperrbestätigung
Nachbedingungen	Zu sperrende Zertifikate sind gesperrt.
Standardablauf	Siehe Abbildung 13 „Abb_100_Sperrung“ und [gem_AFO_0131].
Varianten/Alternativen	[SP-1], [SP-2], [SP-3]. - Bei [SP-2] kann der Kartenherausgeber im Freigabeportal die Karten auswählen, deren Zertifikate gesperrt werden sollen, indem er sie in der Übersichtsansicht in der Spalte „Sperren“ ankreuzt. - Bei [SP-3] können alle Zertifikate einer oder aller Karten des Antragstellers gesperrt werden. - Bei [SP-3] können verschiedene Daten verwendet werden, um alle Anträge eines Antragstellers zu identifizieren.
Fehlerfälle	[SP-1]: - Referenznummer und Sperrkennwort sind in dieser Kombination nicht gültig. [SP-2]: - Authentisierung des Kartenherausgebers am Freigabeportal schlägt fehl. - Das SigG-Zertifikat des Kartenherausgebers ist nicht beim TSP registriert. - Der Kartenherausgeber findet die Karte der zu sperrenden Zertifikate nicht. [SP-3]: - SOAP-Authentisierung schlägt fehl. - Die Identifikationsdaten gehören nicht zu einer sperrbaren Karte. [SP-2] und [SP-3]:

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element		Beschreibung
		• Die Datenstruktur des Sperrauftrags wird nicht eingehalten. • Die qualifizierte elektronische Signatur ist nicht gültig. • Die manuelle Überprüfung ergibt Fehler. Alle Varianten: • Die Karte der zu sperrenden Zertifikate ist nicht in einem sperrbaren Status. • Wenn der Antragsteller oder Kartenherausgeber die geforderten TLS-Versionen oder Ciphersuites nicht unterstützt, lässt der TSP keine Übertragung zu.
Nichtfunktionale Anforderungen	An-	keine
Zugehörige Diagramme	Dia-	Abbildung 12 „Abb_101_Sperrung_über_Antragsportal“Abbildung 13 „Abb_100_Sperrung_über_Freigabeportal“

6.5.2 Ablauf

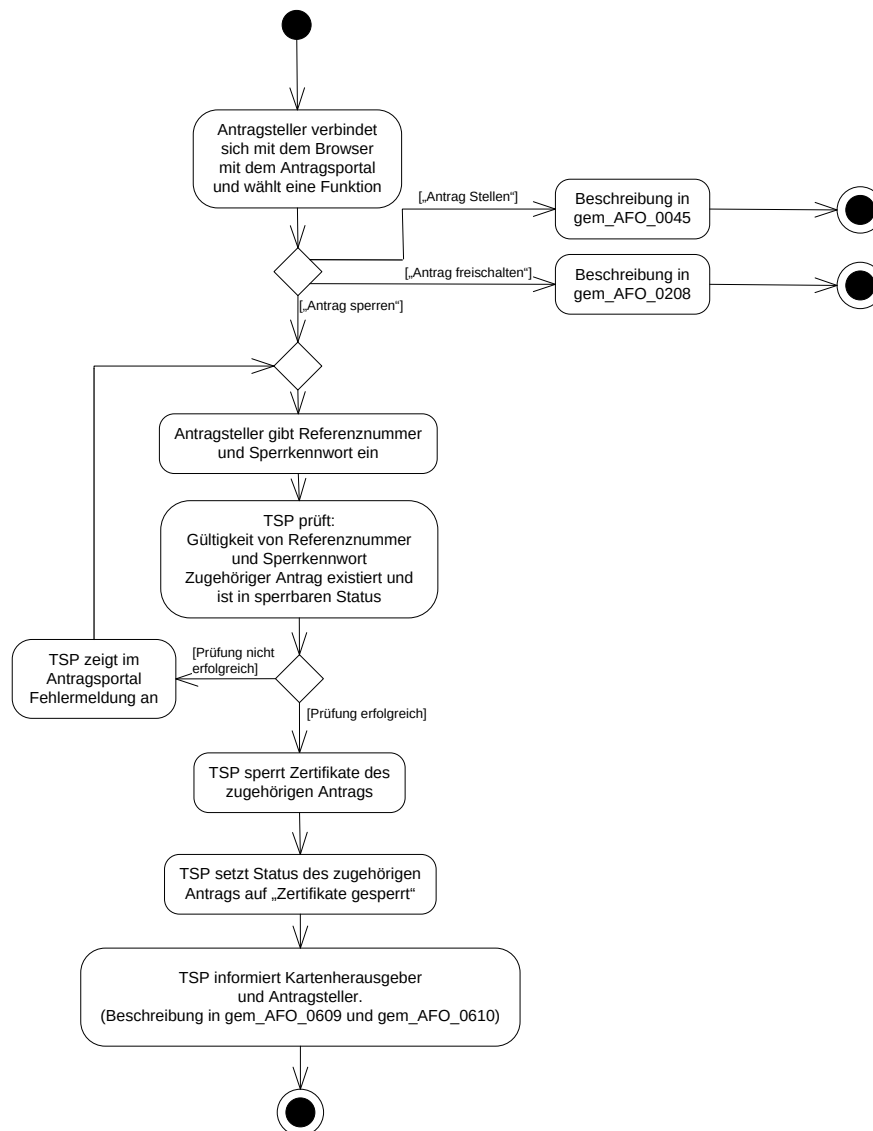


Abbildung 12: Abb_101_Sperrung_über_Antragsportal

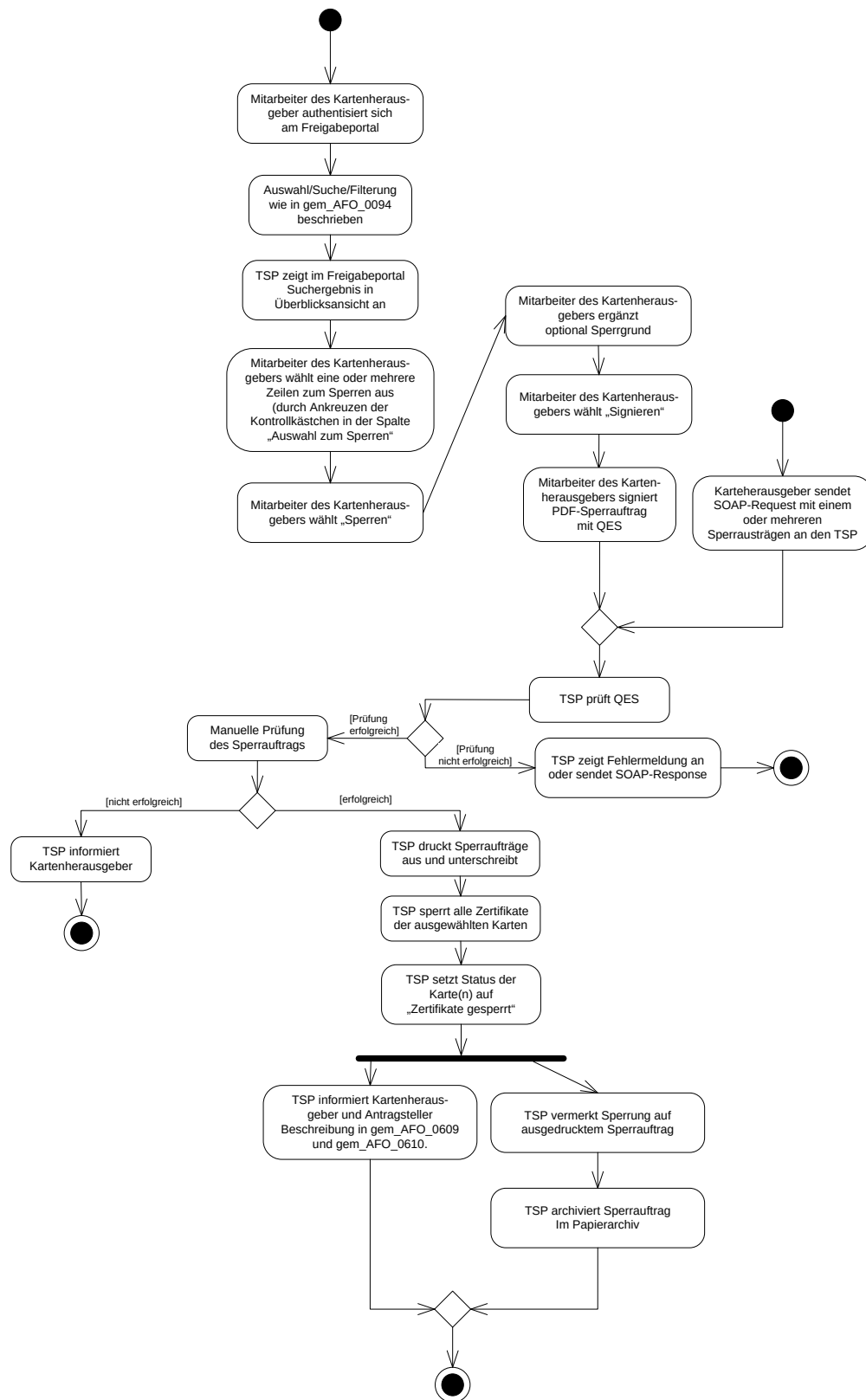


Abbildung 13: Abb_100_Sperrung_über_Freigabeportal

6.5.3 Anforderungen

☒ **gem_AFO_0131 Ablauf der Sperrung wie in Beschreibung**

Der TSP MUSS es den Kartenherausgebern und Antragstellern ermöglichen, die Sperrung wie in „Abb_101_Sperrung_über_Antragsportal“, „Abb_100_Sperrung_über_Freigabeportal“ und „Tab_100_TUC_Sperrung“ dargestellt durchzuführen. Im Fall von [SP-2] und [SP-3] MUSS der Kartenherausgeber wie beschrieben seine Sperraufträge qualifiziert signieren. ☒

☒ **gem_AFO_0181 Prüfung und Sperrung im Antragsportal**

Der TSP MUSS prüfen, ob eine Referenznummer und ein Sperrkennwort, das ein Antragsteller im Antragsportal eingibt, gültig sind. Wenn sie gültig sind und zu einer sperrbaren Karte gehören, dann MUSS der TSP alle Zertifikate sperren, die zu dieser Karte gehören. Wenn Referenznummer und Sperrkennwort nicht gültig sind oder wenn kein zugehöriger sperrbarer Antrag vorhanden ist, dann MUSS der TSP die Sperrung ablehnen. ☒

☒ **gem_AFO_0168 Sperrung von Zertifikaten im Freigabeportal**

Der TSP MUSS gemäß der Anforderungen einer Spitzenorganisation in der TSP-Schnittstelle konfigurieren, ob alle Kartenherausgeber unterhalb dieser Spitzenorganisation sperrberechtigt für eine, mehrere oder alle Karten eines Antragstellers sind, auch wenn sie für diesen nicht bestätigende Stelle waren. Diese Regelung bezieht sich immer nur auf den Kartentyp, für den die jeweilige Spitzenorganisation zuständig ist (HBA oder SMC-B). Falls dies konfiguriert ist, MUSS der TSP es jedem Kartenherausgeber unterhalb dieser Spitzenorganisation ermöglichen, im Freigabeportal alle Zertifikate einer oder mehrerer Karten des jeweiligen Typs, für den die Spitzenorganisation zuständig ist (HBA oder SMC-B) eines Antragstellers sperren zu lassen. Dies gilt auch dann, wenn der sperrende Kartenherausgeber nicht bestätigende Stelle für diesen Antragsteller war, da die Zuständigkeit eines Kartenherausgebers für einen Antragsteller wechseln kann. Der TSP MUSS allen Kartenherausgebern unterhalb der Spitzenorganisation im Freigabeportal in der Übersichtsansicht eine Auswahlmöglichkeit anbieten, welche Karten gesperrt werden sollen. ☒

Anmerkung: Diese Konfigurationsoption wird z.B. nicht für die SMC-B der Zahnärzte eingesetzt. Hier darf nur der jeweils ausgebende Kartenherausgeber sperren.

☒ **gem_AFO_0186 Eingabe eines Sperrgrunds beim Sperren im Freigabeportal**

Der TSP MUSS es den Kartenherausgebern ermöglichen, im Freigabeportal einen Sperrgrund einzugeben, wenn der Kartenherausgeber eine Karte sperren will. Diese Angabe eines Sperrgrunds ist für den Kartenherausgeber optional. ☒

☒ **gem_AFO_0170 Sperraufträge über SOAP-Schnittstelle**

Der TSP MUSS es den Kartenherausgebern ermöglichen, einen oder mehrere Sperraufträge mittels eines SOAP-Requests an den TSP zu übermitteln. ☒

Anmerkung:

Die Signatur der Sperraufträge im Freigabeportal mit einer qualifizierten elektronischen Signatur wird in [gem_AFO_0108] beschrieben, die Prüfung der Signatur in [gem_AFO_0184].

☒ **gem_AFO_0187 Manuelle Prüfung von Sperraufträgen**

Der TSP MUSS Sperraufträge vom Kartenherausgeber (sowohl am Freigabeportal als auch über einen SOAP-Request) manuell prüfen. Wenn die Prüfung einen Fehler ergibt, MUSS der TSP den Kartenherausgeber benachrichtigen, dies erfolgt in einem nicht-technischen Prozess. ☒

☒ **gem_AFO_0172 Reaktion auf erfolgreiche Prüfung eines Sperrauftrags**

Wenn die in [gem_AFO_0184] und [gem_AFO_0187] genannten Prüfungen eines Sperrauftrags vom Kartenherausgeber erfolgreich waren, MUSS der TSP folgendes durchführen:

- Der TSP MUSS den Sperrauftrag ausdrucken und unterschreiben.
- Bei einem Sperrauftrag im Portal MUSS er alle Zertifikate aller angekreuzten Karten sperren.
- Bei einem Sperrauftrag per SOAP MUSS er entsprechend den Angaben in dem Sperrauftrag
 - o alle Zertifikate der Karte sperren
 - o oder alle Zertifikate aller Karten des Antragstellers sperren.

Sollten einige oder alle betroffenen Karten bereits gesperrt sein, führt dies nicht zu einem Fehler. Sollten eine oder mehrere betroffene Karten zwar freigegeben, aber noch nicht produziert sein, führt dies nicht zu einem Fehler. Die betreffenden Produktionsaufträge MÜSSEN in diesem Fall vom TSP storniert werden. Der TSP MUSS einen Sperrauftrag ablehnen, wenn mindestens eine der beiden genannten Prüfungen [gem_AFO_0184] und [gem_AFO_0187] nicht erfolgreich war. ☒

☒ **gem_AFO_0112 Nennung von Identifikationsdaten für Sperrung**

Um alle Karten des gleichen Typs eines Antragsstellers (d. h. entweder alle HBA oder alle SMC-B eines Antragstellers) sperren zu können, MÜSSEN die Spitzenorganisationen dem TSP Identifikationsdaten nennen, mit denen alle Karten eines Antragstellers des betroffenen Typs eindeutig identifizierbar sind. Bezüglich der Sperrberechtigungen MÜSSEN die Festlegungen in [gem_AFO_0168] beachtet werden. ☒

Anmerkung: Die Identifikationsdaten können sich bei den verschiedenen Spitzenorganisationen unterscheiden.

