Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Änderungsbedarf:

Die Technische Richtlinie zur Zertifizierung des Fachmoduls NFDM sieht vor, dass die Zugriffsprotokollierung auf der eGK in jedem Fall gewährleistet ist. Dies kann nicht sichergestellt werden, wenn die Protokollierung erst nach dem eigentlichen eGK-Zugriff erfolgt, da Fehlersituationen vorstellbar sind, in denen nach dem Zugriff auf die eGK eine Protokollierung auf dieser nicht mehr möglich ist.

Änderungen in gemSpec_FM_NFDM

6.1.1.1.1 ReadNFD

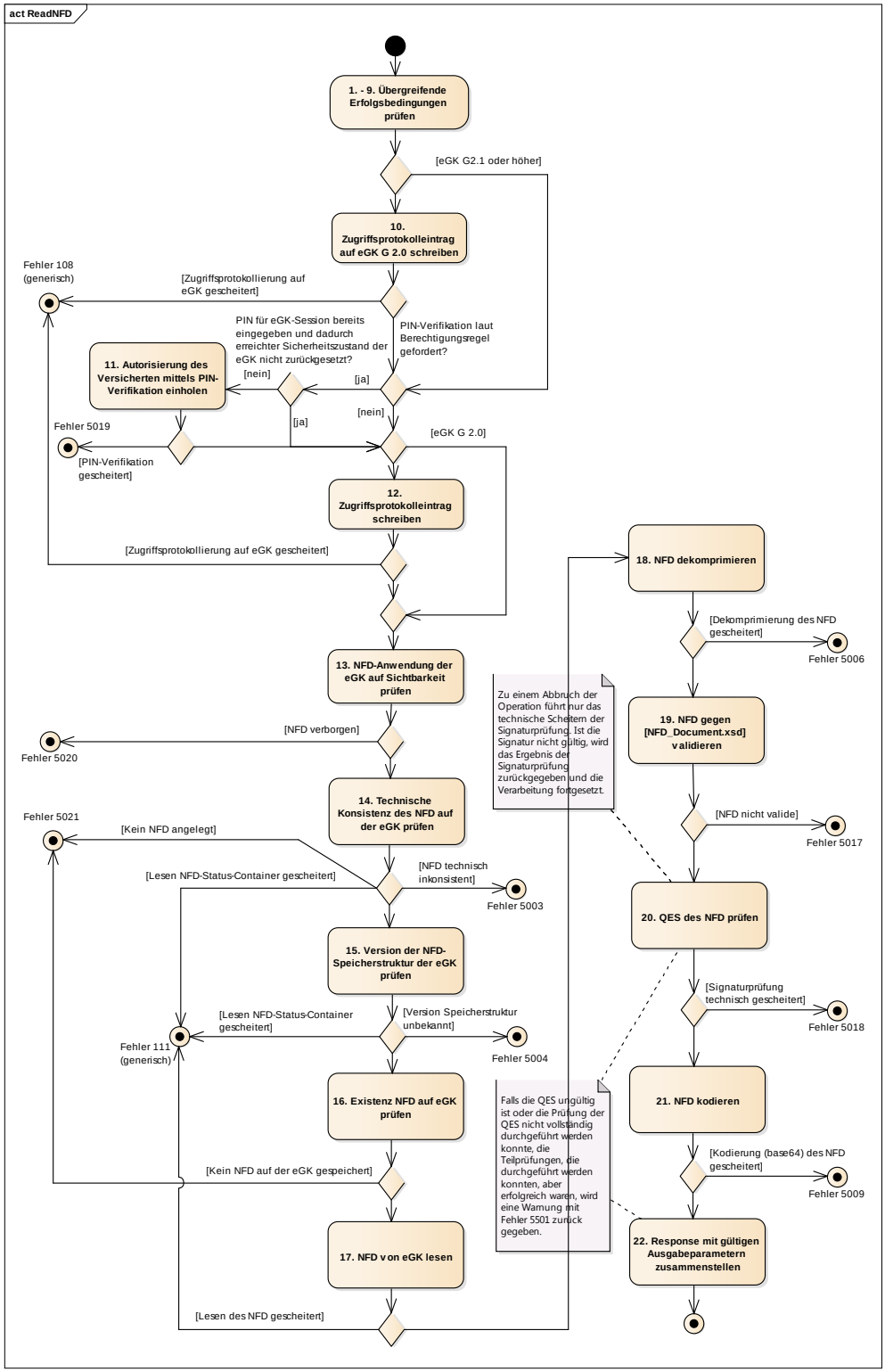

Abbildung 1: Abb_FM_NFDM_003 – Ablauf ReadNFD

6.1.1.2.1 WriteNFD

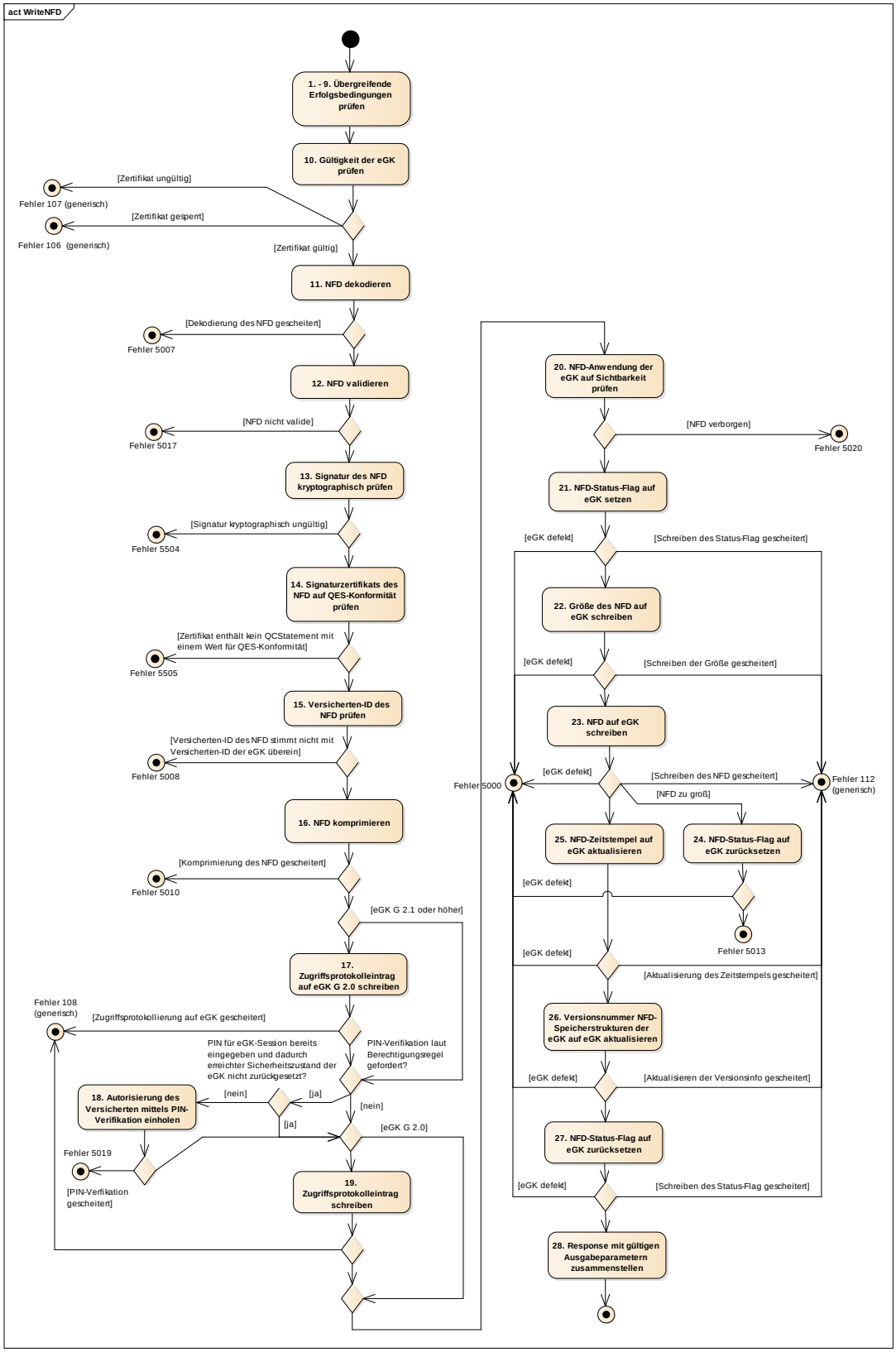

Abbildung 6: Abb_FM_NFDM_004 – Ablauf `WriteNFD`

6.1.1.1.2 EraseNFD

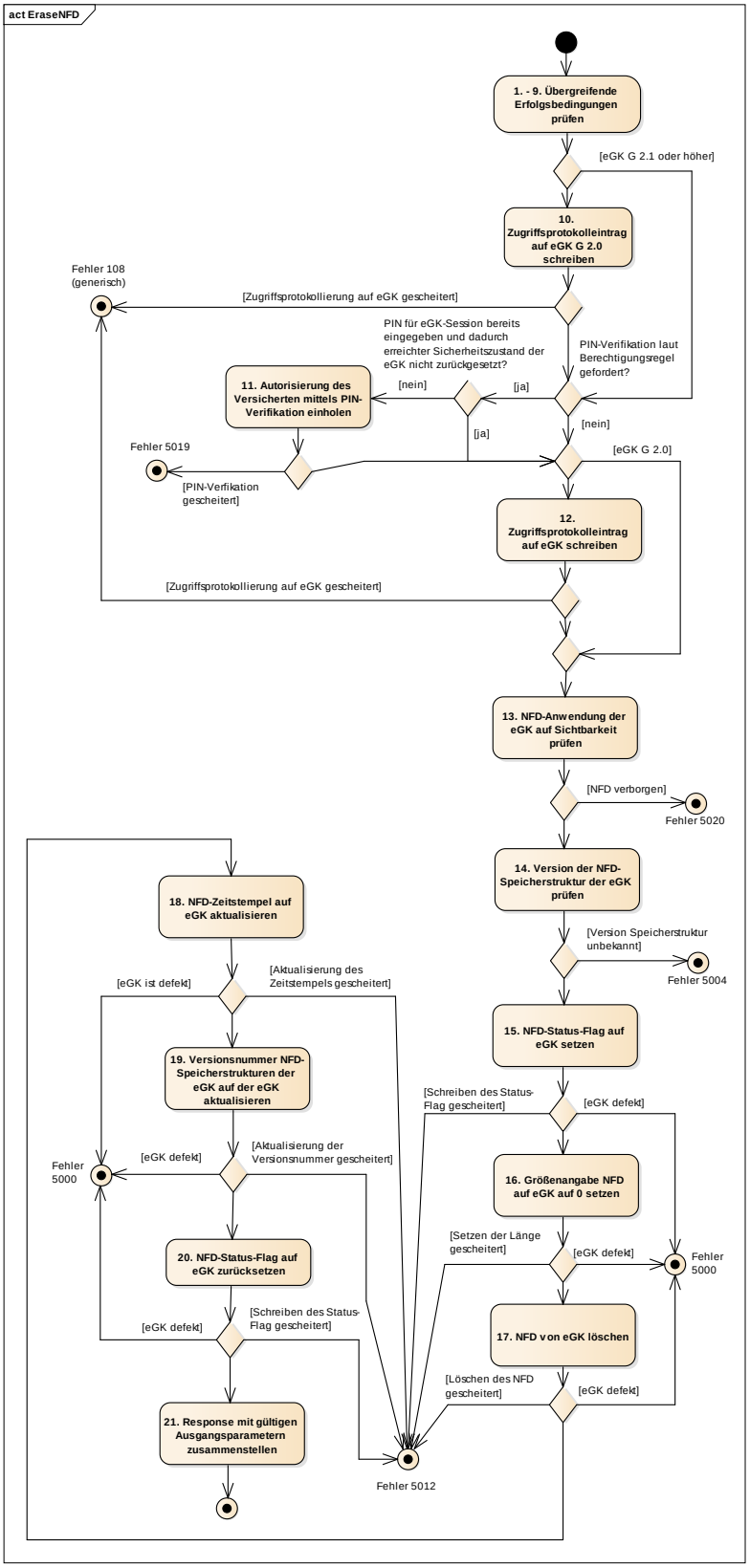

Abbildung 7: Abb_FM_NFDM_005 – Ablauf EraseNFD

6.1.1.2.1 ReadNFD

Tabelle 1: Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD

1	Parameter auf Gültigkeit und Konsistenz prüfen	
	`NFDM:checkArguments`	
	Eingangsdaten	
	Alle Werte der Aufrufparameter der Operation	
	Beschreibung	
	Die übergebenen Parameter werden auf Gültigkeit gemäß XML-Schema für den Service und Konsistenz gemäß zusätzlichen Konsistenzregeln geprüft. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 3 ab.	
2	Zugriffsberechtigung auf eGK prüfen	
	`TUC_KON_000 „Prüfe Zugriffsberechtigung“`	
	Eingangsdaten	
	`mandantId`	`Context.MandantId`
	`clientSystemId`	`Context.ClientSystemId`
	`workplaceId`	`Context.WorkplaceId`
	`userId`	-
	`ctId`	-
	`cardHandle`	`EhcHandle`
	`needCardSession`	true
	`allWorkplaces`	false
	`serviceName`	• Bei Aufruf durch Primärsystem über SOAP: NFDService
	Beschreibung	
	Mittels des TUC-Aufrufs wird überprüft, ob der aufrufende Client (identifiziert über `clientSystemId`) berechtigt (autorisiert) ist, innerhalb des Mandanten (identifiziert durch `mandantId`) über den Arbeitsplatz (identifiziert durch `workplaceId`) auf die lokal gesteckte eGK (identifiziert durch `cardHandle`) zuzugreifen. Dabei wird gleichzeitig sichergestellt, dass die benötigte Kartensitzung der eGK vom Arbeitsplatz `workplaceId` gestartet wurde. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5014 ab.	

3	Zugriffsberechtigung auf HBA/SMC-B prüfen	
	`TUC_KON_000 „Prüfe Zugriffsberechtigung`	
	Eingangsdaten	
	`mandantId`	`Context.MandantId`
	`clientSystemId`	`Context.ClientSystemId`
	`workplaceId`	`Context.WorkplaceId`
	`userId`	**für HBA:** `Context.UserId` **für SMC-B:** -
	`ctId`	-
	`cardHandle`	`HpcHandle`
	`needCardSession`	true
	`allWorkplaces`	false
	`serviceName`	• Bei Aufruf durch Primärsystem über SOAP: NFDService
	Beschreibung	
	Mittels des TUC-Aufrufs wird überprüft, ob der aufrufende Client (identifiziert über `clientSystemId`) berechtigt (autorisiert) ist, innerhalb des Mandanten (identifiziert durch `mandantId`) über den Arbeitsplatz (identifiziert durch `workplaceId`) auf den/die durch `cardHandle` identifizierten HBA/SMC-B zuzugreifen. Dabei wird der Zugriff auf den HBA verhindert, wenn es eine Kartensitzung zum selben Primärsystem, aber einer anderen `userId` gibt, deren Sicherheitszustand erhöht ist. Für eine SMC-B wird sichergestellt, dass es sich um eine im Mandanten verwaltete SMC-B handelt. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5015 ab.	
4	Sperrung Gesundheitsanwendung auf eGK prüfen	
4.1	`TUC_KON_026 „Liefere CardSession“`	
	Eingangsdaten	
	`mandantId`	`Context.MandantId`
	`clientSystemId`	`Context.ClientSystemId`
	`cardHandle`	`EhcHandle`
	`userId`	-
	Beschreibung	
	Für die eGK ist die Sitzung zu ermitteln. Diese wird für den Aufruf des TUCs im nächsten Teilschritt benötigt.	
4.2	`TUC_KON_018 „eGK-Sperrung prüfen“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`checkHcaOnly`	true
	Beschreibung	
	Über den TUC wird geprüft, ob die Gesundheitsanwendung der eGK, also der Ordner `DF.HCA` deaktiviert (= gesperrt) ist. Ist die Gesundheitsanwendung gesperrt, bricht die Operation mit Fehler 114 ab.	

5	Version der eGK prüfen	
5.1	`TUC_KON_254 "Liefere Ressourcendetails"`	
	Eingangsdaten	
	`clientSystemId`	`Context.MandantId`
	`mandantId`	`Context.ClientSystemId`
	`workplaceId`	`Context.WorkplaceId`
	`cardTerminalId` (optional)	-
	`slotId` (optional/zulässig nur, wenn auch `cardTerminalId` angegeben ist)	-
	`cardHandle` (optional)	`EhcHandle`
	`iccsn` (optional)	-
	Beschreibung	
	Der Aufruf des TUC liefert ein Informationsobjekt `CARD:Card` zur über `EhcHandle` referenzierten eGK äquivalent zur Rückgabe der Operation `GetResourceInformation` zurück. Dieses `Card`-Objekt enthält die Versionsinformationen des Betriebssystems und Objektsystems der zugehörigen Karte.	
5.2	`NFDM:checkEgkVersion`	
	Eingangsdaten	
	In 5.1 ermittelte Version der eGK	
	Beschreibung	
	Es wird überprüft, ob das Fachmodul die durch die in 5.1 gelesenen Versionsnummern der eGK repräsentierte eGK-Generation unterstützt. Ist dies nicht der Fall, bricht die Operation mit Fehler 113 ab.	
6	Berechtigungsregel ermitteln	
6.1	`TUC_KON_022 „Liefere PIN-Status“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`pinRef`	MRPIN.NFD
	Beschreibung	
	Über die Abfrage des PIN-Status wird ermittelt, ob die `MRPIN.NFD` aktiviert (Der Rückgabewert von TUC_KON_022 für pinStatus ist nicht DISABLED) ist. Für alle anderen Rückgabewerte des TUC_KON_022 für pinStatus wird von einer aktivierten `MRPIN.NFD` ausgegangen. Dieser Teilschritt ist nur notwendig, wenn zur Bestimmung der Berechtigungsregel zusätzlich die Bedingung bezüglich aktivierter Multireferenz-PIN relevant ist.	
6.2	`NFDM:getAccessRule`	
	Eingangsdaten	
	`EmergencyIndicator`, `UpdateIndicator` und ggf. in 6.1 ermittelter PIN-Status	
	Beschreibung	
	Es wird die Berechtigungsregel gemäß Berechtigungstabelle ermittelt.	

