Use Cases zum elektronischen Arztausweis

Version 1.0
Stand 31.07.2006

Bundesärztekammer **Ärztekammer Nordrhein** **Ärztekammer Westfalen-Lippe**

Referenz auf [HPC-P1, -P2], Version 2.1.0

Bruno Struif
Levona Eckstein
Ulrich Waldmann

Fraunhofer Institut Sichere Informations-Technologie

Änderungsübersicht

Datum	Version	Änderungen
31.07.2006	V1.0	Basisversion

Inhalt

1 Einleitung

In diesem Dokument werden Anwendungsabläufe für den elektronischen Arztausweis (eA) beschrieben, um die Anwendungsentwickler (und die Cryptographic Service Provider) bei der Programmierung von Modulen für Heilberufsausweise, insbesondere für den Praxis- und Klinikeinsatz zu unterstützen. Diese Abläufe lassen sich auf alle Heilberufsausweise (HBA nach Health Professional Card -Spezifikation 2.1.0) übertragen. Das Dokument wird auch Licht auf Möglichkeiten der Entwickler bei der Programmierung von Anwendungen zur elektronischen Gesundheitskarte (eGK) werfen. Bei der konkreten Implementierung dieser Beispiele sind die Vorgaben der Schutzprofile nach Common Criteria zu befolgen.

Der eA unterstützt X.509-Zertifikate, Schlüsselpaare und kryptografische Funktionen zur Realisierung der PKI-Sicherheitsfunktionen: Verschlüsselung, Authentifizierung und qualifizierte elektronische Signatur (QES). Für die QES-Funktion sind die Vorschriften nach Signaturgesetz (SigG) und Verordnung (SigV) zu beachten. Darüber hinaus unterstützt der eA

- Card Verifiable Certifcate (CVC) basierte Authentisierungsfunktionen,
  - zum Nachweis der Identität beim Zugriff auf die eGK,
  - zur Autorisierung der Secure Modul Card (SMC) für den Zugriff auf die eGK, sowie
- Funktionen zum Aufbau einer sicheren Ende-zu-Ende-Verbindung bei Nutzung des eA in Remote-Szenarien.

Die Ärztekammern haben sich bei der Austattung der Ärzte mit elektronischen Arztausweisen für das sogenannte marktoffene Modell entschieden, d.h. der Arzt wählt einen von den Ärztekammern vorab zugelassenen Zertifizierungsdiensteanbieter (zZDA) aus. Dieser zZDA wird dann von seiner Ärztekammer beauftragt, den Arztausweis zu erstellen und mit dem Signaturzertifikat und den anderen Zertifikaten zu versehen. Dabei entscheidet der zZDA, von welchem Kartenhersteller er die HPC 2.1.0 konformen Karten bezieht.

Nach Ausgabe der ersten zur HPC-Spec (HPC-2.0.9) konformen eAs zur Medica 2005 (erstellt von drei ZDAs, unter Verwendung von Karten zweier Kartenhersteller) zeigten sich - nicht unerwartet - Interoperabilitätsprobleme als Preis der marktoffenen Lösung. Anwendungsprogrammierer sahen sich gezwungen den Kartenhersteller und die Betriebssystemversion abzufragen, um dann mit kartenbetriebssystemspezifischen Befehlen die Basisfunktionen des eAs zu unterstützen.

Karten mit Signaturfunktion weisen je nach Hersteller betriebssystemspezifische Eigenheiten auf. Bislang ist es gängige Praxis, dass die ZDAs bei Ausgabe einer Signaturkarte auch einen entsprechenden kartenspezifischen Treiber mitliefern. Würde man dieser Vorgehensweise bei den HPCs folgen, hätte diese zur Konsequenz, dass für jeden HPC-Kartentyp eines Kartenherstellers (z.B. HPC-STARCOS-Karte, HPC-TCOS-Karte, HPC-Micardo-Karte usw.) je ein eigener Treiber installiert werden müsste. Bei der Vielzahl der Akteure in derselben Umgebung ist dies nicht nur aufwändig, sondern birgt Interoperabilitätsrisiken.

Ziel dieses Dokumentes ist es, sich die Abläufe so plausibel und funktionstüchtig vom Autor der HPC und eGK Spezifikation aufzeigen zu lassen, dass sie von den Anwendungsentwicklern überzeugt aufgegriffen werden können. Damit wäre die Integration der HPC-Funktionen in Client-Anwendungen innerhalb der gematik-Infrastruktur und die Nutzung der HPC-PKI-Funktionen mit einer Standard-Middleware außerhalb der Telematikinfrastruktur für das Gesundheitswesen quasi standardisiert.

Die Ärztekammern als Auftraggeber bedanken sich bei Herrn Struif und seinem Team für den Leitfaden. Unsere Intentionen sind vom SIT „beherzt" in einer Weise granuliert, skaliert und präzisiert worden, wie wir das selten in einem EDV-Projekt erlebt haben. Dank auch an Dr. Koch (Nordrheinische Ärzteversorgung) für die strukturell prägenden Aufschläge, Dr. Goetz (KVB) und Herrn Schladweiler (Projektbüro elektronischer Arztausweis der BÄK) für die konstruktive Kritik.

Fragen, Rückmeldungen, Korrekturen und Verbesserungsvorschläge bitte per Email an:

HPC-UseCases@baek.de Bundesärztekammer
HPC-UseCases@aekno.de Ärztekammer Nordrhein
HPC-UseCases@aekwl.de Ärztekammer Westfalen-Lippe

Düsseldorf 31. Juli 2006

Viktor Krön (Ärztekammer Nordrhein) Thomas Althoff (Ärztekammer Westfalen-Lippe)

2 Einführung in die Use Case-Beschreibung

2.1 Use Case-Dokumentation

Ein Use Case beschreibt einen zusammenhängenden Arbeitsablauf aus der Sicht des Heilberufsausweises (HPC). Jeder Anwendungsfall wird auf Basis folgender Tabelle textuell beschrieben:

Tabelle 1 – Use Case-Dokumentation

Identifier	Bezeichner des Anwendungsfalls
Name	Name des Anwendungsfalls
Beschreibung	Kurze Beschreibung, was im Anwendungsfall passiert.
Vorbedingungen	Alle Bedingungen, die erfüllt sein müssen, damit dieser Anwendungsfalls ausgeführt werden kann.
Nachbedingungen	Zustand der HPC, der nach erfolgreichem Durchlauf des Anwendungsfalls erwartet wird
Standardablauf	Beschreibung des Gut-Falls. Die Ablaufschritte werden nummeriert: 1. Schritt: Durchführung des Kommandos x 2. Schritt: Durchführung des Kommandos y 3. ...
Ablauf im Fehlerfall	Beschreibung des Ablaufs, der sich aus dem Fehlerfall ergibt
Häufigkeit	Angabe, wie oft dieser Anwendungsfall durchzuführen ist
Vorangegangene Use Cases	Bezeichnung notwendiger vorangegangener Use Cases
Nachfolgende Use Cases	Bezeichnung der möglichen, nachfolgenden Use Cases
Anmerkungen	Notwendiges zum Verständnis des Use Case
Festlegungen	Ergänzende Nutzungskonventionen, falls sinnvoll

Zu jedem Interaktions-Schritt im Standardablauf erfolgt eine Beschreibung des auszuführenden Kommandos in folgender Form:

x. Schritt (von y):
Tabelle 2 – Kommando: XXX (Referenz in HPC-P2)

CLA	INS	P1	P2	Lc	Daten	Le
00	xx	xx	xx	xx	xx	xx

Tabelle 3 – Korrekte Antworten

Daten	SW1 SW2	Ursache	Aktion
xx	90 00		
xx	xx xx		

Tabelle 4 – Abweichende Antworten (Referenz HPC-P1)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
xx xx	Kurzbeschreibung des Fehlers	Ursachen-Beschreibung	Durchzuführende Aktionen

2.2 Überblick der betrachteten Use Cases

Tabelle 5 – Betrachtete Use Cases

Anwendungs-kontext	Use Case	Identifier	Kapitel, Seite
Initialisierung	Reset-Behandlung	UC_HPC_Reset	4.1, S. 9
	Protokoll-Parameter-Selektion	UC_HPC_PPS	4.2, S. 11
Abrufen von generellen HPC-Informationen	Lesen der Seriellen Chipkartennummer (ICCSN)	UC_HPC_Read_ICCSN	5.1, S. 12
	Lesen der I/O-Puffergrößen	UC_HPC_Read_I/O_Buffer_Size	5.2, S. 14
	Lesen der unterstützten Anwendungen	UC_HPC_Read_Dir	5.3, S. 15
Abrufen von CV-Zertifikaten	Lesen von CV-Zertifikaten	UC_HPC_Read_CVCs	6.1, S. 18
	Retrieval von Cross-CV-Zertifikaten	UC_HPC_Retrieve_Cross_CVC	6.2, S. 20
Wissensbasierte Authentisierung des Karten-inhabers	Verifizieren der Karteninhaber-PIN	UC_HPC_Verify_PIN	7.1, S. 21
	Ändern der Karteninhaber-PIN	UC_HPC_Change_PIN	7.2, S. 23
	Rücksetzen des Retry Counter der Karteninhaber-PIN	UC_HPC_Reset_RC_PIN	7.3, S. 25
	Setzen einer neuen Karteninhaber-PIN	UC_HPC_Set_PIN	7.4, S. 27
	Verifizieren der QES-PIN	UC_HPC_Verify_QES_PIN	7.5, S. 29
	Ändern der QES-PIN	UC_HPC_Change_QES_PIN	7.6, S. 31
	Rücksetzen des Retry Counter der QES-PIN	UC_HPC_Reset_RC_QES_PIN	7.7, S. 33
Anwendungs-selektion	Öffnen der HP-Anwendung	UC_HPC_Open_HPA	8.1, S. 35
	Öffnen der QES-Anwendung	UC_HPC_Open_QES	8.2, S. 37
	Öffnen der ESIGN-Anwendung	UC_HPC_Open_ESIGN	8.3, S. 39
	Öffnen der CIA.ESIGN-Anwendung	UC_HPC_Open_CIA_ESIGN	8.4, S. 41
Nutzung der QES-Anwendung	Erzeugen einer qualifizierten elektronischen Signatur	UC_HPC_SIGN	9.1, S. 43
Nutzung der QES-Zertifikate	Lesen des X.509 Signatur-Basiszertifikats	UC_HPC_Read_QES_BC	10.1, S. 48
	Lesen der Attributzertifikate	UC_HPC_Read_QES_AC	10.2, S. 51
	Ersetzen der Attributzertifikate	UC_HPC_Replace_QES_AC	10.3, S. 55
Nutzung der ESIGN-Authen-tisierungs-Funktion	Authentisieren als Client	UC_HPC_AUT	11.1, S. 57
Nutzung der ESIGN-Verschlüs-selungs-Funktion	Entschlüsseln eines Dokumenten-Chiffrierungs-schlüssels	UC_HPC_DEC	12.1, S. 59
Nutzung der ESIGN-Zertifikate	Lesen des X.509 Authentisierungszertifikats	UC_HPC_Read_AUT	13.1, S. 61
	Lesen des X.509 Verschlüsselungszertifikat	UC_HPC_Read_ENC	13.2, S. 64
Nutzung der CIA.ESIGN-Anwendung	Ermitteln der unterstützten kryptographischen Algorithmen und Algorithmenparameter	UC_HPC_Read_CIA_ESIGN	14.1, S. 67
Interaktion HPC - eGK	Verifizieren der eGK-bezogenen CV-Zertifikate (zweistufig)	UC_HPC_Verify_eGK_CVCs	15.1, S. 70
	Verifizieren der eGK-bezogenen CV-Zertifikate mit Cross-CV-Zertifikat (dreistufig)	UC_HPC_Verify_eGK_Cross_CVCs	15.2, S. 73
	Durchführen der HPC / eGK-Authentisierung	UC_HPC_Authenticate_eGK	15.3, S. 77
Autorisieren einer SMC für die SMC/ eGK-Interaktion	Autorisieren einer SMC für die SMC / eGK-Interaktion	UC_HPC_Authorize_SMC	16.1, S. 80
Nutzung der HP-Anwendung	Lesen der HP-bezogenen Daten	UC_HPC_Read_HP_Data	17.1, S. 82
	Aktualisieren der HP-bezogenen Daten	UC_HPC_Update_HP_Data	17.2, S. 85
Nutzung einer stationären HPC	Einrichten eines logischen Kanals zur HPC	UC_HPC_Open_Logical_Channel	18.1, S. 88
	Schließen eines logischen Kanals zur HPC	UC_HPC_Close_Logical_Channel	18.2, S. 90
	Öffnen einer Anwendung für die Remote-Nutzung	UC_HPC_Open_Remote_Application	18.3, S. 92
	Verifizieren der SMC-bezogenen CV-Zertifikate (zweistufig)	UC_HPC_Verify_SMC_CVCs	18.4, S. 95
	Verifizieren der SMC-bezogenen CV-Zertifikate mit Cross-CV-Zertifikat (dreistufig)	UC_HPC_Verify_SMC_Cross_CVCs	18.5, S. 98
	Durchführen der HPC / SMC-Authentisierung mit SM-Schlüsselvereinbarung	UC_HPC_Authenticate_SMC	18.6, S. 103
	Lesen der Display Message	UC_HPC_Read_DM	18.7, S. 106
	Aktualisieren der Display Message	UC_HPC_Update_DM	18.8, S. 108
	Erzeugen einer qualifizierten elektronischen Signatur in der stationären HPC	UC_HPC_SIGN_With_Stationary_HPC	18.9, S. 109

3 Allgemeine Konventionen

3.1 Generelle Fehlerausgänge bei den HPC-Kommandos

Die in der nachstehenden Tabelle (Auszug aus [HPC-P1], Table A.1) angegebenen Fehlermeldungen beruhen auf Programmierfehler bei der Konstruktion von SmartCard-Kommandos und dürfen im Wirk-betrieb nicht auftreten.

Tabelle 6 – Allgemeine Fehlerbedingungen aufgrund von Programmierfehlern

SW1 SW2	Fehlerbedingung
67 00	Lc is not allowed for command variant
67 00	Lc is not consistent with length of command data
67 00	Lc or Le present while is has to be absent
67 00	Lc or Le absent while it has to be present
68 81	Logical channel not supported
68 84	Command chaining not supported (instead of '688A' also '6E00' may be used)
69 82	Security status not satisfied
69 87	Expected SM DO missing
69 88	Incorrect SM DO
6A 86	Incorrect parameters P1- P2
6D 00	INS not supported
6E 00	Class not supported

Auch die folgenden Fehlermeldungen dürfen im Wirkbetrieb nicht auftreten. Falls dies doch der Fall sein sollte, liegt ein technischer Defekt der HPC vor oder das Kommando wurde mit unzulässigen Daten der HPC übergeben.

Tabelle 7 – Allgemeine Fehlerbedingungen aufgrund HPC-Defekt/falsche Daten

SW1 SW2	Error Condition
64 00	Execution error
65 81	Memory error when reading or writing data

3.2 CLA-Byte

Bei dem CLA-Byte wird grundsätzlich der Wert '00' verwendet. Werden jedoch Kommandos in einem logischen Kanal mit einer Kanal-Nr. zwischen 1 und 3 gesendet, dann ist die entsprechende Kanal-Nr. im CLA-Byte anzugeben (siehe [ISO7816-4], Table 2). Auch die Anwendung von Secure Messaging wird im CLA-Byte angezeigt (siehe [HPC-P1], Annex D und [ISO7816-4], Table 2).

3.3 HPC-Session

Mit »HPC-Session« wird das Zeitintervall zwischen Power-on und Power-off bezeichnet.

3.4 HPC defekt

Der Fehlerausgang »HPC defekt" ist ein allgemeiner Fehlerausgang, der angesprungen wird, falls die Fortsetzung einer Kommunikation mit der betreffenden Karte nicht möglich oder sinnvoll ist. Der Fall darf im Wirkbetrieb nur dann auftreten, wenn die HPC z.B. wegen Chip-Bruchs nicht mehr funktioniert.

Programmiertechnisch wird jedoch dieser Ausgang häufiger angesprungen, da z.B. die Lesbarkeit von CV-Zertifikaten auch zur ordnungsgemäßen Funktionsfähigkeit gehört und wenn diese nicht lesbar sind, dann muss das Primärsystem von einer defekten Karte ausgehen.

4 Initialisierung

4.1 Reset-Behandlung

Tabelle 8 – Reset-Behandlung

Identifier	**UC_HPC_Reset**
Name	Reset-Behandlung
Beschreibung	Durchführen eines Cold Reset nach [ISO/IEC 7816-3] ([HPC-P2], Annex A, Table A.1)
Vorbedingungen	Alle Bedingungen, die erfüllt sein müssen, damit dieser Anwendungsfall ausgeführt werden kann.
Nachbedingungen	HPC kann jetzt auf optimale Übertragungskonventionen eingestellt werden
Standardablauf	1. Schritt: Power-on und Reset-Signal an Reset-Leitung setzen und ATR empfangen
Ablauf im Fehlerfall	Falls die Karte keinen oder einen fehlerhaften ATR sendet, ist sie defekt Aktion: Fehlerausgang »HPC defekt«
Häufigkeit	Einmal zu Beginn einer HPC-Session
Vorangegangene Use Cases	-
Nachfolgende Use Cases	UC_HPC_PPS
Anmerkungen	Das Reset-Kommando wird hardwaremäßig ohne Datenübertragung ausgelöst. Der Reset ist – z.B. getriggert vom Primärsystem - vom Kartenterminal auszuführen. Die Historical Bytes (HB) als Teil des ATR sind an das Primärsystem zu übergeben. Dieses wertet die HB hinsichtlich Card Capabilities (Extended Length und Anzahl unterstützter Kanäle) aus, siehe [ISO7816-4] (andere HB-Angaben sind im Primärsystem-Kontext nicht relevant bzw. als statischer Wert bekannt)
Festlegungen	-

1. Schritt (von 1):
Power-On und Reset-Signal an Reset-Leitung setzen; das Kommando wird hardwaremäßig ausgelöst [ISO7816-3]

Tabelle 9 – Korrekte Antwort - ATR ([HPC-P2], Annex A.1, [HPC-P1], 15)

Wert	Bedeutung	Länge
'3B'	TS	1
'9x'	T0; x = no. of HB	1
'xx'	TA1; s. [HPC-P1], Table 13	1
'81'	TD1	1
'B1'	TD2	1
'FE'	TA3	1
'45'	TB3	1
'1F'	TD3	1
'xx'	TA4	1
---------- Ti = Historical Bytes		
'00'	CI	1
---------- Pre-Issuing Data Object (PIDO)		
'6x'	TPI (x = Länge von PIDO)	1
'xx'	ICM; z.B. '04' für Philips Semiconductors (s. www.sc17.com)	1
'xx'	ICT - IC Type (herstellerspezifisch);	1-2
'xx'	OSV - Betriebssystem-Version (herstellerspezifisch)	1
'xx'	DD - normalerweise nicht vorhanden	max. 12 Bytes
---------- Card Profile Data Objects (CPDO)		
'31'	TCS – Card Service DO ([ISO7816-4], Table 85)	1
'xx'	CS – Card Service	1
'73'	TCC – Card Capabilities DO ([ISO7816-4], Table 86-88)	1
'xx'	1. Byte von CCB; Beispiel: '86' = DF-Selektion mit DF-Name, SFID und Record Number werden unterstützt.	1
'xx'	2. Byte von CCB	1
'xx'	3. Byte von CCB: b8 – Command Chaining b7 – Extended Length b5 + b4 – Logical channel assignment b3 + b2 + b1 – Maximum number of logical channels Wenn die letzten 3 bits gesetzt sind, bedeutet dies, dass 8 und mehr Kanäle unterstützt werden. Beispiel: '53' = Ohne Command Chaining, mit extended Length und 4 Kanälen	1
'xx'	CLS ([ISO7816-4], Table 13); Beispiel: '00' = Keine weiteren Angaben	1
'90 00'	SW1 / SW2	2
'xx'	TCK	1

Tabelle 10 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
-	kein ATR oder ATR fehlerhaft	Indiz für eine defekte Karte	Fehlerausgang »HPC defekt«

4.2 Protokoll-Parameter-Selektion

Tabelle 11 – Protokoll-Parameter-Selektion

Identifier	**UC_HPC_PPS**
Name	Protokoll-Parameter-Selektion
Beschreibung	Für das voreingestellte T=1-Protokoll wird eine PPS-Prozedur durchlaufen und dann die Kommunikation auf die vereinbarten Parameter (Takt, Übertragungsgeschwindigkeit, Information Field Size) umgestellt
Vorbedingungen	Reset erfolgreich
Nachbedingungen	HPC betriebsbereit
Standardablauf	1. Schritt: PPS-Request senden, der von der Karte mit einem PPS-Response zu beantworten ist
Ablauf im Fehlerfall	Falls die Karte keinen oder einen fehlerhaften PPS-Response sendet, fordert [ISO/IEC 7816-3] für diesen Fall die Deaktivierung. Aktion: Fehlerausgang »HPC defekt«
Häufigkeit	Einmal nach Reset
Vorangegangene Use Cases	UC_HPC_Reset
Nachfolgende Use Cases	UP_HPC_ICCSN
Anmerkungen	PPS wird automatisch vom Kartenterminal durchgeführt; es ist die max. Länge des Informationsfeldes eines T=1-Übertragungsblocks zu vereinbaren.
Festlegungen	PPS-Request mit IFSD=254, siehe [ISO/IEC 7816-3] PPS-Response mit IFSC=254, siehe [ISO/IEC 7816-3]

1. Schritt (von 1):
PPS-Request vom Kartenterminal [ISO7816-3]

Korrekte Antwort – PPS-Response von HPC [ISO7816-3]

Tabelle 12 – Abweichende Antworten [ISO7816-3]

SW1 SW2	**Fehlerbedingung**	**Ursache**	**Aktion**
-	Kein PPS-Response oder PPS-Response fehlerhaft	Indiz für eine defekte Karte.	Fehlerausgang »HPC defekt«

5 Abrufen von generellen HPC-Informationen

5.1 Lesen der Seriellen Chipkartennummer (ICCSN)

Tabelle 13 – Lesen der Seriellen Chipkartennummer (ICCSN)