☒ **gem_AFO_0173 Anpassung des Status von Anträgen gesperrter Zertifikate**

Wenn der TSP die Sperrung der Zertifikate einer oder mehrerer Karte durchgeführt hat, MUSS er den Status der Karte(n) auf „Zertifikate gesperrt“ setzen. Dies gilt sowohl für Sperrungen durch den Antragsteller als auch durch den Kartenherausgeber. ☒

☒ **gem_AFO_0188 Archivierung von Sperraufträgen des Kartenherausgebers**

Wenn der TSP die Sperrung der Zertifikate einer oder mehrerer Karte durchgeführt und den Status angepasst hat, MUSS er die Sperrung auf dem ausgedruckten Sperrauftrag vermerken und den Sperrauftrag im Papierarchiv revisionssicher archivieren. Dies gilt nur für Sperraufträge vom Kartenherausgeber (am Freigabeportal oder per SOAP-Request). ☒

☒ **gem_AFO_0189 Benachrichtigung über Sperrung**

Wenn der TSP die Sperrung der Zertifikate einer oder mehrerer Karten durchgeführt und den Status angepasst hat, MUSS er die den Kartenherausgeber und den Antragsteller über die Sperrung informieren. Dies gilt sowohl für Sperrungen durch den Antragsteller als auch durch den Kartenherausgeber. ☒

☒ **gem_AFO_0043 Einhaltung der vereinbarten Datenstruktur für Sperraufträge per SOAP-Request**

Die Kartenherausgeberer MÜSSEN für Sperraufträge für HBA und SMC-B die folgenden Datenstrukturen aus [gemSpec_Pers_HBA] und [gemSpec_Pers_SMC-B] verwenden. Dies gilt für Sperraufträge im XML-Format per SOAP-Request:

- Card-G2-A_3138 Struktur eines HBA-Sperrauftrags
- Card-G2-A_3170 Datenstruktur für die Sammelübertragung von HBA-Sperraufträgen
- Card-G2-A_3108 Struktur eines SMC-B-Sperrauftrags
- Card-G2-A_3177 Datenstruktur für die Sammelübertragung von SMC-B-Sperraufträgen ☒

☒ **gem_AFO_0731 Einhaltung der vereinbarten Datenstruktur für Sperraufträge am Freigabeportal**

Der TSP MUSS bei Sperraufträgen über das Freigabeportal die gleichen Inhaltsdaten wie in den in [gem_AFO_0043] referenzierten Datenstrukturen verwenden, jedoch in einer von ihm wählbaren Übergabedatenstruktur, zum Beispiel in Form eines zu signierenden PDF-Dokuments. ☒

6.5.4 Artefakte

Zu Artefakten im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.5.5 Testunterstützung

Zur Unterstützung von Tests im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.5.6 Hardwaremerkmale

Das Funktionsmerkmal setzt keine besonderen Hardwaremerkmale voraus.

6.6 Monitoring und Benachrichtigungen

6.6.1 Monitoring

Kartenherausgeber und Spitzenorganisationen können am Freigabeportal Monitoring-Funktionen durchführen, sofern sie die entsprechenden Rechte haben. Zur Vereinfachung werden diese Rollen in diesem Kapitel als „Anwender“ bezeichnet.

Zugriff auf das Vorbefüllungsportal ist mit Monitoring Rechten nicht möglich.

Die Kommunikation zwischen den Anwendern und dem Freigabeportal des TSP erfolgt über die Schnittstelle [Sch_Freigabeportal] oder [Sch_SOAP].

Das Freigabeportal wird hier im Allgemeinen und bzgl. Monitoring beschrieben. Außer Monitoring sind im Freigabeportal aber auch andere Funktionen möglich, diese werden in den zugehörigen Kapiteln beschrieben:

- 6.3 Freigabe
- 6.5 Sperrung

6.6.1.1 TUC-Beschreibung

Tabelle 10: Tab_006_TUC_Monitoring

Element	Beschreibung
Name	Monitoring
Beschreibung	Anwender können sich am Freigabeportal über Anträge informieren: • Sie können sich eine Überblicksansicht über alle Anträge anzeigen lassen. • Sie können sich eine Detailansicht eines ausgewählten Antrags anzeigen lassen. • Sie können Anträge nach Zeitraum, Status und/oder einem Suchbegriff filtern. • Sie können die Überblicksansicht exportieren. • Sie können in der Überblicksansicht Anträge sortieren. Außerdem können über eine SOAP-Schnittstelle Statusabfragen durchgeführt werden. Welche dieser Aktionen sie durchführen dürfen und welche Daten sie angezeigt bekommen, hängt von ihren Zugriffsrechten und organisatorischen Zugehörigkeit ab. Beispielsweise erhalten Mitarbeiter von Spitzenorganisationen der Sektoren lediglich das Zugriffsrecht „Monitoring“, das ausschließlich Zugriff auf pseudonymisierte Daten erlaubt. Details sind in [gem_AFO_0117] beschrieben.

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	Zugriff auf das Vorbefüllungsportal ist mit Monitoring Rechten nicht möglich.
Auslöser	Ein Anwender benötigt Informationen über einen oder mehrere Anträge.
Vorbedingungen	Eine TLS/SSL-Verbindung wurde gemäß [gem_AFO_0007] aufgebaut. Für Portalzugriff: • Der Anwender hat sich am Freigabeportal authentisiert. • Dem Anwender sind passende Zugriffsrechte zugewiesen: mindestens „Monitoring“, oder „Freigabe“ oder „Sperrung“. Bei SOAP-Zugriff: • Authentisierung an der SOAP-Schnittstelle und passende Zugriffsrechte.
Eingangsdaten	Such- und Filterkriterien
Komponenten	Kartenpersonalisierung
Ausgangsdaten	Überblicksansicht, Detailansicht und Produktionsrückmeldungen von Anträgen. Statusinformationen.
Nachbedingungen	keine
Standardablauf	Siehe Abbildung 14 „Abb_006_Freigabeportal“.
Varianten/Alternativen	• Die Funktionen und Informationen können eingeschränkt werden, dies ist in [gem_AFO_0117] definiert. • Es ist ein Zugriff über das Freigabeportal oder ein SOAP-Zugriff für Statusabfragen möglich.
Fehlerfälle	Keine im Freigabeportal: Wenn über die Such- und Filterkriterien gemäß [gem_AFO_0121] und [gem_AFO_0117] keine Anträge gefunden werden, werden keine Anträge angezeigt. Dies ist nicht als Fehler anzusehen. Bei der SOAP-Schnittstelle sendet der TSP in den folgenden Fällen eine entsprechende Response: • die übermittelte Datenstruktur ist nicht korrekt • zum angefragten Status ist kein Antrag vorhanden • ein angefragter Antrag ist nicht vorhanden

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element		Beschreibung
Nichtfunktionale Anforderungen	An-	keine
Zugehörige gramme	Dia-	Siehe Abbildung 14 „Abb_006_Freigabeportal“.

6.6.1.2 Ablauf

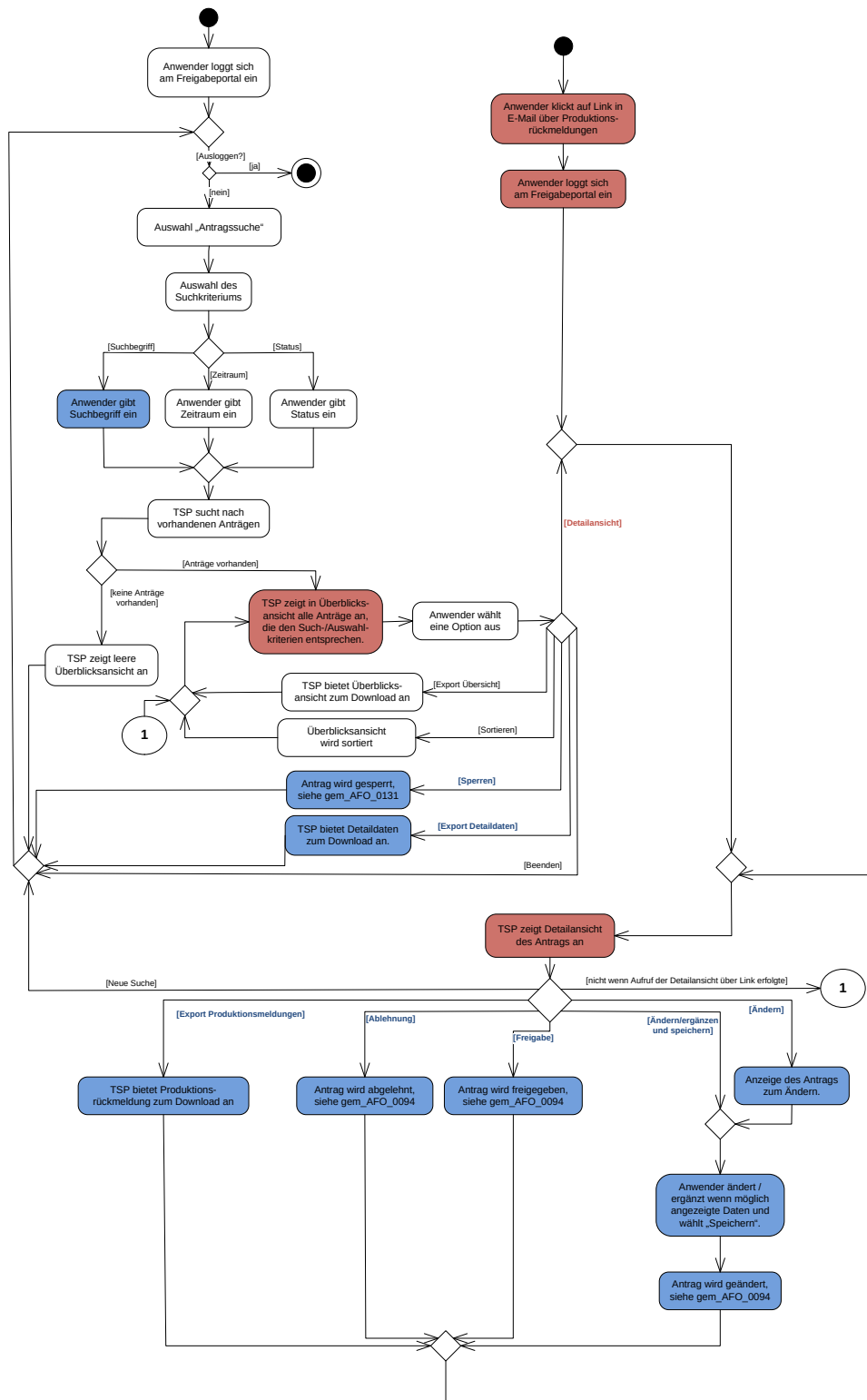


Abbildung 14: Abb_006_Freigabeportal

Legende zu Abbildung 14 „Abb_006_Freigabeportal“:

- nur „Monitoring“-Rechte, d. h. keine „Freigabe“ und keine „Sperrung“-Rechte (diese Rechte haben ausschließlich Mitarbeiter von Spitzenorganisationen):
 - o ohne Füllung ist möglich
 - o rote Füllung ist nur eingeschränkt möglich
 - o blaue Füllung ist nicht möglich
- mit „Freigabe“ oder „Sperrung“-Rechten ist alles möglich

Anmerkung: In Abbildung 14 „Abb_006_Freigabeportal“ ist die SOAP-Schnittstelle nicht dargestellt, sondern nur der Zugriff über das Freigabeportal.

6.6.1.3 Anforderungen

☒ **gem_AFO_0196 Ablauf des Monitoring wie in Beschreibung**

Der TSP MUSS es den Anwendern ermöglichen, das Monitoring wie in „Abb_006_Freigabeportal“ und „Tab_006_TUC_Monitoring“ dargestellt durchzuführen. ☒

☒ **gem_AFO_0103 Nutzung des Freigabeportals nur nach Authentisierung und entsprechend der Zugriffsrechte**

Der TSP MUSS sicherstellen, dass die Nutzung des Freigabeportals nur nach erfolgreicher Authentisierung und nur gemäß den Zugriffsrechten des eingeloggten Anwenders möglich ist. ☒

☒ **gem_AFO_0114 Anzeige von Daten entsprechend dem Anwender**

Ist der Anwender ein Kartenherausgeber, MUSS der TSP die Daten aller Antragsteller anzeigen, die zu dem eingeloggten Kartenherausgeber gehören. Ist der Anwender ein Mitarbeiter einer Spitzenorganisation eines Sektors, MUSS der TSP Überblicksansichten der Daten aller diesem Sektor zugehörigen Antragsteller eingeschränkt auf den Kartentyp, für den die Spitzenorganisation verantwortlich ist (HBA oder SMC-B), in pseudonymisierter Form anzeigen. Details sind in [gem_AFO_0117] beschrieben. ☒

☒ **gem_AFO_0115 Anzeige von Anträgen in einer Überblicksansicht im Freigabeportal**

In einer Überblicksansicht unter dem Menüpunkt „Anträge“ MUSS der TSP die Anträge in einer Tabelle darstellen, die aus den in „Tab_008_Anzeige_im_Freigabeportal“ genannten Tabellenspalten besteht. In einer Überblicksansicht unter dem Menüpunkt „Karten sperren“ MUSS der TSP sicherstellen, dass ausschließlich diejenigen Anträge angezeigt werden und zum Sperren auswählbar sind, die in einem sperrbaren Status sind. Jeder Antrag wird in einer Zeile dargestellt. Falls der TSP die Tabelle aufgrund ihrer Größe auf mehreren Seiten verteilt, MUSS er es ermöglichen, vor- und zurückzublättern. ☒

☒ **gem_AFO_0116 Sortieren von Anträgen in einer Übersichtsansicht im Freigabeportal**

Der TSP MUSS es dem Anwender ermöglichen, die Zeilen in Tabellen der Übersichtsansichten im Freigabeportal auf- bzw. absteigend zu sortieren. Die Sortierung MUSS für jede Spalte möglich sein, zum Beispiel indem der Anwender auf die Tabellenspaltenüberschriften oder darin enthaltene Aufwärts- und Abwärtspfeile klickt. ☒

☒ **gem_AFO_0100 Statusanzeige in der Übersichtsansicht im Freigabeportal**

In der Tabellenspalte „Status“ in den Übersichtsansichten im Freigabeportal MUSS der TSP die folgenden Statuswerte anzeigen können:

- Vom Antragsteller bearbeitet
- Eingang des Papierantrags
- Zur Freigabe
- Freigegeben
- Freigabe abgelehnt
- Antrag verworfen
- Versand PIN-Brief
- Auslieferung
- Karte ausgeliefert
- Karte unzustellbar zurück
- Zertifikate freigeschaltet
- Zertifikate endgültig nicht freigeschaltet
- Zertifikate abgelaufen
- Sperrantrag erhalten
- Zertifikate gesperrt .