Tritt in diesem Schritt ein Fehler auf, bricht die Operation mit Fehler 5011 ab.		
7	Berechtigung fachliche Rolle prüfen	
7.1	`TUC_KON_026 “Liefere CardSession”`	
	Eingangsdaten	
	`mandantId`	`Context.MandantId`
	`clientSystemId`	`Context.ClientSystemId`
	`cardHandle`	`HpcHandle`
	`userId`	**für HBA:** `Context.UserId` **für SMC-B:** -
	Beschreibung	
	Für die LE-Karte ist die Sitzung zu ermitteln. Diese wird für den Aufruf des TUCs im nächsten Teilschritt benötigt.	
7.2	`TUC_KON_036 „LiefereFachlicheRolle“`	
	Eingangsdaten	
	`cardSession`	In 7.1 ermittelte Kartensitzung der LE-Karte
	Beschreibung	
	Der TUC liefert die fachliche Rolle gemäß [gemSpec_PKI#Tab_PKI_254] zurück.	
7.3	`NFDM:checkRoleAccessRights`	
	Eingangsdaten	
	In 6.2 ermittelte Berechtigungsregel und in 7.2 ermittelte fachliche Rolle	
	Beschreibung	
	Es wird überprüft, ob die ermittelte fachliche Rolle gemäß der ermittelten Berechtigungsregel zugriffsberechtigt ist. Ist die fachliche Rolle nicht zugriffsberechtigt, bricht die Verarbeitung mit Fehler 5002 ab.	
8	Freischaltung HBA/SMC-B prüfen	
	Die Prüfung der Freischaltung HBA/SMC-B erfolgt implizit in 9. Ist die LE-Karte nicht freigeschaltet, sind die Zugriffsbedingungen auf der LE-Karte für eine Durchführung der C2C-Authentisierung in 9 nicht erfüllt. Der in 9 aufgerufene `TUC_KON_005 „Card-to-Card authentisieren“` gibt in diesem Fall den Fehler 4085 zurück.	
9	Authentizität und Echtheit der beteiligten Karten mittels C2C prüfen	
	`TUC_KON_005 „Card-to-Card authentisieren“`	
	Eingangsdaten	
	`sourceCardSession`	In 7.1 ermittelte Kartensitzung der LE-Karte
	`targetCardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`authMode`	gegenseitig
	Beschreibung	
	Durch Aufruf des TUCs wird eine gegenseitige C2C-Authentisierung zwischen eGK und LE-Karte durchgeführt, bei der sich die beiden Karten gegenseitig ihre Echtheit und Authentizität als Smartcards des Gesundheitswesens nachweisen. Gibt der TUC den Fehler 4085 (Zugriffsbedingungen nicht erfüllt) zurück, bedeutet dies, die LE-Karte ist nicht freigeschaltet und die Operation bricht mit Fehler 5001 ab. Bei allen anderen Fehlern, die der TUC zurückgibt, bricht die Operation mit Fehler 5016 ab.	

10	Zugriffsprotokolleintrag auf eGK G 2.0 schreiben	
Falls es sich um eine eGK G 2.0 handelt.		
10.1	`TUC_KON_006 „Datenzugriffsaudit eGK schreiben“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`sourceCardSession`	In 7.1 ermittelte Kartensitzung der LE-Karte
	`dataType`	gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK“
	`accessType`	gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK“
	Beschreibung	
	Ein Zugriffsprotokolleintrag wird als Record in die Datei `EF.Logging` auf der eGK geschrieben. Tritt bei der Zugriffsprotokollierung ein Fehler auf, bricht die Operation mit Fehler 108 ab.	
11	Autorisierung des Versicherten mittels PIN-Verifikation einholen	
Falls Berechtigungsregel für die fachliche Rolle eine PIN-Verifikation fordert.		
	`TUC_KON_012 „PIN verifizieren“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`workplaceID`	`Context.WorkplaceID`
	`pinRef`	**für fachliche Rollen Arzt, Zahnarzt:** MRPIN.NFD **für fachliche Rollen Apotheker, Mitarbeiter Apotheke, Psychotherapeut, Versicherter:** MRPIN.NFD_READ
	`actionName`	Wert von actionName für diese Operation gemäß Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe
	`verificationType`	Sitzung
	Beschreibung	
	Es wird die PIN für lesenden Zugriff auf den NFD auf der eGK verifiziert. Dabei wird der fachliche Akteur am Display des Kartenterminals aufgefordert, die entsprechende PIN einzugeben (Terminalanzeigen s. Tabelle „Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe“), falls er dies nicht bereits im Rahmen der Kartensitzung getan hat. Die PIN-Eingabe erfolgt über das PIN-Pad des Kartenterminals. Tritt hier ein Fehler auf, bricht die Operation mit Fehler 5019 ab.	
12	Zugriffsprotokolleintrag auf eGK schreiben	
Falls es sich um eine eGK G 2.1 oder höher handelt.		
12.1	`TUC_KON_006 „Datenzugriffsaudit eGK schreiben“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`sourceCardSession`	In 7.1 ermittelte Kartensitzung der LE-Karte
	`dataType`	gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK“

	accessType	gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK“
	Beschreibung	
	Ein Zugriffsprotokolleintrag wird als Record in die Datei EF.Logging auf der eGK geschrieben. Tritt bei der Zugriffsprotokollierung ein Fehler auf, bricht die Operation mit Fehler 108 ab.	
13	NFD-Anwendung der eGK auf Sichtbarkeit prüfen	
	Die Prüfung, ob die NFD-Anwendung auf der eGK verborgen ist, erfolgt implizit in 14. TUC_KON_202 „LeseDatei“ gibt beim Versuch, den deaktivierten Ordner DF.NFD der eGK zu selektieren, um die darin befindliche Datei EF.StatusNFD zu lesen, den Code ´62 83´ des Betriebssystems der eGK zurück, woraufhin die Operation mit Fehler 5020 abbricht.	
14	Technische Konsistenz des NFD auf eGK prüfen	
14.1	TUC_KON_202 „LeseDatei“	
	Eingangsdaten	
	cardSession	In 4.1 ermittelte Kartensitzung der eGK
	fileIdentifier (optional/verpflichtend, wenn kein sfid angegeben ist)	´D0 0E´
	sfid (optional/verpflichtend, wenn kein fileIdentifier angegeben ist)	-
	folder	´D276 0001 4407´
	offset	-
	length	-
	Beschreibung	
	Es werden alle Informationselemente der Datei EF.StatusNFD der eGK gelesen. Gibt der TUC_KON_202 „LeseDatei“ den Fehlercode '6283' der eGK zurück, bricht die Operation mit Fehler 5020 ab. Tritt dabei ein anderer Lesefehler auf, bricht die Operation mit Fehler 111 ab.	
14.2	NFDM:checkConsistency	
	Eingangsdaten	
	In 14.1 aus der Datei EF.StatusNFD gelesene Daten (= alle Informationselemente)	
	Beschreibung	
	Es wird überprüft, ob der Wert des Informationselements Status der Eingangsdaten „0“ ist. Ist der Wert „0“, ist der NFD technisch konsistent und die Verarbeitung läuft weiter. Ist der Wert „1“, ist der Fehler 5003 mit dem Wert des Informationselements Timestamp der Eingangsdaten im Detailtext zurückzugeben. Ist der Wert weder „0“ noch „1“ gemäß [gemSpec_eGK_Fach_NFDM#2.2], so wurde noch kein NFD angelegt. Die Operation bricht daher mit dem Fehler 5021 ab.	

15	Version der NFD-Speicherstruktur der eGK prüfen	
	`NFDM:checkContainerVersion`	
	Eingangsdaten	
	In 14.1 aus der Datei `EF.StatusNFD` gelesene Daten (= alle Informationselemente)	
	Beschreibung	
	Es wird überprüft, ob dem Fachmodul die im Informationselement `Version_Speicherstruktur` der Eingangsdaten gespeicherte Versionsnummer der NFD-Speicherstruktur der eGK bekannt ist. Ist dies nicht der Fall, bricht die Operation mit Fehler 5004 ab.	
16	Existenz NFD auf eGK prüfen	
	Die Prüfung, ob ein NFD auf der eGK existiert, erfolgt implizit in 17. In 17 werden alle Daten aus der Datei `EF.NFD` (= alle Informationselemente) der eGK gelesen. Das Informationselement `Länge NFD` enthält die Größe (Anzahl Oktette) des im Informationselement `NFD` gespeicherten NFD. Nur wenn ein Wert für dieses Informationselement gesetzt ist und dieser ungleich ´00 00´ ist, existiert ein NFD auf der eGK.	
17	NFD von eGK lesen	
17.1	`TUC_KON_202 „LeseDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 10´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4407´
	`offset`	-
	`length`	-
	Beschreibung	
	Es werden die Daten aus beiden Informationselementen (`Länge NFD` und `NFD`) der Datei `EF.NFD` der eGK gelesen. Tritt dabei ein Fehler auf, bricht die Operation mit Fehler 111 ab.	
17.2	`NFDM:checkSize`	
	Eingangsdaten	
	In 17.1 aus der Datei `EF.NFD` der eGK gelesene Daten (die beiden Informationselemente `Länge NFD` und `NFD`)	
	Beschreibung	
	Es wird das Informationselement `Länge NFD` der in 17.1 gelesenen Daten als Größe des NFD (Anzahl Oktette) ausgewertet. Ist die Größenangabe ´00 00´, bedeutet dies, es existiert kein NFD auf der eGK. In diesem Fall bricht die Operation mit Fehler 5021 ab.	
17.3	`NFDM:extractNfd`	
	Eingangsdaten	
	In 17.1 aus der Datei `EF.NFD` der eGK gelesene Daten (die beiden Informationselemente `Länge NFD` und `NFD`)	

	Beschreibung	
	Die dem Informationselement `Länge NFD` folgende und der in 17.2 ausgewerteten Größe entsprechende Anzahl Oktette wird als NFD zur Weiterverarbeitung extrahiert. Tritt dabei ein Fehler auf, bricht die Operation mit Fehler 111 ab.	
~~**16**~~	~~Zugriffsprotokolleintrag auf eGK schreiben~~	
~~Falls es sich um eine eGK G 2.1 oder höher handelt.~~		
~~16.1~~	~~`TUC_KON_006 „Datenzugriffsaudit eGK schreiben“`~~	
	~~**Eingangsdaten**~~	
	~~`cardSession`~~	~~In 4.1 ermittelte Kartensitzung der eGK~~
	~~`sourceCardSession`~~	~~In 7.1 ermittelte Kartensitzung der LE-Karte~~
	~~`dataType`~~	~~gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK““~~
	~~`accessType`~~	~~gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK““~~
	~~**Beschreibung**~~	
	~~Ein Zugriffsprotokolleintrag wird als Record in die Datei `EF.Logging` auf der eGK geschrieben. Tritt bei der Zugriffsprotokollierung ein Fehler auf, bricht die Operation mit Fehler 108 ab.~~	
18	NFD dekomprimieren	
	`NFDM:decompress`	
	Eingangsdaten	
	Der in 17.3 extrahierte NFD	
	Beschreibung	
	Der NFD wird dekomprimiert. Tritt dabei ein Fehler auf, bricht die Operation mit Fehler 5006 ab.	
19	NFD gegen [NFD_Document.xsd] validieren	
	Die Validierung des NFD gegen das XML-Schema [NFD_Document.xsd] ist in Schritt 20 inkludiert. `TUC_KON_151 „QES Dokumentensignatur prüfen“` beinhaltet einen internen Aufruf von `TUC_KON_080 „Dokument validieren“`.	

20	QES des NFD prüfen	
	TUC_KON_151 „QES Dokumentensignatur prüfen“	
	Eingangsdaten	
	signedDocument	Der in 18 dekomprimierte NFD als Inhalt des Elements Base64XML eines SIG:Document-Elements
	signatureObject	
	/SignaturePtr/@WhichDocument	Wert des ID-Attributs (NFD_DOC_ID) des SIG:Document-Elements des Parameters signedDocument
	/SignaturePtr/@XPath	/NFD_Document/SignatureArzt
	optionalInputParams	
	ReturnVerificationReport	mit gemäß Standardvorgaben des Schemas belegte Unterelemente
	certificates	- (Das Zertifikat ist in der XML-Signatur enthalten.)
	workplaceId	Context.WorkplaceId
	xmlSchemas	[NFD_Document.xsd]
	includeRevocationInfo	false
	Beschreibung	
	Die QES des NFD wird mittels des TUCs geprüft und der NFD gegen das XML-Schema [NFD_Document.xsd] validiert. TUC_KON_151 ruft intern TUC_KON_080 „Dokument validieren“ auf, um die Gültigkeit des NFD gegen sein XML Schema zu prüfen. Bricht TUC_KON_151 mit Fehler 4022 oder 4023 des TUC_KON_080 ab, so bricht die Operation mit Fehler 5017 ab. Liefert der TUC_KON_151 als VerificationResult INVALID oder INCONCLUSIVE, wird die Verarbeitung fortgeführt, jedoch zusätzlich zum VerificationReport an 22 eine Warning mit Fehlercode 5501 übergeben. Bricht TUC_KON_151 die Verarbeitung mit einem Fehler ab, bricht die Operation mit Fehler 5018 ab.	

21	NFD kodieren
	`NFDM:encode`
	Eingangsdaten
	Der in 20 QES-geprüfte NFD
	Beschreibung
	Der NFD wird base64-kodiert. Tritt dabei ein Fehler auf, bricht die Operation mit Fehler 5009 ab.
22	Response mit gültigen Antwortparametern zusammenstellen
	`NFDM:prepareResponse`
	Eingangsdaten
	In 21 kodierter NFD, in 20 vom `TUC_KON_151 „QES-Dokumentensignatur prüfen“` zurückgegebener `VerificationReport` und ggf. von den Basisdiensten des Konnektors erhaltene Warnings.
	Beschreibung
	Zusammenstellung einer gültigen Response (Rückgabe und Statusrückmeldung) gemäß Tabelle „Tab_FM_NFDM_005 – Operation ReadNFD“

6.1.1.2.2 WriteNFD

Tabelle 2: Tab_FM_NFDM_026 – Umsetzung Ablaufaktivitäten `WriteNFD`

1-3	Identisch zu 1-3 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)	
4	Sperrung Gesundheitsanwendung auf eGK prüfen	
4.1	`TUC_KON_026 „Liefere CardSession“`	
	Eingangsdaten	
	`mandantId`	`Context.MandantId`
	`clientSystemId`	`Context.ClientSystemId`
	`cardHandle`	`EhcHandle`
	`userId`	-
	Beschreibung	
	Für die eGK ist die Sitzung zu ermitteln. Diese wird für den Aufruf des TUCs im nächsten Teilschritt benötigt.	

4.2	`TUC_KON_018 „eGK-Sperrung prüfen“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`checkHcaOnly`	false
	Beschreibung	
	Über den TUC wird geprüft, ob die Gesundheitsanwendung der eGK, also der Ordner `DF.HCA` deaktiviert (= gesperrt) ist und ob das Zertifikat C.CH.AUT der eGK zeitlich gültig und nicht gesperrt ist. Der Aufruf des TUC schließt die Gültigkeitsprüfung der eGK aus Schritt 10 mit ein. Ist die Gesundheitsanwendung gesperrt, bricht die Operation mit Fehler 114 ab. Ist das Zertifikat nicht gültig (Ergebnis der Offline-Prüfung „ungültig), bricht die Operation mit Fehler 107 ab. Ist das Zertifikat gesperrt (Sperrstatus = „gesperrt“), bricht die Operation mit Fehler 106 ab.	
5	Identisch zu 5 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)	
6	Berechtigungsregel ermitteln	
6.1	Identisch zu 6.1 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)	
6.2	`NFDM:getAccessRule`	
	Eingangsdaten	
	In 5 ermittelte Version der eGK und ggf. in 6.1 ermittelter PIN-Status	
	Beschreibung	
	Es wird die Berechtigungsregel gemäß der für die eGK-Generation relevanten Berechtigungstabelle ermittelt.	
Tritt in diesem Schritt ein Fehler auf, bricht die Operation mit Fehler 5011 ab.		
7	Berechtigung fachliche Rolle prüfen	
	Erfolgt implizit durch das Betriebssystem der eGK beim Zugriff auf Dateien der eGK. Gibt in den folgenden Schritten einer der TUCs zum Zugriff auf die eGK den Fehler 4085 zurück, bricht die Operation mit Fehler 5002 ab.	
8-9	Identisch zu 8-9 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)	
10	Gültigkeit der eGK prüfen	
	Erfolgt implizit bereits durch Aufruf von TUC_KON_018 in Schritt 4.2	

~~**11**~~	~~Autorisierung des Versicherten mittels PIN-Verifikation einholen~~	
~~Falls Berechtigungsregel für die fachliche Rolle eine PIN-Verifikation fordert~~		
	~~`TUC_KON_012 „PIN verifizieren“`~~	
	~~**Eingangsdaten**~~	
	~~`cardSession`~~	~~In 4.1 ermittelte Kartensitzung der eGK~~
	~~`workplaceID`~~	~~`Context.WorkplaceID`~~
	~~`pinRef`~~	~~**für fachliche Rollen Arzt, Mitarbeiter Arzt, Mitarbeiter Krankenhaus, Zahnarzt, Mitarbeiter Zahnarzt:** MRPIN.NFD~~
	~~`actionName`~~	~~Wert von actionName für diese Operation gemäß Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe~~
	~~`verificationType`~~	~~Sitzung~~
	~~**Beschreibung**~~	
	~~Es wird die PIN für schreibenden Zugriff auf den NFD auf der eGK verifiziert. Dabei wird der fachliche Akteur am Display des Kartenterminals aufgefordert, die entsprechende PIN einzugeben (Terminalanzeigen s. Tabelle „Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe“), falls er dies nicht bereits im Rahmen der Kartensitzung getan hat. Die PIN-Eingabe erfolgt über das PIN-Pad des Kartenterminals.~~ ~~Tritt hier ein Fehler auf, bricht die Operation mit Fehler 5019 ab.~~	
~~**12**~~	~~NFD-Anwendung der eGK auf Sichtbarkeit prüfen~~	
	~~Die Prüfung, ob die NFD-Anwendung auf der eGK verborgen ist, erfolgt implizit in 19.~~ ~~`TUC_KON_203 „SchreibeDatei“` gibt beim Versuch, den deaktivierten Ordner `DF.NFD` der eGK zu selektieren, um in die darin befindliche Datei `EF.StatusNFD` zu schreiben, den Code ´62 83´ des Betriebssystems der eGK zurück, woraufhin die Operation mit Fehler 5020 abbricht.~~	
11	NFD dekodieren	
	`NFDM:decode`	
	Eingangsdaten	
	Der Wert des Aufrufparameters `NFDDocument`	
	Beschreibung	
	Der base64-kodierte NFD wird dekodiert. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5007 ab.	

12	NFD validieren	
	`NFDM:validateDocument`	
	Eingangsdaten	
	Der in 11 dekodierte NFD	
	Beschreibung	
	Die Validierung des NFD besteht aus zwei einzelnen Schritten: • Das Fachmodul prüft das Dokument auf seine Wohgeformtheit und gegen das XML-Schema [NFD_Document.xsd]. • Das Fachmodul prüft das Dokument gegen alle in [gemSpec_InfoNFDM] aufgeführten Validitätskriterien. Schlägt die Validierung fehl, bricht das Fachmodul NFDM die Operation mit dem Fehler 5017 ab.	
13	Signatur des NFD kryptographisch prüfen	
	`TUC_KON_162 „Kryptographische Prüfung der XML-Dokumentensignatur“`	
	Eingangsdaten	
	`signedDocument`	`NFDDocument` als Inhalt des Elements `Base64XML` eines `SIG:Document`-Elements
	`signatureObject`	
	`/SignaturePtr/@XPath`	`/NFD_Document/SignatureArzt`
	Beschreibung	
	Mittels des TUC wird die die Signatur kryptographisch geprüft. Der TUC liefert true als Wert des Ausgabeparameters `Result`, wenn die Signaturprüfung erfolgreich war. Ist die Signatur (kryptographisch) ungültig, liefert der TUC false. In diesem Falle bricht die Operation mit Fehler 5504 ab.	
14	Signaturzertifikat des NFD auf QES-Konformität prüfen	
14.1	`NFDM:extractSignerCert`	
	Eingangsdaten	
	Der in 12 validierte NFD	
	Beschreibung	
	Das base64-codierte Signaturzertifikat des NFD wird extrahiert (Wert des Elements `/NFD_Document/SignatureArzt/Signature/KeyInfo/X509Data/X509Certificate`).	
14.2	`NFDM:decode`	
	Eingangsdaten	
	Das in 14.1 extrahierte Signaturzertifikat	
	Beschreibung	
	Das base64-kodierte Signaturzertifikat wird dekodiert.	