Identifier	**UC_HPC_Read_ICCSN**
Name	Lesen der Seriellen Chipkartennummer (ICCSN)
Beschreibung	Lesen der Seriellen Chipkartennummer (ICCSN) aus der transparenten Datei EF.GDO ([HPC-P2], Annex G, Table G.4)
Vorbedingungen	HPC betriebsbereit MF-Ebene selektiert, d.h. es ist keine Anwendung geöffnet.
Nachbedingungen	MF-Ebene selektiert.
Standardablauf	1. Schritt: Durchführung des Kommandos READ BINARY mit SFID
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Einmal pro HPC-Session
Vorangegangene Use Cases	UC_HPC_PPS
Nachfolgende Use Cases	Wenn ICCSN noch nicht bekannt ist und Extended Length Support in den Historical Bytes angezeigt wird: • UC_HPC_Read_I/O_Buffer_Size Wenn ICCSN noch nicht bekannt ist und kein Extended Length Support in den Historical Bytes angezeigt wird: • UC_HPC_Read_CVCs Wenn ICCSN bekannt ist: Nachfolgender Use Case abhängig von weiterer Verwendung der HPC, z.B. HPC / SMC-Authentisierung
Anmerkungen	Es wird empfohlen, die ICCSN im Primärsystem zu speichern und alle kartenspezifischen Daten, die nur ein einziges Mal ausgelesen werden müssen, unter dieser Kennung abzulegen, siehe Anhang A.2.
Festlegungen	-

1. Schritt (von 1):
Tabelle 14 – Kommando: READ BINARY ([HPC-P2], 5.4.2, Table 4)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten**	**Le**
00	B0	82	00	-	-	00

Tabelle 15 – Korrekte Antwort ([HPC-P2], 5.4.2., Table 5)

Daten (12 Bytes)	**SW1 SW2**	**Ursache**	**Aktion**
5A 0A 80 27 6X XX XX YY YY YY YY YY ([HPC-P2], 5.2.4, Figure 2 und Annex G, Table G.4)	90 00	ICCSN erfolgreich gelesen	Use Case beenden

Tabelle 16 – Abweichende Antworten ([HPC-P1], Annex A, Table A.4)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
62 82	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 81	Datei nicht transparent		
69 86	Kommando ohne SFID; keine Datei selektiert		
6A 82	Datei mit SFID nicht gefunden		
6B 00	Offset größer oder gleich Dateigröße		

5.2 Lesen der I/O-Puffergrößen

Tabelle 17 – Lesen der I/O-Puffergrößen

Identifier	**UC_HPC_Read_I/O-BufferSize**
Name	Lesen der I/O-Puffergrößen
Beschreibung	Lesen der I/O-Puffergrößen aus dem transparenten File EF.ATR
Vorbedingungen	HPC betriebsbereit MF-Ebene selektiert, d.h. keine Anwendung ist geöffnet. Lesen von EF.ATR nur dann, wenn in den HB die Unterstützung von Extended Length angezeigt wurde (siehe UC_HPC_Reset; CPDO – 3. Byte von CCB)
Nachbedingungen	MF-Ebene selektiert
Standardablauf	1. Schritt: Durchführung des Kommandos READ BINARY mit SFID; es ist nur das Datenobjekt mit Tag 'E0' relevant; das DO Card Data (Tag = '66'), das ebenfalls im EF.ATR abgelegt ist, ist für das Primärsystem nicht relevant.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Einmal beim Erstkontakt mit einer bisher unbekannten Karte, falls Info im Primärsystem persistent gespeichert wird (siehe Anhang A.2)
Vorangegangene Use Cases	UC_HPC_Read_ICCSN
Nachfolgende Use Cases	Nachfolgende Use Case abhängig von weiterer Verwendung der HPC, z.B. HPC / SMC-Authentisierung
Anmerkungen	Es wird empfohlen, die I/O-Puffergrößen im Primärsystem unter der Kennung ICCSN zu speichern, siehe Anhang A.2. Das DO I/O-Puffergrößen ist anwendungsrelevant und nicht Kartenterminal-relevant.
Festlegungen	-

1. Schritt (von 1):
Tabelle 18 – Kommando: READ BINARY ([HPC-P2], 5.4.2, Table 4 und 5)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten**	**Le**
00	B0	9D	00	-	-	00

Tabelle 19 – Normale Antwort ([HPC-P2], Table G.1)

Daten	**SW1 SW2**
E0 XX 02 xx xx xx 02 xx xx xx 02 xx xx xx 02 xx xx xx 66 xx 46 xx ...	90 00

Tabelle 20 – Abweichende Antworten ([HPC-P1], Table A.4)

SW1 SW2	**Fehlerbedingung**	**Ursache**	**Aktion**
62 82	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 81	Datei nicht transparent		
69 86	Kommando ohne SFID; keine Datei selektiert		
6A 82	Datei mit SFID nicht gefunden		
6B 00	Offset größer oder gleich Dateigröße		

5.3 Lesen der unterstützten Anwendungen

Tabelle 21 – Lesen der unterstützten Anwendungen

Identifier	**UC_HPC_Read_Dir**
Name	Lesen der unterstützten Anwendungen
Beschreibung	Lesen der Application Templates, welche die Application Identifier der unterstützten Anwendungen HPA, QES, ESIGN, CIA.ESIGN und ggf. nachgeladenen Anwendungen enthalten, aus der Record-Datei EF.DIR ([HPC-P2], Table G.3)
Vorbedingungen	HPC betriebsbereit MF-Ebene selektiert, d.h. keine Anwendung ist geöffnet
Nachbedingungen	MF-Ebene selektiert
Standardablauf	1. Schritt: Durchführung des Kommandos READ RECORD mit SFID und Record-Nummer 1 2. Schritt: Durchführung des Kommandos READ RECORD ohne SFID und mit Record-Nummer 2 3. Schritt: Durchführung des Kommandos READ RECORD ohne SFID und mit Record-Nummer 3 4. Schritt: Durchführung des Kommandos READ RECORD ohne SFID und mit Record-Nummer 4 5. Schritt: Durchführung des Kommandos READ RECORD ohne SFID und mit Record-Nummer 5 Weitere READ RECORD-Befehle mit höheren Record-Nummern, falls im jeweils vorangegangenen Schritt ein Record gefunden wurde.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Einmal beim Erstkontakt mit einer bisher unbekannten Karte, falls Info im Primärsystem persistent gespeichert wird (siehe Anhang A.2). Zu Beginn einer HPC-Session zur Nutzung von zusätzlichen HPC-Anwendungen oder bei der Nutzung der HPC außerhalb des Gesundheitswesens.
Vorangegangene Use Cases	UC_HPC_Read_ICCSN
Nachfolgende Use Cases	Nachfolgender Use Case abhängig von weiterer Verwendung der HPC, z.B. Öffnen der ESIGN-Anwendung
Anmerkungen	Die im Gesundheitswesen unterstützten Anwendungen sind dem Primärsystem implizit bekannt. EF.DIR erlaubt das Hinzufügen von Informationen weiterer (nach Kartenausgabe geladener) Anwendungen. Ein vom Kartenbetriebssystem unabhängiges Versionskonzept der unterstützten Anwendungen, insbesondere der HPA, lässt sich über die "Proprietary application identifier extension" (PIX, maximal 11 Bytes) als Bestandteil eines Application Identifier realisieren. Die verwendete PIX 02 der HPA drückt beispielsweise aus, dass die Karte der 2. HPC-Generation angehört. Der Namensraum und die Handhabung der PIX ist jedoch nicht einfach denen der Versionsnummern der HPC-Spezifikationen gleichzusetzten. Außerdem können durch die Angabe einer Versionsnummer nur schwerlich einzelne unterstützte (oder nicht unterstützte) Features gekennzeichnet werden. Ein verfeinertes Versionskonzept ließe sich z.B. über ein "Discretionary Data Object" ausdrücken, welches beispielsweise die Versionsnummer der unterstützten HPC-Spezifikationen und eine Flagliste der unterstützten Features enthalten könnte.
Festlegungen	Falls wiederholt aus derselben Datei weitergelesen wird, ist es aus Performanzgründen sinnvoll, dass ab dem zweiten READ RECORD die SFID (höherwertige Bits b8-b4 in P2) auf 0 gesetzt wird.

1. Schritt (von 5):
Tabelle 22 – Kommando: READ RECORD ([HPC-P2], 5.4.3, Table 6)

CLA	INS	P1	P2	Lc	Daten	Le
00	B2	01	F4	-	-	00

Tabelle 23 – Korrekte Antwort ([HPC-P2], 5.4.3, Table 7)

Daten (10 Bytes)	SW1 SW2	Ursache	Aktion
61 08 4F 06 D2 76 00 00 40 02 ([HPC-P2], 5.2.3. und Annex G, Table G.3)	90 00	1. Record erfolgreich gelesen	2. Schritt
D2 76 00 00 40 (die ersten 5 Bytes der AID) stellt einen Registered Application Provider Identifier (RID) des Deutschen Gesundheitswesen dar. Inhaber der RID ist das Zentralinstitut für die Kassenärtliche Versorgung in der Bundesrepublik Deutschland. Das der RID folgende Byte mit dem Wert 02 ist die "Proprietary application identifier extension" (PIX), welche für eine der HPC-Version 1.0 folgende HPC-Version der 2. Generation steht.			

Tabelle 24 – Abweichende Antworten ([HPC-P1], Table A.6)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
62 83	Selektierter Record ist deaktiviert	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 81	Datei ist transparent		
69 86	Kommando-Option ohne SFID, keine Datei selektiert		
6A 82	Mit SFID referenzierte Datei nicht gefunden		
6A 83	Record nicht gefunden		

2. Schritt (von 5):
Tabelle 25 – Kommando: READ RECORD ([HPC-P2], 5.4.3, Table 6)

CLA	INS	P1	P2	Lc	Daten	Le
00	B2	02	04	-	-	00

Tabelle 26 – Korrekte Antwort ([HPC-P2], 5.4.3, Table 7)

Daten (10 Bytes)	SW1 SW2	Ursache	Aktion
61 08 4F 06 D2 76 00 00 66 01 ([HPC-P2], 5.2.3. und Table G.3)	90 00	2. Record erfolgreich gelesen	3. Schritt

Abweichende Antworten ([HPC-P1], Table A.6) siehe 1. Schritt

3. Schritt (von 5):
Tabelle 27 – Kommando: READ RECORD ([HPC-P2], 5.4.3, Table 6)

CLA	INS	P1	P2	Lc	Daten	Le
00	B2	03	04	-	-	00

Tabelle 28 – Korrekte Antwort ([HPC-P2], 5.4.3, Table 7)

Daten (14 Bytes)	SW1 SW2	Ursache	Aktion
61 0C 4F 0A A0 00 00 01 67 45 53 49 47 4E ([HPC-P2], 5.2.3. und Table G.3)	90 00	3. Record erfolgreich gelesen	4. Schritt

Abweichende Antworten ([HPC-P1], Table A.6) siehe 1. Schritt

4. Schritt (von 5):
Tabelle 29 – Kommando: READ RECORD ([HPC-P2], 5.4.3, Table 6)

CLA	INS	P1	P2	Lc	Daten	Le
00	B2	04	04	-	-	00

Tabelle 30 – Korrekte Antwort ([HPC-P2], 5.4.3, Table 7)

Daten (19 Bytes)	SW1 SW2	Ursache	Aktion
61 11 4F 0F E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E ([HPC-P2], 5.2.3. und Table G.3)	90 00	4. Record erfolgreich gelesen	5. Schritt

Abweichende Antworten ([HPC-P1], Table A.6) siehe 1. Schritt

5. Schritt (von 5):
Tabelle 31 – Kommando: READ RECORD ([HPC-P2], 5.4.3, Table 6)

CLA	INS	P1	P2	Lc	Daten	Le
00	B2	05	04	-	-	00

Tabelle 32 – Korrekte Antwort ([HPC-P2], 5.4.3, Table 7 und [HPC-P1], Table A.6)

Daten	SW1 SW2	Fehlerbedingung	Ursache	Aktion
-	6A 83	Ein 5. Record konnte nicht gefunden werden	In HPCs ohne nachgeladene Anwendungen sind nur vier Records vorhanden.	Use Case beenden
61 xx ...	90 00	Ein 5. Record konnte gefunden werden	Informationen über eine weitere Anwendung, die auf die HPC nachgeladen wurde, ist vorhanden.	Record auswerten und weiteren Schritt mit READ RECORD ohne SFID und mit Record-Nummer 6 anschließen usw.

Tabelle 33 – Abweichende Antworten ([HPC-P1], Table A.6)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
62 83	Selektierter Record ist deaktiviert	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 81	Datei ist transparent		
69 86	Kommando-Option ohne SFID, keine Datei selektiert		
6A 82	Mit SFID referenzierte Datei nicht gefunden		

6 Abrufen von CV-Zertifikaten

6.1 Lesen von CV-Zertifikaten

Tabelle 34 – Lesen von CV-Zertifikaten

Identifier	**UC_HPC_Read_CVCs**
Name	Lesen von CV-Zertifikaten
Beschreibung	Lesen des HPC-CA-Zertifikats und des HPC-Authentisierungszertifikats aus den transparenten Dateien EF.CVC.CA_HPC.CS ([HPC-P2], 5.2.5) und CVC.HPC.AUT ([HPC-P2], 5.2.6), damit bei einer späteren Card-to-Card-Authentisierung die Zertifikate durch das Primärsystem einer eGK bzw. SMC zur Verfügung gestellt werden können.
Vorbedingungen	HPC betriebsbereit MF-Ebene selektiert, d.h. keine Anwendung ist geöffnet.
Nachbedingungen	MF-Ebene selektiert
Standardablauf	1. Schritt: Durchführung des Kommandos READ BINARY mit SFID 2. Schritt: Durchführung des Kommandos READ BINARY mit SFID
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Einmal beim Erstkontakt mit einer bisher unbekannten Karte, falls Zertifikate im Primärsystem persistent gespeichert werden (siehe Anhang A.2).
Vorangegangene Use Cases	UC_HPC_Read_ICCSN
Nachfolgende Use Cases	Abhängig von der weiteren Verwendung der HPC, z.B. eGK / HPC-Authentisierung: • UC_HPC_Authenticate_eGK Autorisieren einer SMC für die SMC / eGK-Interaktion: • UC_HPC_Authorize_SMC
Anmerkungen	Es wird empfohlen, die Zertifikate im Primärsystem unter der Kennung ICCSN zu speichern, siehe Anhang A.2.
Festlegungen	-

1. Schritt (von 2):
Tabelle 35 – Kommando: READ BINARY ([HPC-P2], 5.4.4, Table 8)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten**	**Le**
00	B0	83	00	-	-	00

Tabelle 36 – Korrekte Antwort ([HPC-P2], 5.4.4, Table 9)

Daten (205 Bytes)	**SW1 SW2**	**Ursache**	**Aktion**
5F37 8180 XX ... 5F38 3C XX ... 42 08 XX XX XX XX XX XX XX XX ([HPC-P1], Annex B, Table B.11)	90 00	CVC.HPC.AUT-Zertifikat erfolgreich gelesen	2. Schritt
CV-Zertifikatsdatenobjekte: CV-Signatur, PK-Remainder und CAR			

Tabelle 37 – Abweichende Antworten ([HPC-P1], Table A.4)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
62 82	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehleraus-gang »HPC defekt«
69 81	Datei nicht transparent		
69 86	Kommando ohne SFID; keine Datei selektiert		
6A 82	Datei mit SFID nicht gefunden		
6B 00	Offset größer oder gleich Dateigröße		

2. Schritt (von 2):
Tabelle 38 – Kommando: READ BINARY ([HPC-P2], 5.4.4, Table 8)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	84	00	-	-	00

Tabelle 39 – Korrekte Antwort ([HPC-P2], 5.4.4, Table 9)

Daten (206 Bytes)	SW1 SW2	Ursache	Aktion
5F37 8180 XX ... 5F38 3D XX ... 42 08 XX XX XX XX XX XX XX XX XX ([HPC-P1], Annex B, Table B.10)	90 00	CVC.CA_HPC.CS-Zertifikat erfolgreich gelesen	Use Case beenden
CV-Zertifikatsdatenobjekte: CV-Signatur, PK-Remainder und CAR			

Tabelle 40 – Abweichende Antworten ([HPC-P1], Table A.4) siehe 1. Schritt

SW1 SW2	Fehlerbedingung	Ursache	Aktion
62 82	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehleraus-gang »HPC defekt«
69 81	Datei nicht transparent		
69 86	Kommando ohne SFID; keine Datei selektiert		
6A 82	Datei mit SFID nicht gefunden		
6B 00	Offset größer oder gleich Dateigröße		

6.2 Retrieval von Cross-CV-Zertifikaten

Tabelle 41 – Retrieval von Cross-CV-Zertifikaten

Identifier	**UC_HPC_Retrieve_Cross_CVC**
Name	Retrieval von Cross-CV-Zertifikaten
Beschreibung	Cross-CV-Zertifikate werden bei Bedarf vom gematik-Server abgerufen und lokal im Primärsystem gespeichert
Vorbedingungen	Falls Primärsystem feststellt, dass der öffentliche Root-CA-Schlüssel der HPC nicht identisch ist mit dem öffentlichen Root-CA-Schlüssel der Partner-Smartcard (eGK oder SMC) und die beiden benötigten Cross-CV-Zertifikate noch nicht lokal im Primärsystem vorhanden, dann ist die Verwendung von Cross-CV-Zertifikaten erforderlich.
Nachbedingungen	Cross-CV-Zertifikate im Primärsystem vorhanden.
Standardablauf	Falls die benötigten Cross-CV-Zertifikate nicht lokal vorhanden sind, wird vom gematik-Server entweder die komplette Cross-CVC-Liste oder gezielt die beiden benötigten Cross-CV-Zertifikate abgerufen.
Ablauf im Fehlerfall	Falls gematik-Server nicht verfügbar, Vorgang wiederholen. Nach 3-maligen Fehlversuch ist Vorgang mit entsprechender Meldung abzubrechen und später erneut zu wiederholen.
Häufigkeit	Einmal pro Cross-CV-Zertifikat (d.h. einmal pro Jahr nach Schlüsselwechsel der Root-CA).
Vorangegangene Use Cases	UC_HPC_Read_ICCSN
Nachfolgende Use Cases	UC_HPC_Verify_Cross_CVC
Anmerkungen	Beim Retrieval von Cross-CV-Zertifikaten ist die HPC nicht involviert.
Festlegungen	Die Interaktionen zum Retrieval von Cross-CV-Zertifikaten ist von der gematik festzulegen. Der Aufbau der Retrieval-Daten sollte der Abb. B.10 in [HPC-P1] entsprechen, da die Datenobjekte DO 5F37 und 5F38 und DO 42 benötigt werden.

7 Wissensbasierte Authentisierung des Karteninhabers

7.1 Verifizieren der Karteninhaber-PIN

Tabelle 42 – Verifizieren der Karteninhaber-PIN

Identifier	**UC_HPC_Verify_PIN**
Name	Verifizieren der Karteninhaber-PIN
Beschreibung	Prüfen der vom Heilberufler eingegebenen Karteninhaber-PIN. Folgende Use Cases setzen eine erfolgreiche PIN-Verifikation voraus: UC_HPC_Authorize_SMC, UC_HPC_Update_HP_Data, UC_HPC_Replace_QES_AC, UC_HPC_AUT, UC_HPC_DEC
Vorbedingungen	HPC betriebsbereit
Nachbedingungen	• Bei Antwort 90 00: Sicherheitsstatus »Karteninhaber-PIN-Verifikation erfolgreich« und Retry Counter der Karteninhaber-PIN auf Maximalwert. • Bei Antwort 63CX: Retry Counter der Karteninhaber-PIN dekrementiert d.h. er war vorher noch nicht Null. Noch X verbleibende Versuche (x=2 oder 1 oder 0). Wenn 63C0 zurückgeliefert wird, wurde die Verifikationsmethode der Karteninhaber-PIN blockiert, d.h. es ist kein weiteres VERIFY möglich, wenn nicht zunächst der Retry Counter der Karteninhaber-PIN (durch UC_HPC_Reset_RC_PIN) zurückgesetzt wird. • Bei Antwort 63 83: PIN-Verifikationsmethode blockiert, Retry Counter der Karteninhaber-PIN auf Null.
Standardablauf	1. Schritt: Durchführung des Kommandos VERIFY mit PIN im Format 2 PIN Block
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Einmal pro HPC-Session mit einem oder mehreren im Folgenden genannten Anwendungskontexte.
Vorangegangene Use Cases	Abhängig vom Anwendungskontext können folgende Use Cases vorangegangen sein: • UC_HPC_Reset • UC_HPC_Select_HP • UC_HPC_Select_QES • UC_HPC_Select_ESIGN • UC_HPC_Verify_PIN (Verifikation nicht erfolgreich)
Nachfolgende Use Cases	Abhängig vom Anwendungskontext können folgende Use Cases folgen: • UC_HPC_Authorize_SMC • UC_HPC_Update_HP_Data • UC_HPC_Replace_QES_AC • UC_HPC_AUT • UC_HPC_DEC • UC_HPC_Verify_PIN (falls Verifikation nicht erfolgreich) • UC_HPC_Reset_RC_PIN (falls Verifikation blockiert) • UC_HPC_Set_PIN (falls Verifikation nicht erfolgreich)
Anmerkungen	Informationen zum PIN-Management: [HPC-P1], 7 und [HPC-P2], 5.2.7. Maximalwert des Retry Counter der Karteninhaber-PIN ist entsprechend dem Initial Value 3.
Festlegungen	-

1. Schritt (von 1):
Tabelle 43 – Kommando: VERIFY ([HPC-P2], 5.5.1, Table 12)

CLA	INS	P1	P2	Lc	Daten (8 Bytes)	Le
00	20	00	01	08	Eingegebene Karteninhaber-PIN im Format 2 PIN Block, z.B. 26 12 34 56 FF FF FF FF für die sechstellige PIN 123456	-

Tabelle 44 – Korrekte Antworten ([HPC-P2], 5.5.1, Table 13 und [HPC-P1], Table A.14)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Karteninhaber-PIN-Verifikation erfolgreich	Use Case beenden
-	63 83	Karteninhaber-PIN-Verifikationsmethode blockiert	UC_HPC_Reset_RC_PIN oder UC_HPC_Set_PIN
-	63 CX	Karteninhaber-PIN-Verifikation nicht erfolgreich, d.h. Karteninhaber-PIN wurde falsch eingegeben, X > 0 bedeutet, X weitere Versuche möglich	UC_HPC_Verify_PIN oder UC_HPC_Set_PIN
-	63 C0	Karteninhaber-PIN-Verifikation nicht erfolgreich, keine weitere Versuche mehr möglich	UC_HPC_Reset_RC_PIN oder UC_HPC_Set_PIN

Tabelle 45 – Abweichende Antworten ([HPC-P1], Table A.14)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in Format 2 PIN Block	Diese Return-Werte sind ein Indiz für ein Programmier-fehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