Weiterhin MUSS der TSP Filter anbieten, um die Übersichtsansicht einzugrenzen. Der TSP MUSS mindestens eine Filterung nach dem Status der Anträge ermöglichen. Weiterhin MUSS der TSP die Anzeige aller Anträge (bei beliebigem Status) ermöglichen. ☒

☒ **gem_AFO_0118 Anzeige von Anträgen in einer Detailansicht im Freigabeportal**

In einer Detailansicht MUSS der TSP alle Daten eines ausgewählten Antrags darstellen, die angezeigt werden sollen und die nicht den Einschränkungen in [gem_AFO_0117] widersprechen. ☒

☒ **gem_AFO_0151 Anzeige von geänderten Vorbefüllungsdaten in einer Detailansicht im Freigabeportal**

Falls ein Antrag auf Basis von Vorbefüllungsdaten erstellt wurde, MUSS der TSP Änderungen gegenüber den Vorbefüllungsdaten in der Detailansicht markieren, indem er sie in einer anderen Farbe darstellt. ☒

☒ **gem_AFO_0152 Verknüpfung eines Antrags mit einer Anwendung im Freigabeportal**

Der TSP MUSS es ermöglichen, dass Antragsidentifikationsdaten (z. B. die Telematik-ID) bei der Anzeige im Freigabeportal als Link angezeigt werden, so dass beim Aufruf des Links der zugehörige Antrag mit einer vorher definierten Anwendung aufgerufen wird. Diese Funktion muss sektorspezifisch konfigurierbar sein. Dabei gelten die Einschränkungen in [gem_AFO_0117]. ☒

☒ **gem_AFO_0122 Aufruf einer Detailansicht über einen Link**

Der TSP MUSS es einem Anwender ermöglichen, durch Aufruf eines Links direkt die Detailansicht eines Antrags aufzurufen. Dabei gelten die Einschränkungen in [gem_AFO_0103] und [gem_AFO_0117]. Die in der Detailansicht dargestellten Daten sind in „Tab_008_Anzeige_im_Freigabeportal“ dargestellt. ☒

☒ **gem_AFO_0099 Funktion „Export Übersicht“ im Freigabeportal**

Der TSP MUSS im Freigabeportal die Funktion „Export Übersicht“ anbieten. Wenn die Funktion „Export Übersicht“ in der Überblicksansicht im Freigabeportal aufgerufen wird, MUSS der TSP die aktuell angezeigte Überblicksansicht als CSV-Datei zum Download anbieten, sofern höchstens eine konfigurierbare Anzahl von Einträgen in der Überblicksansicht vorhanden sind. Bei einer größeren Anzahl von Einträgen MUSS der TSP den Benutzer auffordern, die Anzahl über Suchkriterien zu beschränken. Der TSP MUSS bei Export von Informationen die Einschränkungen in [gem_AFO_0117] umsetzen. ☒

☒ **gem_AFO_0770 Funktion „Export Details“ im Freigabeportal**

Der TSP MUSS im Freigabeportal die Funktion „Export Details“ anbieten. Wenn die Funktion „Export Details“ in der Überblicksansicht im Freigabeportal aufgerufen wird, MUSS der TSP von allen angezeigten Anträgen alle Daten der Anträge, der Freigabesätze und der Kartenproduktion gemäß der definierten Übergabeschnittstellen [gemSpec_Pers_HBA] Card-G2-A_3137 und [gemSpec_Pers_SMC-B] Card-G2-A_3107 im XML-Format zum Download anbieten, sofern höchstens eine konfigurierbare Anzahl von Einträgen in der Überblicksansicht vorhanden sind. Bei einer größeren Anzahl von Einträgen MUSS der TSP den Benutzer auffordern, die Anzahl über Suchkriterien zu beschränken. Der TSP MUSS bei Export von Informationen die Einschränkungen in [gem_AFO_0117] umsetzen. ☒

☒ **gem_AFO_0780 Funktion „Download PDF mit Produktionsrückmeldungen“ im Freigabeportal**

Der TSP MUSS im Freigabeportal den Download einer PDF-Datei mit den Produktionsrückmeldungen eines Antrags anbieten. Wenn die Funktion „Produktionsstatus abfragen“ in der Detailansicht im Freigabeportal aufgerufen wird, MUSS der TSP die Produktionsrückmeldungen anzeigen und diese Daten als PDF Datei zum Download anbieten. Der TSP MUSS bei Export von Informationen die Einschränkungen in [gem_AFO_0117] umsetzen. ☒

☒ **gem_AFO_0117 Einschränkung der Funktionsaufrufe und Informationen im Freigabeportal**

Der TSP DARF NICHT Funktionsaufrufe anzeigen oder ermöglichen, oder Informationen anzeigen oder zum Export zur Verfügung stellen, wenn sie mindestens einer der folgenden Einschränkungen widersprechen:

- Abhängigkeit von den Zugriffsrechten des eingeloggten Anwenders:
 - o Die Übersichtsansicht darf mit Zugriffsrechten mindestens „Monitoring“ aufgerufen werden.
 - o Nach einem Suchbegriff darf man nur mit den Zugriffsrechten „Freigabe“ oder „Sperrung“ suchen. Nach einem Zeitraum oder einem Status darf auch mit nur „Monitoring“-Rechten gesucht werden.
 - o Die Verknüpfung eines Antrags mit einer Anwendung (siehe [gem_AFO_0152]) ist nur mit den Zugriffsrechten „Freigabe“ oder „Sperrung“ möglich.
 - o Weitere Einschränkungen sind in „Tab_008_Anzeige_im_Freigabeportal“ definiert.

Die Zugriffsrechte für „Monitoring“ sind eine Untermenge der Zugriffsrechte für „Freigabe“ und „Sperrung“, d. h., wer die Zugriffsrechte für „Freigabe“ oder „Sperrung“ hat, darf mindestens alles, was man mit „Monitoring“-Zugriffsrechten darf.

- Freigeben und Ablehnen ist nur für Anträge im Status „zur Freigabe“ möglich
- Bei der gleichzeitigen Sperrung mehrerer Karten sind die Regelungen in [gem_AFO_0172] zu beachten. Bezüglich der Sperrberechtigung von Kartenherausgebern, die nicht Ausgeber einer zu sperrenden Karte waren, gilt [gem_AFO_0168].
- Der TSP DARF bei der Freigabe NICHT Anträge anzeigen, die nicht zur Organisation des eingeloggten Anwenders gehören oder die der eingeloggte Anwender nicht sehen darf. ☒

Tabelle 11: Tab_008_Anzeige_im_Freigabeportal

Zugriffrechte des eingeloggten Anwenders	Spalten in Übersichtsansicht	Aktionen in Übersichtsansicht	Daten in Detailansicht	Aktionen in Detailansicht
Freigabe oder Sperrung	• Referenznummer des Antrags (eindeutig pro Antrag) • VorgangsNrAttrBS (falls vorhanden) *)	- Anzeige „Anträge“ • Anzeige Detailansicht • Export Übersichtsansicht • Export	• alle • Bei Praxisregister insbesondere Antragsnummer des Praxisregisters	• Ändern/ Ergänzen: direkt in Detailansicht und über „Ändern“-Aufruf*) • Freigeben*)

Spezifikation Kartenpersonalisierung HBA/SMC-B

Zugriffrechte des eingeloggten Anwenders	Spalten in Übersichtsansicht	Aktionen in Übersichtsansicht	Daten in Detailansicht	Aktionen in Detailansicht
	- VorgangsNrTSP^{*)} - Antragsdatum - Sektorspezifische ID^{*)} - Telematik ID^{*)} - Datum der letzten Bearbeitung, - Institutionsname (nur SMC-B)^{*)} - Nachname (nur HBA)^{*)} - Geburtsdatum (nur HBA)^{*)} - Status - Bei „Karte sperren“: „Auswahl zum Sperren“ in Form von Kontrollkästchen zum Ankreuzen^{*)}	Detailansicht (XML Format gemäß Übergabeschnittstelle)^{*)} - Anzeige „Karten sperren“ Auswahl zum Sperren^{*)} - Sperren^{*)}		- Ablehnen^{*)} - Export Produktionsrückmeldung (PDF) - Sperren^{*)}
nur Monitoring	- Referenznummer des Antrags (eindeutig pro Antrag) - VorgangsNrAttrBS (falls vorhanden)^{*)} - VorgangsNrTSP^{*)}	- Anzeige Detailansicht - Export Übersichtsansicht	- Kartenherausgeber - Antragstyp (Erstantrag/Austauschkarte)^{*)} - Anzahl Karten (bei SMC-B)	keine

Spezifikation Kartenpersonalisierung HBA/SMC-B

Zugriffrechte des eingeloggten Anwenders	Spalten in Überblicks-ansicht	Aktionen in Überblicks-ansicht	Daten in Detailansicht	Aktionen in Detailansicht
	- Antragsdatum - Datum der letzten Bearbeitung - Kartenherausgeber - Status		bzw. Kartentyp (HBA und/oder Ersatzausweis) ^{*)} - Berufsgruppe - Veröffentlichung Zertifikatsdaten (ja/nein)^{*)} - Neue Telematik-ID (ja/nein)^{*)} - keine Markierung von geänderten Vorbefüllungsdaten anzeigen	
nur Monitoring (optionale Funktion)	Statistik über Anzahl eingegangener Anträge, ausgelieferte Karten, freigeschaltete Karten	keine		

^{*)} Nicht bei Anträgen des Praxisregisters.

gem_AFO_0119 Anzeige von Anträgen eines ausgewählten Status im Freigabeportal

Der TSP MUSS dem Anwender ermöglichen, sich in der Überblicksansicht im Freigabeportal aus [gem_AFO_0115] nur Anträge anzeigen zu lassen, die einen bestimmten Status haben. Der TSP MUSS dem Anwender ein Auswahlfeld für die Auswahl des Status anbieten. Wenn der Anwender einen Status auswählt, MUSS der TSP in der Überblicksansicht genau die Anträge anzeigen, deren Status dem eingegebenen entspricht. Dabei MUSS der TSP die Einschränkungen in [gem_AFO_0117] beachten. Der TSP MUSS dem Anwender ermöglichen, sich in der Überblicksansicht im Freigabeportal alle Anträge, ohne Einschränkung des Status, anzeigen zu lassen. 

☒ **gem_AFO_0113 Anzeige von Anträgen eines ausgewählten Zeitraums im Freigabeportal**

Der TSP MUSS dem Anwender ermöglichen, sich in der Übersichtsansicht im Freigabeportal aus [gem_AFO_0115] nur Anträge eines ausgewählten Zeitraums anzeigen zu lassen. Der TSP MUSS dem Anwender Eingabefelder für Datumsangaben anbieten. Wenn der Anwender einen Zeitraum angibt, MUSS der TSP in der Übersichtsansicht genau die Anträge anzeigen, deren Antragsdatum in dem angegebenen Zeitraum liegt. Dabei MUSS der TSP die Einschränkungen in [gem_AFO_0117] beachten. Der TSP MUSS dem Anwender ermöglichen, sich in der Übersichtsansicht im Freigabeportal alle Anträge, ohne Einschränkung des Zeitraums, anzeigen zu lassen. ☒

☒ **gem_AFO_0121 Anzeige von Anträgen gemäß einem Suchbegriff im Freigabeportal**

Der TSP MUSS dem Anwender ermöglichen, sich in der Übersichtsansicht im Freigabeportal aus [gem_AFO_0115] nur Anträge anzeigen zu lassen, die einen eingegebenen Suchbegriff enthalten. Der TSP MUSS dem Anwender Eingabefelder für die Eingabe von Suchbegriffen anbieten. Wenn der Anwender einen Suchbegriff angibt, MUSS der TSP in der Übersichtsansicht genau die Anträge anzeigen, die diesen Suchbegriff enthalten. Dabei MUSS der TSP die Einschränkungen in [gem_AFO_0117] beachten. Der TSP MUSS dem Anwender ermöglichen, sich in der Übersichtsansicht im Freigabeportal alle Anträge, ohne Einschränkung auf einen Suchbegriff, anzeigen zu lassen. ☒

☒ **gem_AFO_0120 Gleichzeitiges Filtern nach Zeitraum, Status und Suchbegriff im Freigabeportal**

Der TSP MUSS dem Anwender ermöglichen, die Filterung nach Zeitraum gemäß [gem_AFO_0113], nach Status gemäß [gem_AFO_0119] und nach einem Suchbegriff gemäß [gem_AFO_0121] beliebig zu kombinieren. ☒

☒ **gem_AFO_0149 SOAP-Schnittstelle für Statusabfragen**

Der TSP MUSS dem Anwender die folgenden Funktionen über SOAP-Requests ermöglichen:

- Der Request enthält einen Status aus [gem_AFO_0100].

Die Response enthält die Daten aller Anträge, die in diesem Status sind in der Datenstruktur gemäß [gemSpec_Pers_HBA] bzw. [gemSpec_Pers_SMC-B], wobei nur die Daten enthalten sind, die gemäß [gem_AFO_0117] erlaubt sind. Wenn kein Antrag im angefragten Status vorhanden ist, enthält die Response die Information, dass kein solcher Antrag vorhanden ist.

- Der Request enthält eine Referenznummer.

Die Response enthält den Status des angefragten Antrags oder die Information, dass der Antrag nicht existiert. Der TSP MUSS alle Informationen übermitteln, die die angefragten Kriterien erfüllen. ☒

6.6.1.4 Artefakte

Zu Artefakten im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.6.1.5 Testunterstützung

Zur Unterstützung von Tests im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.6.1.6 Hardwaremerkmale

Das Funktionsmerkmal setzt keine besonderen Hardwaremerkmale voraus.

6.6.2 Benachrichtigungen

6.6.2.1 TUC-Beschreibung

Tabelle 12: Tab_601_TUC_Benachrichtigungen

Element	Beschreibung
Name	Benachrichtigungen
Beschreibung	Der TSP informiert die Kartenherausgeber und/oder Antragsteller bei bestimmten Ereignissen und Statusänderungen von Anträgen oder Zertifikaten.
Auslöser	Auslöser für das Versenden von Benachrichtigungen sind folgende Ereignisse: • Ein Antrag ist beim TSP eingegangen, wurde geprüft und steht zur Freigabe bereit. • Ein Antrag wurde abgelehnt. • Die Freigabe eines Antrags wurde abgelehnt. • Eine Karte wurde produziert. • Eine Karte wurde ausgeliefert. • Eine Karte wurde als unzustellbar an den TSP zurückgesendet. • Die Zertifikate einer Karte wurden freigeschaltet. • Die Zertifikate einer Karte wurden endgültig nicht freigeschaltet. • Die Zertifikate einer Karte laufen in Kürze ab. • Die Zertifikate einer Karte wurden gesperrt.
Vorbedingungen	Der Kartenherausgeber hat dem TSP eine oder mehrere E-Mail-

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	Adressen für den Empfang der E-Mails benannt.
Eingangsdaten	Referenznummern und Status der Anträge bzw. Zertifikate.
Komponenten	Kartenpersonalisierung.
Ausgangsdaten	E-Mail-Benachrichtigungen an den Kartenherausgeber und/oder Antragsteller.
Nachbedingungen	Keine.
Standardablauf	Siehe Abbildung 15 „Abb_601_Benachrichtigungen“.
Varianten/Alternativen	Je nach Ereignis werden die Kartenherausgeber und/oder Antragsteller benachrichtigt, d.h. es gehen nicht alle Benachrichtigungs-Mails parallel an beide Empfänger
Fehlerfälle	Keine.
Nichtfunktionale Anforderungen	Keine.
Zugehörige Diagramme	Siehe Abbildung 15 „Abb_601_Benachrichtigungen“.