14.3	`NFDM:extractQcStatements`	
	Eingangsdaten	
	Das in 14.2 decodierte Signaturzertifikat	
	Beschreibung	
	Der Wert der Extension `QCStatements` des Signaturzertifikats wird extrahiert Die Verweise auf die Dokumente, welche die Zertifikatsprofile der HBA-Zertifikate definieren, finden sich in [gemSpec_PKI#5.2].	
14.4	`NFDM:checkQcStatement`	
	Eingangsdaten	
	Der in 14.3 aus dem Signaturzertifikat extrahierte Wert der Extension `QCStatements`.	
	Beschreibung	
	Es wird geprüft, ob der in 14.3 aus dem Signaturzertifikat extrahierte Wert der Extension `QCStatements` ein QCStatement zur QES-Konformität (OID `id-etsi-qcs-QcCompliance` (`0.4.0.1862.1.1`)) enthält. Ist kein solcher Wert vorhanden, bricht die Operation die Verarbeitung mit Fehler 5505 ab.	
Tritt in diesem Schritt ein Fehler auf, bricht die Operation mit Fehler 5505 ab.		
15	Versicherten-ID des NFD prüfen	
15.1	`NFDM:extractNfdInsurantId`	
	Eingangsdaten	
	Der in 12 validierte NFD	
	Beschreibung	
	Die Versicherten-ID (Wert des Elements `/NFD_Document/Notfalldaten/NFD_Versicherter/Versicherter/Versicherten_ID`) wird aus dem NFD extrahiert.	
15.2	`TUC_KON_034 „Zertifikatsinformationen extrahieren“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`qes`	false
	Beschreibung	
	Durch den TUC-Aufruf wird das Zertifikat `C.CH.AUT` von der eGK gelesen und sowohl das Zertifikat als auch der Wert des im folgenden Schritt benötigten SubjectDN an das Fachmodul zurückgeliefert. Die Struktur des SubjectDN ist in [gemSpec_PKI#5.1.2] und [gemSpec_PKI#5.1.3.1] definiert.	

15.3	`NFDM:extractCertInsurantId`	
	Eingangsdaten	
	Der in 15.2 gelesene SubjectDN des in 15.2 gelesenen Zertifikats	
	Beschreibung	
	Aus SubjectDN wird die Versicherten-ID im Feld mit dem Namen `organizationalUnitName` extrahiert. *Anmerkung: Es gibt zwei `organizationalUnitName`-Felder. Das zehnstellige, alphanumerische Feld, beinhaltet die Versicherten-ID (unveränderbarer Teil der Krankenversichertennummer), das andere , neunstellige numerische Feld das Institutionskennzeichen der Krankenversichertennummer (s. [gemSpec_PKI#5.1.3.1]).*	
15.4	`NFDM:checkInsurantIdsForEquality`	
	Eingangsdaten	
	In 15.1 aus dem NFD extrahierte Versicherten-ID und die in 15.3 aus dem in15.2 gelesenen Zertifikat extrahierte Versicherten-ID	
	Beschreibung	
	Die beiden extrahierten Versicherten-IDs werden auf Gleichheit getestet. Sind die beiden IDs nicht gleich, bricht die Operation mit Fehler 5008 ab.	
16	NFD komprimieren	
	`NFDM:compress`	
	Eingangsdaten	
	Der in 12 validierte NFD	
	Beschreibung	
	Der in 12 validierte NFD wird komprimiert. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5010 ab.	
17	Zugriffsprotokolleintrag auf eGK schreiben	
Falls es sich um eine eGK G 2.0 handelt.		
17.1	`TUC_KON_026 "Liefere CardSession"`	
	Eingangsdaten	
	`mandantId`	`Context.MandantId`
	`clientSystemId`	`Context.ClientSystemId`
	`cardHandle`	`HpcHandle`
	`userId`	**für HBA:** `Context.UserId` **für SMC-B:** -
	Beschreibung	
	Für die LE-Karte ist die Sitzung zu ermitteln. Diese wird für den Aufruf des TUCs im nächsten Teilschritt benötigt.	
17.2	`TUC_KON_006 „Datenzugriffsaudit eGK schreiben"`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`sourceCardSession`	In 17.1 ermittelte Kartensitzung der LE-Karte
	`dataType`	gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK"

	accessType	gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK“
	Beschreibung	
	Ein Zugriffsprotokolleintrag wird als Record in die Datei EF.Logging auf der eGK geschrieben. Tritt bei der Zugriffsprotokollierung ein Fehler auf, bricht die Operation mit Fehler 108 ab.	
18	Autorisierung des Versicherten mittels PIN-Verifikation einholen	
Falls Berechtigungsregel für die fachliche Rolle eine PIN-Verifikation fordert		
	TUC_KON_012 „PIN verifizieren“	
	Eingangsdaten	
	cardSession	In 4.1 ermittelte Kartensitzung der eGK
	workplaceID	Context.WorkplaceID
	pinRef	**für fachliche Rollen Arzt, Mitarbeiter Arzt, Mitarbeiter Krankenhaus, Zahnarzt, Mitarbeiter Zahnarzt:** MRPIN.NFD
	actionName	Wert von actionName für diese Operation gemäß Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe
	verificationType	Sitzung
	Beschreibung	
	Es wird die PIN für schreibenden Zugriff auf den NFD auf der eGK verifiziert. Dabei wird der fachliche Akteur am Display des Kartenterminals aufgefordert, die entsprechende PIN einzugeben (Terminalanzeigen s. Tabelle „Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe“), falls er dies nicht bereits im Rahmen der Kartensitzung getan hat. Die PIN-Eingabe erfolgt über das PIN Pad des Kartenterminals. Tritt hier ein Fehler auf, bricht die Operation mit Fehler 5019 ab.	
19	Zugriffsprotokolleintrag auf eGK schreiben	
Falls es sich um eine eGK G 2.1 oder höher handelt.		
19.1	TUC_KON_026 “Liefere CardSession”	
	Eingangsdaten	
	mandantId	Context.MandantId
	clientSystemId	Context.ClientSystemId
	cardHandle	HpcHandle
	userId	**für HBA:** Context.UserId **für SMC-B:** -
	Beschreibung	
	Für die LE-Karte ist die Sitzung zu ermitteln. Diese wird für den Aufruf des TUCs im nächsten Teilschritt benötigt.	
19.2	TUC_KON_006 „Datenzugriffsaudit eGK schreiben“	
	Eingangsdaten	
	cardSession	In 4.1 ermittelte Kartensitzung der eGK
	sourceCardSession	In 19.1 ermittelte Kartensitzung der LE-Karte
	dataType	gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK“

	accessType	gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK“
	Beschreibung	
	Ein Zugriffsprotokolleintrag wird als Record in die Datei EF.Logging auf der eGK geschrieben. Tritt bei der Zugriffsprotokollierung ein Fehler auf, bricht die Operation mit Fehler 108 ab.	
20	NFD-Anwendung der eGK auf Sichtbarkeit prüfen	
	Die Prüfung, ob die NFD-Anwendung auf der eGK verborgen ist, erfolgt implizit in 21. TUC_KON_203 „ SchreibeDatei“ gibt beim Versuch, den deaktivierten Ordner DF.NFD der eGK zu selektieren, um in die darin befindliche Datei EF.StatusNFD zu schreiben, den Code ´62 83´ des Betriebssystems der eGK zurück, woraufhin die Operation mit Fehler 5020 abbricht.	
21	NFD-Status-Flag auf eGK setzen	
	TUC_KON_203 „SchreibeDatei“	
	Eingangsdaten	
	cardSession	In 4.1 ermittelte Kartensitzung der eGK
	fileIdentifier (optional/verpflichtend, wenn kein sfid angegeben ist)	´D0 0E´
	sfid (optional/verpflichtend, wenn kein fileIdentifier angegeben ist)	-
	folder	´D276 0001 4407´
	offset	0
	length	1
	dataToBeWritten	„1“
	Beschreibung	
	Zur „Transaktionssicherung“ wird das Status-Flag des NFD-Status-Containers (Wert des Informationselements Status der Datei EF.StatusNFD der eGK) vor Beginn des Schreibvorgangs des NFD auf „1“ gesetzt. Gibt der TUC_KON_203 „SchreibeDatei“ den Fehlercode '6581' der eGK zurück, bricht die Operation mit Fehler 5000 ab. Gibt der TUC_KON_203 „SchreibeDatei“ den Fehlercode ´62 83´ der eGK zurück, bricht die Operation mit Fehler 5020 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 112 ab.	
22	Größe des NFD auf eGK schreiben	
22.1	NFDM:determineSize	
	Eingangsdaten	
	Der in 16 komprimierte NFD	
	Beschreibung	
	Die Größe (Anzahl Oktette) des NFD wird bestimmt.	
22.2	Das Schreiben der in 22.1 ermittelten Größe des NFD auf die eGK erfolgt zusammen mit dem Schreiben des NFD in 23.	
23	NFD auf eGK schreiben	
23.1	NFDM:concatenate	
	Eingangsdaten	

	Die in 22.1 ermittelte Größe (Anzahl Oktette) des NFD und der NFD	
	Beschreibung	
	Die in 22.1 ermittelte Größenangabe wird konkateniert mit dem an 23.1 übergebenen NFD. Die Struktur entspricht [gemSpec_eGK_Fach_NFDM#2.1]). Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 112 ab.	
23.2	`TUC_KON_203 „SchreibeDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 10´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4407´
	`offset`	-
	`length`	-
	`dataToBeWritten`	In 23.1 konkatenierte Oktettkette
	Beschreibung	
	Die in 23.1 konkatenierte Oktettkette (Größenangabe und NFD) wird auf die eGK in die Datei `EF.NFD` geschrieben. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. Hierbei wird die Größe (Anzahl Oktette) des NFD geprüft. Ist die Größe des NFD größer als der in der Datei `EF.NFD` entsprechend des Objektsystems der eGK zur Verfügung stehende Speicherplatz, liefert der TUC den Fehler 4247. In diesem Fall wird Schritt 24 ausgeführt und die Operation mit dem Fehler 5013 abgebrochen. In allen anderen Fehlerfällen bricht die Operation mit Fehler 112 ab.	

24	NFD-Status-Flag auf eGK zurücksetzen	
Falls die Größenprüfung beim Aufruf von `TUC_KON_203 "SchreibeDatei"` in 23.2 mit Fehler 4247 endete.		
24.1	`TUC_KON_203 „SchreibeDatei`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 0E´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	
	`folder`	´D276 0001 4407´
	`offset`	0
	`length`	1
	`dataToBeWritten`	„0“
	Beschreibung	
	Mit Beendigung des Schreibvorgangs des NFD auf die eGK wird das NFD-Status-Flag (Wert des Informationselements `Status` der Datei `EF.StatusNFD` der eGK) wieder zurück auf „0“ gesetzt. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 112 ab.	
24.2	Die Operation bricht mit dem Fehler 5013 ab.	
25	NFD-Zeitstempel auf eGK aktualisieren	
25.1	`TUC_KON_351 „Liefere Systemzeit“`	
	Eingangsdaten	
	Keine	
	Beschreibung	
	Der TUC-Aufruf liefert die aktuelle Systemzeit des Konnektors. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 112 ab.	
25.2	`NFDM:formatSystemTime`	
	Eingangsdaten	
	Im vorherigem Teilschritt ermittelte Systemzeit	
	Beschreibung	
	Die Systemzeit wird für das Schreiben in das Informationselement `Timestamp` der Datei `EF.StatusNFD` auf der eGK gemäß [gemSpec_eGK_Fach_NFDM#2.2] formatiert (14 Oktette; YYYYMMDDhhmmss). Das eigentliche Schreiben des NFD-Zeitstempels in das Informationselement `Timestamp` der Datei `EF.StatusNFD` der eGK erfolgt aus Performancegründen in 27.2. Dort wird die Oktettkette zur Befüllung der Datei `EF.StatusNFD` als Ganzes in die Datei `EF.StatusNFD` der eGK geschrieben. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 112 ab.	

26	Versionsnummer NFD-Speicherstruktur der eGK auf eGK aktualisieren	
	Das Aktualisieren der Versionsnummer der NFD-Speicherstruktur der eGK erfolgt implizit im nächsten Schritt. Dort wird die Oktettkette zur Befüllung der Datei `EF.StatusNFD` als Ganzes in die Datei `EF.StatusNFD` auf der eGK geschrieben.	
27	NFD-Status-Flag auf eGK zurücksetzen	
27.1	`NFDM:concatenate`	
	Eingangsdaten	
	In 25.2 formatierter NFD-Zeitstempel, Versionsnummer der NFD-Speicherstruktur der eGK, gemäß derer der NFD auf die eGK geschrieben wird.	
	Beschreibung	
	Die Oktettkette für den NFD-Status-Container der eGK wird gemäß [gemSpec_eGK_Fach_NFDM#2.2] konkateniert, wobei das Informationselement `Version_XML` mit 5 Oktetten des Wertes ´00´ zu befüllen ist und das Informationselement `Status` den Wert „0“ erhält. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 112 ab.	
27.2	`TUC_KON_203 „SchreibeDatei`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 0E´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4407´
	`offset`	-
	`length`	-
	`dataToBeWritten`	In 27.1. konkatenierte Oktettkette
	Beschreibung	
	Mit Beendigung des Schreibvorgangs des NFD auf die eGK wird das NFD-Status-Flag (Wert des Informationselements `Status` der Datei `EF.StatusNFD` der eGK) wieder zurück auf „0“ gesetzt und der NFD-Zeitstempel sowie die Versionsnummer der NFD-Speicherstruktur der eGK gemäß [gemSpec_eGK_Fach_NFDM#2.2] aktualisiert. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 112 ab.	
~~**26**~~	~~Zugriffsprotokolleintrag auf eGK schreiben~~	
~~26.1~~	~~`TUC_KON_026 “Liefere CardSession”`~~	
	~~**Eingangsdaten**~~	
	~~`mandantId`~~	~~`Context.MandantId`~~
	~~`clientSystemId`~~	~~`Context.ClientSystemId`~~
	~~`cardHandle`~~	~~`HpcHandle`~~
	~~`userId`~~	~~**für HBA:** `Context.UserId`~~ ~~**für SMC-B: -**~~
	~~**Beschreibung**~~	

	~~Für die LE-Karte ist die Sitzung zu ermitteln. Diese wird für den Aufruf des TUCs im nächsten Teilschritt benötigt.~~	
~~26.2~~	~~`TUC_KON_006 „Datenzugriffsaudit eGK schreiben“`~~	
	~~**Eingangsdaten**~~	
	~~`cardSession`~~	~~In 4.1 ermittelte Kartensitzung der eGK~~
	~~`sourceCardSession`~~	~~In 26.1 ermittelte Kartensitzung der LE-Karte~~
	~~`dataType`~~	~~gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK“~~
	~~`accessType`~~	~~gemäß Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK“~~
	~~**Beschreibung**~~	
	~~Ein Zugriffsprotokolleintrag wird als Record in die Datei `EF.Logging` auf der eGK geschrieben. Tritt bei der Zugriffsprotokollierung ein Fehler auf, bricht die Operation mit Fehler 108 ab.~~	
28	Response mit gültigen Antwortparametern zusammenstellen	
	`NFDM:prepareResponse`	
	Eingangsdaten	
	Ggf. von den Basisdiensten des Konnektors erhaltene Warnings.	
	Beschreibung	
	Zusammenstellung einer gültigen Response (Rückgabe und Statusrückmeldung) gemäß Tabelle „Tab_FM_NFDM_008 – Operation `WriteNFD`“	

6.1.1.2.3 EraseNFD

Tabelle 3: Tab_FM_NFDM_027 – Umsetzung zu Ablaufaktivitäten `EraseNFD`

1-9	Übergreifende Erfolgsbedingungen prüfen
	Identisch zu 1-9 von `WriteNFD` (s. Tabelle „Tab_FM_NFDM_026 – Umsetzung Ablaufaktivitäten WriteNFD“)
10	Zugriffsprotokolleintrag auf eGK G 2.0 schreiben
	Identisch zu 10 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten `ReadNFD`“)

11	Autorisierung des Versicherten mittels PIN-Verifikation einholen	
Falls Berechtigungsregel für die fachliche Rolle eine PIN-Verifikation fordert		
	`TUC_KON_012 „PIN verifizieren“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`workplaceID`	`Context.WorkplaceID`
	`pinRef`	MRPIN.NFD
	`actionName`	Wert von actionName für diese Operation gemäß Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe
	`verificationType`	Sitzung
	Beschreibung	
	Es wird die PIN für den löschenden Zugriff auf den NFD auf der eGK verifiziert. Dabei wird der fachliche Akteur am Display des Kartenterminals aufgefordert, die entsprechende PIN einzugeben (Terminalanzeigen s. Tabelle „Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN- Eingabe“), falls er dies nicht bereits im Rahmen der Kartensitzung getan hat. Die PIN-Eingabe erfolgt über das PIN Pad des Kartenterminals. Tritt hier ein Fehler auf, bricht die Operation mit Fehler 5019 ab.	
12	Zugriffsprotokolleintrag auf eGK schreiben	
	Identisch zu 12 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)	
13	NFD-Anwendung der eGK auf Sichtbarkeit prüfen	
	Die Prüfung, ob die NFD-Anwendung verborgen ist, erfolgt implizit im nächsten Schritt. `TUC_KON_202 „LeseDatei“` gibt beim Versuch, die verborgene (deaktivierte) Anwendung `DF.NFD` auf der eGK zu selektieren, um die Versionsnummer der NFD-Speicherstruktur der eGK aus dem Informationselement `Status` der Datei `EF.StatusNFD` der eGK zu lesen, den Code ´62 83´ des Betriebssystems der eGK zurück, woraufhin die Operation mit Fehler 5020 abbricht.	
14	Version der NFD-Speicherstruktur der eGK prüfen	
14.1	`TUC_KON_202 „LeseDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier`	´D0 1E´
	`sfid`	-
	`folder`	´D276 0001 4407´
	`offset`	20
	`length`	5
	Beschreibung	
	Es wird das Informationselement `Version_Speicherstruktur` der Datei `EF.StatusNFD` der eGK ausgelesen. Gibt der `TUC_KON_202 „LeseDatei“` den Fehlercode '6283' der eGK zurück, bricht die Operation mit Fehler 5020 ab.	