7.2 Ändern der Karteninhaber-PIN

Tabelle 46 – Ändern der Karteninhaber-PIN

Identifier	**UC_HPC_Change_PIN**
Name	Ändern der Karteninhaber-PIN
Beschreibung	Prüfen der vom Heilberufler eingegebenen alten Karteninhaber-PIN und Ersetzen der alten Karteninhaber-PIN durch die vom Heilberufler eingegebene neue Karteninhaber-PIN
Vorbedingungen	HPC betriebsbereit
Nachbedingungen	• Bei Antwort 90 00: Retry Counter der Karteninhaber-PIN auf Maximalwert und alte Karteninhaber-PIN durch eine neue Karteninhaber-PIN ersetzt, evt. Sicherheitsstatus »Karteninhaber-PIN-Verifikation erfolgreich« (siehe Anmerkungen). • Bei Antwort 63CX: Retry Counter der Karteninhaber-PIN dekrementiert d.h. er war vorher noch nicht Null. Noch X verbleibende Versuche (x=2 oder 1 oder 0). Wenn 63C0 zurückgeliefert wird, wurde die Verifikationsmethode der Karteninhaber-PIN blockiert, d.h. es ist kein weiteres VERIFY möglich, wenn nicht zunächst der Retry Counter der Karteninhaber-PIN (durch UC_HPC_Reset_RC_PIN) zurückgesetzt wird. • Bei Antwort 63 83: Karteninhaber-PIN-Verifikationsmethode blockiert, Retry Counter der Karteninhaber-PIN auf Null.
Standardablauf	1. Schritt: Durchführung des Kommandos CHANGE RD mit alter Karteninhaber-PIN und neuer Karteninhaber-PIN jeweils im Format 2 PIN Block
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Einmal zu Beginn der HPC-Nutzung, falls es sich bei der alten Karteninhaber-PIN um eine Transport-PIN handelt. Sonst beliebig.
Vorangegangene Use Cases	Mindestens UC_HPC_Reset
Nachfolgende Use Cases	Abhängig vom Anwendungskontext und • UC_HPC_Change_PIN (falls Verifikation nicht erfolgreich) • UC_HPC_Reset_RC_PIN (falls Verifikation blockiert) • UC_HPC_Set_PIN (falls Verifikation nicht erfolgreich
Anmerkungen	• Informationen zum PIN-Management: [HPC-P1], 7 und [HPC-P2], 5.2.7. Maximalwert des Retry Counter der Karteninhaber-PIN ist entsprechend dem Initial Value 3. • Bei der Eingabe der Transport-PIN sind die herstellerspezifischen Angaben zu beachten (z.B. Eingabe einer NULL-PIN bzw. einer 5-stelligen Transport-PIN). • Ob ein Sicherheitsstatus gesetzt wird, wenn es sich bei der alten Karteninhaber-PIN um eine Transport-PIN handelt, ist abhängig vom Transport-PIN-Verfahren der HPC, siehe [HPC-P2], 5.5.2.
Festlegungen	-

1. Schritt (von 1):
Tabelle 47 – Kommando: CHANGE RD ([HPC-P2], 5.5.2, Table 14)

CLA	INS	P1	P2	Lc	Daten (16 Bytes)	Le
00	24	00	01	10	Eingegebene alte Karteninhaber-PIN und eingegebene neue Karteninhaber-PIN in zwei Format 2 PIN Blöcken, z.B. 26 12 34 56 FF FF FF FF 26 65 43 21 FF FF FF FF für die sechsstellige alte PIN 123456 und die sechstellige neue PIN 654321	-

Tabelle 48 – Korrekte Antworten ([HPC-P2], 5.5.2, Table 15 und [HPC-P1], Table A.15)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Karteninhaber-PIN-Verifikation erfolgreich und Karteninhaber-PIN geändert	Use Case beenden
-	63 83	Karteninhaber-PIN-Verifikationsmethode blockiert	UC_HPC_Reset_RC_PIN oder UC_HPC_Set_PIN
-	63 CX (X > 0)	Karteninhaber-PIN-Verifikation nicht erfolgreich, d.h. alte Karteninhaber-PIN wurde falsch eingegeben; X weitere Versuche möglich	UC_HPC_Change_PIN oder UC_HPC_Set_PIN
-	63 C0	Karteninhaber-PIN-Verifikation nicht erfolgreich, keine weitere Versuche mehr möglich	UC_HPC_Reset_RC_PIN oder UC_HPC_Set_PIN

Tabelle 49 – Abweichende Antworten ([HPC-P1], Table A.15)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in Format 2 PIN Block	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

7.3 Rücksetzen des Retry Counter der Karteninhaber-PIN

Tabelle 50 – Rücksetzen des Retry Counter der Karteninhaber-PIN

Identifier	**UC_HPC_Reset_RC_PIN**
Name	Rücksetzen des Retry Counter der Karteninhaber-PIN
Beschreibung	Prüfen des vom Heilberufler eingegebenen Resetting Code (Personal Unblocking Key, PUK) der Karteninhaber-PIN und Rücksetzen des Retry Counter der Karteninhaber-PIN auf seinen Maximalwert.
Vorbedingungen	HPC betriebsbereit
Nachbedingungen	• Bei Antwort 90 00: Retry Counter der Karteninhaber-PIN auf Maximalwert – kein Setzen des Sicherheitsstatus, d.h. vor Zugriff auf PIN-geschützte Funktionen oder Daten muss UC_HPC_Verify_PIN durchgeführt werden. • Bei Antwort 63CX: Usage Limitation der PUK der Karteninhaber-PIN dekrementiert d.h. er war vorher noch nicht Null. Noch X verbleibende Versuche (x= 9, 8, ...1 oder 0). Wenn 63C0 zurückgeliefert wird, wurde die Verifikationsmethode der PUK der Karteninhaber-PIN blockiert, d.h. es ist kein weiteres RESET RC möglich und die mit der Karteninhaber-PIN geschützten Funktionen oder Daten sind nicht mehr nutzbar. • Bei Antwort 63 83: PUK-Verifikationsmethode der Karteninhaber-PIN blockiert, Usage Limitation der PUK der Karteninhaber-PIN auf Null.
Standardablauf	1. Schritt: Durchführung des Kommandos RESET RETRY COUNTER mit PUK der Karteninhaber-PIN im Format 2 PIN Block
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Wenn die Karteninhaber-PIN-Verifikationsmethode blockiert ist, d.h. die Karteninhaber-PIN mehrmals hintereinander (Maximalwert des Retry Counter) falsch eingegeben wurde.
Vorangegangene Use Cases	• UC_HPC_Verify_PIN (falls Verifikation nicht erfolgreich und Verifikationsmethode blockiert)
Nachfolgende Use Cases	• UC_HPC_Verify_PIN • UC_HPC_Reset_RC_PIN (falls PUK-Verifikation nicht erfolgreich) • UC_HPC_Set_PIN (falls PUK-Verifikation nicht erfolgreich)
Anmerkungen	Informationen zum PIN-Management: [HPC-P1], 7 und [HPC-P2], 5.2.7. Maximalwert des Retry Counter der Karteninhaber-PIN ist entsprechend dem Initial Value 3. Maximalwert der Usage Limitation der PUK der Karteninhaber-PIN ist entsprechend dem Initial Value10. Wenn die Karteninhaber-PIN-Verifikationsmethode nicht blockiert ist, kann die Karte unterschiedlich reagieren: Der Befehl wird entweder ausgeführt oder es wird ein Fehler zurückgegeben (z.B. SW1 SW2 = 69 85: Nutzungsbedingungen nicht erfüllt).
Festlegungen	-

1. Schritt (von 1):
Tabelle 51 – Kommando: RESET RC ([HPC-P2], 5.5.3, Table 16)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten (8 Bytes)**	**Le**
00	2C	01	01	08	Eingegebene PUK der Karteninhaber-PIN im Format 2 PIN Block, z.B. 28 12 34 56 78 FF FF FF für die achtstellige PUK 12345678	-

Tabelle 52 – Korrekte Antworten ([HPC-P2], 5.5.3, Table 17 und [HPC-P1], Table A.16)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	PUK-Verifikation der Karteninhaber-PIN erfolgreich, Retry Counter der Karteninhaber-PIN auf Maximalwert gesetzt	Use Case beenden
-	69 85	Retry-Counter kann nur dann zurückgesetzt werden, wenn er auf Null steht, d.h. die Verifikationsmethode der Karteninhaber-PIN blockiert ist. Dies ist nicht der Fall.	Use Case beenden
-	63 83	PUK-Verifikationsmethode der Karteninhaber-PIN blockiert	Mit Karteninhaber-PIN geschützte Funktionen oder Daten nicht mehr nutzbar.
-	63 CX (X > 0)	PUK-Verifikation der Karteninhaber-PIN nicht erfolgreich, d.h. PUK der Karteninhaber-PIN wurde falsch eingegeben; X weitere Versuche möglich	UC_HPC_Reset_RC_PIN oder UC_HPC_Set_PIN
-	63 C0	PUK-Verifikation nicht erfolgreich, keine weiteren Versuche mehr möglich	Mit Karteninhaber-PIN geschützte Funktionen oder Daten nicht mehr nutzbar.

Tabelle 53 – Abweichende Antworten ([HPC-P1], Table A.16)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in Format 2 PIN Block	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

7.4 Setzen einer neuen Karteninhaber-PIN

Tabelle 54 – Setzen einer neuen Karteninhaber-PIN

Identifier	**UC_HPC_Set_PIN**
Name	Setzen einer neuen Karteninhaber-PIN
Beschreibung	Prüfen des vom Heilberufler eingegebenen Resetting Code (Personal Unblocking Key, PUK) der Karteninhaber-PIN und Setzen einer vom Heilberufler eingegebenen neuen Karteninhaber-PIN für den Fall, dass die bisherige Karteninhaber-PIN vergessen wurde.
Vorbedingungen	HPC betriebsbereit
Nachbedingungen	• Bei Antwort 90 00: Neue Karteninhaber-PIN gesetzt – kein Setzen des Sicherheitsstatus, d.h. vor Zugriff auf PIN-geschützte Funktionen oder Daten muss UC_HPC_Verify_PIN durchgeführt werden. • Bei Antwort 63CX: Usage Limitation der PUK der Karteninhaber-PIN dekrementiert d.h. er war vorher noch nicht Null. Noch X verbleibende Versuche (x= 9, 8, ...1 oder 0). Wenn 63C0 zurückgeliefert wird, wurde die Verifikationsmethode der PUK der Karteninhaber-PIN blockiert, d.h. es ist kein weiteres RESET RC möglich und die mit der Karteninhaber-PIN geschützten Funktionen oder Daten sind nicht mehr nutzbar. • Bei Antwort 63 83: PUK-Verifikationsmethode der Karteninhaber-PIN blockiert, Usage Limitation des PUK der Karteninhaber-PIN auf Null.
Standardablauf	1. Schritt: Durchführung des Kommandos RESET RETRY COUNTER mit PUK der Karteninhaber-PIN und neuer Karteninhaber-PIN jeweils im Format 2 PIN Block
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Wenn die Karteninhaber-PIN-Verifikationsmethode blockiert ist, d.h. die Karteninhaber-PIN mehrmals hintereinander (Maximalwert des Retry Counter der Karteninhaber-PIN) falsch eingegeben wurde. Sonst beliebig.
Vorangegangene Use Cases	Mindestens UC_HPC_Reset
Nachfolgende Use Cases	• UC_HPC_Verify_PIN • UC_HPC_Reset_RC_PIN (falls PUK-Verifikation nicht erfolgreich) • UC_HPC_Set_PIN (falls PUK-Verifikation nicht erfolgreich)
Anmerkungen	Informationen zum PIN-Management: [HPC-P1], 7 und [HPC-P2], 5.2.7. Maximalwert des Retry Counter der Karteninhaber-PIN ist entsprechend dem Initial Value 3. Maximalwert der Usage Limitation der PUK der Karteninhaber-PIN ist entsprechend dem Initial Value 10.
Festlegungen	-

1. Schritt (von 1):
Tabelle 55 – Kommando: RESET RC ([HPC-P2], 5.5.3, Table 16)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten (16 Bytes)**	**Le**
00	2C	00	01	10	Eingegebene PUK und eingegebene neue Karteninhaber-PIN in zwei Format 2 PIN Blöcken, z.B. 28 12 34 56 78 FF FF FF 26 65 43 21 FF FF FF FF für die achtstellige PUK 12345678 und die sechstellige neue PIN 654321	-

Tabelle 56 – Korrekte Antworten ([HPC-P2], 5.5.3, Table 17 und [HPC-P1], Table A.16)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	PUK-Verifikation der Karteninhaber-PIN erfolgreich und neue Karteninhaber-PIN gesetzt	Use Case beenden
-	63 83	PUK-Verifikationsmethode der Karteninhaber-PIN blockiert	Mit Karteninhaber-PIN geschützte Funktionen oder Daten nicht mehr nutzbar.
-	63 CX (X > 0)	PUK-Verifikation der Karteninhaber-PIN nicht erfolgreich, d.h. PUK der Karteninhaber-PIN wurde falsch eingegeben; X weitere Versuche möglich	UC_HPC_Set_PIN oder UC_HPC_Reset_RC_PIN
-	63 C0	PUK-Verifikation nicht erfolgreich, keine weitere Versuche mehr möglich	Mit Karteninhaber-PIN geschützte Funktionen oder Daten nicht mehr nutzbar.

Tabelle 57 – Abweichende Antworten ([HPC-P1], Table A.16)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in Format 2 PIN Block	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

7.5 Verifizieren der QES-PIN

Tabelle 58 – Verifizieren der QES-PIN

Identifier	**UC_HPC_Verify_QES_PIN**
Name	Verifizieren der QES-PIN
Beschreibung	Prüfen der vom Heilberufler eingegebenen QES-PIN vor dem Erzeugen einer qualifizierten elektronischen Signatur.
Vorbedingungen	HPC betriebsbereit DF.QES geöffnet
Nachbedingungen	• Bei Antwort 90 00: Sicherheitsstatus »QES-PIN-Verifikation erfolgreich« und Retry Counter der QES-PIN auf Maximalwert. • Bei Antwort 63CX: Retry Counter der QES-PIN dekrementiert d.h. er war vorher noch nicht Null. Noch X verbleibende Versuche (x=2 oder 1 oder 0). Wenn 63C0 zurückgeliefert wird, wurde die Verifikationsmethode der QES-PIN blockiert, d.h. es ist kein weiteres VERIFY möglich, wenn nicht zunächst der Retry Counter der QES-PIN (durch UC_HPC_Reset_RC_QES_PIN) zurückgesetzt wird. • Bei Antwort 63 83: QES-PIN-Verifikationsmethode blockiert, Retry Counter der QES-PIN auf Null.
Standardablauf	1. Schritt: Durchführung des Kommandos VERIFY mit QES-PIN im Format 2 PIN Block
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	In HPC-Sessions mit Erstellen von qualifizierten elektronischen Signaturen in Abhängigkeit vom Security Status Evaluation Counter am privaten Signaturschlüssel PrK.HP.QES, siehe [HPC-P1], 7 (letzter Absatz) und [HPC-P2], 8.1.2.
Vorangegangene Use Cases	• UC_HPC_Select_QES • UC_HPC_Verify_QES_PIN (falls Verifikation nicht erfolgreich)
Nachfolgende Use Cases	• UC_HPC_Verify_QES_PIN (falls Verifikation nicht erfolgreich) • UC_HPC_Reset_RC_QES_PIN (falls Verifikation blockiert) Zum Erstellen einer qualifizierten elektronischen Signatur: • UC_HPC_SIGN
Anmerkungen	Informationen zum PIN-Management: [HPC-P1], 7 und [HPC-P2], 8.1.3. Maximalwert des Retry Counter der QES-PIN ist entsprechend Initial Value 3. Es wird derzeit noch geprüft, ob die Häufigkeit der PIN-Präsentation in Abhängigkeit vom Security Environment wie folgt einstellbar ist: SE#01: kein TC => PIN-Eingabe vor jeder Signatur SE#02: mit TC =>
Festlegungen	-

1. Schritt (von 1):
Tabelle 59 – Kommando: VERIFY ([HPC-P2], 8.5.1, Table 52)

CLA	INS	P1	P2	Lc	Daten (8 Bytes)	Le
00	20	00	81	08	Eingegebene QES-PIN im Format 2 PIN Block, z.B. 26 12 34 56 FF FF FF FF für die sechstellige QES-PIN 123456	-

Tabelle 60 – Korrekte Antworten ([HPC-P2], 8.5.1, Table 53 und [HPC-P1], Table A.14)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	QES-PIN-Verifikation erfolgreich	Use Case beenden
-	63 83	QES-PIN-Verifikationsmethode blockiert	UC_HPC_Reset_RC_QES_PIN
-	63 CX (X > 0)	QES-PIN-Verifikation nicht erfolgreich, d.h. QES-PIN falsch eingegeben: X weitere Versuche möglich	UC_HPC_Verify_QES_PIN
-	63 C0	QES-PIN-Verifikation nicht erfolgreich erfolgreich, keine weitere Versuche mehr möglich	UC_HPC_Reset_RC_QES_PIN

Tabelle 61 – Abweichende Antworten ([HPC-P1], Table A.14)

SW1 SW2	**Fehlerbedingung**	**Ursache**	**Aktion**
6A 80	Formatfehler in Format 2 PIN Block	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

7.6 Ändern der QES-PIN

Tabelle 62 – Ändern der QES-PIN

Identifier	**UC_HPC_Change_QES_PIN**
Name	Ändern der QES-PIN
Beschreibung	Prüfen der vom Heilberufler eingegebenen alten QES-PIN und Ersetzen der alten QES-PIN durch die eingegebene neue QES-PIN.
Vorbedingungen	HPC betriebsbereit DF.QES geöffnet
Nachbedingungen	• Bei Antwort 90 00: Sicherheitsstatus »QES-PIN-Verifikation erfolgreich«, Retry Counter der QES-PIN auf Maximalwert und alte QES-PIN durch neue QES-PIN ersetzt. • Bei Antwort 63CX: Retry Counter der QES-PIN dekrementiert d.h. er war vorher noch nicht Null. Noch X verbleibende Versuche (x=2 oder 1 oder 0). Wenn 63C0 zurückgeliefert wird, wurde die Verifikationsmethode der QES-PIN blockiert, d.h. es ist kein weiteres VERIFY möglich, wenn nicht zunächst der Retry Counter der QES-PIN (durch UC_HPC_Reset_RC_QES_PIN) zurückgesetzt wird. • Bei Antwort 63 83: QES-PIN-Verifikationsmethode blockiert, Retry Counter der QES-PIN auf Null.
Standardablauf	1. Schritt: Durchführung des Kommandos CHANGE RD mit alter QES-PIN und neuer QES-PIN jeweils im Format 2 PIN Block
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Einmal zu Beginn der HPC-Nutzung, falls es sich bei der alten QES-PIN um eine Transport-PIN handelt. Sonst beliebig.
Vorangegangene Use Cases	• UC_HPC_Select_QES • UC_HPC_Change_QES_PIN (falls Verifikation nicht erfolgreich)
Nachfolgende Use Cases	• UC_HPC_Change_QES_PIN (falls Verifikation nicht erfolgreich) • UC_HPC_Reset_RC_QES_PIN (falls Verifikation blockiert) Zum Erstellen einer qualifizierten elektronischen Signatur: • UC_HPC_VERIFY_QES_PIN (siehe Anmerkungen), UC_HPC_SIGN
Anmerkungen	• Informationen zum PIN-Management: [HPC-P1], 7 und [HPC-P2], 8.1.3. Maximalwert des Retry Counter der QES-PIN ist entsprechend dem Initial Value 3. • Bei der Eingabe der Transport-PIN sind die herstellerspezifischen Angaben zu beachten (z.B. Eingabe einer NULL-PIN bzw. einer 5-stelligen Transport-PIN). • Ob ein Sicherheitsstatus gesetzt wird, wenn es sich bei der alten QES-PIN um eine Transport-PIN handelt, ist abhängig vom Transport-PIN-Verfahren der HPC, siehe [HPC-P2], 8.5.2.
Festlegungen	-

1. Schritt (von 1):
Tabelle 63 – Kommando: CHANGE RD ([HPC-P2], 8.5.2, Table 54)

CLA	INS	P1	P2	Lc	Daten (16 Bytes)	Le
00	24	00	81	10	Eingegebene alte QES-PIN und eingegebene neue QES-PIN in zwei Format 2 PIN Blöcken, z.B. 26 12 34 56 FF FF FF FF 26 65 43 21 FF FF FF FF für die sechstellige alte QES-PIN 123456 und die sechstellige neue QES-PIN 654321	-

Tabelle 64 – Korrekte Antworten ([HPC-P2], 8.5.2, Table 55 und [HPC-P1], Table A.15)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	QES-PIN-Verifikation erfolgreich und QES-PIN geändert	Use Case beenden
-	63 83	QES-PIN-Verifikationsmethode blockiert	UC_HPC_Reset_RC_QES_PIN
-	63 CX	QES-PIN-Verifikation nicht erfolgreich, d.h. alte QES-PIN wurde falsch eingegeben, X weitere Versuche möglich	UC_HPC_Change_QES_PIN
-	63 C0	QES-PIN-Verifikation nicht erfolgreich erfolgreich, keine weitere Versuche mehr möglich	UC_HPC_Reset_RC_QES_PIN

Tabelle 65 – Abweichende Antworten ([HPC-P1], Table A.15)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in Format 2 PIN Block	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

7.7 Rücksetzen des Retry Counter der QES-PIN

Tabelle 66 – Rücksetzen des Retry Counter der QES-PIN

Identifier	**UC_HPC_Reset_RC_QES_PIN**
Name	Rücksetzen des Retry Counter der QES-PIN
Beschreibung	Prüfen des vom Heilberufler eingegebenen Resetting Code (Personal Unblocking Key, PUK) der QES-PIN.
Vorbedingungen	HPC betriebsbereit DF.QES geöffnet
Nachbedingungen	• Bei Antwort 90 00: Retry Counter der QES-PIN auf Maximalwert – kein Setzen des Sicherheitsstatus • Bei Antwort 63CX: Usage Limitation der PUK der QES-PIN dekrementiert d.h. er war vorher noch nicht Null. Noch X verbleibende Versuche (x= 9, 8, ...1 oder 0). Wenn 63C0 zurückgeliefert wird, wurde die Verifikationsmethode der PUK der QES-PIN blockiert, d.h. es ist kein weiteres RESET RC möglich und die mit der QES-PIN geschützten Funktionen oder Daten sind nicht mehr nutzbar. • Bei Antwort 63 83: PUK-Verifikationsmethode der QES-PIN blockiert, Usage Limitation der PUK der QES-PIN auf Null.
Standardablauf	1. Schritt: Durchführung des Kommandos RESET RETRY COUNTER mit der PUK der QES-PIN im Format 2 PIN Block
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Wenn die QES-PIN-Verifikationsmethode blockiert ist, d.h. die QES-PIN mehrmals hintereinander (Maximalwert des Retry Counter) falsch eingegeben wurde.
Vorangegangene Use Cases	• UC_HPC_Verify_QES_PIN (falls Verifikation nicht erfolgreich und Verifikationsmethode blockiert) • UC_HPC_Reset_RC_QES_PIN (falls PUK-Verifikation nicht erfolgreich)
Nachfolgende Use Cases	• UC_HPC_Reset_RC_QES_PIN (falls PUK-Verifikation nicht erfolgreich) Zum Erstellen einer qualifizierten elektronischen Signatur: • UC_HPC_Verify_QES_PIN und UC_HPC_SIGN
Anmerkungen	• Informationen zum PIN-Management: [HPC-P1], 7 und [HPC-P2], 8.1.3. Maximalwert des Retry Counter der QES-PIN ist 3. Maximalwert der Usage Limitation der QES-PUK ist 10. • Das Setzen einer neuen QES-PIN ist mit diesem Kommando ist nicht erlaubt. • Wenn die Verifikationsmethode der QES-PIN nicht blockiert ist, kann die Karte unterschiedlich reagieren: Der Befehl wird entweder ausgeführt oder es wird ein Fehler zurückgegeben (z.B. SW1 SW2 = 69 85: Nutzungsbedingungen nicht erfüllt).
Festlegungen	-