6.6.2.2 Ablauf

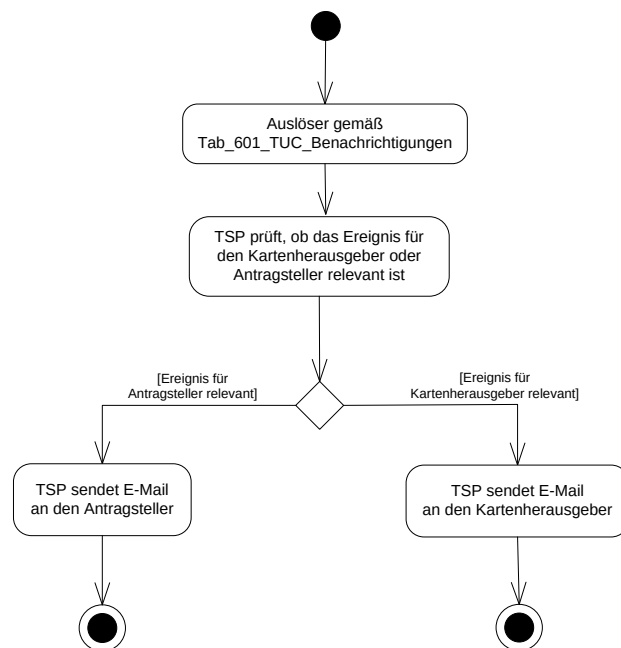


Abbildung 15: Abb_601_Benachrichtigungen

6.6.2.3 Anforderungen

☒ **gem_AFO_0609 Benachrichtigung der Kartenherausgeber**

Der TSP MUSS den betroffenen Kartenherausgeber bei folgenden Ereignissen per E-Mail über die Statusänderung eines Antrags bzw. der Zertifikate informieren:

- Ein Antrag ist beim TSP eingegangen, wurde geprüft und steht zur Freigabe bereit.
- Die Freigabe eines Antrags wurde abgelehnt.
- Ein Antrag auf einen Austauschausweis wurde vom TSP im Auftrag des Kartenherausgebers freigegeben.
- Eine Karte wurde produziert.
- Eine Karte wurde ausgeliefert.
- Eine Karte wurde als unzustellbar an den TSP zurückgesendet.
- Die Zertifikate einer Karte wurden freigeschaltet
- Die Zertifikate einer Karte wurden endgültig nicht freigeschaltet.
- Die Zertifikate einer Karte laufen in Kürze ab.
- Die Zertifikate einer Karte wurden gesperrt.

Die Benachrichtigungsmail MUSS dabei mindestens die Referenznummer und die Vorgangsnummer des Antrags (falls vorhanden: VorgangsNrAttrBS, sonst VorgangsNrTSP) und den aktuellen Status (nach Statusänderung) beinhalten. Es MUSS ein Link aufgeführt sein, so dass der Mitarbeiter des Kartenherausgebers durch Anklicken des Links in der Benachrichtigungsmail automatisch auf die Detailansicht des Antrags im Freigabeportal weitergeleitet wird (vor der Anzeige der Detailansicht ist eine Authentisierung des Kartenherausgebers erforderlich). Darüber hinaus MUSS durch den Kartenherausgeber festgelegt werden, ob die Benachrichtigungsmails abhängig vom Ereignis auch weitere Informationen enthalten, insbesondere bei Produktion einer Karte (Produktionsrückmeldung). In diesem Fall MUSS der TSP alle durch den Kartenherausgeber festgelegten Produktionsdaten in die E-Mails aufnehmen und diese verschlüsseln (siehe [gem_AFO_0611]). ☒

☒ **gem_AFO_0610 Benachrichtigung der Antragsteller**

Der TSP MUSS den Antragsteller bei folgenden Ereignissen per E-Mail über die Statusänderung eines Antrags bzw. der Zertifikate informieren:

- Ein Antrag wurde abgelehnt.
- Die Freigabe eines Antrags wurde abgelehnt.
- Eine Karte wurde produziert.
- Die Zertifikate einer Karte wurden freigeschaltet
- Die Zertifikate einer Karte wurden endgültig nicht freigeschaltet.
- Die Zertifikate einer Karte laufen in Kürze ab.

- Die Zertifikate einer Karte wurden gesperrt.

Die Benachrichtigungsmail MUSS dabei mindestens die Referenznummer des Antrags und den aktuellen Status (nach Statusänderung) beinhalten. Darüber hinaus MÜSSEN in der Benachrichtigungsmail (in Abhängigkeit von der jeweiligen Statusänderung) die daraus für den Antragsteller resultierenden Aktivitäten und Hinweise zu den Ansprechpartnern bei Rückfragen enthalten sein. ☒

☒ **gem_AFO_0611 Verschlüsselung und Signatur der Benachrichtigungsmails**

Unabhängig vom Inhalt MÜSSEN die vom TSP an den Kartenherausgeber oder Antragsteller versendeten E-Mails gemäß [gem_AFO_0023] immer signiert sein. Darüber hinaus MÜSSEN die Mails an die Kartenherausgeber verschlüsselt werden, wenn in den Benachrichtigungsmails detaillierte Angaben zu Anträgen bzw. Karten (Produktionsrückmeldungen) gemacht werden (siehe [gem_AFO_0609]). Dazu MÜSSEN die Kartenherausgeber dem TSP im Rahmen der Registrierung zur Mailverschlüsselung nutzbare S/MIME-Zertifikate übergeben haben. ☒

6.7 Auftrag, Freischaltung und Sperrung über Praxisregister

Das Praxisregister ist ein System zur Verwaltung von SMC-B-Anträgen und –Karten. Es ist als zentrale mandantenfähige Webapplikation realisiert, und bietet eine Web-Service-Schnittstelle zur Kommunikation mit dem TSP. Das Praxisregister stellt dem TSP Aufträge zur Produktion, Freischaltung (hier „Aktivierung“ genannt) und Sperrung von SMC-B-Karten durch den Kartenherausgeber zur Verfügung. Die sogenannte TSP-Praxisregisterapplikation bedient auf Seiten des TSP den Web-Service des Praxisregisters.

Die Beschreibung der Kommunikationsprozesse und Datenstrukturen im Zusammenhang mit dem Praxisregister ist in den Dokumenten [KBV_Benutzerhandbuch Webservice], [KV-T_Praxisregister_Webservice] und [KV-T_ISMS_SMC-B_Ausgabekonzept] enthalten.

Die TSP-Praxisregisterapplikation muss aktiv und regelmäßig im Praxisregister nach Kartenaufträgen, Aktivierungsaufträgen und Sperraufträgen pollen. Diese sind bereits vor Einstellung in das Praxisregister vom Kartenherausgeber geprüft. Der TSP hat keine direkte Schnittstelle zum Antragsteller, die Antragstellung und Freigabe erfolgt beim Kartenherausgeber. Der TSP erledigt den Versand der Karten per PostIdent und zeitversetzt den Versand der PIN/PUK-Briefe im Namen und unter Angabe des Kartenherausgebers als Absender. Der Kartenherausgeber erhält den Status der Kartenübergabe aus dem PostIdent-Verfahren.

Im Folgenden wird zur Vereinfachung der Beschreibungen das Praxisregister zusammen mit der Web-Service-Schnittstelle auf Seiten des Praxisregisters als „Praxisregister“ bezeichnet. Des Weiteren wird zur Vereinfachung der Beschreibung die TSP-Praxisregisterapplikation zusammen mit den nachgelagerten Funktionalitäten als „TSP“ bezeichnet.

Die ausgetauschten Daten werden im Folgenden nicht im Detail und in aller Vollständigkeit beschrieben, sondern nur insoweit sie für das Verständnis des Ablaufs und der Definition der Anforderungen notwendig sind.

6.7.1 TUC-Beschreibung

Tabelle 13: Tab_500_TUC_Praxisregister

Element	Beschreibung
Name	Auftrag, Freischaltung und Sperrung über Praxisregister
Beschreibung	• [PR-1]: TSP fragt nach Aufträgen zur Produktion und Lieferung von SMC-B-Karten beim Praxisregister und erhält eine Liste mit keinem, einem oder mehreren Aufträgen als Antwort. • [PR-2]: TSP übersendet bei Vorliegen eines Fehlerfalls bei der Verarbeitung eines Produktionsauftrags eine Fehlermeldung an das Praxisregister. • [PR-3]: TSP registriert eine oder mehrere produzierte und

Element	Beschreibung
	versendete SMC-B-Karten beim Praxisregister. Es stehen zwei getrennte Funktionen im Web-Service zur Verfügung, um entweder eine Karte oder mehrere Karten zu registrieren. Diese Funktionen werden in der weiteren Beschreibung zur Vereinfachung nicht unterschieden. • [PR-4]: TSP fragt nach Aufträgen zur Aktivierung der Zertifikate von SMC-B-Karten beim Praxisregister und erhält eine Liste mit keinem, einem oder mehreren Aufträgen als Antwort. • [PR-5]: TSP fragt nach Aufträgen zur Sperrung der Zertifikate von SMC-B-Karten beim Praxisregister und erhält eine Liste mit keinem, einem oder mehreren Aufträgen als Antwort. Falls Aufträge im Praxisregister vorliegen und an den TSP gesendet wurden, führt der TSP die jeweiligen Operationen aus.
Auslöser	Der TSP fragt für jede der Auftragsarten [PR-1], [PR-4] und [PR-5] periodisch nach Aufträgen im Praxisregister. Die Frequenz der Anfragen ist konfigurierbar. Tritt bei der Bearbeitung eines Produktionsauftrags ein Fehler ein, löst dies [PR-2] aus. Wurden eine oder mehrere SMC-B-Karten produziert und versendet sowie zeitversetzt die PIN-/PUK-Briefe versendet, löst dies [PR-3] aus. Es liegt in der Verantwortung des TSP, ob er jede produzierte Karte einzeln registriert, oder das Bulk-Verfahren zur Registrierung mehrerer Karten in einem Schritt benutzt.
Vorbedingungen	Eine TLS-Verbindung wurde vom TSP gemäß [gem_AFO_0502], [gem_AFO_0503] und [gem_AFO_0504] aufgebaut. • [PR-1]: - o Praxisregister und TSP haben sich gegenseitig authentisiert. • [PR-2]: - o Praxisregister und TSP haben sich gegenseitig authentisiert. - o Ein Fehlerfall bei der Verarbeitung eines Produktionsauftrags liegt vor. • [PR-3]: - o Praxisregister und TSP haben sich gegenseitig authentisiert.

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	- o Eine oder mehrere SMC-B-Karten wurden produziert und versendet sowie zeitversetzt die PIN-/PUK-Briefe versendet. • [PR-4]: - o Praxisregister und TSP haben sich gegenseitig authentisiert. - o Kartennummer(n) der Karte(n) der zu aktivieren den Zertifikate sind beim Praxisregister bekannt ([PR-3] muss vorher erfolgt sein). • [PR-5]: - o Praxisregister und TSP haben sich gegenseitig authentisiert. - o Kartennummer(n) der Karte(n) der zu sperrenden Zertifikate sind beim Praxisregister bekannt ([PR-3] muss vorher erfolgt sein). - o Die zu sperrenden Zertifikate befinden sich in einem sperrbaren Status.
Eingangsdaten	• [PR-1]: TSP sendet eindeutige Kennung der Nachricht. • [PR-2]: TSP sendet eindeutige Kennung der Nachricht sowie Antragsnummer und Fehlerbeschreibung. • [PR-3]: TSP sendet eindeutige Kennung der Nachricht sowie Informationen zur erzeugten SMC-B (z.B. Kartennummer, Informationen zum Auftrag). • [PR-4]: TSP sendet eindeutige Kennung der Nachricht. • [PR-5]: TSP sendet eindeutige Kennung der Nachricht.
Komponenten	Kartenpersonalisierung.
Ausgangsdaten	• [PR-1]: Praxisregister antwortet mit eindeutiger Kennung der Anfrage, auf die geantwortet wird, sowie Auftragsdaten zur Produktion keiner, einer oder mehrerer SMC-B. • [PR-2]: Praxisregister antwortet mit eindeutiger Kennung der Anfrage, auf die geantwortet wird. • [PR-3]: Praxisregister antwortet mit eindeutiger Kennung der Anfrage, auf die geantwortet wird. • [PR-4]: Praxisregister antwortet mit eindeutiger Kennung der Anfrage, auf die geantwortet wird, sowie einer Liste von keiner, einer oder mehreren Kartennummern, die frei-

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	zuschalten sind. [PR-5]: Praxisregister antwortet mit eindeutiger Kennung der Anfrage, auf die geantwortet wird, sowie einer Liste von keiner, einer oder mehreren Kartennummern, die zu sperren sind.
Nachbedingungen	[PR-1]: Beauftragte SMC-B-Karten sind produziert und versendet. [PR-2]: Beauftragte SMC-B sind nicht produziert. [PR-3]: Produzierte und versendete SMC-B sind im Praxisregister registriert. [PR-4]: Anhand ihrer Kartenummer identifizierte SMC-B sind freigeschaltet. [PR-5]: Anhand ihrer Kartenummer identifizierte SMC-B sind gesperrt.
Standardablauf	Siehe [gem_AFO_0500] und Abbildung 16 „Abb_501_Abholung_von_Produktionsaufträgen“, Abbildung 17 „Abb_502_Abholung_von_Aktivierungsaufträgen“, Abbildung 18 „Abb_503_Abholung_von_Sperraufträgen“.
Varianten/Alternativen	Keine.
Fehlerfälle	[PR-4]: - Die empfangenen Kartennummern gehören nicht zu SMC-B-Karten im Verantwortungsbereich des Kartenherausgebers. - Die SMC-Bs sind nicht im Status „Versand PIN-Brief“. [PR-5]: - Die empfangenen Kartennummern gehören nicht zu SMC-B-Karten im Verantwortungsbereich des Kartenherausgebers. - Die SMC-B-Karten sind nicht in einem sperrbaren Status. Alle: - Wenn der Kartenherausgeber die geforderten TLS-Versionen oder Ciphersuites nicht unterstützt, lässt der TSP keine Übertragung zu. - Wenn die Authentisierung des Praxisregisters fehlschlägt, lässt der TSP keine Übertragung zu.