14.2.	`NFDM:checkContainerVersion`	
	Eingangsdaten	
	In 14.1 gelesener Wert des Informationselements `Version_Speicherstruktur` der Datei `EF.StatusNFD` der eGK	
	Beschreibung	
	Es wird überprüft, ob dem Fachmodul die in 14.1 gelesene Versionsnummer der NFD-Speicherstruktur der eGK bekannt ist. Ist dies nicht der Fall, bricht die Operation mit Fehler 5004 ab.	
15	NFD-Status-Flag auf eGK setzen	
	`TUC_KON_203 „SchreibeDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 0E´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4407´
	`offset`	0
	`length`	1
	`dataToBeWritten`	1
	Beschreibung	
	Zur „Transaktionssicherung“ wird das Status-Flag des NFD-Status-Containers (Wert des Informationselements `Status` der Datei `EF.StatusNFD` der eGK) vor Beginn des Löschvorgangs des NFD auf „1“ gesetzt. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 5012 ab.	
16	Größenangabe NFD auf eGK auf 0 setzen	
	Das Setzen der Größenangabe für den NFD auf der eGK auf 0 erfolgt implizit in 17.	

17	NFD von eGK löschen	
	`TUC_KON_204 „LöscheDateiInhalt“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 10´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4407´
	`offset`	-
	Beschreibung	
	Der Inhalt der Datei `EF.NFD` der eGK wird durch Oktette mit dem Wert ´00´ (NULL) überschrieben. Dadurch wird einerseits der Inhalt des Informationselement `Länge NFD` mit ´00 00´ überschrieben und zudem die Daten des im Informationselement `NFD` gespeicherten NFD „gelöscht“, d. h. mit ´00´ (NULL) überschrieben. Gibt der `TUC_KON_204 „LöscheDateiInhalt“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 5012 ab.	
18	NFD-Zeitstempel auf eGK aktualisieren	
18.1	`TUC_KON_351 „Liefere Systemzeit“`	
	Eingangsdaten	
	Keine	
	Beschreibung	
	Der TUC liefert die aktuelle Systemzeit des Konnektors. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5012 ab.	
18.2	`NFDM:formatSystemTime`	
	Eingangsdaten	
	Im vorherigen Teilschritt ermittelte Systemzeit	
	Beschreibung	
	Die Systemzeit wird für das Schreiben in das Informationselement `Timestamp` der Datei `EF.StatusNFD` der eGK gemäß [gemSpec_eGK_Fach_NFDM#2.2] formatiert (14 Oktette; YYYYMMDDhhmmss). Das eigentliche Schreiben des NFD-Zeitstempels in das Informationselement `Timestamp` der Datei `EF.StatusNFD` der eGK erfolgt aus Performancegründen in 20.2. Dort wird die Oktettkette aus NFD-Status-Flag und NFD-Zeitstempel als Ganzes in die Datei `EF.StatusNFD` der eGK geschrieben. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5012 ab.	
19	Versionsnummer NFD-Speicherstruktur der eGK auf eGK aktualisieren	
	Das Aktualisieren der Versionsnummer der NFD-Speicherstruktur der eGK erfolgt implizit im nächsten Schritt. Dort wird die Oktettkette zur Befüllung des NFD-Status-Containers als Ganzes in die Datei `EF.StatusNFD` der eGK geschrieben.	

20	NFD-Status-Flag auf eGK zurücksetzen	
20.1	`NFDM:concatenate`	
	Eingangsdaten	
	In 18.2 formatierter NFD-Zeitstempel, Versionsnummer der NFD-Speicherstruktur der eGK, gemäß derer auf die eGK geschrieben wird.	
	Beschreibung	
	Die Oktettkette für den NFD-Status-Container der eGK wird gemäß [gemSpec_eGK_Fach_NFDM#2.2] konkateniert, wobei das Informationselement `Version_XML` mit Oktetten des Wertes ´00´ zu befüllen ist und das Informationselement `Status` den Wert „0“ erhält. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5012 ab.	
20.2.	`TUC_KON_203 „SchreibeDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 0E´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4407´
	`offset`	
	`length`	
	`dataToBeWritten`	In 20.1 konkatenierte Oktettkette
	Beschreibung	
	Mit Beendigung des Löschvorgangs des NFD auf der eGK wird das NFD-Status-Flag (Wert des Informationselements `Status` der Datei `EF.StatusNFD` der eGK) wieder zurück auf „0“ gesetzt und der NFD-Zeitstempel sowie die Versionsnummer der NFD-Speicherstruktur der eGK aktualisiert. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 5012 ab.	
~~**19**~~	~~Zugriffsprotokolleintrag auf eGK schreiben~~	
	~~Identisch zu 16 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)~~	
21	Response mit gültigen Antwortparametern zusammenstellen	
	`NFDM:prepareResponse`	
	Eingangsdaten	
	Ggf. von den Basisdiensten des Konnektors erhaltene Warnings	
	Beschreibung	
	Zusammenstellung einer gültigen Response (Rückgabe und Statusrückmeldung) gemäß Tabelle „Tab_FM_NFDM_011 – Operation EraseNFD“	

6.2.1.1.1 ReadDPE

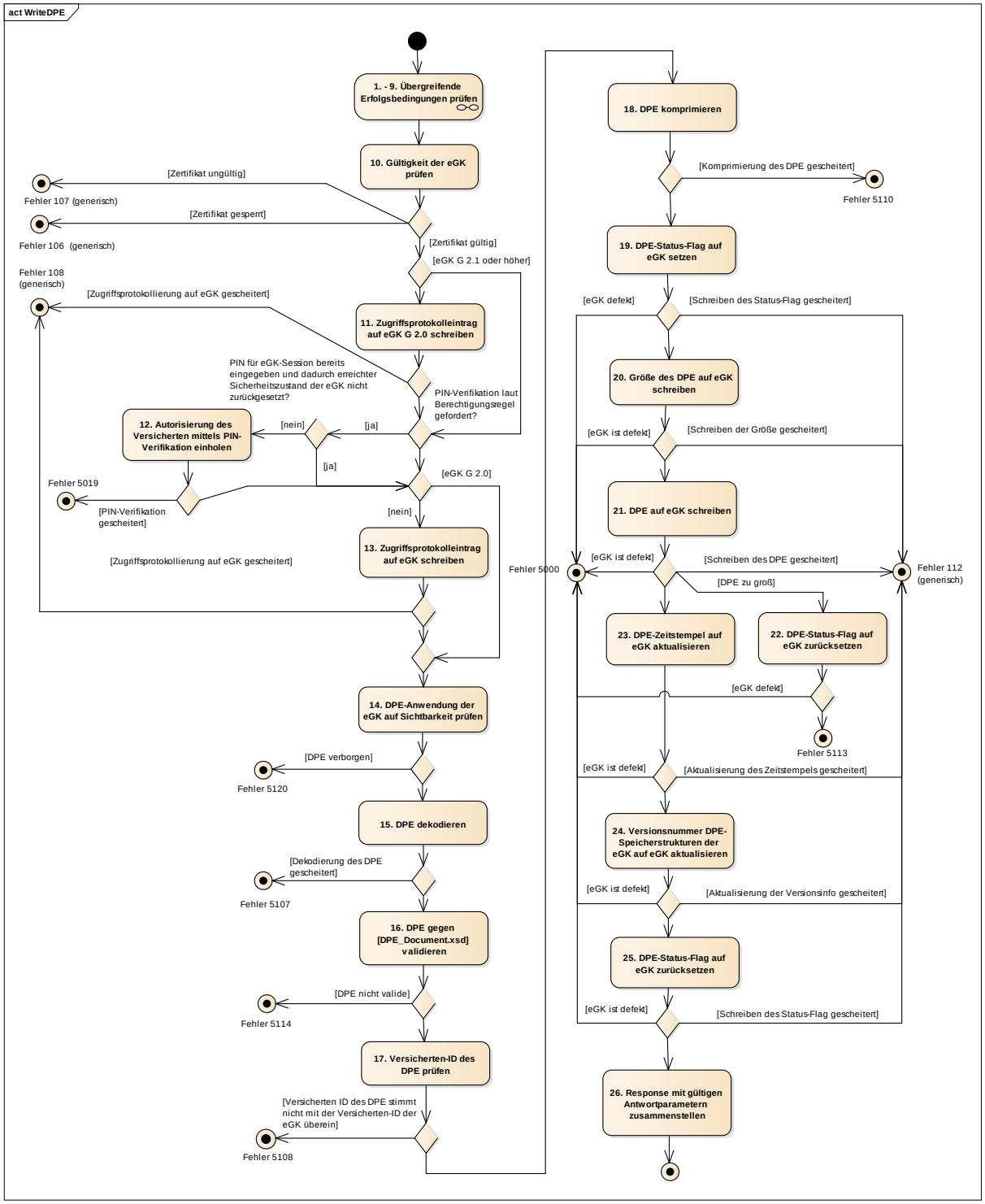

Abbildung 2: Abb_FM_NFDM_006 – Ablauf ReadDPE

6.2.1.1.2 WriteDPE

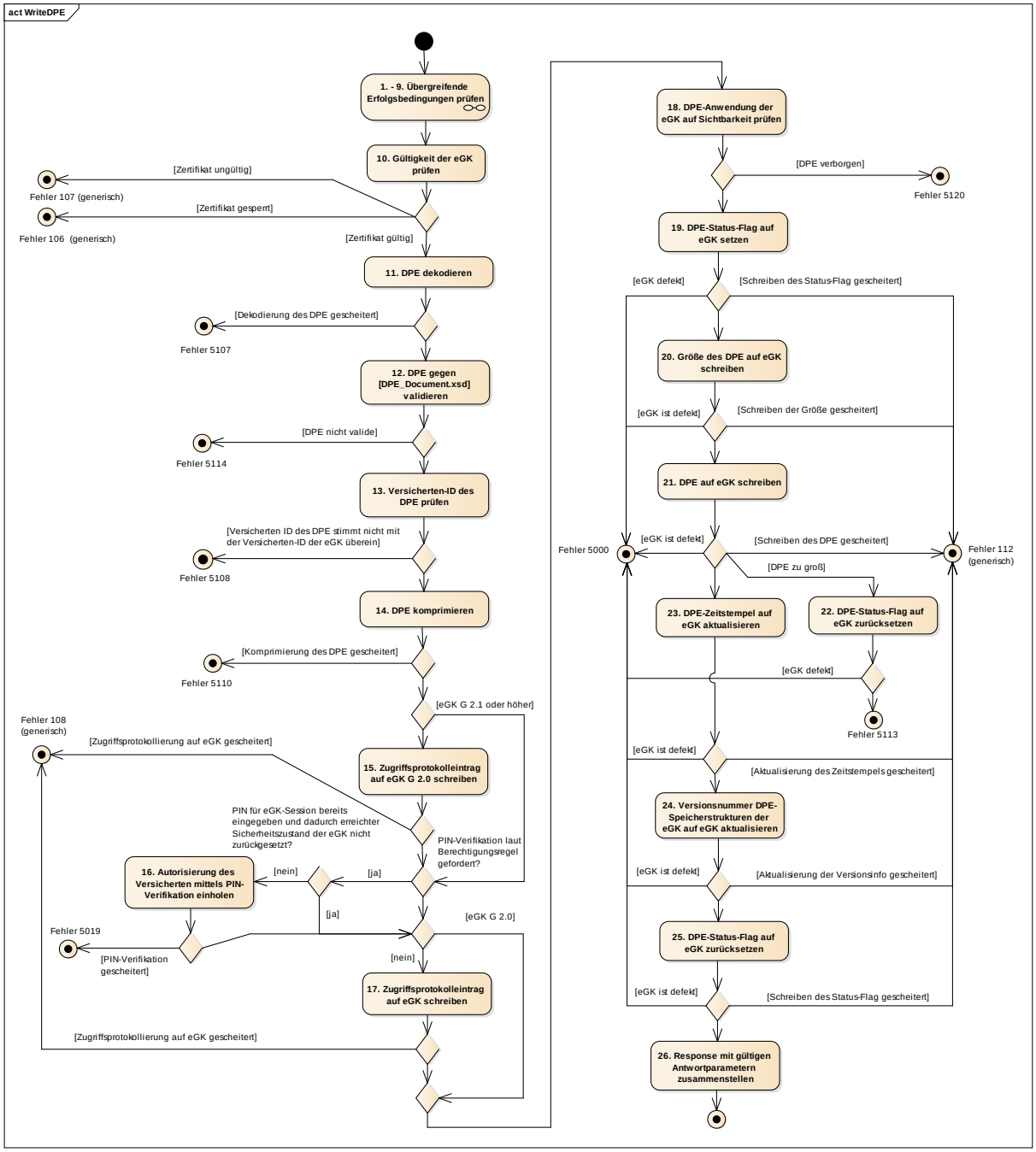

Abbildung 3: Abb_FM_NFDM_007 – Ablauf `WriteDPE`

6.2.1.1.3 EraseDPE

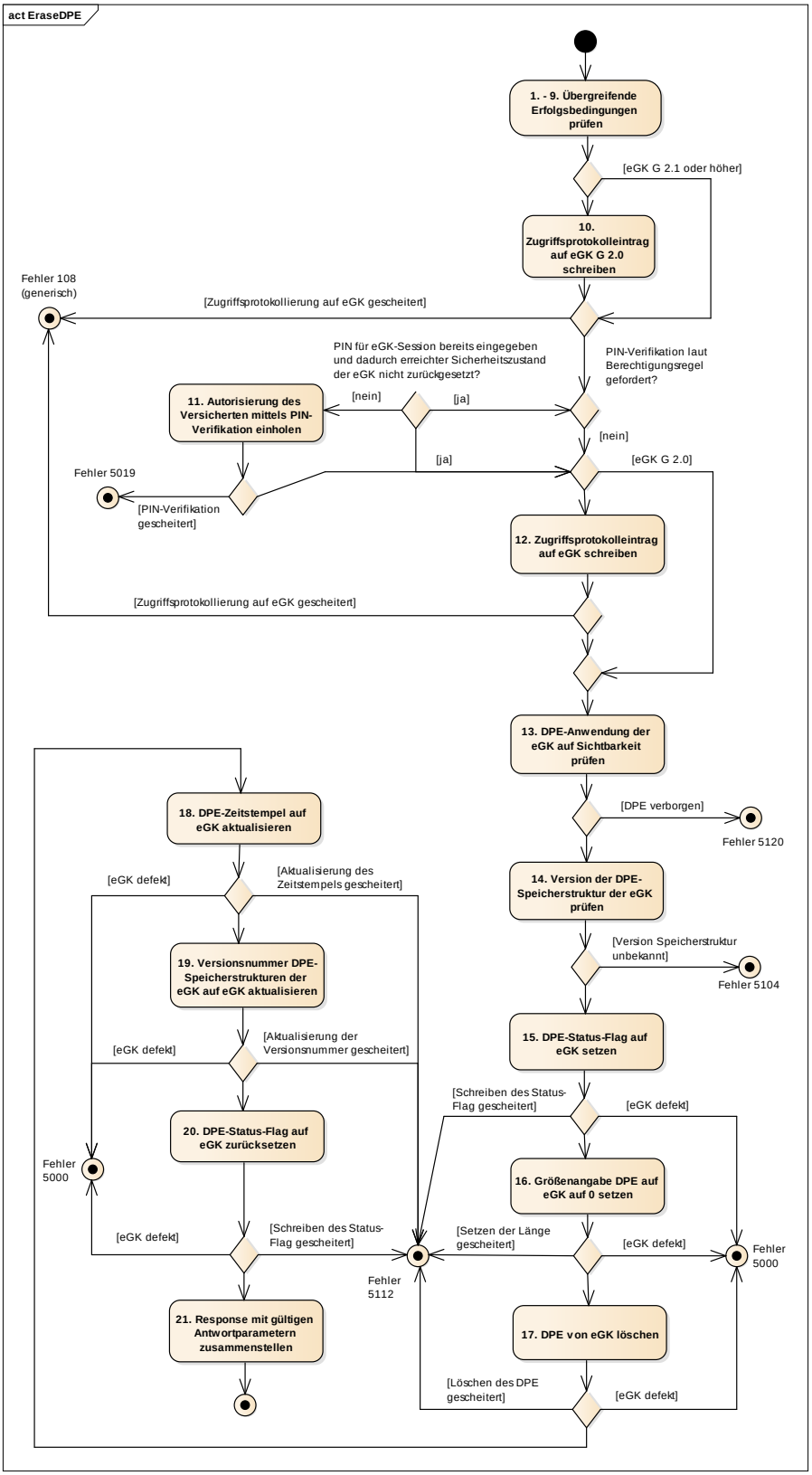

Abbildung 4: Abb_FM_NFDM_008 – Ablauf EraseDPE

6.2.1.2.1 ReadDPE

Tabelle 4: Tab_FM_NFDM_028 – Umsetzung Ablaufaktivitäten ReadDPE

1	Identisch zu 1 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten `ReadNFD`“)	
2	Zugriffsberechtigung auf eGK prüfen	
	`TUC_KON_000 „Prüfe Zugriffsberechtigung“`	
	Eingangsdaten	
	`mandantId`	`Context.MandantId`
	`clientSystemId`	`Context.ClientSystemId`
	`workplaceId`	`Context.WorkplaceId`
	`userId`	-
	`ctId`	-
	`cardHandle`	`EhcHandle`
	`needCardSession`	true
	`allWorkplaces`	false
	`serviceName`	• Bei Aufruf durch Primärsystem über SOAP: DPEService
	Beschreibung	
	Mittels des TUC-Aufrufs wird überprüft, ob der aufrufende Client (identifiziert über `clientSystemId`) berechtigt (autorisiert) ist, innerhalb des Mandanten (identifiziert durch `mandantId`) über den Arbeitsplatz (identifiziert durch `workplaceId`) auf die lokal gesteckte eGK (identifiziert durch `cardHandle`) zuzugreifen. Dabei wird gleichzeitig sichergestellt, dass die benötigte Kartensitzung der eGK vom Arbeitsplatz `workplaceId` gestartet wurde. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5014 ab.	