1. Schritt (von 1):
Tabelle 67 – Kommando: RESET RC ([HPC-P2], 5.5.3, Table 56)

CLA	INS	P1	P2	Lc	Daten (8 Bytes)	Le
00	2C	01	81	08	Eingegebene PUK im Format 2 PIN Block, z.B. 26 12 34 56 78 FF FF FF für die achtstellige PUK 12345678 der QES-PIN	-

Tabelle 68 – Korrekte Antworten ([HPC-P2], 5.5.3, Table 57 und [HPC-P1], Table A.16)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	PUK-Verifikation der QES-PIN erfolgreich, Retry Counter der QES-PIN auf Maximalwert	Use Case beenden
-	69 85	Retry-Counter kann nur dann zurückgesetzt werden, wenn er auf Null steht, d.h. die Verifikationsmethode der QES-PIN blockiert ist. Dies ist nicht der Fall.	Use Case beenden
-	63 83	PUK-Verifikationsmethode der QES-PIN blockiert	Mit QES-PIN geschützte Signatur-Funktion nicht mehr nutzbar
-	63 CX (X > 0)	PUK-Verifikation der QES-PIN nicht erfolgreich, d.h. PUK der QES-PIN wurde falsch eingegeben, X weitere Versuche möglich	UC_HPC_Reset_RC_QES_PIN
-	63 C0	PUK-Verifikation nicht erfolgreich, keine weitere Versuche mehr möglich	Mit QES-PIN geschützte Signatur-Funktion nicht mehr nutzbar

Tabelle 69 – Abweichende Antworten ([HPC-P1], Table A.16)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in Format 2 PIN Block	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

8 Anwendungsselektion

8.1 Öffnen der HP-Anwendung

Tabelle 70 – Öffnen der HP-Anwendung

Identifier	**UC_HPC_Open_HPA**
Name	Öffnen der HP-Anwendung
Beschreibung	Die Health Professional Application (HPA) wird zum Lesen oder Aktualisieren der HP-bezogenen Daten geöffnet.
Vorbedingungen	HPC betriebsbereit
Nachbedingungen	DF.HPA geöffnet
Standardablauf	1. Schritt: Durchführung des Kommandos mit Application Identifier der HPA
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Immer dann, wenn die in EF.HPD ([HPC-P2], 7.1.2) vorhandenen HP-bezogenen Daten gelesen oder aktualisiert werden sollen.
Vorangegangene Use Cases	Alle Use Cases auf MF-Ebene zur Initialisierung und Identifizierung der HPC (Initialisierungsphase)
Nachfolgende Use Cases	Zum Lesen bzw. Aktualisieren der HP-bezogenen Daten: • UC_HPC_Read_HP_Data • UC_HPC_Update_HP_Data
Anmerkungen	Es wird empfohlen, die Selektion der HP-Anwendung erst dann auszuführen, wenn alle globalen Datenobjekte auf MF-Ebene ausgelesen wurden, da ein direkter Zugriff auf EFs auf MF-Ebene von der DF-Ebene aus nicht möglich ist. Die HP-Anwendung bleibt solange aktiv, bis sie durch eine der folgenden Aktionen beendet wird: • Ein Reset wird durchgeführt: UC_HPC_Reset Eine andere Karten-Anwendung wird geöffnet: UC_HPC_Open_ ESIGN, UC_HPC_Open_CIA_ESIGN, UC_HPC_Open_QES • Die »HPC-Session« wird beendet
Festlegungen	-

1. Schritt (von 1):
Tabelle 71 – Kommando: SELECT ([HPC-P2], 7.3, Table 42)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten (6 Bytes)**	**Le**
00	A4	04	0C	06	D2 76 00 00 40 02	-
Application Identifier von DF.HPA im Datenfeld, siehe Anmerkungen in der Beschreibung von UC_HPC_Read_Dir und zum 1. Schritt des Anwendungsfalls.						

Tabelle 72 – Korrekte Antwort ([HPC-P2], 7.3, Table 43)

Daten	**SW1 SW2**	**Ursache**	**Aktion**
-	90 00	DF.HPA erfolgreich selektiert	Use Case beenden

Tabelle 73 – Abweichende Antworten ([HPC-P1], Table A.2)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 82	DF.HPA nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
62 83	DF.HPA deaktiviert		

8.2 Öffnen der QES-Anwendung

Tabelle 74 – Öffnen der QES-Anwendung

Identifier	**UC_HPC_Open_QES**
Name	Öffnen der QES-Anwendung
Beschreibung	Die Signatur-Anwendung QES wird zum Lesen der X.509-Zertifikate, zum Ersetzen der Attribut-Zertifikate, zum Erzeugen einer qualifizierten Signatur, zur Durchführung von PIN.QES-Management-Funktionen und zum Ändern der Display Message geöffnet.
Vorbedingungen	HPC betriebsbereit QES-spezifische Use Cases sollen durchgeführt werden
Nachbedingungen	DF.QES geöffnet
Standardablauf	1. Schritt: Durchführung des Kommandos SELECT mit Angabe des Application Identifiers der QES-Anwendung
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Immer dann, wenn die QES-Anwendung im Zustand »geschlossen« ist und QES-spezifische Use Cases durchgeführt werden sollen.
Vorangegangene Use Cases	Alle Use Cases auf MF-Ebene zur Initialisierung und Identifizierung der HPC (Initialisierungsphase)
Nachfolgende Use Cases	Abhängig vom Anwendungskontext können folgende Use Cases folgen: Zum Abrufen der X.509-Zertifikate: • UC_HPC_Read_QES_BC • UC_HPC_Read_QES_AC Zum Ersetzen der Attribut-Zertifikate bzw. Ändern der Display Message: • UC_HPC_Verify_PIN Für das Management der Signatur-PIN: • UC_HPC_Change_QES_PIN (PIN.QES ändern) • UC_HPC_Reset_RC_QES_PIN Zum Erzeugen einer qualifizierten Signatur: • UC_HPC_Verify_QES_PIN Zum Anzeigen der Display Message Im Kontext Trusted Channel: • UC_HPC_Read_DM
Anmerkungen	Es wird empfohlen, die Selektion der QES-Anwendung erst dann auszuführen, wenn alle globalen Datenobjekte auf MF-Ebene ausgelesen wurden, da ein direkter Zugriff auf EFs auf MF-Ebene von der DF-Ebene aus nicht möglich ist. Die QES-Anwendung bleibt solange geöffnet, bis sie durch eine der folgenden Aktionen geschlossen wird: • Ein Reset wird durchgeführt: UC_HPC_Reset • Eine andere Karten-Anwendung wird selektiert: UC_HPC_Open_HPA, UC_HPC_Open_ESIGN, UC_HPC_Open_CIA_ESIGN • Die »HPC-Session« wird beendet
Festlegungen	-

1. Schritt (von 1):
Tabelle 75 – Kommando: SELECT ([HPC-P2], 8.4, Table 50)

CLA	INS	P1	P2	Lc	Daten	Le
00	A4	04	0C	06	D2 76 00 00 66 01	-
Application Identifier von DF.QES im Datenfeld						

Tabelle 76 – Korrekte Antwort ([HPC-P2], 8.4, Table 51)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	DF.QES erfolgreich selektiert	Use Case beenden

Tabelle 77 – Abweichende Antworten ([HPC-P1], Table A.2)

SW1 SW2	Beschreibung	Ursache	Aktionen
6A 82	DF.QES nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine manipulierte / defekte Karte.	Fehlerausgang »HPC defekt«
62 83	DF.QES deaktiviert		

8.3 Öffnen der ESIGN-Anwendung

Tabelle 78 – Öffnen der ESIGN-Anwendung

Identifier	**UC_HPC_Open_ESIGN**
Name	Öffnen der ESIGN-Anwendung
Beschreibung	Die ESIGN-Anwendung zur Durchführung der PKI-Funktionen Dechiffrierung eines Dokumenten-Chiffrierschlüssels und Client-Authentisierung, zum Lesen der X.509-Zertifikate und zum Ändern der Display Message wird geöffnet.
Vorbedingungen	HPC betriebsbereit ESIGN-spezifische Use Cases sollen durchgeführt werden
Nachbedingungen	DF.ESIGN geöffnet
Standardablauf	1. Schritt: Durchführung des Kommandos SELECT mit Angabe des Application Identifiers der ESIGN-Anwendung
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Immer dann, wenn die ESIGN-Anwendung im Zustand »geschlossen« ist und ESIGN-spezifische Use Cases ausgeführt werden sollen.
Vorangegangene Use Cases	Alle Use Cases auf MF-Ebene zur Initialisierung und Identifizierung der HPC (Initialisierungsphase)
Nachfolgende Use Cases	Abhängig vom Anwendungskontext können folgende Use Cases folgen: Zum Abrufen der X.509-Zertifikat: • UC_HPC_Read_ESIGN_AUT • UC_HPC_Read_ESIGN_DEC Zur Durchführung der Client-Authentisierung / Dechiffrierung eines Dokumenten-Chiffrierschlüssels / Ändern der Display Message: • UC_HPC_Verify_PIN PIN-Management Use Cases: • UC_HPC_Change_PIN • UC_HPC_Reset_RC_PIN • UC_HPC_Set_PIN Zum Anzeigen der Display Message Im Kontext Trusted Channel: • UC_HPC_Read_DM
Anmerkungen	Es wird empfohlen, die Selektion der ESIGN-Anwendung erst dann auszuführen, wenn alle globalen Datenobjekte auf MF-Ebene ausgelesen wurden, da ein direkter Zugriff auf EFs auf MF-Ebene von der DF-Ebene aus nicht möglich ist. Die ESIGN-Anwendung bleibt solange geöffnet, bis sie durch eine der folgenden Aktionen geschlossen wird: • Ein Reset wird durchgeführt: UC_HPC_Reset • Eine andere Karten-Anwendung wird selektiert: UC_HPC_Open_HPA, UC_HPC_Open_QES, UC_HPC_Open_CIA_ESIGN • Die »HPC-Session« wird beendet
Festlegungen	-

1. Schritt (von 1):
Tabelle 79 – Kommando: SELECT ([HPC-P2], 9.3, Table 75)

CLA	INS	P1	P2	Lc	Daten	Le
00	A4	04	0C	0A	A0 00 00 01 67 45 53 49 47 4E	-
Application Identifier von DF.ESIGN im Datenfeld						

Tabelle 80 – Korrekte Antwort ([HPC-P2], 9.3, Table 76)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	DF.ESIGN erfolgreich selektiert	Use Case beenden

Tabelle 81 – Abweichende Antworten ([HPC-P1], Table A.2)

SW1 SW2	Beschreibung	Ursache	Aktionen
6A 82	DF.ESIGN nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine manipulierte / defekte Karte.	Fehlerausgang »HPC defekt«
62 83	DF.ESIGN deaktiviert		

8.4 Öffnen der CIA.ESIGN-Anwendung

Tabelle 82 – Öffnen der CIA_ESIGN-Anwendung

Identifier	**UC_HPC_Open_CIA_ESIGN**
Name	Öffnen der CIA_ESIGN-Anwendung
Beschreibung	Die CIA_ESIGN-Anwendung wird zum Lesen der CIA-Datenfiles geöffnet. Die CIA-Datenfiles enthalten Informationen über Algorithmen, Dateikennungen etc., die für die Nutzung der ESIGN-Anwendung relevant sind.
Vorbedingungen	HPC betriebsbereit Die CIA_ESIGN_Informationsobjekte der HPC sind dem System noch nicht bekannt
Nachbedingungen	DF.CIA.ESIGN geöffnet
Standardablauf	1. Schritt: Durchführung des Kommandos SELECT mit Angabe des Application Identifiers der CIA_ESIGN-Anwendung
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Abhängig vom Design des Karten-Service-Providers. Innerhalb eines Primärsystems sollten aus Gründen der Performanz die CIA-Informationsobjekte nur einmal beim Erstkontakt mit einer unbekannten HPC ausgelesen und dann im Primärsystem persistent gespeichert werden, siehe Anhang A.2. Wird die HPC von einem Karten-Service-Provider bedient, der eine solche Archivierungsfunktion nicht bietet, dann sollte das Lesen der Informationsobjekte immer in der Initialisierungsphase einer Karte erfolgen.
Vorangegangene Use Cases	Alle Use Cases auf MF-Ebene zur Initialisierung und Identifizierung der HPC (Initialisierungsphase)
Nachfolgende Use Cases	Lesen der CIA-Datenfiles: • UC_HPC_Read_CIA_ESIGN_Info
Anmerkungen	Es wird empfohlen, die Selektion der CIA_ESIGN-Anwendung erst dann auszuführen, wenn alle globalen Datenobjekte auf MF-Ebene ausgelesen wurden, da ein direkter Zugriff auf EFs auf MF-Ebene von der DF-Ebene aus nicht möglich ist. Die CIA_ESIGN-Anwendung bleibt solange geöffnet, bis sie durch eine der folgenden Aktionen geschlossen wird: • Ein Reset wird durchgeführt (UC_HPC_Reset) • Eine andere Karten-Anwendung wird selektiert (UC_HPC_Open_HPA, UC_HPC_Open_ESIGN, UC_HPC_Open_QES) • Die »HPC-Session« wird beendet
Festlegungen	-

1. Schritt (von 1):
Tabelle 83 – Kommando: SELECT ([HPC-P2], 10.2, Table 87)

CLA	INS	P1	P2	Lc	Daten	Le
00	A4	04	0C	0F	E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E	-
Application Identifier von CIA_ESIGN im Datenfeld						

Tabelle 84 – Korrekte Antwort ([HPC-P2], 10.2, Table 88)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	DF.CIA.ESIGN erfolgreich selektiert	Use Case beenden

Tabelle 85 – Abweichende Antworten ([HPC-P1], Table A.2)

SW1 SW2	Beschreibung	Ursache	Aktionen
6A 82	DF.CIA.ESIGN nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine manipulierte / defekte Karte.	Fehlerausgang »HPC defekt«
62 83	DF.CIA.ESIGN deaktiviert		

9 Nutzung der QES-Funktion

9.1 Erzeugen einer qualifizierten elektronischen Signatur (mit / ohne Attributzertifikate)

Tabelle 86 – Erzeugen einer qualifizierten elektronischen Signatur

Identifier	**UC_HPC_SIGN**
Name	Erzeugen einer qualifizierten elektronischen Signatur
Beschreibung	Über einen Hashwert wird unter Verwendung des privaten Signatur-Schlüssels PrK.HP.QES eine qualifizierte Signatur erzeugt. Für das Hashen stehen zwei Verfahren zur Verfügung: • Hashen komplett außerhalb des HPC • Finales Hashen im HPC.
Vorbedingungen	HPC betriebsbereit Daten sind zu signieren Der Hashwert der zu signierenden Daten (z.B. eVerordnung) wurde vollständig außerhalb der HPC berechnet und liegt vor Der im Datenfeld zu übergebende DigestInfo ist gemäß PKCS#1 formatiert ([HPC-P2], Table E.1.2) DF.QES geöffnet Der Leistungserbringer ist mit QES-PIN authentisiert und der Security Status Evaluation Counter (SSEC) hat einen Wert ungleich Null
Nachbedingungen	Falls die Signaturberechnung erfolgreich war, erhalten die Ausgabedaten die elektronische Signatur. Der Zustand in der Karte ist unverändert, falls SSEC den Wert "unendlich" hat; falls SSEC einen bestimmten Wert hat, wird SSEC um 1 dekrementiert. Weitere Signaturen sind möglich, falls SSEC ungleich Null.
Standardablauf	a) Signieren mit Hashen außerhalb des HPC 1. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) mit Option SET zur Selektion des privaten Signatursschlüssels und des Algorithmus. 2. Schritt: Durchführung des Kommandos PSO:COMPUTE DS mit DigestInfo ohne Padding im Datenfeld. Das Padding erfolgt in der Karte. b) Signieren mit »Final Hashing« im HPC 1. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) mit Option SET zur Selektion des Hash-Algorithmus. 2. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) mit Option SET zur Selektion des privaten Signatursschlüssels und des Algorithmus. 3. Schritt: Durchführung des Kommandos PSO: HASH mit Hash-Zwischenwert, Anzahl der bereits gehashten Bits und letztem Teil der zu hashenden Daten. 4. Durchführung des Kommandos PSO:COMPUTE DS ohne Daten
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Pro Erstellung eines zu signierenden Datensatzes.
Vorangegangene Use Cases	UC_HPC_Open_QES UC_HPC_Read_QES_AC, wenn Attributszertifikate in das zu signierende Dokument einfließen sollen und diese der Signaturanwendung noch nicht vorliegen UC_HPC_Verify_QES_PIN, vor dem ersten Aufruf und wenn Security Status Evaluation Counter abgelaufen

Nachfolgende Use Cases	Abhängig vom Anwendungskontext Wenn weitere Daten zu signieren sind, dann sind folgende Use Cases durchzuführen: • UC_HPC_Verify_QES_PIN (wenn PIN-Eingabe jedes Mal gefordert bzw. Status Evaluation Counter abgelaufen ist) • UC_HPC_SIGN
Anmerkungen	Der Security Status Evaluation Counter kann nicht abgefragt werden und [7816-15] sieht ein solches Key-Attribut nicht vor. Will ein Karten-Service-Provider die Anzahl der möglichen Signaturen nach PIN.QES kontrollieren und überwachen, müsste der Wert über ein Konfig-File konfiguriert werden. In Bezug auf das Hashen sind beide Verfahren vom HPC zu unterstützen, da sie auch in [HPC-P1] beschrieben sind. Es kann empfohlen werden, das weniger komplexe Verfahren »Hashen außerhalb der Karte« zu implementieren.
Festlegungen	In der HPC wird das Padding-Verfahren nach PKCS#1 eingesetzt, d.h. im Datenfeld ist immer DigestInfo zu übergeben, d.h. als Algorithmusreferenz ist entweder '12' bei Verwendung von SHA-1 oder '42' bei Verwendung von SHA-256 mit 256 bit (siehe [HPC-P1], Table 10) anzugeben. Ob '12'oder '42' anzugeben ist, hängt von der im X.509-QES-Zertifikat angegebenen OID ab. Welche AlgRef zu nehmen ist, sollte einmal pro HPC ermittelt und dann in den HPC-Stack aufgenommen werden, siehe Anhang A.2.

a) Signieren mit Hashen außerhalb des HPC

1. Schritt (von 2):
Tabelle 87 – Kommando: MSE Option SET ([HPC-P2], 8.6.2, Table 66)

CLA	INS	P1	P2	Lc	Daten (6 Bytes)	Le
00	22	41	B6	06	84 01 84 80 01 xx (3 Byte Referenz des privaten Signaturschlüssels PrK.HP.QES, [HPC-P2], 8.1.2, Table 48 || 3 Byte Referenz des Algorithmus [HPC-P1], Table 10, in Abhängigkeit vom OID im X.509 Signaur-Basisizertifikat) Beispiel für RSA mit SHA-1und PKCS#1-Padding: 84 01 84 80 01 12	-

Tabelle 88 – Korrekte Antwort ([HPC-P2], 8.6.2, Table 67)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz und Algorithmusreferenz erfolgreich registriert.	2. Schritt

Tabelle 89 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
6A 88	Referenzierte Daten nicht gefunden	Dieser Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

2. Schritt (von 2):
Tabelle 90 – Kommando: PSO: COMPUTE DS ([HPC-P2], 8.6.2, Table 66)

CLA	INS	P1	P2	Lc	Daten	Le
00	2A	9E	9A	xx	DigestInfo ([HPC-P2], E.1.2) Beispiel: SHA-1 mit OID {1 3 14 3 2 26} ([HPC-P1], Table 7) 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 || 20 Byte Hash Value	00
Aus Gründen der Sicherheit darf die Länge des Datenfeldes (DigestInfo) höchstens 40% der Moduluslänge des Signatur-Schlüssels betragen ([HPC-P1],4.1, Table 6) (Angriff: Desmedt / Odlytzko-Attacke); dies wird durch die im Algorithmen-Katalog [ALGCAT] vorgegebenen Algorithmen-Kombinationen sichergestellt.						