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element		Beschreibung
		Die empfangene Datenstruktur ist fehlerhaft und kann nicht verarbeitet werden.
Nichtfunktionale Anforderungen	An-	Keine
Zugehörige Diagramme	Dia-	Abbildung 16 „Abb_501_Abholung_von_Produktionsaufträgen“, Abbildung 17 „Abb_502_Abholung_von_Aktivierungsaufträgen“, Abbildung 18 „Abb_503_Abholung_von_Sperraufträgen“

6.7.2 Ablauf

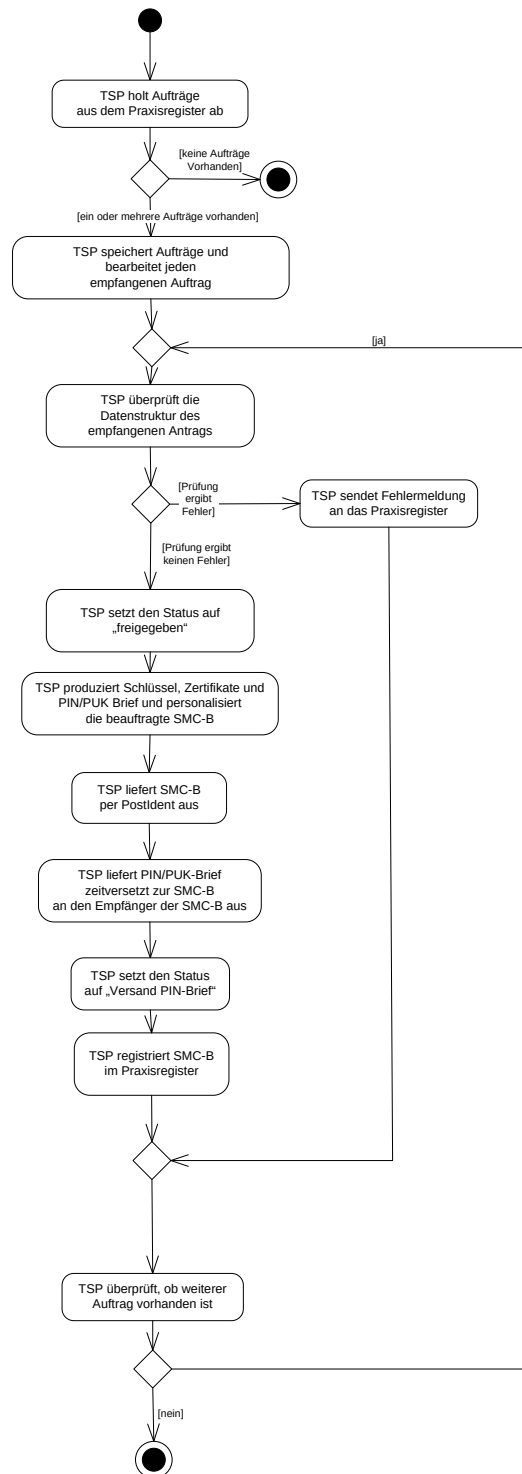


Abbildung 16: Abb_501_Abfrage_von_Produktionsaufträgen

Anmerkung zu Abbildung 16: Die Registrierung der SMC-B-Karten im Praxisregister kann auch im Bulk-Verfahren für alle Karten aus dem Antrag erfolgen.

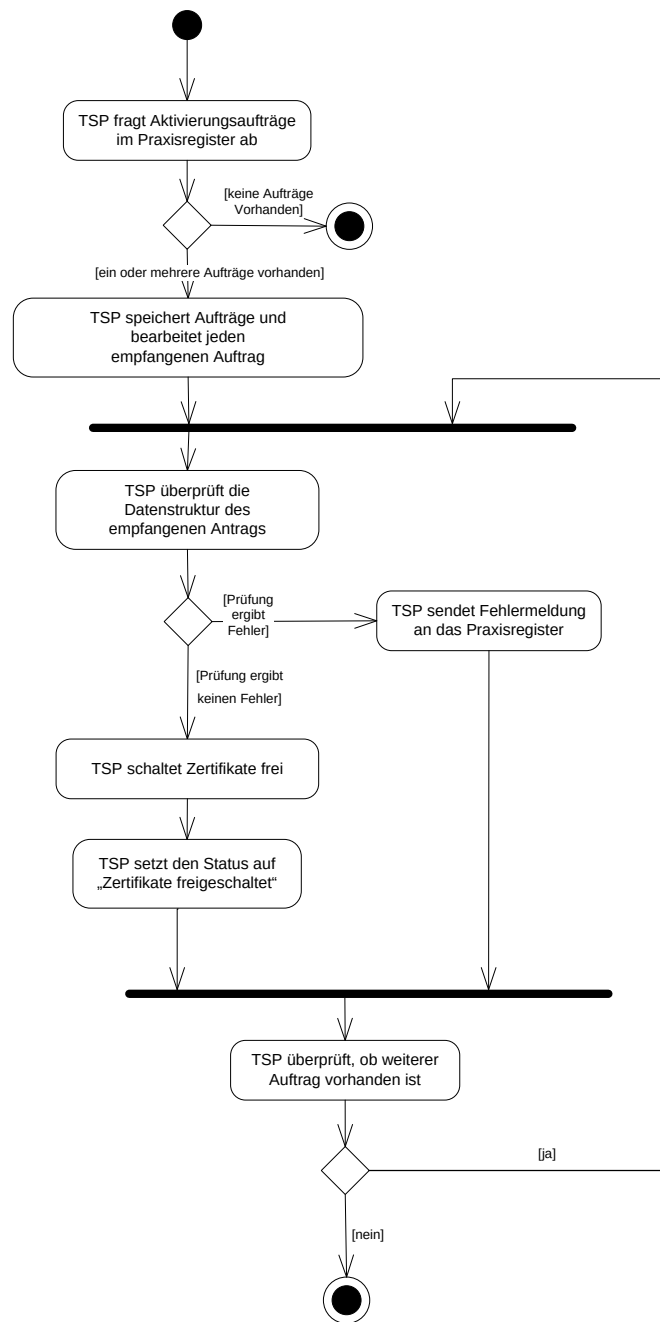


Abbildung 17: Abb_502_Abfrage_von_Aktivierungsaufträgen

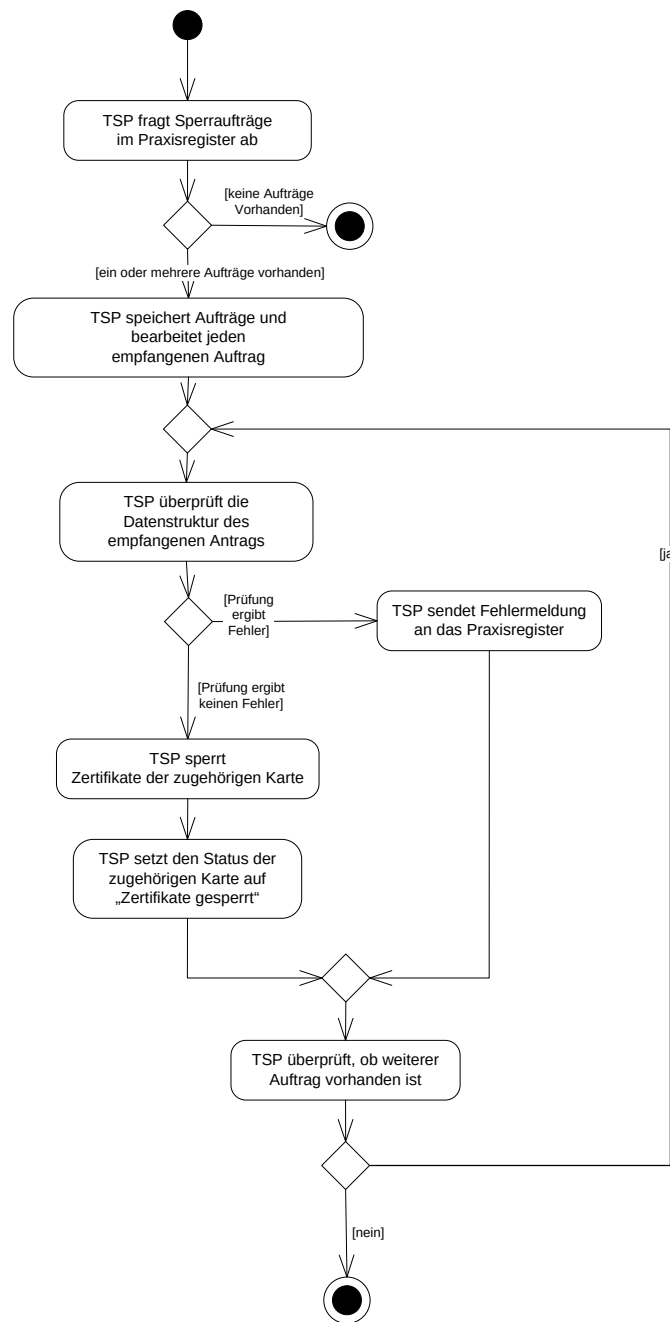


Abbildung 18: Abb_503_Abfrage_von_Sperraufträgen

6.7.3 Anforderungen

☒ gem_AFO_0500 Ablauf der Prozesse zwischen TSP und Praxisregister

Der TSP MUSS die Kommunikation mit dem Praxisregister und die nachgelagerten Prozesse gemäß der Vorgaben von [KBV_Benutzerhandbuch Webservice], [KV-T_Praxisregister_Webservice] und [KV-T_ISMS_SMC-B_Ausgabekonzept] realisieren und wie in „Tab_500_TUC_Praxisregister“, „Abb_501_Abfrage_von_Produktionsaufträgen“,

„Abb_502_Abfrage_von_Aktivierungsaufträgen“ und
„Abb_503_Abfrage_von_Sperraufträgen“ dargestellt durchführen. ☒

☒ **gem_AFO_0501 Bereitstellung eines Web-Service-Clients zur Kommunikation mit dem Praxisregister**

Der TSP MUSS einen Web-Service-Client bereitstellen, der die für die Rolle „SMC_ISSUER“ definierten Web-Services aus [KV-T_Praxisregister_Webservice] und [KBV_Benutzerhandbuch Webservice] Kapitel 3.3 realisiert. ☒

☒ **gem_AFO_0502 Absicherung der Kommunikationsverbindung mit dem Praxisregister**

Der TSP MUSS bei jeder Nutzung eines Web-Service eine TLS-Verbindung zum Praxisregister mit serverseitiger Authentisierung und clientseitiger HTTP-Basic-Authentication aufbauen. Der TSP MUSS die sicherheitstechnischen Anforderungen gemäß [KBV_Benutzerhandbuch Webservice] Kapitel 4 implementieren. ☒

☒ **gem_AFO_0503 Prüfung des TLS-Server-Zertifikats des Praxisregisters**

Der TSP MUSS das Serverzertifikat, mit dem sich das Praxisregister in der TLS-Verbindung authentisiert, auf Übereinstimmung mit dem beim TSP hinterlegten Zertifikat sowie auf seine Gültigkeit prüfen (z. B. durch eine OCSP-Abfrage). Das vom Praxisregister verwendet Serverzertifikat MUSS auf Anforderung des Praxisregisters änderbar sein. ☒

☒ **gem_AFO_0504 HTTP-Basic-Authentication des TSP gegenüber dem Praxisregister**

Der TSP MUSS in der HTTP-Basic-Authentication UserID und Passwort verwenden, die ihm vom Praxisregister vor Inbetriebnahme der Schnittstelle zugewiesen wurde. UserID und Passwort MÜSSEN auf Anforderung des Praxisregisters änderbar sein. ☒

☒ **gem_AFO_0505 Absicherung des Datenaustauschs des TSP mit dem Praxisregister mittels Web Service Security (WSS)**

Der TSP MUSS Nachrichten an das Praxisregister gemäß der Vorgaben in [KBV_Benutzerhandbuch Webservice] Kapitel 4 mittels WSS absichern, so dass alle Nachrichten signiert und verschlüsselt sind. ☒

☒ **gem_AFO_0506 Absicherung des Datenaustauschs des Praxisregisters mit dem TSP mittels Web Service Security (WSS)**

Das Praxisregister MUSS Nachrichten an den TSP gemäß der Vorgaben in [KBV_Benutzerhandbuch Webservice] Kapitel 4 mittels WSS absichern, so dass alle Nachrichten signiert und verschlüsselt sind. ☒

☒ **gem_AFO_0507 Verschlüsselungszertifikat des Praxisregisters zur WSS-Verschlüsselung im Web-Service des Praxisregisters**

Der TSP MUSS zur WSS-Verschlüsselung ein X.509-Zertifikat verwenden, das ihm vom Betreiber des Praxisregisters vor Inbetriebnahme der Schnittstelle mitgeteilt wurde. Das Verschlüsselungszertifikat MUSS auf Anforderung des Praxisregisters änderbar sein. ☒

☒ gem_AFO_0508 Verschlüsselungszertifikat des TSP zur WSS-Verschlüsselung im Web-Service des Praxisregisters

Das Praxisregister MUSS zur WSS-Verschlüsselung ein X.509-Zertifikat verwenden, das ihm vom TSP vor Inbetriebnahme der Schnittstelle mitgeteilt wurde. Dieses Verschlüsselungszertifikat MUSS auf Anforderung des TSP änderbar sein. ☒

☒ gem_AFO_0509 Signaturzertifikat des TSP zur WSS-Signatur im Web-Service des Praxisregisters

Der TSP MUSS zur WSS-Signatur ein X.509-Zertifikat verwenden, das er dem Betreiber des Praxisregisters vor Inbetriebnahme der Schnittstelle mitgeteilt hat. Der TSP KANN sein Signaturzertifikat ändern. In einer angemessenen Zeitspanne vor Nutzung eines neuen Signaturzertifikats MUSS dieses dem Betreiber des Praxisregisters mitgeteilt werden. ☒

☒ gem_AFO_0510 Signaturzertifikat des Praxisregisters zur WSS-Signatur im Web-Service des Praxisregisters

Das Praxisregister MUSS zur WSS-Signatur ein X.509-Zertifikat verwenden, das dem TSP vor Inbetriebnahme der Schnittstelle mitgeteilt wird. Das Praxisregister KANN sein Signaturzertifikat ändern. In einer angemessenen Zeitspanne vor Nutzung eines neuen Signaturzertifikats MUSS dieses dem TSP mitgeteilt werden. ☒

☒ gem_AFO_0511 Prüfung und Speicherung signierter Nachrichten des Praxisregisters

Der TSP MUSS alle vom Praxisregister empfangenen signierten Nachrichten speichern, die Auftragsdaten enthalten. Der TSP MUSS für alle empfangenen Nachrichten die Signatur mathematisch prüfen, und das verwendete Signaturzertifikat auf Gültigkeit prüfen. Der TSP MUSS prüfen, dass das verwendete Signaturzertifikat mit dem bei ihm hinterlegten übereinstimmt. ☒

☒ gem_AFO_0512 Regelmäßige Anfragen des TSP an das Praxisregister

Der TSP MUSS regelmäßig in konfigurierbaren Abständen Anfragen gemäß [PR-1], [PR-4] und [PR-5] an das Praxisregister stellen. ☒

☒ gem_AFO_0513 Versendung einer Fehlermeldung an das Praxisregister

Der TSP MUSS eine Nachricht gemäß [PR-2] an das Praxisregister senden, wenn bei der Bearbeitung eines Produktionsauftrags aus [PR-1] ein Fehler aufgetreten ist. ☒

☒ gem_AFO_0514 Produktion und Versand von SMC-B-Karten unter Nutzung des Praxisregisters

Der TSP MUSS (falls kein Fehler aus [PR-1] vorliegt) die SMC-B gemäß der Daten aus [PR-1] produzieren und per PostIdent an den übermittelten Empfänger versenden. Der TSP MUSS die PIN/PUK-Briefe zeitversetzt dazu an den übermittelten Empfänger versenden. Der TSP MUSS die übermittelte Adresse des Kartenherausgebers als Absenderadresse verwenden. Der TSP MUSS den Status auf „Versand PIN-Brief“ setzen. ☒

☒ gem_AFO_0515 Produktionsrückmeldungen an das Praxisregister

Spezifikation Kartenpersonalisierung HBA/SMC-B

Der TSP MUSS eine Nachricht gemäß [PR-3] an das Praxisregister senden, wenn eine SMC-B-Karte erfolgreich produziert und versendet wurde. 

gem_AFO_0730 Mehrere Produktionsrückmeldungen an das Praxisregister in einer Nachricht

Der TSP KANN die Produktionsrückmeldungen zu mehreren SMC-B in einer Nachricht versenden. 

gem_AFO_0516 Aktivierung von SMC-B-Karten unter Nutzung des Praxisregisters

Der TSP MUSS im Fall von [PR-4] prüfen, ob die zu aktivierenden Karten in der Verantwortung des Kartenherausgebers liegen und sich im Zustand „Versand PIN-Brief“ befinden, bevor die Aktivierung (entspricht der Freischaltung) durchgeführt wird. Nach der Freischaltung MUSS der TSP den Status auf „freigegeben“ setzen. 

gem_AFO_0517 Sperrung von SMC-B-Karten unter Nutzung des Praxisregisters

Der TSP MUSS im Fall von [PR-5] prüfen, ob die zu sperrenden Karten in der Verantwortung des Kartenherausgebers liegen und sich in einem sperrbaren Status befinden, bevor die Sperrung durchgeführt wird. Nach der Sperrung MUSS der TSP den Status auf „Zertifikate gesperrt“ setzen. 