3	Zugriffsberechtigung auf HBA/SMC-B prüfen	
	`TUC_KON_000 „Prüfe Zugriffsberechtigung`	
	Eingangsdaten	
	`mandantId`	`Context.MandantId`
	`clientSystemId`	`Context.ClientSystemId`
	`workplaceId`	`Context.WorkplaceId`
	`userId`	**für HBA:** `Context.UserId` **für SMC-B:** -
	`ctId`	-
	`cardHandle`	`HpcHandle`
	`needCardSession`	true
	`allWorkplaces`	false
	`serviceName`	• Bei Aufruf durch Primärsystem über SOAP: DPEService
	Beschreibung	
	Mittels des TUC-Aufrufs wird überprüft, ob der aufrufende Client (identifiziert über `clientSystemId`) berechtigt (autorisiert) ist, innerhalb des Mandanten (identifiziert durch `mandantId`) über den Arbeitsplatz (identifiziert durch `workplaceId`) auf den/die durch `cardHandle` identifizierten HBA/SMC-B zuzugreifen. Dabei wird der Zugriff auf den HBA verhindert, wenn es eine Kartensitzung zum selben Primärsystem, aber einer anderen `userId` gibt, deren Sicherheitszustand erhöht ist. Für eine SMC-B wird sichergestellt, dass es sich um eine im Mandanten verwaltete SMC-B handelt. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5015 ab.	
4 - 5	Identisch zu 4-5 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten `ReadNFD`“)	
6	Berechtigungsregel ermitteln	
6.1	`TUC_KON_022 „Liefere PIN-Status“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`pinRef`	MRPIN.DPE
	Beschreibung	
	Über die Abfrage des PIN-Status wird ermittelt, ob die `MRPIN.DPE` aktiviert (Der Rückgabewert von TUC_KON_022 für pinStatus ist nicht DISABLED) ist. Für alle anderen Rückgabewerte des TUC_KON_022 für pinStatus wird von einer aktivierten `MRPIN.NFD` ausgegangen. Dieser Teilschritt ist nur notwendig, wenn zur Bestimmung der Berechtigungsregel zusätzlich die Bedingung bezüglich aktivierter Multireferenz-PIN relevant ist.	
6.2	identisch zu 6.2 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten `ReadNFD`“)	
Tritt in diesem Schritt ein Fehler auf, bricht die Operation mit Fehler 5011 ab.		
7 - 9	Identisch zu 7-9 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten `ReadNFD`“)	
10	Zugriffsprotokolleintrag auf eGK G 2.0 schreiben	

	Identisch zu 10 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)	
11	Autorisierung des Versicherten mittels PIN-Verifikation einholen	
Falls Berechtigungsregel für die fachliche Rolle eine PIN-Verifikation fordert		
	`TUC_KON_012 „PIN verifizieren“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`workplaceID`	`Context.WorkplaceID`
	`pinRef`	**für fachliche Rolle Versicherter:** MRPIN.DPE_READ **für alle anderen fachlichen Rollen:** MRPIN.DPE
	`actionName`	Wert von actionName für diese Operation gemäß Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe
	`verificationType`	Sitzung
	Beschreibung	
	Es wird die PIN für lesenden Zugriff auf den DPE auf der eGK verifiziert. Dabei wird der fachliche Akteur am Display des Kartenterminals aufgefordert, die entsprechende PIN einzugeben (Terminalanzeigen s. Tabelle „Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe“), falls er dies nicht bereits im Rahmen der Kartensitzung getan hat. Die PIN-Eingabe erfolgt über das PIN Pad des Kartenterminals. Tritt hier ein Fehler auf, bricht die Operation mit Fehler 5019 ab.	
12	Zugriffsprotokolleintrag auf eGK schreiben	
	Identisch zu 12 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)	
13	DPE-Anwendung der eGK auf Sichtbarkeit prüfen	
	Die Prüfung, ob die DPE-Anwendung der eGK verborgen ist, erfolgt implizit in 14. `TUC_KON_202 „LeseDatei“` gibt beim Versuch, den deaktivierten Ordner `DF.DPE` der eGK zu selektieren, um die darin befindliche Datei `EF.StatusDPE` zu lesen, den Code ´62 83´ des Betriebssystems der eGK zurück, woraufhin die Operation mit Fehler 5120 abbricht.	
14	Technische Konsistenz des DPE auf eGK prüfen	
14.1	`TUC_KON_202 „LeseDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 18´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4408´
	`offset`	-
	`length`	-

	Beschreibung
	Es werden alle Informationselemente der Datei `EF.StatusDPE` der eGK gelesen. Gibt der `TUC_KON_202 „LeseDatei“` den Fehlercode '6283' der eGK zurück, bricht die Operation mit Fehler 5120 ab. Tritt dabei ein anderer Lesefehler auf, bricht die Operation mit Fehler 111 ab.
14.2	`NFDM:checkConsistency`
	Eingangsdaten
	In 14.1 aus der Datei `EF.StatusDPE` gelesene Daten (= alle Informationselemente)
	Beschreibung
	Es wird überprüft, ob der Wert des Informationselements `Status` der Eingangsdaten „0“ ist. Ist der Status „0“, ist der DPE technisch konsistent und die Verarbeitung läuft weiter. Ist der Status „1“, ist der Fehler 5103 mit dem Wert des Informationselements `Timestamp` der Eingangsdaten im Detailtext zurückzugeben. Ist der Wert weder „0“ noch „1“ gemäß [gemSpec_eGK_Fach_NFDM#2.2], so wurde noch kein DPE angelegt. Die Operation bricht daher mit dem Fehler 5121 ab.
15	Version der DPE-Speicherstruktur der eGK prüfen
	`NFDM:checkContainerVersion`
	Eingangsdaten
	In 14.1 aus dem DPE-Statuscontainer der eGK gelesene Daten (= alle Informationselemente)
	Beschreibung
	Es wird überprüft, ob dem Fachmodul die im Informationselement `Version_Speicherstruktur` der Eingangsdaten gespeicherte Versionsnummer der DPE-Speicherstruktur der eGK bekannt ist. Ist dies nicht der Fall, bricht die Operation mit Fehler 5104 ab.
16	Existenz DPE auf eGK prüfen
	Die Prüfung, ob ein DPE auf der eGK existiert, erfolgt implizit in 17. In 17 werden alle Daten aus der Datei `EF.DPE` der eGK gelesen. Das Informationselement `Länge DPE` enthält die Größe (Anzahl Oktette) des im Informationselement `DPE` gespeicherten DPE. Nur wenn ein Wert für dieses Informationselement gesetzt ist und dieser ungleich ´00 00´ ist, existiert ein DPE auf der eGK.

17	DPE von eGK lesen	
17.1	`TUC_KON_202 „LeseDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 1B´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4408´
	`offset`	-
	`length`	-
	Beschreibung	
	Es werden die Daten aus beiden Informationselementen (`Länge DPE` und `DPE`) der Datei `EF.DPE` der eGK gelesen. Tritt dabei ein Fehler auf, bricht die Operation mit Fehler 111 ab.	
17.2	`NFDM:checkSize`	
	Eingangsdaten	
	In 17.1 aus der Datei `EF.DPE` der eGK gelesene Daten (die beiden Informationselemente `Länge DPE` und `DPE`)	
	Beschreibung	
	Es wird das Informationselement `Länge DPE` der Eingangsdaten als Größe des DPE (Anzahl Oktette) ausgewertet. Ist die Größe ´00 00´, bedeutet dies, es existiert kein DPE auf der eGK. In diesem Fall bricht die Operation mit Fehler 5121 ab.	
17.3	`NFDM:extractDpe`	
	Eingangsdaten	
	In 17.1 aus der Datei `EF.DPE` der eGK gelesene Daten (die beiden Informationselemente `Länge DPE` und `DPE`)	
	Beschreibung	
	Die dem Informationselement `Länge DPE` folgende und der in 17.2 ausgewerteten Größe entsprechende Anzahl Oktette wird als DPE zur Weiterverarbeitung extrahiert. Tritt dabei ein Fehler auf, bricht die Operation mit Fehler 111 ab.	
~~**16**~~	~~Zugriffsprotokolleintrag auf eGK schreiben~~	
	~~Identisch zu 12 von ReadNFD (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)~~	
18	DPE dekomprimieren	
	`NFDM:decompress`	
	Eingangsdaten	
	Der in 17.3 extrahierte DPE	
	Beschreibung	
	Der DPE wird dekomprimiert. Tritt dabei ein Fehler auf, bricht die Operation mit Fehler 5106 ab.	

19	DPE gegen [DPE_Document.xsd] validieren
	`NFDM:validateDocument`
	Eingangsdaten
	Der in 18 dekomprimierte DPE
	Beschreibung
	Der DPE wird gegen das XML-Schema [DPE_Document.xsd] validiert. Ergibt die Validierung, dass der NFD entweder nicht wohlgeformt oder nicht valide zum Schema ist, so bricht die Operation mit Fehler 5114 ab.
20	DPE kodieren
	`NFDM:encode`
	Eingangsdaten
	Der in 19 validierte DPE
	Beschreibung
	Der DPE wird base64-kodiert. Tritt dabei ein Fehler auf, bricht die Operation mit Fehler 5109 ab.
21	Response mit gültigen Antwortparametern zusammenstellen
	`NFDM:prepareResponse`
	Eingangsdaten
	In ~~18 validierter~~ 20 base64-kodierter DPE und ggf. von den Basisdiensten des Konnektors erhaltene Warnings
	Beschreibung
	Zusammenstellung einer gültigen Response (Rückgabe und Statusrückmeldung) gemäß Tabelle „Tab_FM_NFDM_015 – Operation ReadDPE“

6.2.1.2.2 WriteDPE

Tabelle 5: Tab_FM_NFDM_029 – Umsetzung Ablaufaktivitäten WriteDPE

1 - 3	Identisch zu 1-3 von `ReadDPE` (s. TabelleTab_FM_NFDM_028 – Umsetzung Ablaufaktivitäten `ReadDPE`)

4	Sperrung Gesundheitsanwendung auf eGK prüfen	
4.1	`TUC_KON_026 „Liefere CardSession“`	
	Eingangsdaten	
	`mandantId`	`Context.MandantId`
	`clientSystemId`	`Context.ClientSystemId`
	`cardHandle`	`EhcHandle`
	`userId`	-
	Beschreibung	
	Für die eGK ist die Sitzung zu ermitteln. Diese wird für den Aufruf des TUCs im nächsten Teilschritt benötigt.	
4.2	`TUC_KON_018 „eGK-Sperrung prüfen“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`checkHcaOnly`	false
	Beschreibung	
	Über den TUC wird geprüft, ob die Gesundheitsanwendung der eGK, also der Ordner `DF.HCA` deaktiviert (= gesperrt) ist und ob das Zertifikat C.CH.AUT der eGK zeitlich gültig und nicht gesperrt ist. Der Aufruf des TUC schließt die Gültigkeitsprüfung der eGK aus Schritt 10 mit ein. Ist die Gesundheitsanwendung gesperrt, bricht die Operation mit Fehler 114 ab. Ist das Zertifikat nicht gültig (Ergebnis der Offline-Prüfung „ungültig), bricht die Operation mit Fehler 107 ab. Ist das Zertifikat gesperrt (Sperrstatus = „gesperrt“), bricht die Operation mit Fehler 106 ab.	
5	Version der eGK prüfen	
	Identisch zu 5 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten `ReadNFD`“)	
6	Berechtigungsregel ermitteln	
6.1	Identisch zu 6.1 von `ReadDPE` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten `ReadNFD`)	
6.2	`NFDM:getAccessRule`	
	Eingangsdaten	
	Ggf. in 6.1 ermittelter PIN-Status	
	Beschreibung	
	Es wird die Berechtigungsregel gemäß Berechtigungstabelle ermittelt.	
Tritt in diesem Schritt ein Fehler auf, bricht die Operation mit Fehler 5011 ab.		
7 - 9	Identisch zu 7-9 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten `ReadNFD`“)	
10	Gültigkeit der eGK prüfen	
	Erfolgt implizit bereits durch Aufruf von TUC_KON_018 in Schritt 4.2	
~~**11**~~	~~Autorisierung des Versicherten mittels PIN-Verifikation einholen~~	
~~Falls Berechtigungsregel für die fachliche Rolle eine PIN-Verifikation fordert~~		

	~~TUC_KON_012 „PIN verifizieren“~~	
	~~**Eingangsdaten**~~	
	~~cardSession~~	~~In 4.1 ermittelte Kartensitzung der eGK~~
	~~workplaceID~~	~~Context.WorkplaceID~~
	~~pinRef~~	~~MRPIN.DPE~~
	~~actionName~~	~~Wert von actionName für diese Operation gemäß Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe~~
	~~verificationType~~	~~Sitzung~~
	~~**Beschreibung**~~	
	~~Es wird die PIN für den schreibenden Zugriff auf den DPE auf der eGK verifiziert. Dabei wird der fachliche Akteur am Display des Kartenterminals aufgefordert, die entsprechende PIN einzugeben (Terminalanzeigen s. Tabelle „Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe), falls er dies nicht bereits im Rahmen der Kartensitzung getan hat. Die PIN-Eingabe erfolgt über das PIN-Pad des Kartenterminals.~~ ~~Tritt hier ein Fehler auf, bricht die Operation mit Fehler 5019 ab.~~	
~~**12**~~	~~DPE-Anwendung der eGK auf Sichtbarkeit prüfen~~	
	~~Die Prüfung, ob die DPE-Anwendung auf der eGK verborgen ist, erfolgt implizit in 19.~~ ~~TUC_KON_203 „SchreibeDatei“ gibt beim Versuch, den deaktivierten Ordner DF.DPE der eGK zu selektieren, um in die darin befindliche Datei EF.StatusDPE zu schreiben, den Code ´62 83´ des Betriebssystems der eGK zurück, woraufhin die Operation mit Fehler 5120 abbricht.~~	
11	DPE dekodieren	
	`NFDM:decode`	
	Eingangsdaten	
	Der Wert des Aufrufparameters `DPEDocument`	
	Beschreibung	
	Der base64-kodierte DPE wird dekodiert. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5107 ab.	
12	DPE gegen [DPE_Document.xsd] validieren	
	`NFDM:validateDocument`	
	Eingangsdaten	
	Der in 11 dekodierte DPE	
	Beschreibung	
	Der DPE wird gegen das XML-Schema [DPE_Document.xsd] validiert. Ergibt die Validierung, dass der NFD entweder nicht wohlgeformt oder nicht valide zum Schema ist, so bricht die Operation mit Fehler 5114 ab.	
13	Versicherten-ID des DPE prüfen	
13.1	`NFDM:extractDpeInsurantId`	
	Eingangsdaten	
	Der in 12 validierte DPE	
	Beschreibung	
	Die Versicherten-ID (Wert des Elements `/DPEDocument/Persönliche_Erklärungen/DPE_Versicherter/Versicherter/Versicherten_ID`) wird aus dem DPE extrahiert.	

13.2	TUC_KON_034 „Zertifikatsinformationen extrahieren“	
	Eingangsdaten	
	cardSession	In 4.1 ermittelte Kartensitzung der eGK
	qes	false
	Beschreibung	
	Durch den TUC-Aufruf wird das Zertifikat C.CH.AUT von der eGK gelesen und sowohl das Zertifikat als auch der Wert des im folgenden Schritt benötigten SubjectDN an das Fachmodul zurückgeliefert. Die Struktur des SubjectDN ist in [gemSpec_PKI#5.1.2] und [gemSpec_PKI#5.1.3.1] definiert.	
13.3	NFDM:extractCertInsurantId	
	Eingangsdaten	
	Der in 13.2 gelesene SubjectDN des in 13.2 gelesenen Zertifikats	
	Beschreibung	
	Aus SubjectDN wird die Versicherten-ID im Feld mit dem Namen organizationalUnitName extrahiert. *Anmerkung: Es gibt zwei organizationalUnitName-Felder. Das zehnstellige, alphanumerische Feld beinhaltet die Versicherten-ID (unveränderbarer Teil der Krankenversichertennummer), das andere, neunstellige numerische Feld, das Institutionskennzeichen der Krankenversichertennummer (s. [gemSpec_PKI#5.1.3.1]).*	
13.4	NFDM:checkInsurantIdsForEquality	
	Eingangsdaten	
	In 13.1 aus dem DPE extrahierte Versicherten ID und die in 13.3 aus dem in 13.2 gelesenen Zertifikat extrahierte Versicherten-ID	
	Beschreibung	
	Die beiden extrahierten Versicherten-IDs werden auf Gleichheit getestet. Sind die beiden IDs nicht gleich, bricht die Operation mit Fehler 5108 ab.	
14	DPE komprimieren	
	NFDM:compress	
	Eingangsdaten	
	Der in 12 validierte DPE	
	Beschreibung	
	Der in 12 validierte DPE wird komprimiert. Tritt in diesem Schritt ein Fehler auf, bricht die Operation mit Fehler 5110 ab.	
15	Zugriffsprotokolleintrag auf eGK G 2.0 schreiben	
	Identisch zu 10 von ReadNFD (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)	
16	Autorisierung des Versicherten mittels PIN-Verifikation einholen	
Falls Berechtigungsregel für die fachliche Rolle eine PIN-Verifikation fordert		
	TUC_KON_012 „PIN verifizieren“	
	Eingangsdaten	
	cardSession	In 4.1 ermittelte Kartensitzung der eGK
	workplaceID	Context.WorkplaceID
	pinRef	MRPIN.DPE

	`actionName`	Wert von actionName für diese Operation gemäß Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe
	`verificationType`	Sitzung
	Beschreibung	
	Es wird die PIN für den schreibenden Zugriff auf den DPE auf der eGK verifiziert. Dabei wird der fachliche Akteur am Display des Kartenterminals aufgefordert, die entsprechende PIN einzugeben (Terminalanzeigen s. Tabelle „Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe), falls er dies nicht bereits im Rahmen der Kartensitzung getan hat. Die PIN-Eingabe erfolgt über das PIN Pad des Kartenterminals. Tritt hier ein Fehler auf, bricht die Operation mit Fehler 5019 ab.	
17	Zugriffsprotokolleintrag auf eGK schreiben	
	Identisch zu 12 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten ReadNFD“)	
18	DPE-Anwendung der eGK auf Sichtbarkeit prüfen	
	Die Prüfung, ob die DPE-Anwendung auf der eGK verborgen ist, erfolgt implizit in 19. `TUC_KON_203 „ReadNFD“` gibt beim Versuch, den deaktivierten Ordner `DF.DPE` der eGK zu selektieren, um in die darin befindliche Datei `EF.StatusDPE` zu schreiben, den Code ´62 83´ des Betriebssystems der eGK zurück, woraufhin die Operation mit Fehler 5120 abbricht.	
19	DPE-Status-Flag auf eGK setzen	
	`TUC_KON_203 „SchreibeDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 18´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4408´
	`offset`	0
	`length`	1
	`dataToBeWritten`	„1“
	Beschreibung	
	Zur „Transaktionssicherung“ wird der Wert des Informationselements `Status` der Datei `EF.StatusDPE` der eGK vor Beginn des Schreibvorgangs des DPE auf „1“ gesetzt. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode ´62 83´ der eGK zurück, bricht die Operation mit Fehler 5120 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 112 ab.	

20	Größe des DPE auf eGK schreiben
20.1	`NFDM:determineSize`
	Eingangsdaten
	Der in 14 komprimierte DPE
	Beschreibung
	Die Größe (Anzahl Oktette) des DPE wird bestimmt.
20.2	Das Schreiben der in 20.1 ermittelten Größe des DPE auf die eGK erfolgt zusammen mit dem Schreiben des DPE in 21.