Tabelle 91 – Korrekte Antwort ([HPC-P2], 8.6.2, Table 67)

Daten	SW1 SW2	Ursache	Aktion
Signatur	90 00	Signatur erfolgreich berechnet	Use Case beenden

Tabelle 92 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
6A 88	Referenzierte Daten nicht gefunden	Dieser Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

b) Signieren mit »Final Hashing« in der HPC

1. Schritt (von 4):

Tabelle 93 – Kommando: MSE Option SET ([HPC-P2], 8.6.1, Table 58)

CLA	INS	P1	P2	Lc	Daten (6 Bytes)	Le
00	22	41	AA	03	80 01 xx (3 Byte Referenz des Algorithmus [HPC-P1], Table 10, in Abhängigkeit vom OID im X.509 Signaur-Basisizertifikat) Beispiel für SHA-1: 80 01 10	-

Tabelle 94 – Korrekte Antwort ([HPC-P2], 8.6.1, Table 59)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Algorithmusreferenz erfolgreich registriert.	2. Schritt

Tabelle 95 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
6A 88	Referenzierte Daten nicht gefunden	Dieser Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

2. Schritt (von 4):
Tabelle 96 – Kommando: MSE Option SET ([HPC-P2], 8.6.1, Table 60)

CLA	INS	P1	P2	Lc	Daten (6 Bytes)	Le
00	22	41	B6	06	84 01 84 80 01 xx (3 Byte Referenz des privaten Signaturschlüssels PrK.HP.QES, [HPC-P2], 8.1.2, Table 48 || 3 Byte Referenz des Algorithmus [HPC-P1], Table 10, in Abhängigkeit vom OID im X.509 Signaur-Basisizertifikat) B Beispiel für RSA mit SHA-1und PKCS#1-Padding: 84 01 84 80 01 12	-

Tabelle 97 – Korrekte Antwort ([HPC-P2], 8.6.2, Table 61)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz und Algorithmusreferenz erfolgreich registriert.	3. Schritt

Tabelle 98 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
6A 88	Referenzierte Daten nicht gefunden	Dieser Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

3. Schritt (von 4):
Tabelle 99 – Kommando: PSO: PSO: HASH ([HPC-P2], 8.6.1, Table 62)

CLA	INS	P1	P2	Lc	Daten	Le
00	2A	90	A0	xx	90 xx Intermediate Hash-Value 80 xx Final block (ohne Padding)	-
Beispiel für SHA1 (Intermediate Value = 20 Byte + 8 Byte für Anzahl der bereits gehashten bits): 00 2A 90 A0 25 **90 1c** 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 00 00 00 00 00 00 01 08 **80 05** 54 85 41 36 19						

Tabelle 100 – Korrekte Antwort ([HPC-P2], 8.6.2, Table 63)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Kommando erfolgreich ausgeführt	4. Schritt

Tabelle 101 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
6A 88	Referenzierte Daten nicht gefunden	Dieser Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

4. Schritt (von 4):
Tabelle 102 – Kommando: PSO: COMPUTE DS ([HPC-P2], 8.6.1, Table 64)

CLA	INS	P1	P2	Lc	Daten	Le
00	2A	9E	9A	-	-	00

Tabelle 103 – Korrekte Antwort ([HPC-P2], 8.6.1, Table 65)

Daten	SW1 SW2	Ursache	Aktion
Signatur	90 00	Signatur erfolgreich berechnet	Use Case beenden

Tabelle 104 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
6A 88	Referenzierte Daten nicht gefunden	Dieser Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

10 Nutzung QES-Zertifikate

10.1 Lesen QES-X.509-Basiszertifikat

Tabelle 105 – Lesen des X.509 Signatur-Basiszertifikats

Identifier	**UC_HPC_Read_QES_BC**
Name	Lesen des X.509 Signatur-Basiszertifikats
Beschreibung	Das im HPC gespeicherte X.509 Signatur-Basiszertifikat wird gelesen.
Vorbedingungen	HPC betriebsbereit DF.QES geöffnet
Nachbedingungen	Falls das Lesen erfolgreich war, enthalten die Ausgabedaten das X.509-Signatur-Basiszertifikat. Weitere QES-Use Cases sind möglich.
Standardablauf	a) Ohne Extended Length: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP.QES 2. Schritt: Senden von weiteren READ BINARY-Kommandos, bis X.509-QES-Zertifikat vollständig gelesen. b) Mit Extended Length und n > Dateilänge: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP.QES und Le = 00 00 00 (3 Byte) c) Mit Extended Length und n < Dateilänge: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP.QES und Le = 00 xx xx (3 Byte) 2. Schritt: Senden von weiteren READ BINARY-Kommandos, bis X.509-QES-Zertifikat vollständig gelesen.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Einmal beim Erstkontakt mit einer bisher unbekannten Karte, falls das Zertifikat im Primärsystem persistent gespeichert wird (siehe Anhang A.2).
Vorangegangene Use Cases	UC_HPC_Open_QES
Nachfolgende Use Cases	Abhängig vom Anwendungskontext
Anmerkungen	-
Festlegungen	Falls wiederholt aus derselben Datei gelesen wird, ist es aus Performanz-gründen sinnvoll, dass ab dem zweiten READ BINARY der SFID in P1 nicht angegeben wird, sondern P1 und P2 für den Offset zur Verfügung stehen.

a) Ohne Extended Length

1. Schritt (von 2):
Tabelle 106 – Kommando: READ BINARY ([HPC-P2], 8.7, Table 70)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten**	**Le**
00	B0	90	00	-	-	00
P1 enthält Short File identifier 16 für EF.C.HP.QES ([HPC-P2], Table B.5)						

Tabelle 107 – Korrekte Antwort ([HPC-P2], 8.7, Table 71)

Daten (256 Bytes)	SW1 SW2	Ursache	Aktion
Byte 0 bis Byte 255 aus EF.C.HP.QES	90 00	1. Teil des Zertifikats gelesen	2. Schritt
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens erhältlichen xx Bytes Daten verwendet wird.			

Tabelle 108 – Abweichende Antworten ([HPC-P1], Table A.4)

SW1 SW2	Bedeutung	Ursache	Aktion
62 81	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 81	Datei nicht transparent		
69 86	Kommando ohne SFID; keine Datei selektiert		
6A 82	Datei mit SFID nicht gefunden		
6B 00	Offset größer oder gleich Dateigröße		

2. Schritt (von 2):
Tabelle 109 – Kommando: READ BINARY ([HPC-P2], 8.7, Table 70)

CLA	INS	P1-P2	Lc	Daten	Le
00	B0	01 00 02 00 ...	-	-	00
P1-P2: Fortschaltung des Offset in Schritten von 256 Byte					

Tabelle 110 – Korrekte Antwort ([HPC-P2], 8.7, Table 71)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 256 bis Byte 511 aus EF.C.HP.QES Byte 512 bis Byte 767 aus EF.C.HP.QES ...	90 00	2. Teil des Zertifikats gelesen 3. Teil des Zertifikats gelesen ... Letzten Teil des Zertifikats gelesen	2. Schritt 2. Schritt .... Use Case beenden
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

b) Mit Extended Length und n (=I/O-Puffergröße-2) > Dateilänge

Falls n > Dateilänge (n = Wert enstprechend DO max. length of response APDU without SM, siehe [HPC-P1], Table 10) – 2, da 2 Byte für Status-Info benötigt werden):

1. Schritt (von 1):
Tabelle 111 – Kommando: READ BINARY ([HPC-P2], 8.7, Table 70)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	90	00	-	-	00 00 00
P1 enthält Short File identifier 16 für EF.C.HP.QES ([HPC-P2], Table B.5)						

Tabelle 112 – Korrekte Antwort ([HPC-P2], 8.7, Table 71)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Alle Bytes aus EF.C.HP.QES	62 82 (EOF reached before reading 65535 Byte)	Zertifikat erfolgreich gelesen (Achtung: möglicherweise Nullen am Ende, die nicht zum Zertifikat gehören)	Use Case beenden

c) Mit Extended Length und n (= I/O-Puffergröße – 2) < Dateilänge:

1. Schritt (von 2):
Tabelle 113 – Kommando: READ BINARY ([HPC-P2], 8.7, Table 70)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	90	00	-	-	00 xx xx
P1 enthält Short File identifier 16 für EF.C.HP.QES ([HPC-P2], Table B.5) Le: xx xx = n = (Wert enstprechend DO max. length of response APDU without SM, siehe [HPC-P1], Table 10) – 2, da 2 Byte für Status-Info benötigt werden						

Tabelle 114 – Korrekte Antwort ([HPC-P2], 8.7, Table 71)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 0 bis Byte n-1	90 00	n Byte des Zertifikats gelesen	2. Schritt
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

2. Schritt (von 2):
Tabelle 115 – Kommando: READ BINARY ([HPC-P2], 8.7, Table 70)

CLA	INS	P1-P2	Lc	Daten	Le
00	B0	xx xx (= n) xx xx (= 2n) …	-	-	00
P1-P2: Fortschaltung des Offset in Schritten von n Byte					

Tabelle 116 – Korrekte Antwort ([HPC-P2], 8.7, Table 71)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte n bis Byte 2n-1 aus EF.C.HP.QES Byte 2n bis Byte 3n-1 aus EF.C.HP.QES …	90 00 90 00 … 62 82 (EOF reached before reading 256 Byte)	2. Teil des Zertifikats gelesen 3. Teil des Zertifikats gelesen … Letzten Teil des Zertifikats gelesen	2. Schritt 2. Schritt …. Use Case beenden
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

10.2 Lesen QES-X.509-Attribut-Zertifikate

Tabelle 117 – Lesen der Attributzertifikate

Identifier	**UC_HPC_Read_QES_AC**
Name	Lesen der Attributzertifikate
Beschreibung	Die im HPC gespeicherten Attributzertifikate werden gelesen. Im Gegensatz zu anderen Berufsgruppen ist bei den Ärzten die Berufsgruppenangehörigkeit »Arzt/Ärztin« im Attributzertifikat in dem „admission"-Attribut enthalten. Das Auslesen der Berufsgruppenzugehörigkeit ist für bestimmte Anwendungen wichtig, da damit der Leistungserbringer nachweist, dass er über eine Approbation verfügt. Bei Bedarf ist über den das Attributzertifikat herausgebenden ZDA die Berufsgruppenangehörigkeit abfragbar/bestätigbar.
Vorbedingungen	HPC betriebsbereit DF.QES geöffnet
Nachbedingungen	Falls das Lesen erfolgreich war, enthalten die Ausgabedaten das spezifische Attributzertifikat. Weitere QES-Use Cases sind möglich.
Standardablauf	a) Ohne Extended Length: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP.QES-AC1, -AC2 bzw. -AC3 2. Schritt: Senden von weiteren READ BINARY-Kommandos, bis Attributzertifikat vollständig gelesen. b) Mit Extended Length und n > Dateilänge: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP.QES-AC1, -AC2 bzw. -AC3 und Le = 00 00 00 (3 Byte) c) Mit Extended Length und n < Dateilänge: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP.QES-AC1, -AC2 bzw. -AC3 und Le = 00 xx xx (3 Byte) 2. Schritt: Senden von weiteren READ BINARY-Kommandos, bis Attributzertifikat vollständig gelesen.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Die Nutzung von Attributzertifikaten ist abhängig von dem signierten Objekt und den Formerfordernissen für das betreffende Objekt (z.B. bei Signaturen außerhalb des Primärsystem-Kontextes werden keine Attribut-Zertifikate verwendet und auch be eRezept-Signaturen werden Zertifikate nicht angehangen). Attributzertifikate werden üblicherweise wie das QES-Zertifikat nur einmal gelesen und dann in den HPC Stack aufgenommen. Da Attributzertifikate ersetzt werden können, sollte Bestandteil des Austausch-Prozesses auch die Aktualisierung des HPC-Stacks sein.
Vorangegangene Use Cases	UC_HPC_Open_QES
Nachfolgende Use Cases	Abhängig vom Anwendungskontext.
Anmerkungen	Die Anzahl der tatsächlich in der HPC gespeicherten Attributzertifikate ist derzeit nicht abfragbar. Aus Performanzgründen wird empfohlen, dass die ersten zwei Bytes eines EFs gelesen werden. Sind diese auf den Wert '00 00 ' gesetzt, dann liegt kein Attributzertifikat vor. Dieser Fall ist derzeit nicht in [HPC-P2] explizit beschrieben.
Festlegungen	Falls wiederholt aus derselben Datei gelesen wird, ist es aus Performanzgründen sinnvoll, dass ab dem zweiten READ BINARY der SFID in P1 nicht angegeben wird, sondern P1 und P2 für den Offset zur Verfügung stehen.

a) Ohne Extended Length

1. Schritt (von 2):
Tabelle 118 – Kommando: READ BINARY ([HPC-P2], 8.7, Table 70)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	8x	00	-	-	00
P1 = 81 Short File identifier 1 für EF.C.HP.QES-AC1 ([HPC-P2], Table B.5) P1 = 82 Short File identifier 2 für EF.C.HP.QES-AC2 ([HPC-P2], Table B.5) P1 = 83 Short File identifier 3 für EF.C.HP.QES-AC3 ([HPC-P2], Table B.5)						

Tabelle 119 – Korrekte Antwort ([HPC-P2], 8.7, Table 71)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 0 bis Byte 255 aus EF.C.HP.ACx	90 00	1. Teil des Attributzertifikats gelesen	2. Schritt
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens erhältlichen xx Bytes Daten verwendet wird.			

Tabelle 120 – Abweichende Antworten ([HPC-P1], Table A.4)

SW1 SW2	Bedeutung	Ursache	Aktion
62 82	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 81	Datei nicht transparent		
69 86	Kommando ohne SFID; keine Datei selektiert		
6A 82	Datei mit SFID nicht gefunden		
6B 00	Offset größer oder gleich Dateigröße		

2. Schritt (von 2):
Tabelle 121 – Kommando: READ BINARY ([HPC-P2], 8.7, Table 70)

CLA	INS	P1-P2	Lc	Daten	Le
00	B0	01 00 02 00 …	-	-	00
P1-P2: Fortschaltung des Offset in Schritten von 256 Byte					

Tabelle 122 – Korrekte Antwort ([HPC-P2], 8.7, Table 71)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 256 bis Byte 511 aus EF.C.HP.ACx Byte 512 bis Byte 767 aus EF.C.HP.ACx …	90 00	2. Teil des Attribut-Zertifikats gelesen 3. Teil des Attribut-Zertifikats gelesen … Letzten Teil des Attribut-Zertifikats gelesen	2. Schritt 2. Schritt … Use Case beenden
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

b) Mit Extended Length und n (=I/O-Puffergröße-2) > Dateilänge

Falls n > Dateilänge (n = Wert enstprechend DO "Maximal length of response APDU without SM", siehe [HPC-P1], Table 10) – 2, da 2 Bytes für Status-Info benötigt werden):

1. Schritt (von 1):
Tabelle 123 – Kommando: READ BINARY ([HPC-P2], 8.7, Table 70)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	8x	00	-	-	00 00 00
P1 = 81 Short File identifier 1 für EF.C.HP.QES-AC1 ([HPC-P2], Table B.5) P1 = 82 Short File identifier 2 für EF.C.HP.QES-AC2 ([HPC-P2], Table B.5) P1 = 83 Short File identifier 3 für EF.C.HP.QES-AC3 ([HPC-P2], Table B.5)						

Tabelle 124 – Korrekte Antwort ([HPC-P2], 8.7, Table 71)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Alle Bytes aus EF.C.HP.ACx	62 82 (EOF reached before reading 65535 Byte)	Attribut-Zertifikat erfolgreich gelesen (Achtung: möglicherweise Nullen am Ende, die nicht zum Attribut-Zertifikat gehören)	Use Case beenden

c) Mit Extended Length und n (= I/O-Puffergröße – 2) < Dateilänge:

1. Schritt (von 2):
Tabelle 125 – Kommando: READ BINARY ([HPC-P2], 8.7, Table 70)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	8x	00	-	-	00 xx xx
P1 = 81 Short File identifier 1 für EF.C.HP.QES-AC1 ([HPC-P2], Table B.5) P1 = 82 Short File identifier 2 für EF.C.HP.QES-AC2 ([HPC-P2], Table B.5) P1 = 83 Short File identifier 3 für EF.C.HP.QES-AC3 ([HPC-P2], Table B.5) Le: xx xx = n = (Wert enstprechend DO max. length of response APDU without SM, siehe [HPC-P1], Tab. 10) – 2, da 2 Byte für Status-Info SW1 SW2 benötigt werden						

Tabelle 126 – Korrekte Antwort ([HPC-P2], 8.7, Table 71)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 00 bis Byte n-1	90 00	n Byte des Attribut-Zertifikats gelesen	2. Schritt
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

2. Schritt (von 2):
Tabelle 127 – Kommando: READ BINARY ([HPC-P2], 8.7, Table 70)

CLA	INS	P1-P2	Lc	Daten	Le
00	B0	xx xx (= n) xx xx (= 2n) ...	-	-	00
P1-P2: Fortschaltung des Offset in Schritten von n Byte					

Tabelle 128 – Korrekte Antwort ([HPC-P2], 8.7, Table 71)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte n bis Byte 2n-1 aus EF.C.HP.ACx Byte 2n bis Byte 3n-1 aus EF.C.HP.ACx ...	90 00 90 00 ... 62 82 (EOF reached before reading 256 Byte)	2. Teil des Attribut-Zertifikats gelesen 3. Teil des Attribut-Zertifikats gelesen ... Letzten Teil des Attribut-Zertifikats gelesen	Use Case beenden
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

10.3 Ersetzen eines QES-X.509-Attribut-Zertifikats

Tabelle 129 – Ersetzen der Attributzertifikate

Identifier	**UC_HPC_Replace_QES_AC**
Name	Ersetzen der Attributszertifikate
Beschreibung	Die im HPC gespeicherten Attributszertifikate werden ersetzt.
Vorbedingungen	HPC betriebsbereit DF.QES geöffnet Der Leistungserbringer ist mit Karteninhaber-PIN authentisiert Das zu ersetzende Attributszertifikat liegt vor
Nachbedingungen	Das spezifizierte Attributszertifikat ist ersetzt Weitere QES-Use Cases sind möglich.
Standardablauf	1. Schritt: Durchführung des Kommandos UPDATE BINARY mit Angabe von Short File Identifier für EF.C.HP.QES-AC1, EF.C.HP.QES-AC2 oder EF.C.HP.QES-AC3 Wenn Zertifikat > 255 Byte: 2. Schritt: Durchführung des Kommandos UPDATE BINARY mit Offset-Angabe
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	-
Vorangegangene Use Cases	UC_HPC_Open_QES UC_HPC_Verify_PIN
Nachfolgende Use Cases	Abhängig vom Anwendungskontext
Anmerkungen	Falls das Zertifikat > 255 Bytes und Extended Length nicht unterstützt wird, ist das UPDATE BINARY mit Offset-Angabe solange zu wiederholen, bis das Zertifikat komplett gespeichert ist. Der Fall mit Extended Length wird hier nicht weiterbetrachtet.
Festlegungen	Falls wiederholt in die derselbe Datei geschrieben wird, ist es aus Performanzgründen sinnvoll, dass ab dem zweiten UPDATE BINARY der SFID in P1 nicht angegeben wird, sondern P1 und P2 für den Offset zur Verfügung stehen.

1. Schritt (von 2):
Tabelle 130 – Kommando: UPDATE BINARY ([HPC-P2], 8.8, Table 72)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten**	**Le**
00	B0	8x	00	FF	Die ersten 255 Bytes des Attributzertifikats schreiben	-
P1 = 81 Short File identifier 1 für AC1 P1 = 82 Short File Identifier 2 für AC2 P1 = 83 Short File Identifier 3 für AC 3 ([HPC-P2], Table B.5):						

2. Schritt (von 2):
Solange wiederholen, bis AC komplett geschrieben
Tabelle 131 – Kommando: UPDATE BINARY ([HPC-P2], 8.8, Table 72)

CLA	INS	P1 - P2	Lc	Daten	Le
00	B0	00 FF 01 FE … xx xx	FF	Die nächsten 255 Bytes schreiben Die restlichen xx Bytes schreiben	-
P1-P2: Fortschaltung des Offset in Schritten von 255 Byte					

Folgende Antworten gelten für jedes UPDATE BINARY Kommando:

Tabelle 132 – Korrekte Antwort ([HPC-P2], 8.8, Table 73)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
-	90 00	Daten erfolgreich geschrieben	Schritt 2, falls weitere Daten zu Schreiben sind

Tabelle 133 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
69 81	Datei nicht transparent	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 86	Kommando ohne SFID; Datei nicht selektiert		
6A 82	Datei mit SFID nicht gefunden		
6A 87	Offset + Lc größer Dateogröße		
6B 00	Offset größer oder gleich Dateigröße		

11 Nutzung der ESIGN-Authentisierungsfunktion

11.1 Authentisieren als Client

Tabelle 134 – Authentisieren als Client

Identifier	UC_HPC_AUT
Name	Authentisieren als Client
Beschreibung	Im Rahmen eines PKI-basierten Authentisierungsprotokolls (z.B. Kerberos, SSL/TSL, WTSL) wird der Leistungserbringer mit der HPC als Client gegenüber einem Server authentisiert. Durch den HPC wird mittels INTERNAL AUTHENTICATE unter Verwendung des privaten Authentisierungsschlüssels PrK.HP.AUT eine Signatur über die authentisierungsrelevanten Daten berechnet.
Vorbedingungen	HPC betriebsbereit DF.ESIGN geöffnet Leistungserbringer mit Karteninhaber-PIN authentisiert Die zu signierenden Authentisierungsdaten werden übergeben
Nachbedingungen	Falls die Signaturberechnung erfolgreich war, enthalten die Ausgabedaten die Signatur. Weitere ESIGN-Use Cases sind möglich.
Standardablauf	1. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) mit Option SET zur Selektion des privaten Authentisierungsschlüssels und des Algorithmus für RSA mit PKCS#1-Padding. 2. Schritt: Durchführung des Kommandos INTERNAL AUTHENTICATE mit den authentisierungsrelevanten Daten im Datenfeld. In der Karte wird das PKCS#1-Padding eingesetzt.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Pro Aufbau einer sicheren Client-/Server-Verbindung.
Vorangegangene Use Cases	UC_HPC_Open_ESIGN UC_HPC_Verify_PIN
Nachfolgende Use Cases	Abhängig vom Anwendungskontext, z.B. UC_HPC_DEC
Anmerkungen	In der Karte wird das PKCS#1-Padding eingesetzt.
Festlegungen	-

1. Schritt (von 2):
Tabelle 135 – Kommando: MSE Option SET ([HPC-P2], 9.6, Table 79)

CLA	INS	P1	P2	Lc	Daten (6 Bytes)	Le
00	22	41	A4	06	84 01 82 80 01 05 (3 Byte Referenz des privaten Authentisierungsschlüssels PrK.HP.AUT, [HPC-P2], 9.1.2, Table 74 || 3 Byte Referenz des Algorithmus, [HPC-P2], Table E.2)	-

Tabelle 136 – Korrekte Antwort ([HPC-P2], 9.6, Table 80)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz und Algorithmusreferenz erfolgreich registriert.	2. Schritt

Tabelle 137 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
6A 88	Referenzierte Daten nicht gefunden	Dieser Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

2. Schritt (von 2):
Tabelle 138 – Kommando: INTERNAL AUTHENTICATE ([HPC-P2], 9.6, Table 81)

CLA	INS	P1	P2	Lc	Daten	Le
00	88	00	00	xx	DigestInfo ([HPC-P1], Table E.6)	00
Aus Gründen der Sicherheit darf die Länge des Datenfeldes (DigestInfo) höchstens 40% der Moduluslänge des Signatur-Schlüssels betragen ([HPC-P1],4.1, Table 6) (Angriff: Desmedt / Odlytzko-Attacke); dies wird durch die im Algorithmen-Katalog [ALGCAT] vorgegebenen Algorithmen-Kombinationen sichergestellt.						