6.7.4 Artefakte

Zu Artefakten im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.7.5 Testunterstützung

Zur Unterstützung von Tests im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.7.6 Hardwaremerkmale

Das Funktionsmerkmal setzt keine besonderen Hardwaremerkmale voraus.

6.8 Beantragung, Personalisierung und Lieferung von Verifikationskarten

Die Beantragung, Personalisierung und Lieferung von Verifikationskarten läuft anders ab als bei HBA und SMC-B, es wird daher in diesem Kapitel auf die Besonderheiten eingegangen.

Die Beantragung von Verifikationskarten läuft wie folgt ab:

1. Beantragung von Verifikationskarten durch den GKV-SV als Kartenherausgeber

Ein berechtigter und registrierter Mitarbeiter des GKV-SV, der „Beauftragte Verifikationskarte Kartenherausgeber“ (BVK, siehe Kap. 6.8.3) beantragt die Verifikationskarten für die gesetzlichen Krankenkassen beim TSP per Fax.

2. Prüfung des Antrags durch den TSP

Der TSP prüft den Absender sowie die Berechtigung des BVK zur Beantragung von Verifikationskarten gegen die registrierten Berechtigungen und die Unterschriftsprobe des BVK (siehe Kap. 6.8.3). Bei erfolgreicher Prüfung wird der Antrag ausgedruckt und zur Kartenproduktion übergeben.

3. Kartenpersonalisierung und Auslieferung von Verifikationskarten

Der TSP gibt die Antragsdaten in das System ein und stößt die Produktion der Karten an. Nach der Produktion werden die Verifikationskarten sowie die zugehörigen PIN/PUK-Briefe getrennt und zeitlich versetzt an den BVK via Einschreiben mit Rückschein (oder vergleichbarem Verfahren wie z.B. PostIdent oder persönliche Übergabe mit Empfangsbestätigung) gesendet.

6.8.1 TUC-Beschreibung

Tabelle 14: Tab_602_TUC_Ausgabe_Verifikationskarten

Element	Beschreibung
Name	Ausgabe Verifikationskarten
Beschreibung	Der Prozess beschreibt die Beantragung, Personalisierung und Lieferung von Verifikationskarten.
Auslöser	Der BVK als Beauftragter des GKV-Spitzenverbandes als Kartenherausgeber beantragt für die gesetzlichen Krankenkassen Verifikationskarten.
Vorbedingungen	Die Beauftragten Verifikationskarte Kartenherausgeber (BVK) sind registriert.
Eingangsdaten	Anträge des BVK
Komponenten	Kartenpersonalisierung
Ausgangsdaten	Verifikationskarten sowie zugehörige PIN- und PUK-Briefe
Nachbedingungen	Karte und PIN-Brief sind BVK zugestellt (Nachweis durch Rück-scheine oder Vergleichbares).
Standardablauf	Siehe Abbildung 19 „Abb_602_Beantragung_und_Ausgabe_von_Verifikationskarten“ Die Beantragung durch den BVK erfolgt per Fax anhand des An-tragsformulars von T-Systems (wird vorab mit dem GKV-SV ab-gestimmt).
Varianten/Alternativen	
Fehlerfälle	• Antragsteller ist nicht berechtigt • Unterschrift auf dem Fax des BVK fehlt oder stimmt nicht mit der registrierten Unterschriftenprobe überein • Karte und/oder PIN-Brief an BVK ist nicht zustellbar
Nichtfunktionale An-forderungen	Keine.
Zugehörige Dia-gramme	Abbildung 19 „Abb_602_Beantragung_und_Ausgabe_von_Verifikationskarten“

6.8.2 Ablauf

Der Ablauf ergibt sich aus der folgenden Abbildung:

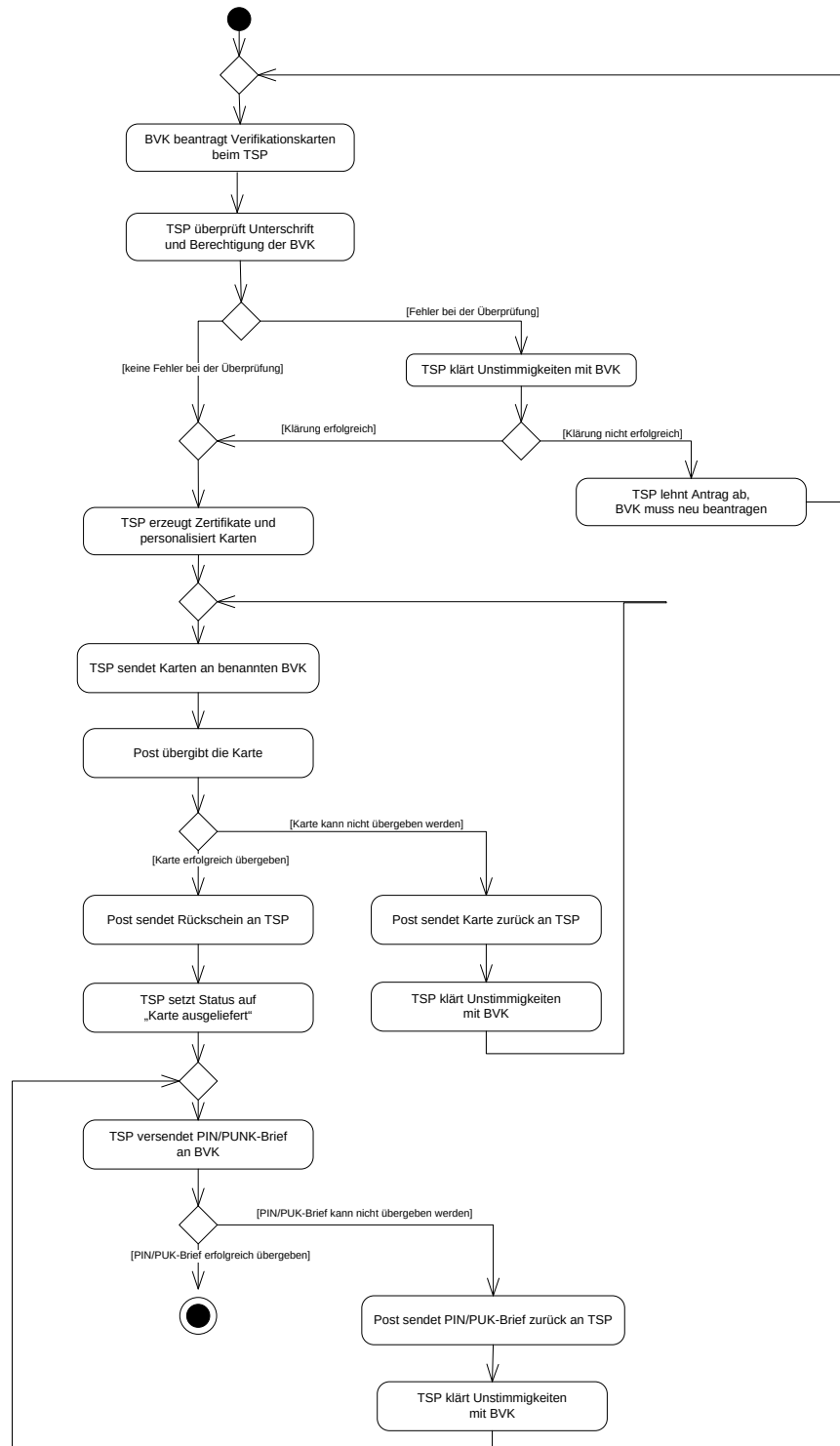


Abbildung 19: Abb_602_Beantragung_und_Ausgabe_von_Verifikationskarten

6.8.3 Registrierung der BVK

Die zur Beantragung berechtigten BVK müssen einmalig vor der Beantragung von Verifikationskarten registriert werden. Die Registrierung läuft wie folgt ab:

Der GKV-SV benennt einen oder mehrere BVK schriftlich gegenüber dem TSP (Adresse wird dem GKV-SV vorab mitgeteilt). Das Schreiben enthält alle relevanten Informationen, die der TSP zur Registrierung der BVKs benötigt:

- Identifizierungsdaten der BVKs: Name, Vorname,
- Unterschriftsprobe jedes BVKs
- Kontaktdaten der BVKs: Telefon, E-Mail-Adresse, Fax-Nr.

Hinweise zu den Kontaktdaten:

- Die Fax-Nr. wird immer benötigt. Sie dient zum einen der Prüfung des Absenders bei der Übermittlung der Anträge per Fax und zum anderen optional auch zur Übermittlung von Informationen vom TSP an den BVK über den Versand der Karten oder PIN/PUK-Briefe.

Der TSP speichert die erhaltenen Registrierungsinformationen und hält sie in seinem System vor. Bzgl. der Aufbewahrungs- und Löschrufen gelten analog zu den Accounts der Mitarbeiter der Kartenherausgeber HBA und SMC-B die Anforderungen an die Mitarbeiterdaten gem_AFO_0608 und gem_AFO_0622.

Wenn sich bei den BVK Änderungen bei den Identifizierungs- oder Kontaktdaten ergeben oder weitere BVK hinzukommen oder BVK wegfallen, erfolgt die Meldung dazu analog vom GKV-SV an den TSP über den oben beschriebenen Weg.

6.8.4 Anforderungen

☒ **gem_AFO_0612 Ablauf des Prozesses wie in Beschreibung**

Der TSP MUSS es dem BVK ermöglichen, den Prozess wie in „Abb_602_Beantragung_und_Ausgabe_von_Verifikationskarten“ und „Tab_602_TUC_Ausgabe_Verifikationskarten“ dargestellt durchzuführen. ☒

☒ **gem_AFO_0613 Registrierung des BVK**

Der TSP MUSS den BVK wie in Kap. 6.8.3 „Registrierung der BVK“ beschrieben registrieren. Der GKV-SV MUSS dem TSP bei der Benennung der BVK deren Identifizierungs- und Kontaktdaten sowie entweder eine Unterschriftenprobe für die Beantragung per Fax übergeben. Das Anschreiben des GKV-SV an den TSP MUSS mit einem Stempel des GKV-SV versehen und von einem Zeichnungsberechtigtem unterzeichnet sein. ☒

☒ **gem_AFO_0614 Bereitstellung des Antragsformulars**

Der TSP MUSS dem Kartenherausgeber eine Vorlage für das Antragsformular als PDF zur Verfügung stellen. Das Antragsformular muss über entsprechende Formularfelder im PDF-Dokument elektronisch ausfüllbar sein. ☒

☒ **gem_AFO_0615 Bereitstellung von Informationen**

Der Kartenherausgeber MUSS dem TSP den Empfänger im Antrag benennen. ☒

☒ **gem_AFO_0616 Beantragung der Karten**

Der BVK KANN die Kartenanträge durch unterschriebenen Antrag per Fax in mehreren Chargen übermitteln. ☒

☒ **gem_AFO_0617 Prüfung des Antrags**

Der TSP MUSS vor Produktion der Karten den Antrag des BVK prüfen. Dazu zählt neben der Prüfung der formalen Korrektheit und Vollständigkeit des Antrags insbesondere die Prüfung des Absenders und dessen Berechtigung. Zur Prüfung des Absenders MUSS die im Rahmen der Registrierung übergebene Unterschriftsprobe geprüft werden. ☒

☒ **gem_AFO_0618 Versand der Karten**

Der TSP MUSS die Karten an den BVK mindestens per Einschreiben mit den Optionen „Eigenhändig“ und „Rückschein“ oder alternativ mit vergleichbaren oder höherwertigen Verfahren, z. B. PostIdent Spezial, versenden oder eigenhändig übergeben. ☒

☒ **gem_AFO_0619 Versand der PIN-Briefe**

Der TSP MUSS die PIN-Briefe an die benannten BVK mindestens per Einschreiben mit den Optionen „Eigenhändig“ und „Rückschein“ oder alternativ mit vergleichbaren oder höherwertigen Verfahren, z. B. PostIdent Spezial, versenden oder eigenhändig übergeben. ☒

☒ **gem_AFO_0620 Zeitversetzter Versand**

Der TSP MUSS die Karten und PIN-Briefe zeitversetzt versenden. Der TSP MUSS mit dem Versand des PIN-Briefs warten, bis er den zu der korrespondierenden Karte gehörenden Rückschein erhalten hat. Der TSP MUSS grundsätzlich mindestens eine Frist von 3 Tagen zwischen dem Versand der Karte und dem Versand des PIN Briefs einhalten. ☒

6.8.5 Artefakte

Zu Artefakten im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.8.6 Testunterstützung

Zur Unterstützung von Tests im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.8.7 Hardwaremerkmale

Das Funktionsmerkmal setzt keine besonderen Hardwaremerkmale voraus.

6.9 Ausgabe von Austauschausweisen

Bei Verlust oder Defekt oder Kompromittierung eines HBA oder einer HBA-Ersatzkarte oder einer SMC-B (im Folgenden als „Originalausweis“ bezeichnet) innerhalb der ersten 6 Monate nach Ausstellung muss in einem vereinfachten Verfahren ein sogenannter „Austauschausweis“ beantragt und freigegeben werden können, sofern der freigegebene Ausweis nicht durch den Kartenherausgeber gesperrt wurde. Die Prozesse nach der Freigabe (Auslieferung, Freischaltung, Sperrung) bleiben unverändert.

Dieser Prozess kann nicht wiederholt werden, d. h. für einen Austauschausweis kann kein weiterer Austauschausweis beantragt werden. Ebenso kann für einen Originalausweis kein weiterer Austauschausweis beantragt werden.