21	DPE auf eGK schreiben	
21.1	`NFDM:concatenate`	
	Eingangsdaten	
	DPE und die in 20.1 ermittelte Größe (Anzahl Oktette) des DPE	
	Beschreibung	
	Die in 20.1 ermittelte Größenangabe wird konkateniert mit dem an 21.1 übergebenen DPE. Die Struktur entspricht [gemSpec_eGK_Fach_NFDM#3.1]. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 112 ab.	
21.2	`TUC_KON_203 „SchreibeDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 1B´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4408´
	`offset`	-
	`length`	-
	`dataToBeWritten`	In 21.1 konkatenierte Oktettkette
	Beschreibung	
	Die in 21.1 konkatenierte Oktettkette (Größenangabe und DPE) wird auf die eGK in die Datei `EF.DPE` geschrieben. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. Hierbei wird die Größe (Anzahl Oktette) des DPE geprüft. Ist die Größe des DPE größer als der in der Datei `EF.DPE` entsprechend des Objektsystems der eGK zur Verfügung stehende Speicherplatz, liefert der TUC den Fehler 4247. In diesem Fall wird Schritt 22 ausgeführt und die Operation mit dem Fehler 5113 abgebrochen. In allen anderen Fehlerfällen bricht die Operation mit Fehler 112 ab.	
22	DPE-Status-Flag auf eGK zurücksetzen	
Falls die Größenprüfung beim Aufruf von `TUC_KON_203 "SchreibeDatei"` in 21.2 mit Fehler 4247 endete.		
22.1	`TUC_KON_203 „SchreibeDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 18´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	
	`folder`	´D276 0001 4408´

	`offset`	0
	`length`	1
	`dataToBeWritten`	„0“
	Beschreibung	
	Mit Beendigung des Schreibvorgangs des DPE auf die eGK wird das DPE-Status-Flag (Wert des Informationselements `Status` der Datei `EF.StatusDPE` der eGK) wieder zurück auf „0“ gesetzt. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 112 ab.	
22.2	Die Operation bricht mit dem Fehler 5113 ab.	
23	DPE-Zeitstempel auf eGK aktualisieren	
23.1	`TUC_KON_351 „Liefere Systemzeit“`	
	Eingangsdaten	
	Keine	
	Beschreibung	
	Der TUC liefert die aktuelle Systemzeit des Konnektors. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 112 ab.	
23.2	`NFDM:formatSystemTime`	
	Eingangsdaten	
	Im vorherigen Teilschritt ermittelte Systemzeit	
	Beschreibung	
	Die Systemzeit wird für das Schreiben in das Informationselement `Timestamp` der Datei `EF.StatusDPE` der eGK gemäß [gemSpec_eGK_Fach_NFDM#3.2] formatiert (14 Oktette; YYYYMMDDhhmmss). Das eigentliche Schreiben des DPE-Zeitstempels in das Informationselement `Timestamp` der Datei `EF.StatusDPE` der eGK erfolgt aus Performancegründen in 25.2. Dort wird die Oktettkette zur Befüllung der Datei `EF.StatusDPE` als Ganzes in die Datei `EF.StatusDPE` der eGK geschrieben. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 112 ab.	
24	Versionsnummer DPE-Speicherstruktur der eGK auf eGK aktualisieren	
	Das Aktualisieren der Versionsnummer erfolgt implizit im nächsten Schritt. Dort wird die Oktettkette zur Befüllung der Datei `EF.StatusDPE` als Ganzes in die Datei `EF.StatusDPE` auf der eGK geschrieben.	
25	DPE-Status-Flag auf eGK zurücksetzen	
25.1	`NFDM:concatenate`	
	Eingangsdaten	
	In 23.2 formatierter DPE-Zeitstempel, Versionsnummer der DPE-Speicherstruktur der eGK, gemäß derer der DPE auf die eGK geschrieben wird.	
	Beschreibung	
	Die Oktettkette für den DPE-Status-Container wird gemäß [gemSpec_eGK_Fach_NFDM#3.2] konkateniert, wobei das Informationselement `Version_XML` mit 5 Oktetten des Wertes ´00´ zu befüllen ist und das Informationselement `Status` den Wert „0“ erhält. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 112 ab.	
25.2	`TUC_KON_203 „SchreibeDatei“`	
	Eingangsdaten	

	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 18´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4408´
	`offset`	
	`length`	
	`dataToBeWritten`	In 25.1 konkatenierte Oktettkette
	Beschreibung	
	Mit Beendigung des Schreibvorgangs des DPE auf die eGK wird das DPE-Status-Flag (Wert des Informationselements `Status` der Datei `EF.StatusDPE` der eGK) wieder zurück auf „0“ gesetzt und der DPE-Zeitstempel sowie die Versionsnummer der DPE-Speicherstruktur der eGK gemäß [gemSpec_eGK_Fach_NFDM#3.2] aktualisiert. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 112 ab.	
24	~~Zugriffsprotokolleintrag auf eGK schreiben~~	
	~~Identisch zu 16 von `ReadNFD` (s. Tabelle „Tab_FM_NFDM_025 – Umsetzung Ablaufaktivitäten `ReadNFD`“)~~	
26	Response mit gültigen Antwortparametern zusammenstellen	
	`NFDM:prepareResponse`	
	Eingangsdaten	
	Ggf. von den Basisdiensten des Konnektors erhaltene Warnings	
	Beschreibung	
	Zusammenstellung einer gültigen Response (Rückgabe und Statusrückmeldung) gemäß Tabelle „Tab_FM_NFDM_017 – Operation `WriteDPE`“	

6.2.1.2.3 EraseDPE

Tabelle 6: Tab_FM_NFDM_030 – Umsetzung Ablaufaktivitäten `EraseDPE`

1-9	Übergreifende Erfolgsbedingungen prüfen
	Identisch zu 1-9 von `WriteDPE` (s. Tabelle „Tab_FM_NFDM_029 – Umsetzung Ablaufaktivitäten `WriteDPE`“)
10	Zugriffsprotokolleintrag auf eGK G 2.0 schreiben
	Identisch zu 10 von `ReadDPE` (s. Tabelle „Tab_FM_NFDM_028 – Umsetzung Ablaufaktivitäten `ReadDPE`“)

11	Autorisierung des Versicherten mittels PIN-Verifikation einholen	
Falls Berechtigungsregel für die fachliche Rolle eine PIN-Verifikation fordert		
	`TUC_KON_012 „PIN verifizieren“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`workplaceID`	`Context.WorkplaceID`
	`pinRef`	MRPIN.DPE
	`actionName`	Wert von actionName für diese Operation gemäß Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe
	`verificationType`	Sitzung
	Beschreibung	
	Es wird die PIN für den löschenden Zugriff auf den DPE auf der eGK verifiziert. Dabei wird der fachliche Akteur am Display des Kartenterminals aufgefordert, die entsprechende PIN einzugeben (Terminalanzeigen s. Tabelle „Tab_FM_NFDM_036 – Anwendungs-Parameter für PIN-Eingabe“), falls er dies nicht bereits im Rahmen der Kartensitzung getan hat. Die PIN-Eingabe erfolgt über das PIN Pad des Kartenterminals. Tritt hier ein Fehler auf, bricht die Operation mit Fehler 5019 ab.	
12	Zugriffsprotokolleintrag auf eGK schreiben	
	Identisch zu 12 von `ReadDPE` (s. Tabelle „Tab_FM_NFDM_028 – Umsetzung Ablaufaktivitäten `ReadDPE`“)	
13	DPE-Anwendung der eGK auf Sichtbarkeit prüfen	
	Die Prüfung, ob die DPE-Anwendung verborgen ist, erfolgt implizit im nächsten Schritt. `TUC_KON_202 „LeseDatei“` gibt beim Versuch, die verborgene (deaktivierte) Anwendung `DF.DPE` der eGK zu selektieren, um die Versionsnummer der DPE-Speicherstruktur der eGK aus dem Informationselement Status der Datei `EF.StatusDPE` der eGK zu lesen, den Code ´62 83´ des Betriebssystems der eGK zurück, woraufhin die Operation mit Fehler 5120 abbricht.	
14	Version der DPE-Speicherstruktur der eGK prüfen	
14.1	`TUC_KON_202 „LeseDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 18´
	`sfid`	-
	`folder`	´D276 0001 4408´
	`offset`	20
	`length`	5
	Beschreibung	
	Es wird das Informationselement `Version_Speicherstruktur` der Datei `EF.StatusDPE` der eGK ausgelesen. Gibt der `TUC_KON_202 „LeseDatei“` den Fehlercode '6283' der eGK zurück, bricht die Operation mit Fehler 5120 ab.	

14.2	NFDM:checkContainerVersion	
	Eingangsdaten	
	In 14.1 gelesener Wert des Informationselements Version_Speicherstruktur der Datei EF.StatusDPE der eGK.	
	Beschreibung	
	Es wird überprüft, ob dem Fachmodul die in 14.1 gelesene Versionsnummer der DPE-Speicherstruktur der eGK bekannt ist. Ist dies nicht der Fall, bricht die Operation mit Fehler 5104 ab.	
15	DPE-Status-Flag auf eGK setzen	
	TUC_KON_203 „SchreibeDatei“	
	Eingangsdaten	
	cardSession	In 4.1 ermittelte Kartensitzung der eGK
	fileIdentifier (optional/verpflichtend, wenn kein sfid angegeben ist)	´D0 18´
	sfid (optional/verpflichtend, wenn kein fileIdentifier angegeben ist)	-
	folder	´D276 0001 4408´
	offset	0
	length	1
	dataToBeWritten	1
	Beschreibung	
	Zur „Transaktionssicherung“ wird das Status-Flag des DPE-Status-Containers (Wert des Informationselements Status der Datei EF.StatusDPE der eGK) vor Beginn des Löschvorgangs des DPE auf „1“ gesetzt. Gibt der TUC_KON_203 „SchreibeDatei“ den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 5112 ab.	
16	Größenangabe DPE auf eGK auf 0 setzen	
	Das Setzen der Größenangabe für den DPE auf der eGK auf 0 erfolgt implizit in 17.	

17	DPE von eGK löschen	
	`TUC_KON_204 „LöscheDateiInhalt“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 1B´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4408´
	`offset`	-
	Beschreibung	
	Der Inhalt der Datei `EF.DPE` auf der eGK wird durch Oktette mit dem Wert ´00´ (NULL) überschrieben. Dadurch wird einerseits der Inhalt des Informationselements `Länge DPE` mit ´00 00´ überschrieben und zudem die Daten des im Informationselement `DPE` gespeicherten DPE „gelöscht“, d. h. mit ´00´ (NULL) überschrieben. Gibt der `TUC_KON_204 „LöscheDateiInhalt“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 5112 ab.	
18	DPE_Zeitstempel auf eGK aktualisieren	
18.1	`TUC_KON_351 „Liefere Systemzeit“`	
	Eingangsdaten	
	Keine	
	Beschreibung	
	Der TUC liefert die aktuelle Systemzeit des Konnektors Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5112 ab.	
18.2	`NFDM:formatSystemTime`	
	Eingangsdaten	
	Im vorherigen Teilschritt ermittelte Systemzeit.	
	Beschreibung	
	Die Systemzeit wird für das Schreiben in das Informationselement `Timestamp` der Datei `EF.StatusDPE` der eGK gemäß [gemSpec_eGK_Fach_NFDM#3.2] formatiert (14 Oktette; YYYYMMDDhhmmss). Das eigentliche Schreiben des DPE-Zeitstempels in die Datei `EF.StatusDPE` der eGK erfolgt aus Performancegründen in 20.2. Dort wird die Oktettkette aus DPE-Status-Flag und DPE-Zeitstempel als Ganzes in die Datei `EF.StatusDPE` der eGK geschrieben. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5112 ab.	
19	Versionsnummer DPE-Speicherstruktur der eGK auf eGK aktualisieren	
	Das Aktualisieren der Versionsnummer der DPE-Speicherstruktur der eGK erfolgt implizit im nächsten Schritt. Dort wird die Oktettkette zur Befüllung des DPE-Status-Containers als Ganzes in die Datei `EF.StatusDPE` der eGK geschrieben.	

20	DPE-Status-Flag auf eGK zurücksetzen	
20.1	`NFDM:concatenate`	
	Eingangsdaten	
	In 18.2 formatierter Zeitstempel, Versionsnummer der DPE-Speicherstruktur der eGK, gemäß derer auf die eGK geschrieben wird.	
	Beschreibung	
	Die Oktettkette für den DPE-Status-Container der eGK wird gemäß [gemSpec_eGK_Fach_NFDM#3.2] konkateniert, wobei das Informationselement `Version_XML` mit Oktetten des Wertes ´00´ zu befüllen ist und das Informationselement `Status` den Wert „0“ erhält. Tritt hierbei ein Fehler auf, bricht die Operation mit Fehler 5112 ab.	
20.2	`TUC_KON_203 „SchreibeDatei“`	
	Eingangsdaten	
	`cardSession`	In 4.1 ermittelte Kartensitzung der eGK
	`fileIdentifier` (optional/verpflichtend, wenn kein `sfid` angegeben ist)	´D0 18´
	`sfid` (optional/verpflichtend, wenn kein `fileIdentifier` angegeben ist)	-
	`folder`	´D276 0001 4408´
	`offset`	
	`length`	
	`dataToBeWritten`	In 20.1 konkatenierte Oktettkette
	Beschreibung	
	Mit Beendigung des Löschvorgangs des DPE auf der eGK wird das DPE-Status-Flag (Wert des Informationselements `Status` der Datei `EF.StatusDPE` der eGK) wieder zurück auf „0“ gesetzt und der DPE-Zeitstempel sowie die Versionsnummer der DPE-Speicherstruktur geschrieben. Gibt der `TUC_KON_203 „SchreibeDatei“` den Fehlercode 6581 der eGK zurück, bricht die Operation mit Fehler 5000 ab. In allen anderen Fehlerfällen bricht die Operation mit Fehler 5112 ab.	
~~**19**~~	~~Zugriffsprotokolleintrag auf eGK schreiben~~	
	~~Identisch zu 24 von `WriteDPE` (s. Tabelle „Tab_FM_NFDM_029 – Umsetzung Ablaufaktivitäten `WriteDPE`“)~~	
21	Response mit gültigen Antwortparametern zusammenstellen	
	`NFDM:prepareResponse`	
	Eingangsdaten	
	Ggf. von den Basisdiensten des Konnektors erhaltene Warnings	
	Beschreibung	
	Zusammenstellung einer gültigen Response (Rückgabe und Statusrückmeldung) gemäß Tabelle „Tab_FM_NFDM_020 – Operation `EraseDPE`“	

Änderungen in gemSysL_NFDM

4.2.3 Anwendungsfall „NFD auf eGK schreiben “ (NFDM-UC_100)

Tabelle 7: Anwendungsfallbeschreibung „NFD auf eGK schreiben

ID	NFDM-UC_100
Name	NFD auf eGK schreiben
Kurzbeschreibung	Das Fachmodul NFDM schreibt einen mit einer QES des Arztes versehenen NFD auf die eGK des Versicherten.
Initiierender Akteur	Berechtigter über PS
Vorbedingungen	Anwendungsfallübergreifende Vorbedingungen aus Kapitel 4.1 NFD ist valide gegen das Informationsmodell und enthält eine gültige QES. Der NFD ist mit einer mathematisch gültigen Signatur signiert, die auf einem QES-konformen (qualifizierten) Zertifikat beruht. Der Versicherte der eGK ist mit dem Versicherten des NFD identisch. Der NFD auf der eGK ist nicht verborgen. Der NFD ist nicht größer als der auf der eGK für seine Speicherung zur Verfügung stehende Speicherplatz.
Eingangsdaten	NFD mit zugehöriger QES des Arztes Aufrufkontext gemäß [gemKPT_Arch_TIP#4.2] Identifikator eGK Identifikator LE-Karte
Auslöser	Das PS ruft die Operation „WriteNFD“ an der externen Schnittstelle „I_NFD_Management“ des Fachmoduls NFDM auf.
Nachbedingungen	Der gültige NFD mit gültiger QES ist komprimiert auf der eGK im vorgesehen Container gespeichert. Der Zugriffsprotokolleintrag ist auf die eGK des Versicherten in den vorgesehenen Container geschrieben.
Ausgangsdaten	Status
Essentielle Aktivitäten	

Aktivität	Aufrufe TI-Plattform	Details
Sperrung Gesundheitsanwendung und Gültigkeit des AUT-Zertifikats der eGK prüfen	verify_eGK	
Version der eGK prüfen	read_Card_Data	Version von eGK lesen und prüfen
Berechtigungsregel ermitteln	get_PIN_Status	Berechtigungsregel gemäß Berechtigungsmatrix ermitteln
Freischaltung HBA/SMC-B prüfen	do_C2C	
Authentizität und Echtheit der beteiligten Karten durch C2C prüfen		
NFD gegen Infomodell validieren		
Signatur der NFD auf mathematische Gültigkeit prüfen		
Signaturzertifikat des NFD auf QES-Konformität prüfen		
Versicherten-ID des NFD prüfen	extract_card_data	Das Fachmodul prüft anhand des unveränderlichen Teils der KVNR, ob der Versicherte der eGK mit dem Versicherten im NFD identisch ist.
NFD komprimieren		
Zugriffsprotokolleintrag auf eGK schreiben	write_eGK_Protocol	Es erfolgt die Protokollierung des Zugriffs auf der eGK. Bei G2.0-Karten muss die Protokollierung vor einer Eingabe der PIN des Versicherten erfolgen.
Autorisierung des Versicherten mittels PIN-Verifikation einholen	verify_PIN	falls die Berechtigungsregel eine PIN-Verifikation fordert, PIN-Verifikation durchführen

Zugriffsprotokolleintrag auf eGK schreiben	write_eGK_Protocol	Es erfolgt die Protokollierung des Zugriffs auf der eGK. Bei G2.1-Karten erfolgt die Protokollierung nach einer eventuellen Eingabe der PIN des Versicherten. Es wird dann auch protokolliert, ob eine PIN-Eingabe stattgefunden hat.
NFD-Anwendung der eGK auf Sichtbarkeit prüfen	read_Card_Data	
Version der NFD-Speicherstrukturen der eGK prüfen		Version von eGK lesen und prüfen
~~**NFD gegen Infomodell validieren**~~		
~~**Signatur der NFD auf mathematische Gültigkeit prüfen**~~		
~~**Signaturzertifikat des NFD auf QES-Konformität prüfen**~~		
~~**Versicherten-ID des NFD prüfen**~~	~~extract_card_data~~	~~Das Fachmodul prüft anhand des unveränderlichen Teils der KVNR, ob der Versicherte der eGK mit dem Versicherten im NFD identisch ist.~~
~~**NFD komprimieren**~~		
Größe des NFD prüfen	write_Card_Data	.
NFD auf eGK schreiben		
~~**Zugriffsprotokolleintrag auf eGK schreiben**~~	~~write_eGK_Protocol~~	