Tabelle 139 – Korrekte Antwort ([HPC-P2], 9.6, Table 82)

Daten	SW1 SW2	Ursache	Aktion
Signatur	90 00	Signatur wurde erfolgreich erzeugt	Use Case beenden

Tabelle 140 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
6A 88	Referenzierte Daten nicht gefunden	Dieser Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

12 Nutzung der ESIGN-Verschlüsselungsfunktion

12.1 Entschlüsseln eines Dokumenten-Chiffrierungsschlüssels

Tabelle 141 – Entschlüsseln eines Dokumenten-Chiffrierungsschlüssels

Identifier	UC_HPC_DEC
Name	Entschlüsseln eines Dokumenten-Chiffrierungsschlüssels
Beschreibung	Ein asymmetrisch verschlüsselter Dokumenten-Chiffrierungsschlüssel, mit dem ein medizinisches Datenobjekte verschlüsselt wurde, wird unter Verwendung des privaten Verschlüsselungsschlüssels PrK.HP.ENC entschlüsselt.
Vorbedingungen	HPC betriebsbereit DF.ESIGN geöffnet Leistungserbringer mit Karteninhaber-PIN authentisiert
Nachbedingungen	Falls die Entschlüsselung erfolgreich war, enthalten die Ausgabedaten den Dokumenten-Chiffrierungsschlüssel ohne Padding. Weitere ESIGN-Use Cases sind möglich.
Standardablauf	1. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) mit Option SET zur Selektion des privaten Entschlüsselungsschlüssels. Der Algorithmus ist implizit bekannt. 2. Schritt: Durchführung des Kommandos PSO: DECIPHER mit Padding Indicator und Kryptogramm im Datenfeld. In der Karte wird RSA mit PKCS#1-Padding eingesetzt.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Pro abgerufenes verschlüsseltes Datenobjekt vom Server.
Vorangegangene Use Cases	UC_HPC_Open_ESIGN UC_HPC_Verify_PIN
Nachfolgende Use Cases	Anhängig vom Anwendungskontext, z.B. UC_HPC_DEC
Anmerkungen	Als Verfahren wird in der Karte implizit RSA mit PKCS#11-Padding eingesetzt. Der Dokumenten-Chiffrierungsschlüssel ist auf der Seite des Produzenten, der den Schlüssel verschlüsselt, wie folgt zu kodieren: PI=81: 02 || RND || 00 || Session-Key Beispiel: Session-Key = 3DES-Schlüssel = 16 Byte & RSA mit 1024 Bit Schlüssellänge : 02 || 110 Byte RND || 00 || 16 Byte 3DES-Schlüssel => Länge des Kryptogramms = 128 Byte
Festlegungen	-

1. Schritt (von 2):
Tabelle 142 – Kommando: MSE Option SET ([HPC-P2], 9.7, Table 83)

CLA	INS	P1	P2	Lc	Daten (3 Byte)	Le
00	22	41	B8	03	84 01 83 (Referenz des privaten Entschlüsselungsschlüssels PrK.HP.ENC, [HPC-P2], 9.1.2, Table 74)	-

Tabelle 143 – Korrekte Antwort ([HPC-P2], 9.7, Table 84)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz erfolgreich registriert	2. Schritt

Tabelle 144 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
6A 88	Referenzierte Daten nicht gefunden	Dieser Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

2. Schritt (von 2):
Tabelle 145 – Kommando: PSO: DECIPHER ([HPC-P2], 9.7, Table 85)

CLA	INS	P1	P2	Lc	Daten	Le
00	2A	80	86	xx	81 yy … yy (81 = PI / yy = Kryptogramm)	00
Lc = 1 + Länge des Kryptogramms (entspricht Moduluslänge des Schlüssels)						

Tabelle 146 – Korrekte Antwort ([HPC-P2], 9.7, Table 86)

Daten	SW1 SW2	Ursache	Aktion
Dokumenten-Chiffrierungsschlüssel (bei einem 3DES-Schlüssel 16 Byte) (ohne 02 || RND)	90 00	Kryptogramm erfolgreich entschlüsselt	Use Case beenden

Tabelle 147 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
6A 80	Bei RSA: Eingabewert außerhalb des zugelassenen Bereichs	Dieser Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzierte Daten nicht gefunden		

13 Nutzung ESIGN-Zertifikate

13.1 Lesen AUT-X.509-Zertifikat

Tabelle 148 – Lesen des X.509 Authentisierungszertifikats

Identifier	**UC_HPC_Read_AUT**
Name	Lesen des X.509 Authentisierungszertifikats
Beschreibung	Das im HPC gespeicherte Authentisierungzertifikat zum Nachweis der Identität wird gelesen.
Vorbedingungen	HPC betriebsbereit DF.ESIGN geöffnet
Nachbedingungen	Falls das Lesen erfolgreich war, enthalten die Ausgabedaten das Authentisierungszertifikat. Weitere ESIGN-Use Cases sind möglich.
Standardablauf	a) Ohne Extended Length: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP.AUT 2. Schritt: Senden von weiteren READ BINARY-Kommandos, bis Authentisierungszertifikat vollständig gelesen. b) Mit Extended Length und n > Dateilänge: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP.AUT und Le = 00 00 00 (3 Byte) c) Mit Extended Length und n < Dateilänge: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP.AUT und Le = 00 xx xx (3 Byte) 2. Schritt: Senden von weiteren READ BINARY-Kommandos, bis Authentisierungszertifikat vollständig gelesen.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Einmal beim Erstkontakt mit einer bisher unbekannten Karte, falls das Zertifikat im Primärsystem persistent gespeichert wird (siehe Anhang A.2).
Vorangegangene Use Cases	UC_HPC_Open_ESIGN
Nachfolgende Use Cases	Abhängig vom Anwendungskontext.
Anmerkungen	Einmal beim Erstkontakt mit einer bisher unbekannten Karte, falls das Zertifikat im Primärsystem persistent gespeichert wird (siehe Anhang A.2).
Festlegungen	Falls wiederholt aus derselben Datei gelesen wird, ist es aus Performanzgründen sinnvoll, dass ab dem zweiten READ BINARY der SFID in P1 nicht angegeben wird, sondern P1 und P2 für den Offset zur Verfügung stehen.

a) Ohne Extended Length

1. Schritt (von 2):
Tabelle 149 – Kommando: READ BINARY ([HPC-P2], 9.4, Table 77)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	81	00	-	-	00
P1 enthält Short File identifier 1 für EF.C.HP.AUT ([HPC-P2], Table B.7)						

Tabelle 150 – Korrekte Antwort ([HPC-P2], 9.4, Table 78)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 0 bis byte 255 aus EF.C.HP.AUT ([HPC-P2], 9.1.4)	90 00	1. Teil des Authentisierungszertifikats gelesen	2. Schritt
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens erhältlichen xx Bytes Daten verwendet wird.			

Tabelle 151 – Abweichende Antworten ([HPC-P1], Table A.4)

SW1 SW2	Bedeutung	Ursache	Aktion
62 82	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 81	Datei nicht transparent		
69 86	Kommando ohne SFID; keine Datei selektiert		
6A 82	Datei mit SFID nicht gefunden		
6B 00	Offset größer oder gleich Dateigröße		

2. Schritt (von 2):
Tabelle 152 – Kommando: READ BINARY ([HPC-P2], 9.4, Table 77)

CLA	INS	P1-P2	Lc	Daten	Le
00	B0	01 00 02 00 ...	-	-	00
P1-P2: Fortschaltung des Offset in Schritten von 256 Byte					

Tabelle 153 – Korrekte Antwort ([HPC-P2], 9.4, Table 78)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 256 bis Byte 511 aus EF.C.HP.AUT Byte 512 bis Byte 767 aus EF.C.HP.AUT ...	90 00	2. Teil des Authentisierungszertifikats gelesen 3. Teil des Authentisierungszertifikats gelesen ... Letzten Teil des Authentisierungszertifikats gelesen	2. Schritt 2. Schritt … Use Case beenden
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

b) Mit Extended Length und n (=I/O-Puffergröße-2) > Dateilänge

Falls n > Dateilänge (n = Wert enstprechend DO "Maximal length of response APDU without SM", siehe [HPC-P1], Table 10) – 2, da 2 Byte für Status-Info benötigt werden):

1. Schritt (von 1):
Tabelle 154 – Kommando: READ BINARY ([HPC-P2], 9.4, Table 77)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	81	00	-	-	00 00 00
P1 enthält Short File identifier für EF.C.HP.AUT 1 ([HPC-P2], Table B.7)						

Tabelle 155 – Korrekte Antwort ([HPC-P2], 9.4, Table 78)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Alle Bytes aus EF.C.HP.AUT	62 82 (EOF reached before reading 65535 Byte)	Authentisierungszertifikat erfolgreich gelesen (Achtung: möglicherweise Nullen am Ende, die nicht zum Authentisierungszertifikat gehören)	Use Case beenden

c) Mit Extended Length und n (= I/O-Puffergröße – 2) < Dateilänge:

1. Schritt (von 2):
Tabelle 156 – Kommando: READ BINARY ([HPC-P2], 9.4, Table 77)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	81	00	-	-	00 xx xx
P1 enthält SFID für EF.C.HP.AUT 1 ([HPC-P2], Table B.7) Le: xx xx = n = (Wert enstprechend DO max. length of response APDU without SM, siehe [HPC-P1], Tab. 10) – 2, da 2 Byte für Status-Info SW1 SW2 benötigt werden						

Tabelle 157 – Korrekte Antwort ([HPC-P2], 9.4, Table 78)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 00 bis Byte n-1	90 00	n Byte des Authentisierungszertifikats gelesen	2. Schritt
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

2. Schritt (von 2):
Tabelle 158 – Kommando: READ BINARY ([HPC-P2], 9.4, Table 77)

CLA	INS	P1-P2	Lc	Daten	Le
00	B0	xx xx (= n) xx xx (= 2n) …	-	-	00
P1-P2: Fortschaltung des Offset in Schritten von n Byte					

Tabelle 159 – Korrekte Antwort ([HPC-P2], 9.4, Table 78)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte n bis Byte 2n-1 aus EF.C.HP.AUT Byte 2n bis Byte 3n-1 aus EF.C.HP.AUT …	90 00 90 00 … 62 82 (EOF reached before reading 256 Byte)	2. Teil des Authentisierungszertifikats gelesen 3. Teil des Authentisierungszertifikats gelesen … Letzten Teil des Authentisierungszertifikats gelesen	2. Schritt 2. Schritt … Use Case beenden
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

13.2 Lesen ENC-X.509-Zertifikat

Tabelle 160 – Lesen des X.509 Verschlüsselungszertifikats

Identifier	**UC_HPC_Read_ENC**
Name	Lesen des X.509 Verschlüsselungszertifikats
Beschreibung	Das im HPC gespeicherte Verschlüsselungszertifikat wird gelesen.
Vorbedingungen	HPC betriebsbereit DF.ESIGN geöffnet
Nachbedingungen	Falls das Lesen erfolgreich war, enthalten die Ausgabedaten das Verschlüsselungszertifikat. Weitere ESIGN-Use Cases sind möglich.
Standardablauf	a) Ohne Extended Length: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP.ENC 2. Schritt: Senden von weiteren READ BINARY-Kommandos, bis Authentisierungszertifikat vollständig gelesen. b) Mit Extended Length und n > Dateilänge: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP. ENC und Le = 00 00 00 (3 Byte) c) Mit Extended Length und n < Dateilänge: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.C.HP. ENC und Le = 00 xx xx (3 Byte) 2. Schritt: Senden von weiteren READ BINARY-Kommandos, bis Verschlüsselungszertifikat vollständig gelesen.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Einmal beim Erstkontakt mit einer bisher unbekannten Karte, falls das Zertifikat im Primärsystem persistent gespeichert wird (siehe Anhang A.2).
Vorangegangene Use Cases	UC_HPC_Open_ESIGN
Nachfolgende Use Cases	Abhängig vom Anwendungskontext
Anmerkungen	-
Festlegungen	Falls wiederholt aus derselben Datei gelesen wird, ist es aus Performanzgründen sinnvoll, dass ab dem zweiten READ BINARY der SFID in P1 nicht angegeben wird, sondern P1 und P2 für den Offset zur Verfügung stehen.

a) Ohne Extended Length

1. Schritt (von 2):
Tabelle 161 – Kommando: READ BINARY ([HPC-P2], 9.4, Table 77)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	82	00	-	-	00
P1 enthält Short File identifier für EF.C.HP.AUT 2 ([HPC-P2], Table B.7)						

Tabelle 162 – Korrekte Antwort ([HPC-P2], 9.4, Table 78)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 0 bis byte 255 aus EF.C.HP.ENC ([HPC-P2], 9.1.5)	90 00	1. Teil des Verschlüsselungszertifikats gelesen	2. Schritt
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens erhältlichen xx Bytes Daten verwendet wird.			

Tabelle 163 – Abweichende Antworten ([HPC-P1], Table A.4)

SW1 SW2	Bedeutung	Ursache	Aktion
62 82	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmier-fehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 81	Datei nicht transparent		
69 86	Kommando ohne SFID; keine Datei selektiert		
6A 82	Datei mit SFID nicht gefunden		
6B 00	Offset größer oder gleich Dateigröße		

2. Schritt (von 2):
Tabelle 164 – Kommando: READ BINARY ([HPC-P2], 9.4, Table 77)

CLA	INS	P1-P2	Lc	Daten	Le
00	B0	01 00 02 00 …	-	-	00
P1-P2: Fortschaltung des Offset in Schritten von 256 Byte					

Tabelle 165 – Korrekte Antwort ([HPC-P2], 9.4, Table 78)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 256 bis Byte 511 aus EF.C.HP.ENC Byte 512 bis Byte 767 aus EF.C.HP.ENC …	90 00	2. Teil des Verschlüsselungs-zertifikats gelesen 3. Teil des Verschlüsselungs-zertifikats gelesen … Letzten Teil des Verschlüsse-lungszertifikats gelesen	2. Schritt 2. Schritt … Use Case beenden
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

b) Mit Extended Length und n (=I/O-Puffergröße-2) > Dateilänge

Falls n > Dateilänge (n = Wert enstprechend DO "Maximal length of response APDU without SM", siehe [HPC-P1], Table 10) – 2, da 2 Byte für Status-Info benötigt werden):

1. Schritt (von 1):
Tabelle 166 – Kommando: READ BINARY ([HPC-P2], 9.4, Table 77)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	82	00	-	-	00 00 00
P1 enthält Short File identifier für EF.C.HP.AUT 2 ([HPC-P2], Table B.7)						

Tabelle 167 – Korrekte Antwort ([HPC-P2], 9.4, Table 78)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Alle Bytes aus EF.C.HP.AUT	62 82 (EOF reached before reading 65535 Byte)	Verschlüsselungszertifikat erfolgreich gelesen (Achtung: möglicherweise Nullen am Ende, die nicht zum Verschlüsselungszertifikats gehören)	Use Case beenden

c) Mit Extended Length und n (= I/O-Puffergröße – 2) < Dateilänge:

1. Schritt (von 2):
Tabelle 168 – Kommando: READ BINARY ([HPC-P2], 9.4, Table 77)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	82	00	-	-	00 xx xx
P1 enthält Short File identifier für EF.C.HP.AUT 2 ([HPC-P2], Table B.7) Le: xx xx = n = (Wert enstprechend DO max. length of response APDU without SM, siehe [HPC-P1], Tab. 10) – 2, da 2 Byte für Status-Info SW1 SW2 benötigt werden						

Tabelle 169 – Korrekte Antwort ([HPC-P2], 9.4, Table 78)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 00 bis Byte n-1	90 00	n Byte des Verschlüsselungszertifikats gelesen	2. Schritt
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

2. Schritt (von 2):
Tabelle 170 – Kommando: READ BINARY ([HPC-P2], 9.4, Table 77)

CLA	INS	P1-P2	Lc	Daten	Le
00	B0	xx xx (= n) xx xx (= 2n) …	-	-	00
P1-P2: Fortschaltung des Offset in Schritten von n Byte					

Tabelle 171 – Korrekte Antwort ([HPC-P2], 9.4, Table 78)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte n bis Byte 2n-1 aus EF.C.HP.ENC Byte 2n bis Byte 3n-1 aus EF.C.HP.ENC …	90 00 90 00 … 62 82 (EOF reached before reading 256 Byte)	2. Teil des Verschlüsselungszertifikats gelesen 3. Teil des Verschlüsselungszertifikats gelesen … Letzten Teil des Verschlüsselungszertifikats gelesen	2. Schritt 2. Schritt … Use Case beenden
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

14 Nutzung der CIA_ESIGN-Anwendung

14.1 Ermitteln der unterstützten kryptografischen Algorithmen und Algorithmenparameter

Tabelle 172 – Ermitteln der unterstützten kryptografischen Algorithmen und Algorithmenparameter

Identifier	**UC_HPC_Read_CIA.ESIGN_Info**
Name	Ermitteln der unterstützten kryptografischen Algorithmen und Algorithmenparameter
Beschreibung	Die CIA-Datenfiles werden gelesen.
Vorbedingungen	HPC betriebsbereit DF.CIA_ESIGN geöffnet
Nachbedingungen	Falls das Lesen erfolgreich war, enthalten die Ausgabedaten das gelesene Informationsobjekt. DF.CIA_ESIGN geöffnet
Standardablauf	1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.CIAInfo 2. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.OD 3. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.AOD 4. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.PrKD 5. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.CD
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«
Häufigkeit	Einmal beim Erstkontakt mit einer bisher unbekannten Karte, falls die Informationsobjekte im Primärsystem persistent gespeichert werden (siehe Anhang A.2).
Vorangegangene Use Cases	UC_HPC_Open_CIA_ESIGN
Nachfolgende Use Cases	Abhängig vom Anwendungskontext
Anmerkungen	-
Festlegungen	Es wird immer bis EOF gelesen (Le = 00)
Hinweis zur Spek	In H.1.2 / H.1.3, H.4.2 / H.4.3, H.5.2 falsche Längenangaben

1. Schritt (von 5):
Tabelle 173 – Kommando: READ BINARY ([HPC-P2], 10.3, Table 89)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten**	**Le**
00	B0	92	00	-	-	00
Short File identifier für EF.CIAInfo 18 ([HPC-P2], Table B.9)						

Tabelle 174 – Korrekte Antwort ([HPC-P2], 10.3, Table 90)

Daten (59 Bytes)	**SW1 SW2**	**Ursache**	**Aktion**
30 39 … ([HPC-P2], H.1.3)	90 00	Daten erfolgreich gelesen	2. Schritt

Tabelle 175 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
62 81	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 81	Datei nicht transparent		
69 86	Kommando ohne SFID; Datei nicht selektiert		
6A 82	Datei mit SFID nicht gefunden		
6B 00	Offset größer oder gleich Dategröße		

2. Schritt (von 5):
Tabelle 176 – Kommando: READ BINARY ([HPC-P2], 10.3, Table 89)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	91	00	-	-	00
Short File identifier 17 für EF.OD ([HPC-P2], Table B.9)						

Tabelle 177 – Korrekte Antwort ([HPC-P2], 10.3, Table 90)

Daten	SW1 SW2	Ursache	Aktion
A8 05 … …. ([HPC-P2], H.2.3)	90 00	Daten erfolgreich gelesen	3. Schritt

Abweichende Antworten ([HPC-P1], Table A.17) siehe Schritt 1

3. Schritt (von 5):
Tabelle 178 – Kommando: READ BINARY ([HPC-P2], 10.3, Table 89)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	94	00	-	-	00
Short File identifier 20 für EF.AOD ([HPC-P2], Table B.9)						

Tabelle 179 – Korrekte Antwort ([HPC-P2], 10.3, Table 90)

Daten (100 Bytes)	SW1 SW2	Ursache	Aktion
30 32… …. ([HPC-P2], H.3.3)	90 00	Daten erfolgreich gelesen	4. Schritt

Abweichende Antworten ([HPC-P1], Table A.17) siehe Schritt 1

4. Schritt (von 5):
Tabelle 180 – Kommando: READ BINARY ([HPC-P2], 10.3, Table 89)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	95	00	-	-	00
Short File identifier 21 für EF.PrKD ([HPC-P2], Table B.9)						

Tabelle 181 – Korrekte Antwort ([HPC-P2], 10.3, Table 90)

Daten (131 Bytes)	SW1 SW2	Ursache	Aktion
30 40 …. ([HPC-P2], H.4.3)	90 00	Daten erfolgreich gelesen	5. Schritt

Abweichende Antworten ([HPC-P1], Table A.17) siehe Schritt 1

5. Schritt (von 5):
Tabelle 182 – Kommando: READ BINARY ([HPC-P2], 10.3, Table 89)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	96	00	-	-	00
Short File identifier 22 für EF.CD ([HPC-P2], Table B.9)						

Tabelle 183 – Korrekte Antwort ([HPC-P2], 10.3, Table 90)

Daten (64 Byte)	SW1 SW2	Ursache	Aktion
30 1E… …. ([HPC-P2], H.5.3)	90 00	Daten erfolgreich gelesen	Use Case beenden

Abweichende Antworten ([HPC-P1], Table A.17) siehe Schritt 1

15 Interaktion HPC / eGK

15.1 Verifizieren der eGK-bezogenen CV-Zertifikate (zweistufig)

Tabelle 184 – Verifizieren der eGK-bezogenen CV-Zertifikate (zweistufig)

Identifier	**UC_HPC_Verify_eGK_CVCs**
Name	Verifizieren der eGK-bezogenen CV-Zertifikate (zweistufig)
Beschreibung	Prüfen der eGK-bezogenen CV-Zertifikate und Speichern (temporär) der darin enthaltenen öffentlichen Schlüssel in der HPC, damit die HPC bei einer anschließenden eGK / HPC-Authentisierung den öffentlichen eGK-Authentisierungsschlüssel kennt und die Authentizität der eGK prüfen kann. Das CHA-Feld des eGK-Authentisierungszertifikats wird im HPC ebenfalls temporär gespeichert, es wird jedoch in keiner Zugriffsregel benutzt, da ein Versicherter keine Zugriffsrechte auf Daten/Funktionen der HPC hat, wie auch die Rollenkennung 00 in CHA zeigt.
Vorbedingungen	HPC betriebsbereit MF-Ebene selektiert
Nachbedingungen	MF-Ebene selektiert Öffentlicher eGK-Authentisierungsschlüssel und CHA der eGK in der HPC vorhanden.
Standardablauf	1. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des öffentlichen Root-CA-Schlüssels der HPC 2. Schritt: Durchführung des Kommandos VERIFY CERTIFICATE zum Prüfen des eGK-CA-Zertifikats und zum temporären Speichern des öffentlichen eGK-CA-Schlüssels. 3. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des öffentlichen eGK-CA-Schlüssels 4. Schritt: Durchführung des Kommandos VERIFY CERTIFICATE zum Prüfen des eGK-Authentisierungszertifikats und zum temporären Speichern des öffentlichen eGK-Authentisierungsschlüssels und der CHA der eGK (CHA wird jedoch nicht benutzt).
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Einmal pro eGK-Anwendungssession mit der HPC, in der die eGK ihre Authentizität nachweisen muss, bevor geschützte eGK-Daten vom Heilberufler gelesen und / oder geschrieben werden können.
Vorangegangene Use Cases	• UC_HPC_Reset Falls Root-CA-Schlüssel einer eGK bzw. einer SMC dem Primärsystem unbekannt war: • UC_HPC_Retrieve_Cross-CVCs und UC_HPC_Verify_Cross_CVC
Nachfolgende Use Cases	UC_HPC_Authenticate_eGK
Anmerkungen	Die öffentlichen Root-CA-Schlüssel einer eGK und der entsprechenden HPC können nach einem Wechsel des Root-CA-Schlüssels (oder später im europäischen Kontext) unterschiedlich sein. Dann ist zunächst das Abrufen und Prüfen eines Cross-Zertifikats erforderlich.
Festlegungen	-

1. Schritt (von 4):
Tabelle 185 – Kommando: MSE Option SET ([HPC-P2], 5.6.3, Table 18)

CLA	INS	P1	P2	Lc	Daten (10 Bytes)	Le
00	22	81	B6	0A	83 08 ... ([HPC-P2], 5.6.2, Figure 3)	-
Die Referenz des öffentlichen Root-CA-Schlüssels PuK.RCS.CS ist im Wertefeld des Datenobjektes CAR des HPC-CA-Zertifikats im Klartext angeben und somit dem Primärsystem zugänglich.						