Der Austauschausweis ist bezüglich der Antragsdaten identisch zum auszutauschenden Originalausweis:

- derselbe Ausweistyp (HBA oder HBA-Ersatzkarte oder SMC-B),
- dieselben Daten des Antragstellers,
- bei HBA bzw. HBA-Ersatzausweis:
 1. ursprüngliche Identifizierung (des Originalausweises),
 2. dasselbe Foto,
 3. dieselben Druckzeilen,
- dasselbe „gültig bis“-Datum der Zertifikate auf der Karte (dies bedeutet, dass ein Austauschausweis dann abläuft, wenn auch der Originalausweis abgelaufen wäre),
- dieselben Berufsattribut(e)
- dieselben Vorgangsnummern (VorgangsNrTSP und VorgangsNrAttrBS, falls diese vorhanden ist).

Der Austauschausweis bzw. der Antrag dazu unterscheidet sich durch:

- neue Referenznummer,
- neue Passworte,
- neue ICCSN,
- neues Ausstellungsdatum,
- neue SubjectDN Serialnumber,
- neue Seriennummern der Zertifikate,
- neues Schlüsselmaterial,
- neue PIN- und PUK-Werte.

Eine Freigabe durch den Kartenherausgeber ist bei unveränderten Antragsdaten 6 Monate gültig. Daher kann bei der Austauschkarte auf eine Freigabe durch den Kartenherausgeber verzichtet werden. Der TSP gibt in diesem Fall im Auftrag des Kartenherausgebers den Antrag frei.

Spezifikation Kartenpersonalisierung HBA/SMC-B

Zur Beantragung eines Austauschausweises sind die Eingabe der Referenznummer des Originalausweises (zur Identifizierung des zu ersetzenden HBA bzw. HBA-Ersatzkarte bzw. SMC-B) und des Servicepassworts des Originalausweises (zur Authentisierung des Antragstellers) erforderlich.

Falls das Ausstellungsdatum des Originalausweises länger als 6 Monate zurückliegt oder der Originalausweis durch den Kartenherausgeber gesperrt wurde oder bereits ein Austauschausweis beantragt wurde, erfolgt eine Fehlermeldung mit dem Hinweis an den Antragsteller, einen neuen HBA bzw. HBA-Ersatzausweis bzw. SMC-B zu beantragen (keinen „Austauschausweis“).

Falls dies nicht der Fall ist, zeigt das System eine Übersichtsansicht der zum Originalausweis gehörigen Daten an (analog zur jetzigen Übersichtsansicht auf der letzten Seite der Antragstellung).

Eine Änderung von Daten durch den Antragsteller ist nicht möglich. Einverständniserklärungen des Antragstellers bzgl. des Originalausweises gelten weiterhin.

Zusätzlich muss der Antragsteller sein Einverständnis geben, dass der auszutauschende Originalausweis gesperrt wird.

Das Download-PDF enthält ein neues Passwortblatt, den Kartenantrag und bei HBA bzw. HBA-Ersatzausweis den Zertifikatsantrag, aber KEIN Ident-Formular (weder PostIdent noch KammerIdent).

Nur für HBA und HBA-Ersatzausweis gilt: Die Anträge sind zu unterschreiben und per Post an den TSP zu senden (Identitätsprüfung entfällt). Der TSP prüft die unterschriebenen Antragsformulare auf Übereinstimmung mit dem Antrag des Originalausweises und auf Übereinstimmung mit den gespeicherten Antragsdaten.

Im Fall einer SMC-B-Austauschkarte gilt ausschließlich der elektronische Antrag.

Der TSP gibt bei Fehlerfreiheit den Antrag im Auftrag des Kartenherausgebers frei. Der Kartenherausgeber erhält eine E-Mail Benachrichtigung über die in seinem Namen erfolgte Freigabe für den Austauschausweis.

Bevor nach erfolgter Freigabe der Austauschausweis personalisiert und versendet wird, erfolgt automatisch die Sperrung des Originalausweises.

6.9.1 TUC-Beschreibung

Tabelle 15: Tab_900_TUC_Ausgabe_von_Austauschausweisen

Element	Beschreibung
Name	Ausgabe von Austauschausweisen
Beschreibung	Ausgabe eines Austauschausweises innerhalb eines begrenzten Zeitraums in einem vereinfachten Verfahren
Auslöser	Defekt, Verlust oder Kompromittierung eines Originalausweises innerhalb von 6 Monaten nach Ausstellung und darauf folgend Beantragung eines Austauschausweises durch den Antragsteller
Vorbedingungen	Antragsteller hat vor weniger als 6 Monaten einen HBA oder HBA-Ersatzausweis oder eine SMC-B (Originalausweis) bekommen

Spezifikation Kartenpersonalisierung HBA/SMC-B

Element	Beschreibung
	- Antragsteller kennt die Referenznummer und das Servicepasswort des Originalausweises - Originalausweis wurde nicht durch den Kartenherausgeber gesperrt - Es wurde noch kein Austauschausweis beantragt
Eingangsdaten	Referenznummer und Servicepasswort des Originalausweises
Komponenten	Portale und Kartenpersonalisierung
Ausgangsdaten	Austauschausweis und zugehöriger PIN-/PUK-Brief E-Mail Benachrichtigung des Kartenherausgebers über die in seinem Namen erfolgte Freigabe
Nachbedingungen	- Austauschausweis und PIN-/PUK-Brief sind dem Antragsteller zugestellt - Kartenherausgeber ist über die Ausstellung und den Versand von Austauschkarte und PIN-/PUK-Brief informiert. - Originalausweis ist gesperrt
Standardablauf	Siehe Abbildung 20 „Abb_900_Ausgabe_von_Austauschausweisen“
Varianten/Alternativen	Keine.
Fehlerfälle	- Originalausweis wurde vor mehr als 6 Monaten ausgestellt - Originalausweis wurde durch den Kartenherausgeber gesperrt - Es wurde bereits ein Austauschausweis beantragt - Referenznummer und Servicepasswort passen nicht zueinander oder sind falsch - Karte konnte nicht ausgeliefert werden
Nichtfunktionale Anforderungen	Keine.
Zugehörige Diagramme	Abbildung 20 „Abb_900_Ausgabe_von_Austauschausweisen“

6.9.2 Ablauf

Der Ablauf ergibt sich aus der folgenden Abbildung:

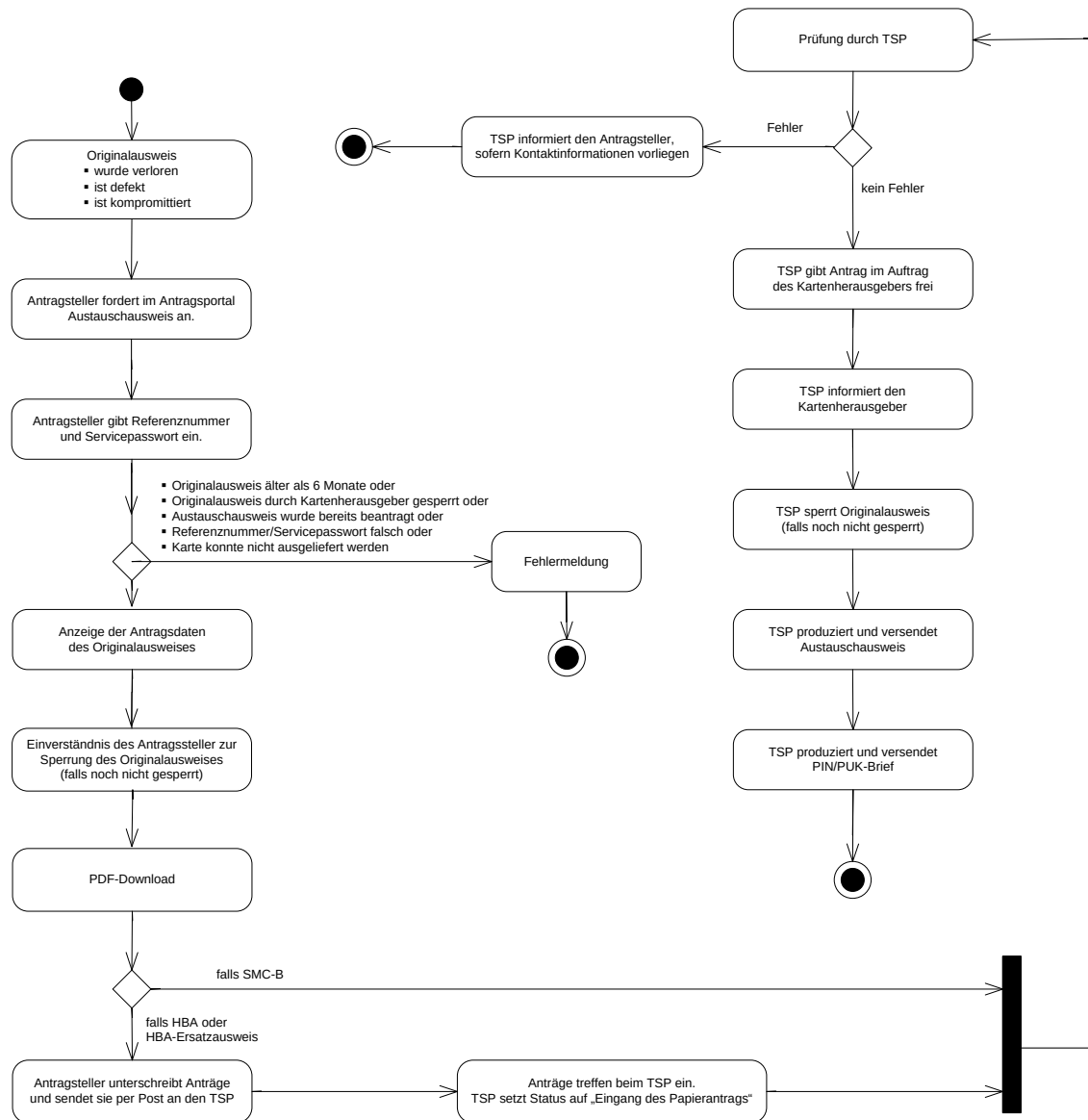


Abbildung 20: Abb_900_Ausgabe_von_Austauschausweisen

6.9.3 Anforderungen

☒ gem_AFO_0900 Ablauf des Prozesses wie in Beschreibung

Der TSP MUSS es ermöglichen, den Prozess wie in „Abb_900_Ausgabe_von_Austauschausweisen“ und „Tab_900_Ausgabe_von_Austauschausweisen“ dargestellt durchzuführen. ☒

☒ gem_AFO_0901 Bereitstellung der Funktion „Beantragung Austauschweis“ im Antragsportal

Der TSP MUSS dem Antragsteller im Antragsportal eine Funktion zur Beantragung eines Austauschweises unter Angabe von Referenznummer und Servicepasswort des Originalausweises anbieten. ☒

☒ gem_AFO_0902 Nicht-Anzeige des Antragsformulars für einen Austauschweis im Antragsportal

Der TSP DARF dem Antragsteller nach Aufruf der Funktion „Beantragung Austauschweis“ das Antragsformular NICHT anzeigen, wenn eine der folgenden Bedingungen erfüllt ist:

- Referenznummer oder Servicepasswort wurden nicht eingegeben
- Die eingegebene Referenznummer ist unbekannt
- Eingegebene Referenznummer und Servicepasswort passen nicht zueinander
- Der durch die Referenznummer identifizierte Originalausweis wurde nicht ausgestellt
- Der durch die Referenznummer identifizierte Originalausweis wurde vor mehr als 6 Monaten ausgestellt
- Der durch die Referenznummer identifizierte Originalausweis wurde durch den Kartenherausgeber gesperrt
- Für den durch die Referenznummer identifizierten Originalausweis wurde bereits ein Austauschweis beantragt. ☒

☒ gem_AFO_0903 Anzeige und Absenden des Antragsformulars für einen Austauschweis im Antragsportal

Der TSP MUSS dem Antragsteller nach Aufruf der Funktion zur Beantragung eines Austauschweises ein Antragsformular anzeigen, das mit den Freigabedaten des Originalausweises gefüllt ist, sofern nicht eine der Bedingungen aus [gem_AFO_0904] zutrifft. Der TSP MUSS sicherstellen, dass die Daten des Originalausweises nicht änderbar durch den Antragsteller sind, und dass der Antragsteller einer Sperrung des Originalausweises zustimmt, bevor er den Antrag absendet. ☒

☒ gem_AFO_0904 Bereitstellung von PDF-Dokumenten nach Absenden des Antrags auf einen Austauschweis

Nachdem der Antragsteller den Antrag im Antragsportal gemäß [gem_AFO_0903] an den TSP abgesendet hat, MUSS der TSP dem Antragsteller ein PDF-Dokument bereitstellen, dass bis auf das Identitätsformular [gem_AFO_0070] und [gem_AFO_0165] entspricht. Das PDF-Dokument enthält kein Identitätsformular. ☒

☒ gem_AFO_0905 Weiterverarbeitung der ausgedruckten Anträge für einen Austauschweis für HBA oder HBA-Ersatzkarte

Nachdem der TSP dem Antragsteller das PDF-Dokument aus [gem_AFO_0904] zur Verfügung gestellt hat, MUSS der Antragsteller die folgenden Schritte ausführen:

- Der Antragsteller druckt beide Anträge (Kartenantrag und Zertifikatsantrag) aus.
- Der Antragsteller unterschreibt die Anträge.
- Der Antragsteller sendet die beiden unterschriebenen Anträge per Post an den TSP. ☒

☒ **gem_AFO_0906 Statuswechsel bei Eingang der Papieranträge auf einen Austauschausweis für HBA oder HBA-Ersatzkarte**

Wenn beim TSP die Papieranträge per Post eintreffen, dann MUSS der TSP den Status des Antrags auf „Eingang des Papierantrags“ setzen. ☒

☒ **gem_AFO_0907 TSP-interne Prüfung von gesendeten Anträgen auf einen Austauschausweis**

Wenn der elektronische Antrag für einen Austauschausweis für eine SMC-B oder die Papieranträge für eine Austauschkarte für HBA oder HBA-Ersatzkarte per Post eintreffen, dann MUSS beim TSP eine manuelle Prüfung durch eine Person durchgeführt werden. Dabei MUSS er die folgenden im System gespeicherten Eingabefelder prüfen:

- Mindestens die Pflichtfelder aus den Antragsdaten. Diese sind in [gem_AFO_0042] definiert.
- Optionale Felder, sofern sie ausgefüllt sind.
- die SigG-relevanten Antragsdaten im Fall von HBA und HBA-Ersatzkarte.

Er MUSS diese Eingabefelder nach folgenden Prüfkriterien prüfen:

- Vollständigkeit (Sind die Pflichtfelder ausgefüllt?)
- Plausibilität
- Ausschluss von „Spam“
- Nimmt der Antragsteller an der Erprobung teil?