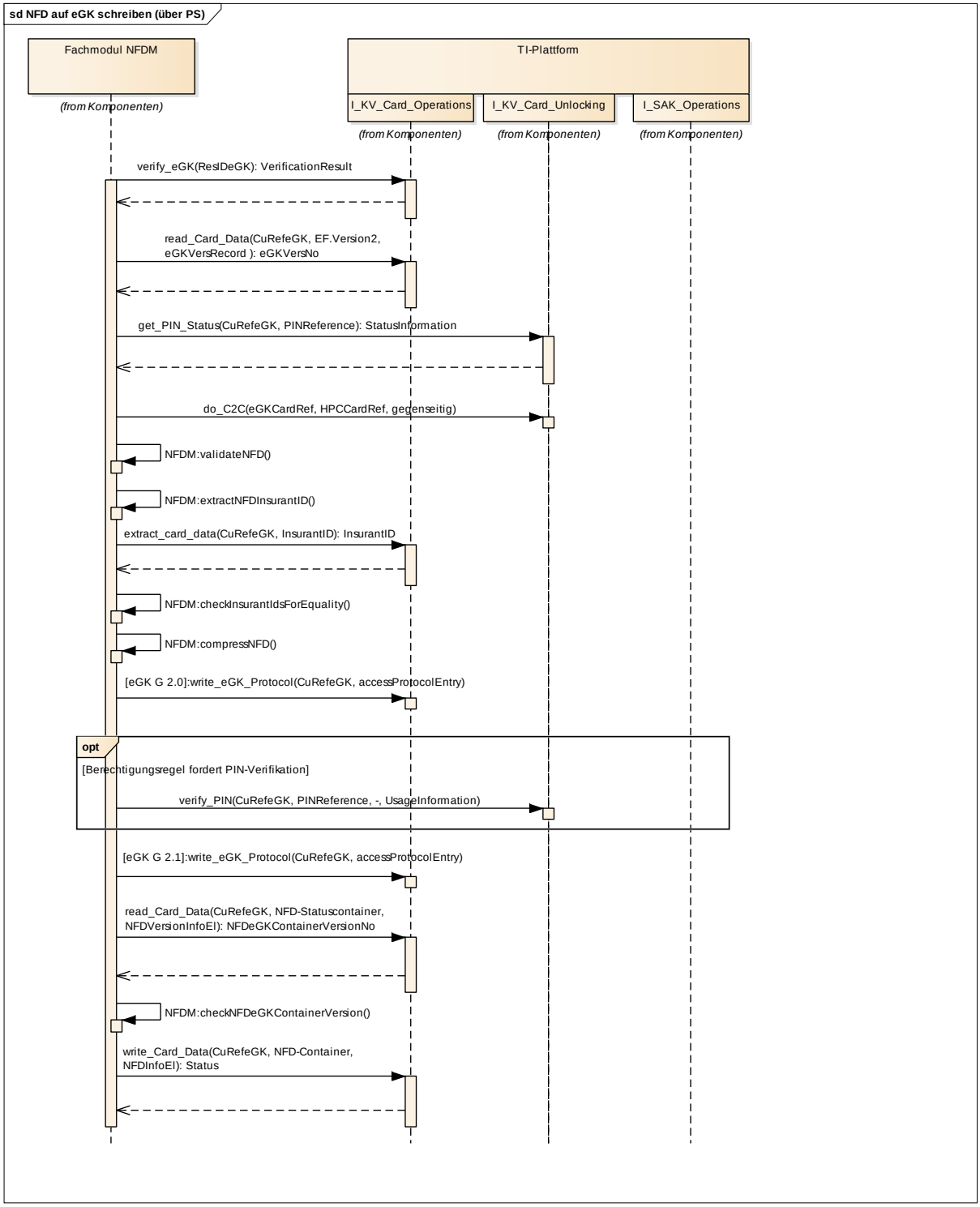

Abbildung 5: Sequenzdiagramm „NFD auf eGK schreiben“

4.2.4 Anwendungsfall: „NFD von eGK lesen “ (NFDM-UC_101)

Tabelle 8: Anwendungsfallbeschreibung „NFD von eGK lesen“

ID	NFDM-UC_101	
Name	NFDM von eGK lesen	
Kurzbeschreibung	Das Fachmodul NFDM liest einen mit einer QES eines Arztes versehenen NFD von der eGK des Versicherten.	
Initiierender Akteur	Berechtigter über PS	
Vorbedingungen	Anwendungsfallübergreifende Vorbedingungen aus Kapitel 4.1 Es ist ein komprimierter NFD auf der eGK gespeichert. Der auf der eGK gespeicherte NFD ist valide gegen das Infomodell. Der NFD auf der eGK ist nicht verborgen.	
Eingangsdaten	Notfallindikator Aktualisierungsindikator Aufrufkontext gemäß [gemKPT_Arch_TIP#4.2] Identifikator eGK Identifikator LE-Karte	
Auslöser	• Das PS ruft die Operation „ReadNFD“ an der externen Schnittstelle „I_NFD_Management“ des Fachmoduls NFDM auf.	
Nachbedingungen	Der NFD steht dem PS dekomprimiert zur weiteren Verarbeitung zur Verfügung. Der Zugriffsprotokolleintrag ist auf die eGK des Versicherten in den vorgesehenen Container geschrieben.	
Ausgangsdaten	NFD der eGK Status QES-Prüfprotokoll	
Essentielle Aktivitäten		
Aktivität	Aufrufe TI-Plattform	Details
Sperrung Gesundheitsanwendung der eGK prüfen	verify_eGK	
Version der eGK prüfen	read_Card_Data	Version von eGK lesen und prüfen

Berechtigungsregel ermitteln	get_PIN_Status	Berechtigungsregel gemäß Berechtigungsmatrix ermitteln
Berechtigung fachliche Rollen prüfen	get_Role	falls die Berechtigungsregel nicht alleine von der eGK durchsetzbar ist
Freischaltung HBA/SMC-B prüfen	do_C2C	
Authentizität und Echtheit der beteiligten Karten durch C2C prüfen		
Zugriffsprotokolleintrag auf eGK schreiben	write_eGK_Protocol	Es erfolgt die Protokollierung des Zugriffs auf der eGK.
Autorisierung des Versicherten mittels-PIN-Verifikation einholen	verify_PIN	falls die Berechtigungsregel eine PIN-Verifikation fordert, PIN-Verifikation durchführen
NFD-Anwendung der eGK auf Sichtbarkeit prüfen	read_Card_Data	
Version der NFD-Speicherstrukturen der eGK prüfen		
Existenz NFD auf eGK prüfen	read_Card_Data	
NFD von eGK lesen		
~~**Zugriffsprotokolleintrag auf eGK schreiben**~~	~~write_eGK_Protocol~~	~~Es erfolgt die Protokollierung des Zugriffs auf der eGK.~~
NFD dekomprimieren		
QES des NFD prüfen	verify_Document_QES	Ergibt die Prüfung keine gültige QES, darf der Anwendungsfall nicht abgebrochen werden. Der NFD ist in jedem Fall zurückzugeben inklusive des Prüfprotokolls.

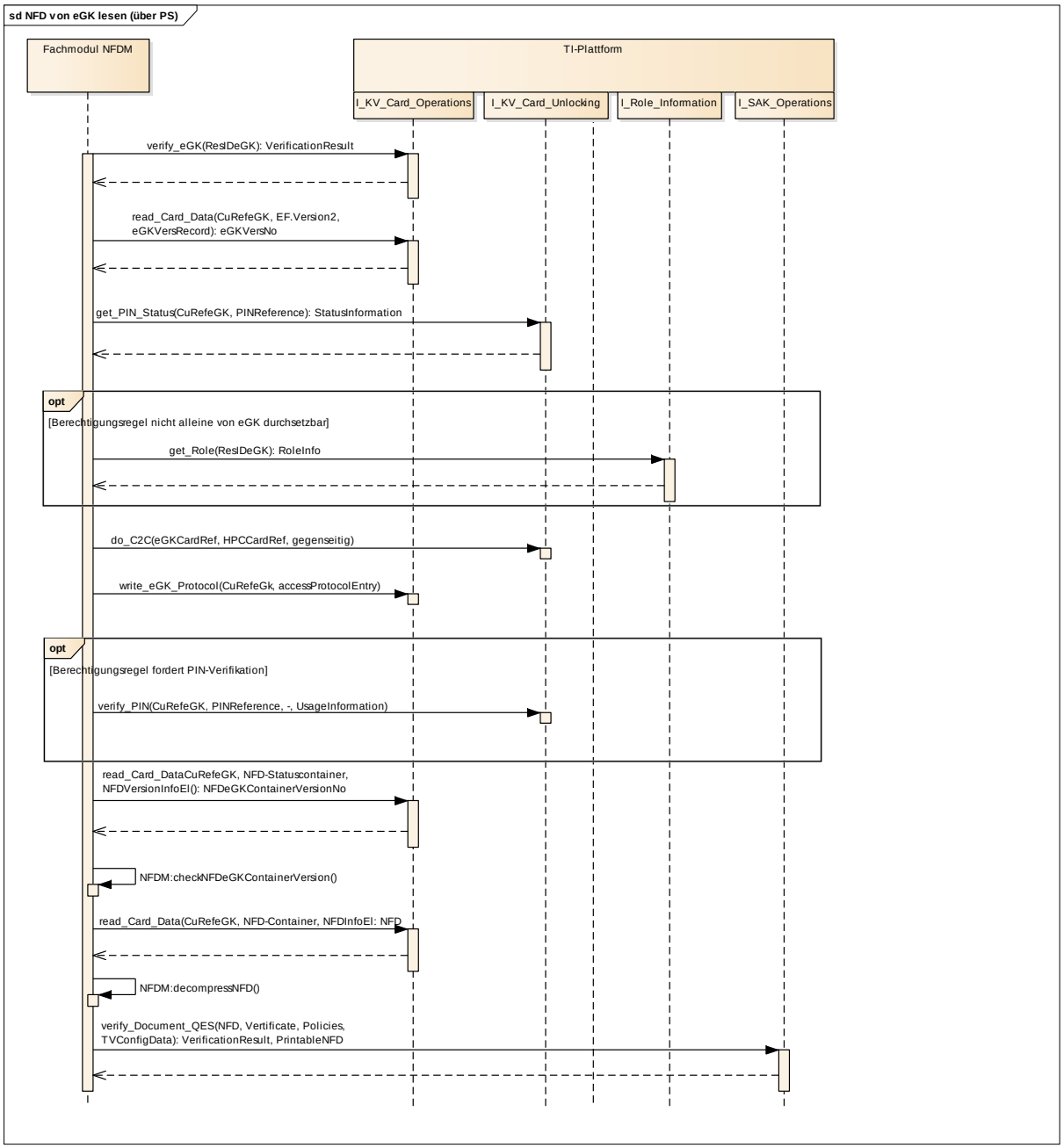

Abbildung 6: Sequenzdiagramm „NFD von eGK lesen“

4.2.5 Anwendungsfall: „NFD von eGK löschen “ (NFDM-UC_102)

Tabelle 9: Anwendungsfall „NFD von eGK löschen“

ID	NFDM-UC_102	
Name	NFD von eGK löschen	
Kurzbeschreibung	Das Fachmodul NFDM löscht den NFD des Versicherten von der eGK des Versicherten.	
Initiierender Akteur	Berechtigter über PS	
Vorbedingungen	Anwendungsfallübergreifende Vorbedingungen aus Kapitel 4.1 Es ist ein NFD auf der eGK gespeichert. Der NFD auf der eGK ist nicht verborgen.	
Eingangsdaten	Identifikator eGK Identifikator LE-Karte Aufrufkontext gemäß [gemKPT_Arch_TIP#4.2]	
Auslöser	• Das PS ruft die Operation „EraseNFD“ an der externen Schnittstelle „I_NFD_Management“ des Fachmoduls NFDM auf.	
Nachbedingungen	Es ist kein NFD mehr auf der eGK des Versicherten gespeichert. Der Zugriffsprotokolleintrag ist auf die eGK des Versicherten in den vorgesehenen Container geschrieben.	
Ausgangsdaten	Status	
Essentielle Aktivitäten		
Aktivität	Aufrufe TI-Plattform	Details
Sperrung Gesundheitsanwendung der eGK prüfen	verify_eGK	
Version der eGK prüfen	read_Card_Data	Version von eGK lesen und prüfen
Berechtigungsregel ermitteln	get_PIN_Status	Berechtigungsregel gemäß Berechtigungsmatrix ermitteln
Freischaltung HBA/SMC-B prüfen	do_C2C	

Authentizität und Echtheit der beteiligten Karten durch C2C prüfen		
Zugriffsprotokolleintrag auf eGK schreiben	write_eGK_Protocol	Es erfolgt die Protokollierung des Zugriffs auf der eGK.
Autorisierung des Versicherten mittels-PIN-Verifikation einholen	verify_PIN	falls die Berechtigungsregel eine PIN-Verifikation fordert, PIN-Verifikation durchführen
NFD-Anwendung der eGK auf Sichtbarkeit prüfen	read_Card_Data	
Version der NFD-Speicherstrukturen der eGK prüfen		Version von eGK lesen und prüfen
Existenz NFD auf eGK prüfen	read_Card_Data	
NFD von eGK löschen	erase_Card_Data	
~~**Zugriffsprotokolleintrag auf eGK schreiben**~~	~~write_eGK_Protocol~~	~~Es erfolgt die Protokollierung des Zugriffs auf der eGK.~~

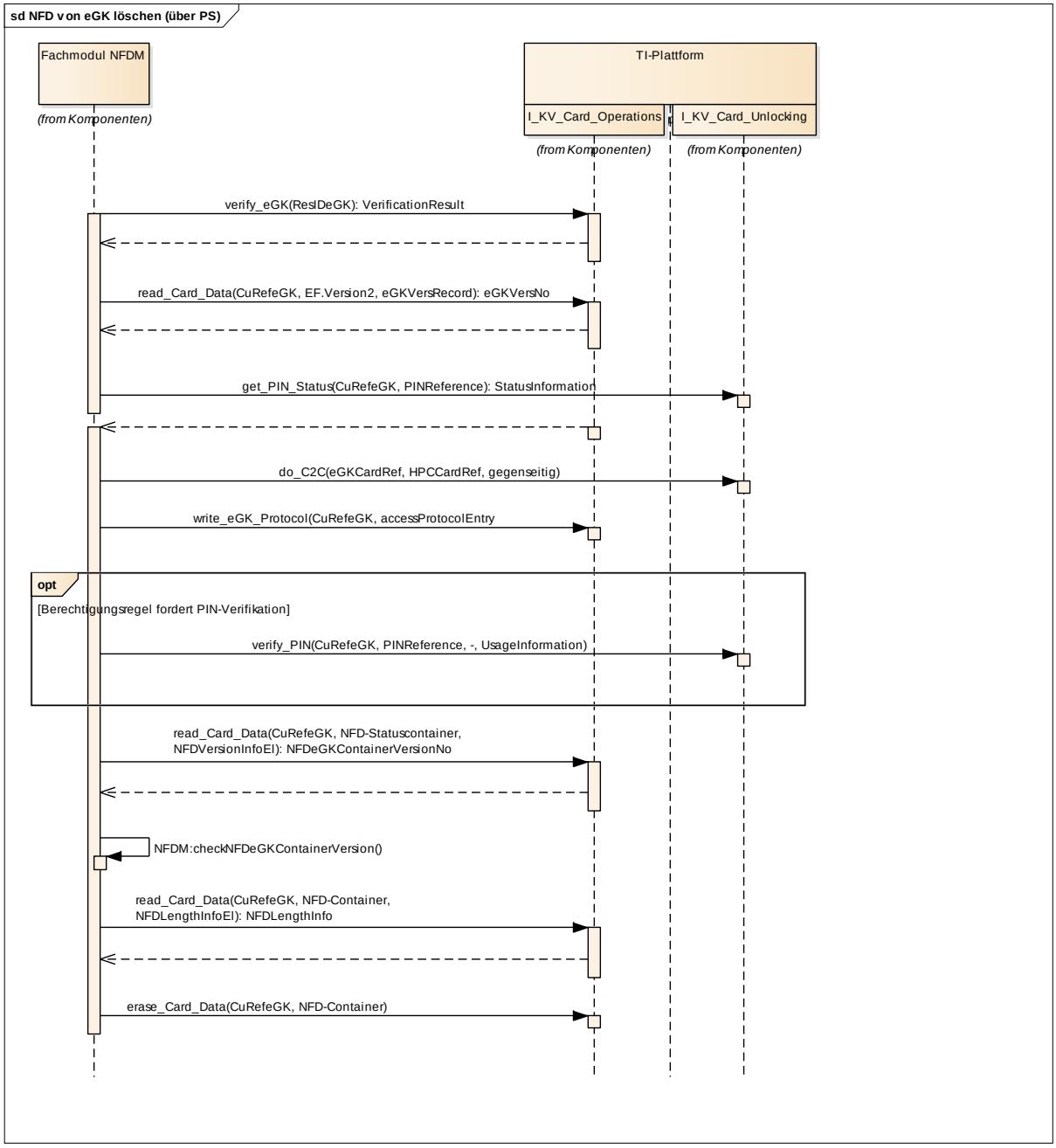

Abbildung 7: Sequenzdiagramm „NFD von eGK löschen“

4.3.3 Anwendungsfall „DPE auf eGK schreiben “ (NFDM-UC_200)

Tabelle 10: Anwendungsfall „DPE auf eGK schreiben“

ID	NFDM-UC_200	
Name	DPE auf eGK schreiben	
Kurzbeschreibung	Das Fachmodul NFDM schreibt den DPE des Versicherten auf die eGK des Versicherten.	
Initiierender Akteur	Berechtigter über PS	
Vorbedingungen	Anwendungsfallübergreifende Vorbedingungen aus Kapitel 4.1 DPE ist valide gegen das Informationsmodell Der Versicherte der eGK ist mit dem Versicherten des NFD identisch Der DPE auf der eGK ist nicht verborgen Der DPE ist nicht größer als der auf der eGK für seine Speicherung zur Verfügung stehende Speicherplatz	
Eingangsdaten	DPE Aufrufkontext gemäß [gemKPT_Arch_TIP#4.2] Identifikator eGK Identifikator LE-Karte	
Auslöser	• Das PS ruft die Operation „WriteDPE“ an der externen Schnittstelle „I_DPE_Management“ des Fachmoduls NFDM auf.	
Nachbedingungen	Der gültige DPE liegt komprimiert auf der eGK im vorgesehen Container vor. Der Zugriffsprotokolleintrag ist auf die eGK des Versicherten in den vorgesehenen Container geschrieben.	
Ausgangsdaten	Status	
Essentielle Aktivitäten		
Aktivität	Aufrufe TI-Plattform	Details
Sperrung Gesundheitsanwendung und Gültigkeit des AUT-Zertifikats der eGK prüfen	verify_eGK	

Version der eGK prüfen	read_Card_Data	Version von eGK lesen und prüfen
Berechtigungsregel ermitteln	get_PIN_Status	Berechtigungsregel gemäß Berechtigungsmatrix ermitteln
Freischaltung HBA/SMC-B prüfen	do_C2C	
Authentizität und Echtheit der beteiligten Karten durch C2C prüfen		
DPE gegen Infomodell validieren		
Versicherten-ID des DPE prüfen	extract_card_data	Das Fachmodul prüft anhand des unveränderlichen Teils der KVNR, ob der Versicherte der eGK mit dem Versicherten im NFD identisch ist.
DPE komprimieren		
Zugriffsprotokolleintrag auf eGK schreiben	write_eGK_Protocol	Es erfolgt die Protokollierung des Zugriffs auf der eGK. Bei G2.0-Karten muss die Protokollierung vor einer Eingabe der PIN des Versicherten erfolgen.
Autorisierung des Versicherten mittels PIN-Verifikation einholen	verify_PIN	falls die Berechtigungsregel eine PIN-Verifikation fordert, PIN-Verifikation durchführen
Zugriffsprotokolleintrag auf eGK schreiben	write_eGK_Protocol	Es erfolgt die Protokollierung des Zugriffs auf der eGK. Bei G2.1-Karten erfolgt die Protokollierung nach einer eventuellen Eingabe der PIN des Versicherten. Es wird dann auch protokolliert, ob eine PIN-Eingabe stattgefunden hat.
DPE-Anwendung der eGK auf Sichtbarkeit prüfen	read_Card_Data	
Version der DPE-Speicherstrukturen der eGK prüfen		Version von eGK lesen und prüfen

~~**DPE gegen Infomodell validieren**~~		
~~**Versicherten-ID des DPE prüfen**~~	~~extract_card_data~~	~~Das Fachmodul prüft anhand des unveränderlichen Teils der KVNR, ob der Versicherte der eGK mit dem Versicherten im NFD identisch ist.~~
~~**DPE komprimieren**~~		
Größe des DPE prüfen	write_Card_Data	
DPE auf eGK schreiben		
~~**Zugriffsprotokolleintrag auf eGK schreiben**~~	~~write_eGK_Protocol~~	~~Es erfolgt die Protokollierung des Zugriffs auf der eGK.~~