Tabelle 186 – Korrekte Antworten ([HPC-P2], 5.6.3, Table 19 und [HPC-P1], Table A.17)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den öffentlichen Root-CA-Schlüssels erfolgreich registriert.	2. Schritt

Tabelle 187 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Öffentlicher Root-CA-Schlüssel der eGK ist auf der HPC nicht vorhanden. Das hätte das Primärsystem zuvor durch einen Vergleich der Root-CA-Referenz der eGK mit der im Primärsystem-Stack gespeicherten Root-CA-Referenz der HPC feststellen müssen (siehe Anwendungsfälle UC_HPC_Retrieve_Cross_CVC und UC_HPC_Verify_Cross_CVC.	Fehlerausgang »HPC defekt«

2. Schritt (von 4):
Tabelle 188 – Kommando: VERIFY CERTIFICATE ([HPC-P2], 5.6.3, Table 20)

CLA	INS	P1	P2	Lc	Daten (196 Bytes)	Le
00	2A	00	AE	C4	5F37 8180 xx ... 5F38 3D xx ... ([HPC-P1], B.2, Table B.10, ohne DO CAR)	-

Tabelle 189 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 21)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Prüfen des eGK-CA-Zertifikats erfolgreich	3. Schritt

Tabelle 190 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in den Kommandodaten	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

3. Schritt (von 4):
Tabelle 191 – Kommando: MSE Option SET ([HPC-P2], 5.6.3, Table 22)

CLA	INS	P1	P2	Lc	Daten (14 Bytes)	Le
00	22	81	B6	0E	83 0C ... ([HPC-P2], 5.6.2, Figure 3)	-
Als Referenz des öffentlichen eGK-CA-Schlüssels PuK.CA_NN_eGK.CS (12 Bytes) dient der für das Primärsystem zugängliche Wert des Datenobjektes CAR (8 Bytes) des eGK-Authentisierungszertifikats mit vier vorangestellten Null-Bytes (d.h. insgesamt 12 Bytes).						

Tabelle 192 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 23)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den öffentlichen eGK-Authentisierungsschlüssels erfolgreich registriert.	4. Schritt

Tabelle 193 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

4. Schritt (von 4):
Tabelle 194 – Kommando: VERIFY CERTIFICATE ([HPC-P2], 5.6.3, Table 24)

CLA	INS	P1	P2	Lc	Daten (195 Bytes)	Le
00	2A	00	AE	C3	5F37 8180 xx ... 5F38 3C xx ... ([HPC-P1], B.2, Table B.11, ohne DO CAR)	-

Tabelle 195 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 25)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Prüfen des eGK-Authentisierungszertifikats erfolgreich	Use Case beenden

Tabelle 196 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in den Kommandodaten	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

15.2 Verifizieren der eGK-bezogenen CV-Zertifikate mit Cross-CV-Zertifikat (dreistufig)

Tabelle 197 – Verifizieren der eGK-bezogenen CV-Zertifikate mit Cross-CV-Zertifikat (dreistufig)

Identifier	**UC_HPC_Verify_eGK_Cross_CVCs**
Name	Verifizieren der eGK-bezogenen CV-Zertifikate mit Cross-Zertifikat (dreistufig)
Beschreibung	Prüfen eines Cross-CV-Zertifikats und temporäres Speichern des darin enthaltenen öffentlichen Root-CA-Schlüssel der eGK in der HPC. Anschließend Prüfen der eGK-bezogenen CV-Zertifikate und temporäres Speichern der darin enthaltenen öffentlichen Schlüssel in der HPC, damit die HPC bei einer anschließenden eGK / HPC-Authentisierung den öffentlichen eGK-Authentisierungsschlüssel kennt und die Authentizität der eGK prüfen kann. Das CHA-Feld des eGK-Authentisierungszertifikats wird ebenfalls in der HPC temporär gespeichert, es wird jedoch in keiner Zugriffsregel benutzt, da ein Versicherter keine Zugriffsrechte auf Daten / Funktionen der HPC hat, wie auch die Rollenkennung 00 in CHA zeigt.
Vorbedingungen	HPC betriebsbereit, MF-Ebene selektiert, Cross-Zertifikat des Root-CA-Schlüssels der eGK im Primärsystem vorhanden.
Nachbedingungen	MF-Ebene selektiert, öffentlicher Authentisierungschlüssel der eGK (und CHA.eGK) für die nachfolgende HPC / eGK-Authentisierung in der HPC vorhanden.
Standardablauf	1. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des öffentlichen Root-CA-Schlüssels der HPC 2. Schritt: Durchführung des Kommandos VERIFY CERTIFICATE zum Prüfen des Cross-CV-Zertifikats und zum temporären Speichern des öffentlichen Root-CA-Schlüssels der eGK. 3. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des öffentlichen Root-CA-Schlüssels der eGK 4. Schritt: Durchführung des Kommandos VERIFY CERTIFICATE zum Prüfen des CA-Zertifikats der eGK und zum temporären Speichern des öffentlichen CA-Schlüssels der eGK. 5. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des öffentlichen CA-Schlüssels der eGK 6. Schritt: Durchführung des Kommandos VERIFY CERTIFICATE zum Prüfen des eGK-Authentisierungszertifikats u. zum temp. Speichern des öffentl. Authentisierungsschlüssels (und der CHA) d. eGK.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Einmal pro eGK-Anwendungssession mit der HPC, wenn die Referenz des Root-CA-Schlüssels der eGK von dem der HPC abweicht.
Vorangegangene Use Cases	Falls nicht bereits im PVS / KIS vorhanden: • UC_HPC_Retrieve_Cross_CVC
Nachfolgende Use Cases	• UC_HPC_Authenticate_eGK
Anmerkungen	Beim Vergleich der KeyNames der Root_CA-Schlüssel von HPC und eGK wurde durch das Primärsystem festgestellt, dass diese ungleich sind. Die benötigten Cross-CV-Zertifikate sind entweder schon vorhanden, oder müssen vom gematik-Server abgerufen werden (siehe Anhang A.2). Das Abrufen und Prüfen eines Cross-CV-Zertifikats ist erforderlich, wenn der öffentliche Root-CA-Schlüssel der eGK und der HPC nach dem Wechsel eines Root-CA-Schlüssels (oder später zum Import eines Root-CA-Schlüssels im europäischen Kontext) unterschiedlich sind.
Festlegungen	Falls Cross-CV-Zertifikate noch nicht im PVS / KIS vorhanden und auch nicht abrufbar von gematik-Server, dann ist die betreffende HPC-eGK-Authentisierung nicht möglich.

1. Schritt (von 6):
Tabelle 198 – Kommando: MSE Option SET ([HPC-P2], 5.6.3, Table 18)

CLA	INS	P1	P2	Lc	Daten (10 Bytes)	Le
00	22	81	B6	0A	83 08 ... ([HPC-P2], 5.6.2, Figure 3)	-
Die Referenz des öffentlichen Root-CA-Schlüssels PuK.RCA_HPC.CS ist im Wertefeld des Datenobjektes CAR des HPC-CA-Zertifikats im Klartext angeben (siehe [HPC-P1], Table. B.10) und ist im HPC-Stack gespeichert (siehe Anhang A.2).						

Tabelle 199 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 19 und [HPC-P1], Table A.17)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den öffentlichen Root-CA-Schlüssel der HPC erfolgreich registriert.	2. Schritt

Tabelle 200 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

2. Schritt (von 6):
Tabelle 201 – Kommando: VERIFY CERTIFICATE ([HPC-P2], 5.6.3, Table 20)

CLA	INS	P1	P2	Lc	Daten (196 Bytes)	Le
00	2A	00	AE	C4	5F37 8180 xx ... 5F38 3D xx ... ([HPC-P1], B.2, Table B.10, nur DO 5F37 und DO 5F38)	-

Tabelle 202 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 21)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Prüfen des Cross-CV-Zertifikats erfolgreich	3. Schritt

Tabelle 203 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in den Kommandodaten	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

3. Schritt (von 6):
Tabelle 204 – Kommando: MSE Option SET ([HPC-P2], 5.6.3, Table 22)

CLA	INS	P1	P2	Lc	Daten (12 Bytes)	Le
00	22	81	B6	0E	83 0C ... ([HPC-P2], 5.6.2, Figure 3)	-
Als Referenz des öffentlichen Root-CA-Schlüssels PuK.RCA_eGK.CS (12 Bytes) dient der Wert des Datenobjektes CAR (8 Bytes) des Cross-Zertifikats mit vier vorangestellten Null-Bytes (d.h. insgesamt 12 Bytes).						

Tabelle 205 – Korrekte Antworten ([HPC-P2], 5.6.3, Table 23 und [HPC-P1], Table A.17)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den öffentlichen Root-CA-Schlüssels der eGK erfolgreich registriert.	4. Schritt

Tabelle 206 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

4. Schritt (von 6):
Tabelle 207 – Kommando: VERIFY CERTIFICATE ([HPC-P2], 5.6.3, Table 24)

CLA	INS	P1	P2	Lc	Daten (196 Bytes)	Le
00	2A	00	AE	C4	5F37 8180 xx ... 5F38 3D xx ... ([HPC-P1], B.2, Table B.10, ohne DO CAR)	-

Tabelle 208 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 25)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Prüfen des eGK-CA-Zertifikats erfolgreich	5. Schritt

Tabelle 209 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in den Kommandodaten	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

5. Schritt (von 6):
Tabelle 210 – Kommando: MSE Option SET ([HPC-P2], 5.6.3, Table 22)

CLA	INS	P1	P2	Lc	Daten (14 Bytes)	Le
00	22	81	B6	0E	83 0C ... ([HPC-P2], 5.6.2, Figure 3)	-
Als Referenz des öffentlichen eGK-CA-Schlüssels PuK.CA_NN_eGK (12 Bytes) dient der für das Primärsystem zugängliche Wert des Datenobjektes CAR (8 Bytes) des eGK-Authentisierungszertifikats mit vier vorangestellten Null-Bytes (d.h. insgesamt 12 Bytes).						

Tabelle 211 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 23)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den öffentlichen eGK-Authentisierungsschlüssels erfolgreich registriert.	6. Schritt

Tabelle 212 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

6. Schritt (von 6):
Tabelle 213 – Kommando: VERIFY CERTIFICATE ([HPC-P2], 5.6.3, Table 24)

CLA	INS	P1	P2	Lc	Daten (195 Bytes)	Le
00	2A	00	AE	C3	5F37 8180 xx ... 5F38 3C xx ... ([HPC-P1], B.2, Table B.11, ohne DO CAR)	-

Tabelle 214 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 25)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Prüfen des eGK-Authentisierungszertifikats erfolgreich	Use Case beenden

Tabelle 215 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in den Kommandodaten	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		

15.3 Durchführen der HPC / eGK-Authentisierung

Tabelle 216 – Durchführen der HPC / eGK-Authentisierung

Identifier	**UC_HPC_Authenticate_eGK**
Name	Durchführen der HPC / eGK-Authentisierung
Beschreibung	• Nachweis der Authentizität der eGK durch das Anwenden des privaten Authentisierungsschlüssels der eGK gegenüber der HPC. • Nachweis der Zugriffsrechte der HPC (d.h. das bei der Verifikation des HPC-Authentisierungszertifikats der eGK präsentierte Zugriffsprofil der HPC) durch das Anwenden des privaten Authentisierungsschlüssels der HPC gegenüber der eGK.
Vorbedingungen	HPC betriebsbereit Das eGK-Authentisierungszertifikat ist verifiziert, d.h. der öffentliche Authentisierungsschlüssel der eGK ist in der HPC vorhanden. Der Leistungserbringer ist mit Karteninhaber-PIN authentisiert
Nachbedingungen	Die eGK und die HPC sind gegenseitig authentisiert
Standardablauf	1. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des öffentlichen eGK-Authentisierungsschlüssels und des privaten HPC-Authentisierungsschlüssels 2. Schritt: Durchführung des Kommandos GET CHALLENGE zum Abrufen einer Zufallszahl (Challenge) von der HPC 3. Schritt: Durchführung des Kommandos EXTERNAL AUTHENTICATE zum Prüfen der eGK-Authentisierungsdaten 4. Schritt: Durchführung des Kommandos INTERNAL AUTHENTICATE zum Abrufen der HPC-Authentisierungsdaten
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Einmal pro eGK-Session mit der HPC zum Lesen und Schreiben geschützter Daten auf der eGK.
Vorangegangene Use Cases	UC_HPC_Verify_eGK_CVCs und UC_HPC_Verify_PIN
Nachfolgende Use Cases	Abhängig vom Anwendungskontext
Anmerkungen	Nach der eGK / HPC-Authentisierung ist in der eGK der Sicherheitsstatus »CHA.x mit Rollenkennung / Zugriffsprofil x wurde erfolgreich präsentiert« gesetzt, d.h. der HPC-Inhaber hat seine Zugriffsberechtigung gegenüber der eGK nachgewiesen.
Festlegungen	-

1. Schritt (von 4):
Tabelle 217 – Kommando: MSE Option SET ([HPC-P2], 5.6.4, Table 26)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten (17 Bytes)**	**Le**
00	22	C1	A4	11	83 0C ... (Referenz des öffentl. eGK-Authentisierungsschlüssels, PuK.eGK.AUT [HPC-P2], 5.6.4, NOTE unter Table 26) 84 01 10 ... (Referenz des privaten HPC-Authentisierungsschlüssels für eGK / HPC-Authentisierung PrK.HPC.AUT im SE#01, [HPC-P2], 5.2.8, Table 2)	-
P1 ist in [HPC-P2], 5.6.4 fälschlicherweise mit 81 angegeben. Die entsprechenden Schlüsselreferenzen sind im entsprechenden MSE SET-Kommando in der eGK-Spezifikation in umgekehrten Reihenfolge angegeben. Die Karten sollten beide Reihenfolgen beherrschen.						

Tabelle 218 – Korrekte Antwort ([HPC-P1], 5.6.4, Table 27)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenzen erfolgreich registriert.	2. Schritt

Tabelle 219 – Abweichende Antworten ([HPC-P2], Annex A, Table A.17)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

2. Schritt (von 4):
Tabelle 220 – Kommando: GET CHALLENGE ([HPC-P2], 5.6.4, Table 28)

CLA	INS	P1	P2	Lc	Daten	Le
00	84	00	00	-	-	08

Tabelle 221 – Korrekte Antwort ([HPC-P2], 5.6.4, Table 29)

Daten (8 Bytes)	SW1 SW2	Ursache	Aktion
XX XX XX XX XX XX XX XX ([HPC-P1], Annex E.2, Figure E.1)	90 00	Zufallszahl erzeugt und ausgegeben	3. Schritt

Tabelle 222 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
-	-	-	-

3. Schritt (von 4):
Tabelle 223 – Kommando: EXTERNAL AUTHENTICATE ([HPC-P2], 5.6.4, Table 30)

CLA	INS	P1	P2	Lc	Daten (128 Bytes)	Le
00	82	00	00	80	XX ... ([HPC-P1], Annex E.2, Figure E.1)	-

Tabelle 224 – Korrekte Antwort ([HPC-P2], 5.6.4, Table 31)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	eGK-Authentisierungsdaten erfolgreich verifiziert	4. Schritt

Tabelle 225 – Abweichende Antworten ([HPC-P1], Annex A, Table A.12)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

4. Schritt (von 4):
Tabelle 226 – Kommando: INTERNAL AUTHENTICATE ([HPC-P2], 5.6.4, Table 32)

CLA	INS	P1	P2	Lc	Daten (128 Bytes)	Le
00	82	00	00	80	XX ...	-

Tabelle 227 – Korrekte Antwort ([HPC-P2], 5.6.4, Table 33)

Daten (128 Bytes)	SW1 SW2	Ursache	Aktion
XX ... ([HPC-P1], Annex E.2, Figure E.1)	90 00	HPC-Authentisierungsdaten erfolgreich erzeugt und ausgegeben	Use Case beenden

Tabelle 228 – Abweichende Antworten ([HPC-P1], Annex A, Table A.11)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

16 Autorisierung einer SMC für die SMC / eGK-Interaktion

16.1 Autorisieren einer SMC für die SMC / eGK-Interaktion

Tabelle 229 – Autorisieren einer SMC für die SMC / eGK-Interaktion

Identifier	UC_HPC_Authorize_SMC
Name	Autorisieren einer SMC für die SMC / eGK-Interaktion
Beschreibung	Erzeugen von HPC-Authentisierungsdaten, mit denen sich die HPC gegenüber einer SMC authentisiert, um dadurch die SMC zur Interaktion mit eGKs zu autorisieren (siehe HPC-P3, 6.6.2).
Vorbedingungen	HPC betriebsbereit MF-Ebene selektiert
Nachbedingungen	MF-Ebene selektiert.
Standardablauf	1. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des privaten HPC-Authentisierungsschlüssels 2. Schritt: Durchführung des Kommandos INTERNAL AUTHENTICATE zur Erzeugung und zum Abrufen der HPC-Authentisierungsdaten
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Einmal pro SMC-Session, in der die SMC mit eGKs interagiert.
Vorangegangene Use Cases	UC_HPC_Reset
Nachfolgende Use Cases	Abhängig vom Anwendungskontext
Anmerkungen	
Festlegungen	Le-Feld von INTERNAL AUTHENTICATE auf 00 gesetzt (statt Länge der erwarteten Signatur)

1. Schritt (von 2):
Tabelle 230 – Kommando: MSE Option SET ([HPC-P2], 5.7, Table 34)

CLA	INS	P1	P2	Lc	Daten	Le
00	22	41	A4	06	84 01 10	-

Tabelle 231 – Korrekte Antwort ([HPC-P2], 5.7, Table 35)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den privaten HPC-Authentisierungsschlüssels PrK.HPC.AUT erfolgreich registriert.	2. Schritt

Tabelle 232 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

2. Schritt (von 2):
Tabelle 233 – Kommando: INTERNAL AUTHENTICATE ([HPC-P2], 5.7, Table 36)

CLA	INS	P1	P2	Lc	Daten (16 Bytes)	Le
00	88	00	00	10	Authentisierungs-bezogene Daten ([HPC-P1], E.2)	00
Die Authentisierungs-bezogenen Daten enthalten eine Zufallszahl der SMC, die zuvor mit GET CHALLENGE von der SMC angefordert wurde (HPC-P3, 6.6.2, Table 29 und 30).						

Tabelle 234 – Korrekte Antwort ([HPC-P2], 5.7, Table 37)

Daten	SW1 SW2	Ursache	Aktion
HPC-Authentisierungdaten ([HPC-P1], E.2, Figure E.1)	90 00	Erzeugen und Ausgeben der HPC-Authentisierungsdaten erfolgreich	Use Case beenden
Die HPC-Authentisierungdaten werden anschließend mit EXTERNAL AUTHENTICATE zur SMC gesendet und dort verifiziert (HPC-P3, 6.6.2, Table 31 und 32). Bei erfolgreicher Verifikation wird in der SMC der Sicherheitsstatus gesetzt, der für die SMC / eGK-Interaktion erforderlich ist.			

Tabelle 235 – Abweichende Antworten ([HPC-P1], Table A.11)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«

17 Nutzung der HP-Anwendung

17.1 Lesen der HP-bezogenen Daten

Tabelle 236 – Lesen der HP-bezogenen Daten

Identifier	**UC_HPC_Read_HP_Data**
Name	Lesen der HP-bezogenen Daten
Beschreibung	Lesen der HP-bezogenen Daten in der transparenten Datei EF.HPD ([HPC-P2], 7.1.2).
Vorbedingungen	HPC betriebsbereit DF.HPA geöffnet.
Nachbedingungen	DF.HPA geöffnet.
Standardablauf	a) Ohne Extended Length: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.HPD 2. Schritt: Senden von weiteren READ BINARY-Kommandos, bis HP-bezogene Daten vollständig gelesen. b) Mit Extended Length und n > Dateilänge: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.HPD und Le = 00 00 00 (3 Byte) c) Mit Extended Length und n < Dateilänge: 1. Schritt: Durchführung des Kommandos READ BINARY mit Angabe von Short File Identifier für EF.HPD und Le = 00 xx xx (3 Byte) 2. Schritt: Senden von weiteren READ BINARY-Kommandos, bis HP-bezogene Daten vollständig gelesen.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Abhängig vom Anwendungskontext, welcher die HP-bezogenen Daten verwendet.
Vorangegangene Use Cases	UC_HPC_Open_HPA
Nachfolgende Use Cases	Wenn die HP-bezogenen Daten nicht mehr aktuell sind: UC_HPC_Update_HP_Data
Anmerkungen	-
Festlegungen	Falls wiederholt aus derselben Datei gelesen wird, ist es aus Performanzgründen sinnvoll, dass ab dem zweiten READ BINARY der SFID in P1 nicht angegeben wird, sondern P1 und P2 für den Offset zur Verfügung stehen.

a) Ohne Extended Length

1. Schritt (von 2):
Tabelle 237 – Kommando: READ BINARY ([HPC-P2], 7.4, Table 44)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten**	**Le**
00	B0	81	00	-	-	00
P1 enthält in den niederwertigen Bits b5-b1 den Short File identifier für EF.HPD 1 ([HPC-P2], Table B.3) Der Wert von Le ist in HPC-P2 fälschlicherweise mit 08 angegeben.						