Dabei MUSS er für HBA und HBA-Ersatzkarte:

- diese Daten mit den Daten im schriftlichen Zertifikats-Antrag und Kartenantrag vergleichen
- die Unterschrift auf dem Zertifikats-Antrag und Kartenantrag prüfen
- die Antragsdaten auf Übereinstimmung mit den Daten des ausgestellten Originalausweises prüfen. ☒

☒ **gem_AFO_0909 Fehler bei TSP-interner Prüfung von gesendeten Anträgen**

Wenn der TSP bei der Prüfung eines Antrags wie in [gem_AFO_0907] beschrieben einen oder mehrere Fehler oder Abweichungen findet, DARF er den Antrag NICHT im Auftrag des zugehörigen Kartenherausgebers freigeben. ☒

☒ **gem_AFO_0910 Kontakt zum Antragsteller bei Fehler bei TSP-interner Prüfung von gesendeten Anträgen**

Wenn der TSP bei der Prüfung eines Antrags wie in [gem_AFO_0907] beschrieben einen oder mehrere Fehler oder Abweichungen findet, MUSS er sich mit dem Antragsteller (unter Verwendung von Telefon, E-Mail oder Post) in Verbindung setzen, sofern Kontaktinformationen vorliegen. Dies ist ein manueller Prozess. ☒

Hinweis: Das Vorliegen von Kontaktdaten des Antragstellers ist von der Sektorspezifischen Konfiguration abhängig.

☒ **gem_AFO_0908 Fehlerfreien Antrag auf einen Austauschausweis freigeben**

Wenn der TSP bei der Prüfung eines Antrags wie in [gem_AFO_0907] beschrieben keinen Fehler oder Abweichungen findet, MUSS er den Antrag im Auftrag des zugehörigen Kartenherausgebers freigeben. Der TSP MUSS den Kartenherausgeber darüber mit einer E-Mail Benachrichtigung informieren, siehe auch [gem_AFO_0609].

In der E-Mail Benachrichtigung MÜSSEN mindestens die folgenden Informationen enthalten sein:

- Referenznummer des Austauschausweises
- Referenznummer des Originalausweises
- VorgangsNrAttrBS, falls diese nicht vorhanden: VorgangsNrTSP (die Vorgangsnummern sind identisch bei Originalausweis und Austauschausweis)
- Link zu den Daten des Austauschausweises im Freigabeportal. ☒

☒ **gem_AFO_0919 Funktionen des Freigabeportals und der SOAP Interfaces für Austauschkarten**

Der TSP MUSS in Freigabeportal und SOAP Schnittstellen für Austauschkarten die gleichen Funktionen bereitstellen wie für Originalausweise, mit Ausnahme der Freigabe/Ablehnung. Die Freigabe MUSS der TSP im Auftrag des Kartenherausgebers durchführen. ☒

☒ **gem_AFO_0920 Verknüpfung der Daten von Originalausweis und Austauschkarte im Freigabeportal**

In der Detailansicht der Daten der Originalkarte im Freigabeportal MUSS der TSP eine Verknüpfung zu den Daten des Austauschausweises durch Nennung der Referenznummer des Austauschausweises und Link zur Detailansicht des Antrags des Austauschausweises bereitstellen. In der Detailansicht der Daten des Austauschausweises im Freigabeportal MUSS der TSP eine Verknüpfung zu den Antragsdaten und dem signierten Freigabedokument der Originalkarte durch Nennung der Referenznummer der Originalkarte und Links zur Detailansicht des Antrags der Originalkarte und deren Freigabedokument bereitstellen. ☒

☒ **gem_AFO_0921 Unterstützung der Datenformate für Austauschkarten**

Der TSP MUSS in Freigabeportal und SOAP Schnittstellen bei den für Austauschkarten anwendbaren Funktionen, die einen Datentransfer mit dem Kartenherausgeber beinhalten (Datenexport, Statusabfragen und Sperranträge via SOAP) die gleichen Datenformate unterstützen wie für Originalausweise. Siehe hierzu

[gem_AFO_0040], [gem_AFO_0042], [gem_AFO_0043], [gem_AFO_0770], [gem_AFO_0149]. Die von der gematik definierten Übergabedatenformate sehen keine Datenfelder zur Kennzeichnung von Austauschweisen oder Verknüpfung zwischen Originalkarte und Austauschweis vor. 

Erläuterung: Alle weiteren Abläufe der Auslieferung, Freischaltung und Sperrung bleiben unverändert.

6.9.4 Artefakte

Zu Artefakten im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.9.5 Testunterstützung

Zur Unterstützung von Tests im Zusammenhang mit dem Funktionsmerkmal werden keine gesonderten Festlegungen getroffen.

6.9.6 Hardwaremerkmale

Das Funktionsmerkmal setzt keine besonderen Hardwaremerkmale voraus.

7 Informationsmodell

Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten wird nicht benötigt.

8 Verteilungssicht

Eine Darstellung der hardwareseitigen Verteilung des Produkttyps bzw. seiner Teilsysteme und der Einbettung in die physikalische Umgebung wird nicht benötigt.

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AFO	Anforderung
BÄK	Bundesärztekammer
BPTK	Bundespsychotherapeutenkammer
BVK	Beauftragter Verifikationskarte Kartenherausgeber
BZÄK	Bundeszahnärztekammer
CA	Certification Authority
CR-1	Credential 1: Benutzernamen/Passwort für die Authentisierung am Vorbefüllungsportal, am Freigabeportal oder bei der Vorbefüllung per http-POST.
CR-2	Credential 2: Authentisierungszertifikat für die Authentisierung am Vorbefüllungsportal oder am Freigabeportal mit einer Standard-Signaturkarte.
CR-3	Credential 3: TLS- bzw. Web-Service-Security-Zertifikate zur Signatur, Authentisierung und Verschlüsselung im Rahmen der Kommunikation über SOAP.
CR-4	Credential 4: QES-Zertifikat(e) zur qualifizierten Signatur von Freigaben oder Sperrungen.
CR-5	Credential 5: „restrictedID“ bei Nutzung der Online-Ausweisfunktion des nPA zur Authentisierung am Vorbefüllungsportal oder am Freigabeportal.
DKG	Deutsche Krankenhausgesellschaft
DKTIG	Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH
eGK	elektronische Gesundheitskarte
FG-1	Freigabeauftrag per Freigabeportal
FG-2	Freigabeauftrag über SOAP
FG-3	schriftliche Freigabe per Post (nur bei KammerIdent)
GKV	Gesetzliche Krankenversicherungen
HBA	Heilberufsausweis
HTML	Hypertext Markup Language
ICCSN	Kartenkennnummer
ID	Identifizier
KBV	Kassenärztliche Bundesvereinigung
KV	Kassenärztliche Vereinigung

Spezifikation Kartenpersonalisierung HBA/SMC-B

Kürzel	Erläuterung
KZBV	Kassenzahnärztliche Bundesvereinigung
KZV	Kassenzahnärztliche Vereinigung
LÄK	Landesärztekammer
LZÄK	Landeszahnärztekammer
OCSP	Online Card Status Protocol
OPB	Online-Produktiv-Betrieb
PDF	Portable Document Format
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PR-1	Praxisregister-1: TSP fragt nach Aufträgen zur Produktion und Lieferung von SMC-B-Karten beim Praxisregister und erhält eine Liste mit keinem, einem oder mehreren Aufträgen als Antwort.
PR-2	Praxisregister-2: TSP übersendet bei Vorliegen eines Fehlerfalls bei der Verarbeitung eines Produktionsauftrags eine Fehlermeldung an das Praxisregister.
PR-3	Praxisregister-3: TSP registriert eine oder mehrere produzierte und versendete SMC-B-Karten beim Praxisregister. Es stehen zwei getrennte Funktionen im Web-Service zur Verfügung, um entweder eine Karte oder mehrere Karten zu registrieren. Diese Funktionen werden in der weiteren Beschreibung zur Vereinfachung nicht unterschieden.
PR-4	Praxisregister-4: TSP fragt nach Aufträgen zur Aktivierung der Zertifikate von SMC-B-Karten beim Praxisregister und erhält eine Liste mit keinem, einem oder mehreren Aufträgen als Antwort.
PR-5	Praxisregister-5: TSP fragt nach Aufträgen zur Sperrung der Zertifikate von SMC-B-Karten beim Praxisregister und erhält eine Liste mit keinem, einem oder mehreren Aufträgen als Antwort.
PTK	Psychotherapeutenkammer
PUK	Personal Unblocking Key
RA	Registration Authority
RFC	Request for Comments
SAK	Signaturanwendungskomponente
SCH	Schnittstelle
SigG	Signaturgesetz
SigV	Signaturverordnung
SMC-B	Security Module Card Typ B
SOAP	Simple Object Access Protocol
SPOC	Single Point of Contact
SP-1	Sperrung-1: Antragsteller sperrt Zertifikate im Antragsportal

Spezifikation Kartenpersonalisierung HBA/SMC-B

Kürzel	Erläuterung
SP-2	Sperrung-2: Kartenherausgeber sperrt Zertifikate im Freigabeportal
SP-3	Sperrung-3: Kartenherausgeber sperrt Zertifikate über die SOAP-Schnittstelle
SP-4	Sperrung-4: Antragsteller sperrt Zertifikate über die telefonische Sperrhotline des Trust Centers
SP-5	Sperrung-5: Kartenherausgeber sperrt Zertifikate schriftlich
SP-6	Sperrung-6: Antragsteller sperrt Zertifikate schriftlich
TLS	Transport Layer Security
TSP	Trust Service Provider
TUC	Technischer Use Cases
VB-1	Vorbefüllung-1: Vorbefüllung über Datei-Upload am Vorbefüllungsportal.
VB-2	Vorbefüllung-2: Vorbefüllung über Eingabe am Vorbefüllungsportal.
VB-3	Vorbefüllung-3: Vorbefüllung über Online-Schnittstelle mit Authentisierung des Kartenherausgebers.
VB-4	Vorbefüllung-4: Vorbefüllung über SOAP-Schnittstelle.
VB-5	Vorbefüllung-5: Vorbefüllung über synchrone Online-Schnittstelle ohne Authentisierung des Kartenherausgebers.
VorgangsNrAttrBS	Der Kartenherausgeber erzeugt optional zu einer Vorbefüllung eine Vorgangsnummer, die er zusammen mit den restlichen Vorbefüllungsdaten an den TSP übermittelt (Übergabe im Attribut „VorgangsNrAttrBS“).
VorgangsNrTSP	Der TSP erzeugt für jede Vorbefüllung eine losübergreifend eindeutige Vorgangsnummer und teilt sie dem Kartenherausgeber mit (Übergabe im Attribut „VorgangsNr“ der Rückmeldung des TSP).
XML	Extensible Markup Language
ZÄK	Zahnärztekammer
ZDA	Zertifizierungsdiensteanbieter

A2 – Glossar

Siehe [gemGlossar].

A3 – Abbildungsverzeichnis

Abbildung 1: Abb_008_Ablauf_der_Kartenpersonalisierung_von_HBA_und_SMC-B	8
Abbildung 2: Abb_009_Ablauf_der_Kartenpersonalisierung_über_das_Praxisregister	9
Abbildung 3: Abb_010_Ablauf_der_Kartenpersonalisierung_von_Verifikationskarten.....	9
Abbildung 4: Abb_002_Leistungserbringer_und_Kostenträger	12

Abbildung 5: Abb_001_Vorbefüllung_mit_KH_Authentisierung	40
Abbildung 6: Abb_003_Vorbefüllung_ohne_KH_Authentisierung.....	41
Abbildung 7: Abb_102_Vereinfachter_Ablauf_bei_Antragstellung_HBA	51
Abbildung 8: Abb_004_Antragstellung_ohne_nPA.....	57
Abbildung 9: Abb_005_Freigabe.....	74
Abbildung 10: Abb_206_Lieferung	82
Abbildung 11: Abb_207_Lieferung_Praxisregister	83
Abbildung 12: Abb_101_Sperrung_über_Antragsportal	89
Abbildung 13: Abb_100_Sperrung_über_Freigabeportal	90
Abbildung 14: Abb_006_Freigabeportal.....	97
Abbildung 15: Abb_601_Benachrichtigungen	106
Abbildung 16: Abb_501_Abfrage_von_Produktionsaufträgen	114
Abbildung 17: Abb_502_Abfrage_von_Aktivierungsaufträgen.....	115
Abbildung 18: Abb_503_Abfrage_von_Sperraufträgen	116
Abbildung 19: Abb_602_Beantragung_und_Ausgabe_von_Verifikationskarten	122
Abbildung 20: Abb_900_Ausgabe_von_Austauschweisen	128

A4 – Tabellenverzeichnis

Tabelle 1: Tab_010_Akteure und Rollen	10
Tabelle 2: Tab_001_Schnittstellen	13
Tabelle 3: Tab_004_Löschfristen	30
Tabelle 4: Tab_002_TUC_Vorbefüllung	36
Tabelle 5: Tab_009_Anzeige_und Aktionen im_Vorbefüllungsportal.....	46
Tabelle 6: Tab_003_TUC_Antragstellung	53
Tabelle 7: Tab_005_TUC_Freigabe.....	70
Tabelle 8: Tab_202_TUC_Lieferung	79
Tabelle 9: Tab_100_TUC_Sperrung	85
Tabelle 10: Tab_006_TUC_Monitoring	94
Tabelle 11: Tab_008_Anzeige_im_Freigabeportal.....	101
Tabelle 12: Tab_601_TUC_Benachrichtigungen.....	105
Tabelle 13: Tab_500_TUC_Praxisregister	109
Tabelle 14: Tab_602_TUC_Ausgabe_Verifikationskarten.....	121
Tabelle 15: Tab_900_TUC_Ausgabe_von_Austauschweisen	126

A5 – Referenzierte Dokumente

A5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktiv-Betrieb (OPB)
[gem-Meth_SichAnalyse]	gematik: Einheitliche Methoden der Informationssicherheit Methode der Sicherheitsanalyse in der Telematikinfrastruktur
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_PIN_PUK_TI]	gematik: Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[SigG01]	Bundesgesetzblatt I (2001), S.876: Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 Abs. 111 des Gesetzes vom 7.8.2013
[SigV01]	Bundesgesetzblatt I (2001), S. 3074: Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 4 Abs. 112 der Verordnung vom 07.08.2013 (BGBl. I S 3154)
[BDSG]	Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954), neugefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 29.07.2009 (BGBl. I, S. 2254), durch Artikel 5 des Gesetzes vom 29.07.2009 (BGBl. I, S. 2355 [2384] und durch Gesetz vom 14.08.2009 (BGBl. I, S. 2814)
[OWASP]	Open Web Application Security Project, veröffentlicht auf https://www.owasp.org/index.php/Main_Page
[KBV_Benutzer]	KBV: Praxisregister Nutzungs- und Implementierungsleitfaden

Spezifikation Kartenpersonalisierung HBA/SMC-B

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
handbuch Webservice]	
[KV- T_Praxisregiste r_Webservice]	KV-Telematik ARGE: Sammlung Webservice-Dokumentation
[KV- T_ISMS_SMC- B_Ausgabekon zept]	KV-Telematik ARGE: ISMS der KV-Telematik ARGE
[GKV- SV_Spec_Veri Card_G2]	GKV-SV: Spezifikation der Verifikationskarte Kostenträger G2
[Ver- iCard_PolicyG2]	GKV-SV: Richtlinie zur Herstellung und Nutzung von Verifikationskarten Kostenträger G2
[gemSpec_Pers _HBA]	Übergabeschnittstelle für die Produktion von HBAs der Generation 2
[gemSpec_Pers _SMC-B]	Übergabeschnittstelle für die Produktion von SMC-Bs der Generation 2
[gemSpec_SST _TSP]	Spezifikation TSP-Schnittstelle