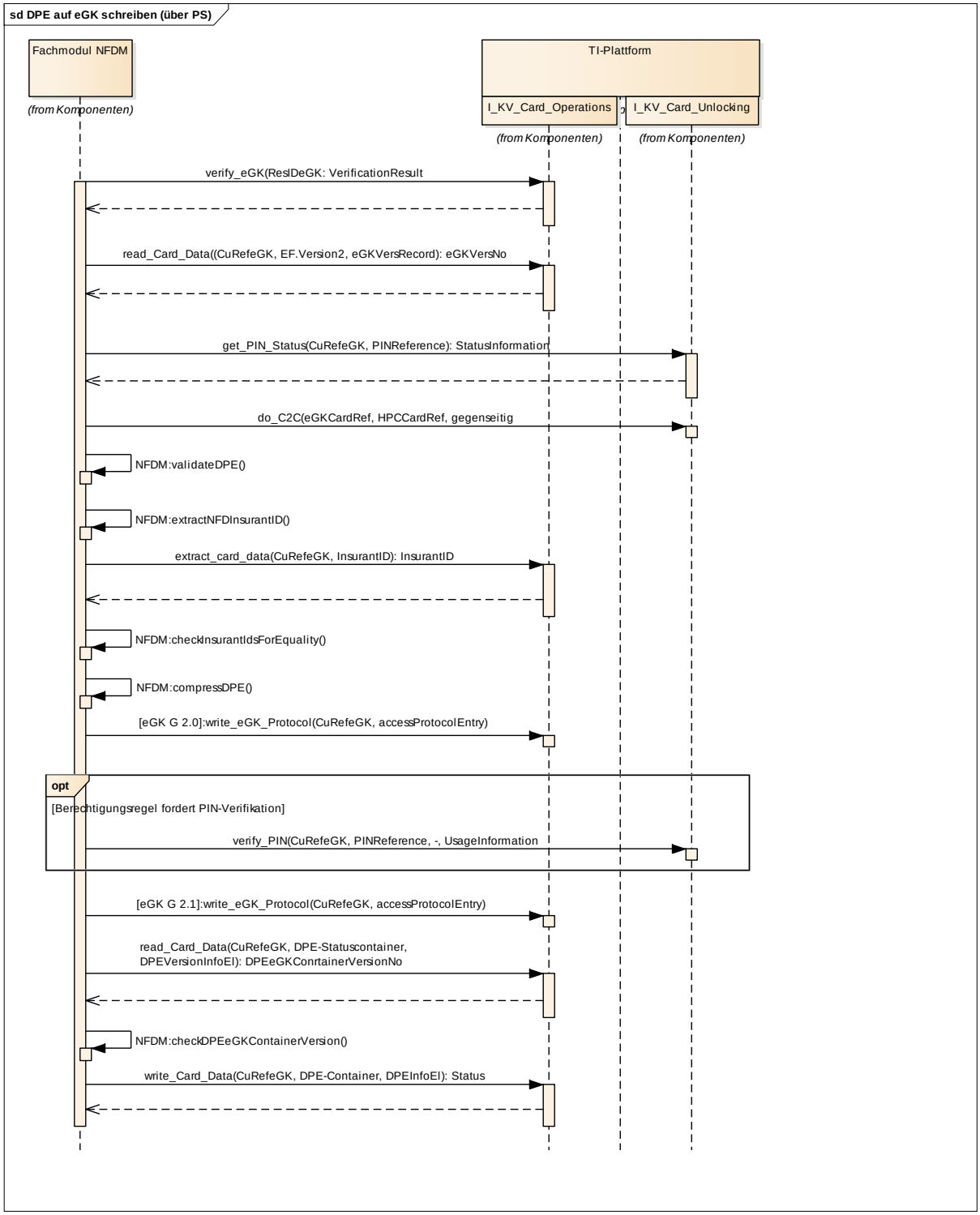

Abbildung 8: Sequenzdiagramm „DPE auf eGK schreiben“

4.3.4 Anwendungsfall „DPE von eGK lesen “ (NFDM-UC_201)

Tabelle 11: Anwendungsfall „DPE von eGK lesen“

ID	NFDM-UC_201	
Name	DPE von eGK lesen	
Kurzbeschreibung	Das Fachmodul NFDM liest den DPE von der eGK des Versicherten.	
Initiierender Akteur	Berechtigter über PS	
Vorbedingungen	Anwendungsfallübergreifende Vorbedingungen aus Kapitel 4.1 Es ist ein komprimierter DPE auf der eGK gespeichert. Der auf der eGK gespeicherte DPE ist valide gegen das Infomodell. Der DPE auf der eGK ist nicht verborgen.	
Eingangsdaten	Notfallindikator Aktualisierungsindikator Aufrufkontext gemäß [gemKPT_Arch_TIP#4.2] Identifikator eGK Identifikator LE-Karte	
Auslöser	• Das PS ruft die Operation „ReadDPE“ an der externen Schnittstelle „I_DPE_Management“ des Fachmoduls NFDM auf.	
Nachbedingung	Der DPE steht dem PS dekomprimiert zur weiteren Verarbeitung zur Verfügung. Der Zugriffsprotokolleintrag ist auf die eGK des Versicherten in den vorgesehenen Container geschrieben.	
Ausgangsdaten	DPE Status	
Essentielle Aktivitäten		
Aktivität	Aufrufe TI-Plattform	Details
Sperrung Gesundheitsanwendung der eGK prüfen	verify_eGK	

Version der eGK prüfen	read_Card_Data	Version von eGK lesen und prüfen
Berechtigungsregel ermitteln	get_PIN_Status	Berechtigungsregel gemäß Berechtigungsmatrix ermitteln
Berechtigung fachliche Rollen prüfen	get_Role	falls die Berechtigungsregel nicht alleine von der eGK durchsetzbar ist
Freischaltung HBA/SMC-B prüfen	do_C2C	
Authentizität und Echtheit der beteiligten Karten durch C2C prüfen		
Zugriffsprotokolleintrag auf eGK schreiben	write_eGK_Protocol	Es erfolgt die Protokollierung des Zugriffs auf der eGK.
Autorisierung des Versicherten mittels-PIN-Verifikation einholen	verify_PIN	falls die Berechtigungsregel eine PIN-Verifikation fordert, PIN-Verifikation durchführen
DPE-Anwendung der eGK auf Sichtbarkeit prüfen	read_Card_Data	
Version der DPE-Speicherstrukturen der eGK prüfen		
Existenz DPE auf eGK prüfen	read_Card_Data	
DPE von eGK lesen		
~~**Zugriffsprotokolleintrag auf eGK schreiben**~~	~~write_eGK_Protocol~~	~~Es erfolgt die Protokollierung des Zugriffs auf der eGK.~~
DPE dekomprimieren		
DPE gegen Infomodell validieren		

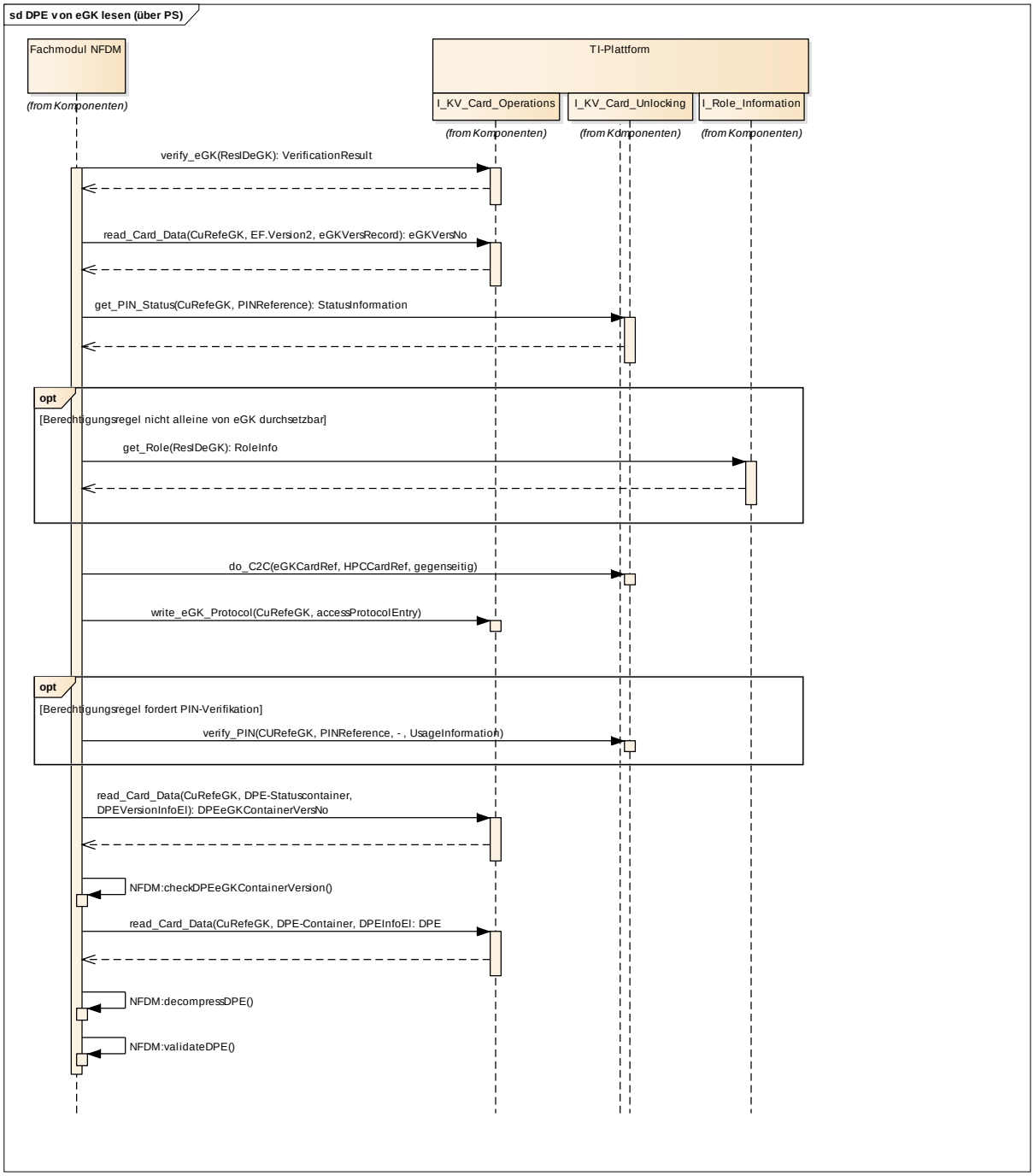

Abbildung 9: Sequenzdiagramm „DPE von eGK lesen“

4.3.5 Anwendungsfall „DPE von eGK löschen “ (NFDM-UC_202)

Tabelle 12: Anwendungsfall „DPE von eGK löschen“

ID	NFDM-UC_202	
Name	DPE von eGK löschen	
Kurzbeschreibung	Das Fachmodul NFDM löscht den DPE des Versicherten von dessen eGK.	
Initiierender Akteur	Berechtigter über PS	
Vorbedingungen	Anwendungsfallübergreifende Vorbedingungen aus Kapitel 4.1 Es ist ein DPE auf der eGK gespeichert. Der DPE auf der eGK ist nicht verborgen.	
Eingangsdaten	Identifikator eGK Identifikator LE-Karte Aufrufkontext gemäß [gemKPT_Arch_TIP#4.2]	
Auslöser	• Das PS ruft die Operation „EraseDPE“ an der externen Schnittstelle „I_DPE_Management“ des Fachmoduls NFDM auf.	
Nachbedingung	Es ist kein DPE mehr auf der eGK des Versicherten gespeichert. Der Zugriffsprotokolleintrag ist auf die eGK des Versicherten in den vorgesehenen Container geschrieben.	
Ausgangsdaten	Status- ggf. mit Fehlermeldung	
Essentielle Aktivitäten		
Aktivität	Aufrufe TI-Plattform	Details
Sperrung Gesundheitsanwendung der eGK prüfen	verify_eGK	
Version der eGK prüfen	read_Card_Data	Version von eGK lesen und prüfen
Berechtigungsregel ermitteln	get_PIN_Status	Berechtigungsregel gemäß Berechtigungsmatrix ermitteln
Freischaltung HBA/SMC-B prüfen	do_C2C	

Authentizität und Echtheit der beteiligten Karten durch C2C prüfen		
Zugriffsprotokolleintrag auf eGK schreiben	write_eGK_Protocol	Es erfolgt die Protokollierung des Zugriffs auf der eGK.
Autorisierung des Versicherten mittels-PIN-Verifikation einholen	verify_PIN	falls die Berechtigungsregel eine PIN-Verifikation fordert, PIN-Verifikation durchführen
DPE-Anwendung der eGK auf Sichtbarkeit prüfen	read_Card_Data	
Version der DPE-Speicherstrukturen der eGK prüfen		Version von eGK lesen und prüfen
Existenz DPE auf eGK prüfen	read_Card_Data	
DPE von eGK löschen	erase_Card_Data	
~~**Zugriffsprotokolleintrag auf eGK schreiben**~~	~~write_eGK_Protocol~~	~~Es erfolgt die Protokollierung des Zugriffs auf der eGK.~~

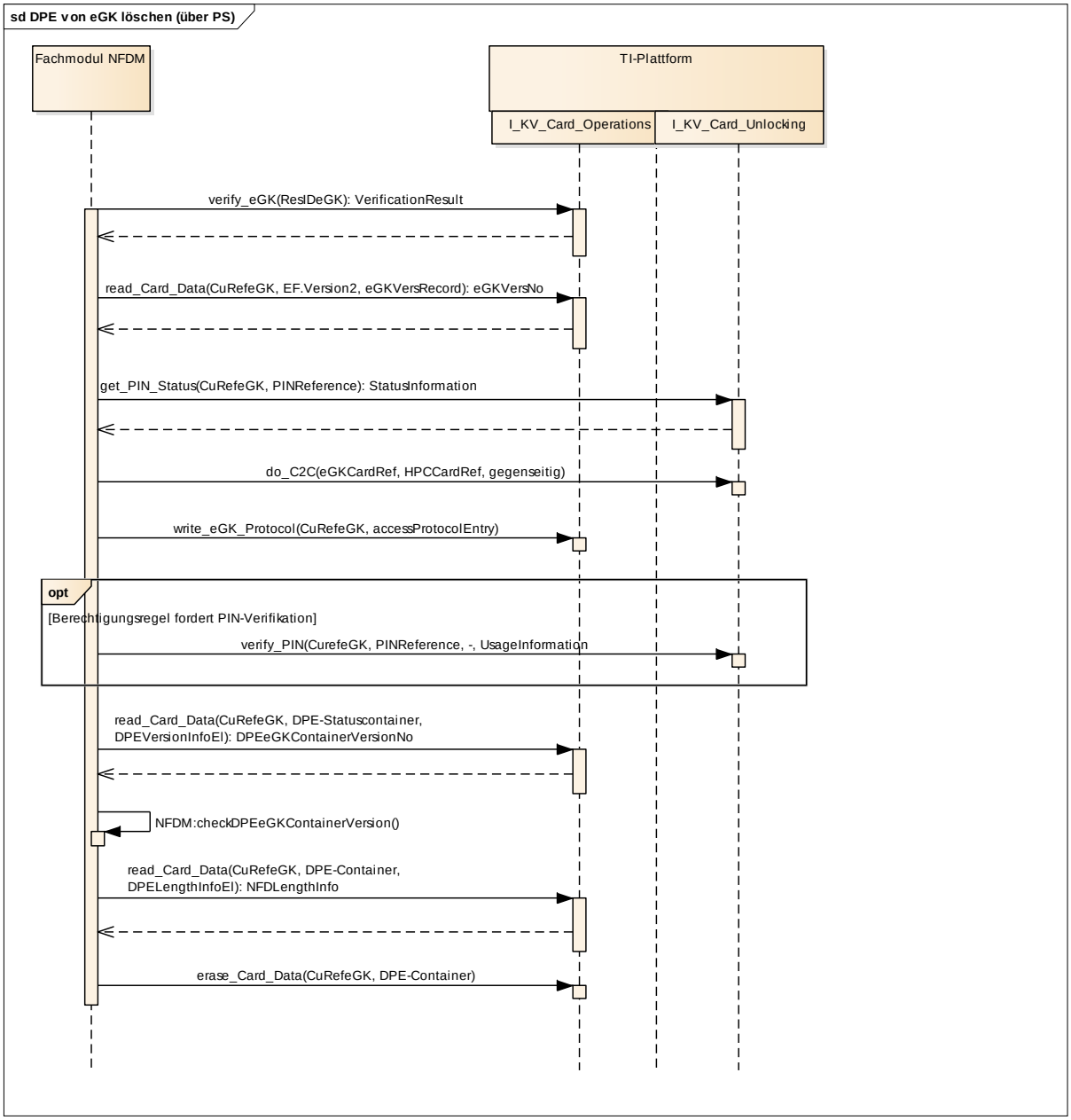

Abbildung 10: Sequenzdiagramm „DPE von eGK löschen“

5.7.2 Zugriffsprotokolleinträge auf der eGK

Die Zugriffsprotokolleinträge werden mittels TUC_KON_006 „Datenzugriffsaudit eGK schreiben“ des Kartendienstes erstellt (siehe [gemSpec_Kon#4.1.5]).

⌦ **NFDM-A_2135 Zugriffsprotokollierung auf der eGK**

Das Fachmodul NFDM MUSS die in Tabelle „Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK“ definierten Werte für die Informationselemente eines Zugriffsprotokolleintrags auf der eGK verwenden.

Tabelle 13: Tab_FM_NFDM_007 – Werte der Zugriffsprotokolleinträge auf der eGK

Operation	Data Type	Type of Access		Timestamp, Actor-ID, Actor-Name
`ReadNFD`	2	N	Lesen im Notfall	gemäß Tabelle „Tab_Karten_Fach_TIP_010_Struktur“ in [gemSpec_Karten_Fach_TIP# 4.1]
		A	Lesen zum Zwecke der Aktualisierung	
		Lesen außerhalb des Notfalls und der Aktualisierung...		
		R	...bei aktivierter `MRPIN.NFD`	
		r	…bei nicht aktivierter `MRPIN.NFD`	
`WriteNFD`	2	W		
`EraseNFD`	2	E		
`ReadDPE`	3	N	Lesen im Notfall	
		A	Lesen zum Zwecke der Aktualisierung	
		Lesen außerhalb des Notfalls und der Aktualisierung...		
		R	...bei aktivierter `MRPIN.DPE`	
		r	bei nicht aktivierter `MRPIN.DPE`	
`WriteDPE`	3	W		
`EraseDPE`	3	E		
~~`GetData`~~	~~2~~	~~c~~	~~Lesen des NFD zum Kopieren~~	
	~~3~~	~~c~~	~~Lesen des DPE zum Kopieren~~	
~~`PutData`~~	~~2~~	~~C~~	~~Kopierter NFD der alten eGK~~	
	~~3~~	~~C~~	~~Kopierter DPE der alten eGK~~	

⌫