Tabelle 238 – Korrekte Antwort ([HPC-P2], 7.4, Table 45)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 0 bis byte 255 aus EF.HPD ([HPC-P2], 7.1.2)	90 00	1. Teil der HP-bezogenen Daten gelesen	2. Schritt
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens erhältlichen xx Bytes Daten verwendet wird.			

Tabelle 239 – Abweichende Antworten ([HPC-P1], Table A.4)

SW1 SW2	Bedeutung	Ursache	Aktion
62 82	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 81	Datei nicht transparent		
69 86	Kommando ohne SFID; keine Datei selektiert		
6A 82	Datei mit SFID nicht gefunden		
6B 00	Offset größer oder gleich Dateigröße		

2. Schritt (von 2):
Tabelle 240 – Kommando: READ BINARY ([HPC-P2], 7.4, Table 44)

CLA	INS	P1-P2	Lc	Daten	Le
00	B0	01 00 02 00 ...	-	-	00
P1-P2: Fortschaltung des Offset in Schritten von 256 Byte					

Tabelle 241 – Korrekte Antwort ([HPC-P2], 7.4, Table 45)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 256 bis Byte 511 aus EF.HPD Byte 512 bis Byte 767 aus EF.HPD ...	90 00	2. Teil der HP-bezogenen Daten gelesen 3. Teil der HP-bezogenen Daten gelesen ... Letzten Teil der HP-bezogenen Daten gelesen	2. Schritt 2. Schritt … Use Case beenden
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

b) Mit Extended Length und n (=I/O-Puffergröße-2) > Dateilänge

Falls n > Dateilänge (n = Wert enstprechend DO "Maximal length length of response APDU without SM", siehe [HPC-P1], Table 10) – 2, da 2 Byte für Status-Info benötigt werden):

1. Schritt (von 1):
Tabelle 242 – Kommando: READ BINARY ([HPC-P2], 7.4, Table 44)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	81	00	-	-	00 00 00
P1 enthält Short File identifier 1 für EF.HPD ([HPC-P2], Table B.3)						

Tabelle 243 – Korrekte Antwort ([HPC-P2], 7.4, Table 45)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Alle Bytes aus EF.HPD	62 82 (EOF reached before reading 65535 Byte)	HP-bezogene Daten erfolgreich gelesen (Achtung: möglicherweise Nullen am Ende, die nicht zu den HP-bezogenen Daten gehören)	Use Case beenden
Anmerkung:			

c) Mit Extended Length und n (= I/O-Puffergröße – 2) < Dateilänge:

1. Schritt (von 2):
Tabelle 244 – Kommando: READ BINARY ([HPC-P2], 7.4, Table 44)

CLA	INS	P1	P2	Lc	Daten	Le
00	B0	81	00	-	-	00 xx xx
P1 enthält Short File identifier 1 für EF.HPD ([HPC-P2], Table B.3) Le: xx xx = n = (Wert enstprechend DO max. length of response APDU without SM, siehe [HPC-P1], Tab. 10) – 2, da 2 Byte für Status-Info SW1 SW2 benötigt werden						

Tabelle 245 – Korrekte Antwort ([HPC-P2], 7.4, Table 45)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte 00 bis Byte n-1	90 00	n Byte der HP-bezogenen Daten gelesen	2. Schritt
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

2. Schritt (von 2):
Tabelle 246 – Kommando: READ BINARY ([HPC-P2], 7.4, Table 44)

CLA	INS	P1-P2	Lc	Daten	Le
00	B0	xx xx (= n) xx xx (= 2n) ...	-	-	00
P1-P2: Fortschaltung des Offset in Schritten von n Byte					

Tabelle 247 – Korrekte Antwort ([HPC-P2], 7.4, Table 45)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
Byte n bis Byte 2n-1 aus EF.HPD Byte 2n bis Byte 3n-1 aus EF.HPD ...	90 00 90 00 ... 62 82 (EOF reached before reading 256 Byte)	2. Teil der HP-bezogenen Daten gelesen 3. Teil der HP-bezogenen Daten gelesen ... Letzten Teil der HP-bezogenen Daten gelesen	Use Case beenden
Anmerkung: SW1 SW2 = 61 xx ist ein erlaubter Returncode (ISO 7816-4, 5.1.3), der von einigen Betriebssystemen zur Anzeige der noch in der Datei mindestens noch erhältlichen xx Bytes Daten verwendet wird.			

17.2 Aktualisieren der HP-bezogenen Daten

Tabelle 248 – Aktualisieren der HP-bezogenen Daten

Identifier	**UC_HPC_Update_HP_Data**
Name	Aktualisieren der HP-bezogenen Daten
Beschreibung	Schreiben der HP-bezogenen Daten in die transparenten Datei EF.HPD ([HPC-P2], 7.1.2).
Vorbedingungen	HPC betriebsbereit DF.HPA geöffnet Leistungserbringer mit Karteninhaber-PIN authentisiert
Nachbedingungen	DF.HPA geöffnet
Standardablauf	1. Schritt: Durchführung des Kommandos UPDATE BINARY mit SFID Falls HP-bezogene Daten > 255 Bytes 2. Schritt: Durchführung des Kommandos UPDATE BINARY mit SFID
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Abhängig vom Anwendungskontext, welcher die HP-bezogenen Daten verwendet.
Vorangegangene Use Cases	UC_HPC_Open_HPA und UC_HPC_Verify_PIN
Nachfolgende Use Cases	Abhängig vom Anwendungskontext
Anmerkungen	Falls das HP-bezogene Daten > 255 Bytes und Extended Length nicht unterstützt wird, ist das UPDATE BINARY mit Offset-Angabe solange zu wiederholen, bis die HP-bezogenen Daten komplett gespeichert sind. Der Fall mit Extended Length wird hier nicht weiterbetrachtet.
Festlegungen	Falls wiederholt aus derselben Datei gelesen wird, ist es aus Performanz-gründen sinnvoll, dass ab dem zweiten Update BINARY der SFID in P1 nicht angegeben wird, sondern P1 und P2 für den Offset zur Verfügung stehen.

1. Schritt (von 2):
Tabelle 249 – Kommando: UPDATE BINARY ([HPC-P2], 7.4, Table 46)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten (maximal 255 Bytes)**	**Le**
00	D6	81	00	xx	HP-bezogene Daten der Länge xx	00

2. Schritt (von 2):
Solange wiederholen, bis HP-bezogene Daten komplett geschrieben
Tabelle 250 – Kommando: UPDATE BINARY ([HPC-P2], 8.8, Table 72)

CLA	**INS**	**P1 - P2**	**Lc**	**Daten**	**Le**
00	D6	00 FF 01 FE … xx xx	FF	Die nächsten 255 Bytes schreiben Die restlichen xx Bytes schreiben	-
P1-P2: Fortschaltung des Offset in Schritten von 255 Byte					

Folgende Antworten gelten für jedes UPDATE BINARY Kommando:

Tabelle 251 – Korrekte Antwort ([HPC-P2], 8.8, Table 73)

Daten (n Bytes)	SW1 SW2	Ursache	Aktion
-	90 00	Daten erfolgreich geschrieben	Use Case beenden oder 2. Schritt, wenn weitere HP-bezogene Daten zu aktualisieren sind

Tabelle 252 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Bedeutung	Ursache	Aktion
69 81	Datei nicht transparent	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 86	Kommando ohne SFID; Datei nicht selektiert		
6A 82	Datei mit SFID nicht gefunden		
6A 87	Offset + Lc größer Dateogröße		
6B 00	Offset größer oder gleich Dateigröße		

18 Nutzung einer stationären HPC mit Trusted Channel

In den Arztpraxen und in den Apotheken gibt es verteilte Arbeitsplätze, die jeweils mit einem PC und einem Kartenleser mit integrierter SMC ausgestattet sind. Ein Konfigurationsbeispiel bezogen auf ein Arztpraxis-Szenario zeigt Abbildung 1. Sind nun z.B. elektronische Signaturen an diesen verteilten PCs von demselben Heilberufler erforderlich, dann erfordert dies die Nutzung der HPC an diesen verteilten Arbeitsplätzen. Da das permanente Herausziehen der HPC mit Wiedereinstecken und erneuter PIN-Eingabe als keine praktikable Lösung angesehen wird, verbleibt die HPC stationär an einem verschlossenen Ort und kann „remote“ von den verschiedenen Arbeitsplätzen genutzt werden.

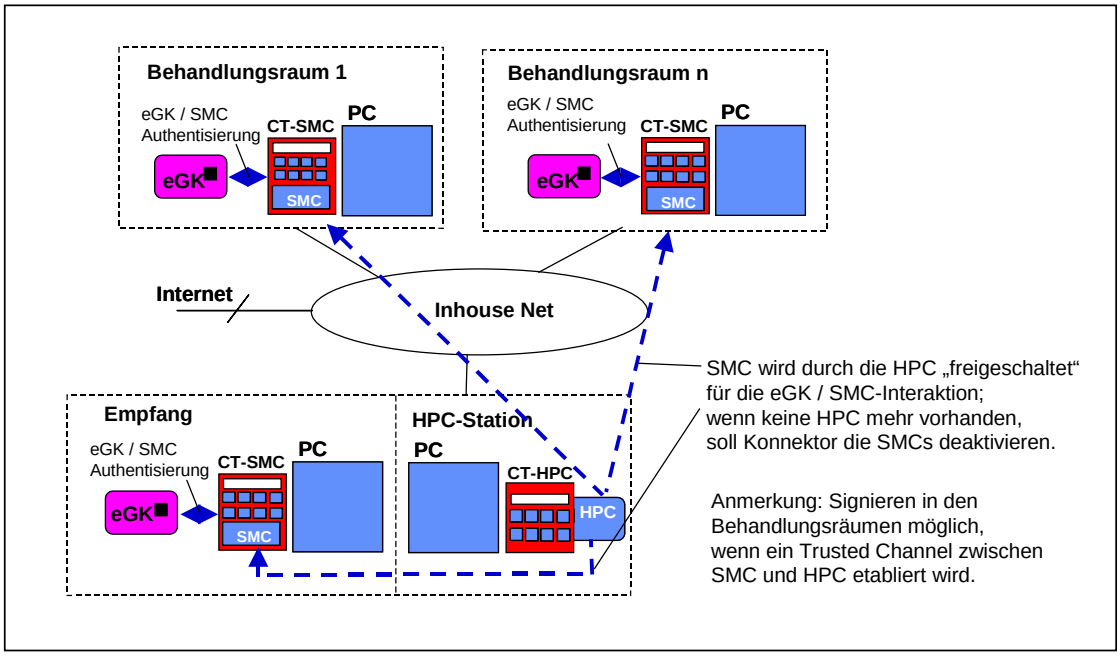

Abbildung 1 - Beispielkonfiguration (vereinfacht) mit logischen Kanälen zur stationären HPC

Bei der Nutzung der QES- und der ESIGN-Anwendung werden sicherheitssensitive Daten (z.B. PIN-Daten und Hashwerte im Vorfeld der Signaturerzeugung) zur HPC gesendet. Dazu muss ein Trusted Channel zwischen SMC und HPC etabliert sein. Die Kommunikation zwischen den verteilten Arbeitsplätzen und der stationären HPC erfolgt darin mit Kommandos und Antworten im Übertragungsmodus Secure Messaging (SM). Das Erzeugen von SM-Kommandos und das Verarbeiten von SM-Antworten gehört zur Funktionalität der SMC. Um koexistent zu verschiedenen SMCs einen Trusted Channel aufbauen zu können, existiert das Konzept der logischen Kanäle. Das Autorisieren der SMC für die SMC / eGK-Interaktion und das Öffnen von logischen Kanälen erfolgt stets im Basiskanal der HPC.

Das Autorisieren der SMC ist kein spezifischer Use Case für die stationäre Verwendung der HPC und wird daher unter einem eigenen Anwendungskontext (siehe 16.1, S. 80) beschrieben. Die Unterscheidung der SMC in Typ A und B ist bei keinem hier aufgeführten Use Case relevant.

Im folgenden Anwendungsszenario wird zunächst in der HPC ein logischer Kanal zur Nutzung einer HPC-Anwendung geöffnet (siehe 18.1, S. 88). Anschließend kann im geöffneten logischen Kanal eine Anwendung (QES oder ESIGN) für die Remote-Nutzung geöffnet werden (siehe 18.3, S. 92). Die SMC-bezogenen CV-Zertifikate werden verifiziert (siehe 18.4, S. 95) und die HPC / SMC-Authentisierung mit SM-Schlüsselvereinbarung wird durchgeführt (siehe 0, S. 103). Zur visuellen Bestätigung, dass ein Trusted Channel etabliert worden ist, kann anschließend die Display Message der geöffneten Anwendung aus der HPC gelesen und dem Karteninhaber angezeigt werden (siehe 18.7, S. 106). Als Anwendungsfall dient in diesem Beispiel das Erzeugen einer qualifizierten elektronischen Signatur in der stationären HPC (siehe 18.9, S. 109).

Der etablierte Trusted Channel steht aus Sicherheitsgründen nur für die aktuell geöffnete Anwendung zur Verfügung. Wird also eine andere Anwendung selektiert, sind der zuvor erreichte Sicherheitsstatus und die SM-Schlüssel verloren und der Trusted Channel muss bei Bedarf erneut aufgebaut werden.

18.1 Einrichten eines logischen Kanals zur HPC

Tabelle 253 – Einrichten eines logischen Kanals zur HPC

Identifier	**UC_HPC_Open_Logical_Channel**
Name	Einrichten eines logischen Kanals zur HPC
Beschreibung	Einrichten eines logischen Kanals zur HPC, initiiert z.B. von einem Arbeitsplatzsystem in Behandlungsraum x.
Vorbedingungen	Es muss mindestens ein freier logischer Kanal verfügbar und der Basic Channel darf nicht im SM-Modus sein. Ob ein freier Kanal verfügbar ist, kann nur dann festgestellt werden, wenn das betreffende Primärsystem Kenntnis über die Kanalbelegung hat.
Nachbedingungen	Nach Etablierung ist der Kanal für die Bearbeitung von SmartCard-Kommandos offen
Standardablauf	1. Schritt: Durchführung des Kommandos MANAGE CHANNEL zum Einrichten des neuen logischen Kanals
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Anwendungsabhängig
Vorangegangene Use Cases	Mindestens UC_HPC_Reset
Nachfolgende Use Cases	Abhängig vom Anwendungskontext, z.B. UC_HPC_Open_Remote_Application
Anmerkungen	• Logische Kanäle können auch in einer lokalen HPC genutzt werden. Die folgenden Anwendungsfälle nutzen logische Känale jedoch in einer Remote-HPC mit Trusted Channel. • Das Senden von Kommandos in einem logischen Kanal zur HPC erfolgt z.B. von dem Arbeitsplatzsystem aus, von dem aus der logische Kanal geöffnet wurde. Das Senden ist aber auch von einem anderen Arbeitsplatzsystem möglich, solange kein Trusted Channel mit der SMC eines bestimmten Arbeitsplatz etabliert wurde. • Der einzige Unterschied zum Senden von Kommandos im Basis-Kanal (Default-Kanal mit Nummer 0) besteht darin, dass die Bits b2-b1 des CLA-Byte einen Wert ungleich Null aufweisen.
Festlegungen	-

1. Schritt (von 1):

Tabelle 254 – Kommando: MANAGE CHANNEL ([HPC-P2], Table 4 , Annex G, Table G.1 und [HPC-P1], Table 11)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten**	**Le**
00	70	00	00	-	-	01

Tabelle 255 – Korrekte Antwort

Daten	SW1 SW2	Ursache	Aktion
01 oder 02 oder 03 (Kanal-Nr.)	90 00	Öffnen eines logischen Kanals erfolgreich	Use Case beenden
-	68 81	Alle Kanäle sind belegt.	Anzeige an Benutzer und ggf. Angebot, einen existierenden Kanal zu schließen

Tabelle 256 – Abweichende Antworten ([HPC-P1], Table A.5)

SW1 SW2	**Ursache**	**Aktion**
-	-	-

18.2 Schließen eines logischen Kanals zur HPC

Tabelle 257 – Schließen eines logischen Kanals zur HPC

Identifier	**UC_HPC_Close_Logical_Channel**
Name	Schließen eines logischen Kanals zur HPC
Beschreibung	Schließen eines logischen Kanals zur HPC, initiiert z.B. von dem Arbeitsplatzsystem, von dem aus der logische Kanal geöffnet wurde. Die Schließung auch von einem anderen Arbeitsplatzsystem möglich.
Vorbedingungen	Das Schließen eines Kanals setzt das Vorhandensein desselben voraus.
Nachbedingungen	Nach erfolgreichem Schließen ist der Kanal wieder frei und kann neu benutzt werden. Eventuell vorher vorhandene SM-Schlüssel sind nicht mehr nutzbar.
Standardablauf	1. Schritt Durchführung des Kommandos MANAGE CHANNEL zum Schließen eines logischen Kanals
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Abhängig von konkreter Nutzungsumgebung
Vorangegangene Use Cases	Abhängig vom Anwendungskontext, z.B. UC_HPC_SIGN_With_Stationary_HPC
Nachfolgende Use Cases	Abhängig vom Anwendungskontext
Anmerkungen	Das Schließen eines Kanals kann nicht nur von dem Arbeitsplatzsystem aus, von dem der Kanal geöffnet wurde, durchgeführt werden, sondern auch von jedem anderen Arbeitsplatzsystem
Festlegungen	-

1. Schritt (von 1):

Tabelle 258 – Kommando: MANAGE CHANNEL ([HPC-P2], Table 40)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten**	**Le**
0X	70	80	00	-	-	-
In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.						

Tabelle 259 – Korrekte Antwort ([HPC-P2], Table 40 und [HPC-P1], Annex A, Table A.3)

Daten	**SW1 SW2**	**Ursache**	**Aktion**
-	90 00	Schließen des logischen Kanals erfolgreich	Use Case beenden
-	68 81	Alle Kanäle sind belegt.	Anzeige an Benutzer und ggf. Angebot, einen existierenden Kanal zu schließen
-	xxxx, z.B. 62 00	Kommando wurde nicht ausgeführt. Kanal-Nr. falsch, d.h. der angegebene Kanal war nicht geöffnet oder die Kanal-Nr. war größer als zulässig	Anzeige an Benutzer und ggf. Angebot, einen geöffneten Kanal zu schließen

Tabelle 260 – Abweichende Antworten ([HPC-P1], Table A.5)

SW1 SW2	Ursache	Aktion
-	-	-

18.3 Öffnen einer Anwendung für die Remote-Nutzung

Tabelle 261 – Öffnen einer Anwendung für die Remote-Nutzung

Identifier	**UC_HPC_Open_Remote_Application**
Name	Öffnen einer Anwendung für die Remote-Nutzung
Beschreibung	Setzen der Sicherheitsumgebung 2 auf MF-Ebene für die HPC / SMC-Interaktion, Öffnen der Anwendung, die im Secure Messaging (SM)-Modus genutzt werden soll, z.B. die ESIGN oder QES-Anwendung, und Setzen der Sicherheitsumgebung 2 auf DF-Ebene.
Vorbedingungen	HPC betriebsbereit
Nachbedingungen	Anwendung für die Remote-Nutzung in der Sicherheitsumgebung 2 geöffnet.
Standardablauf	1. Schritt: Kommando MANAGE SECURITY ENVIRONMENT (MSE) mit der Option RESTORE zur Selektion der Sicherheitsumgebung 2 auf MF-Ebene für die HPC / SMC-Interaktion 2. Schritt: Kommando SELECT zum Öffnen der QES- oder ESIGN-Anwendung, die im Trusted Channel genutzt werden soll. 3. Schritt: Kommando MANAGE SECURITY ENVIRONMENT (MSE) mit der Option RESTORE zur Selektion der Sicherheitsumgebung 2 auf Anwendungsebene zum Aufbau eines Trusted Channel in der nachfolgenden HPC / SMC-Authentisierung
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Bei Anwendungswechsel ist das Authentisierungsverfahren erneut zu durchlaufen
Vorangegangene Use Cases	HPC betriebsbereit
Nachfolgende Use Cases	UC_HPC_Verify_SMC_CVCs (bzw. UC_HPC_Verify_SMC_Cross_CVCs) und UC_HPC_Authenticate_SMC
Anmerkungen	Weil das Öffnen einer Anwendung immer ohne Trusted Channel vorgenommen wird, geht ein Trusted Channel verloren, sobald eine Anwendung geöffnet wird. Dann muss erneut ein Trusted Channel aufgebaut werden.
Festlegungen	-

1. Schritt (von 3):
Tabelle 262 – Kommando: MSE Option RESTORE ([HPC-P2], 5.3 und 5.4.5, Table 10)

CLA	INS	P1	P2	Lc	Daten	Le
0X	22	F3	02	-	-	-
In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.						

Tabelle 263 – Korrekte Antworten ([HPC-P2], 5.4.5, Table 11)

Daten	**SW1 SW2**	**Ursache**	**Aktion**
-	90 00	Setzen der Sicherheitsumgebung 2 auf MF-Ebene erfolgreich	2. Schritt

Tabelle 264 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehleraus-gang »HPC defekt«
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

2. Schritt (von 3):
Tabelle 265 – Kommando: SELECT ([HPC-P2], 8.4, Table 50)

CLA	INS	P1	P2	Lc	Daten	Le
0X	A4	04	0C	06 bzw. 0A	D2 76 00 00 66 01 (AID von DF.QES) bzw. A0 00 00 01 67 45 53 49 47 4E (AID von DF.ESIGN)	-

- Application Identifier von DF.QES bzw. DF.ESIGN im Datenfeld
- In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 266 – Korrekte Antwort ([HPC-P2], 8.4, Table 51)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	DF.QES bzw. DF.ESIGN erfolg-reich selektiert	3. Schritt

Tabelle 267 – Abweichende Antworten ([HPC-P1], Table A.2)

SW1 SW2	Beschreibung	Ursache	Aktionen
6A 82	QES-Anwendung bzw. ESIGN-Anwen-dung nicht vorhanden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine manipulierte / de-fekte Karte.	Fehleraus-gang »HPC defekt«
62 83	QES-Anwendung bzw. ESIGN-Anwen-dung deaktiviert		
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht ge-öffnet.		

3. Schritt (von 3):
Tabelle 268 – Kommando: MSE Option RESTORE ([HPC-P2], 11.4, Table 91)

CLA	INS	P1	P2	Lc	Daten	Le
0X	22	F3	02	-	-	-

In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 269 – Korrekte Antworten ([HPC-P2], 11.4, Table 92)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Setzen der Sicherheitsumgebung 2 auf DF-Ebene erfolgreich	Use Case beenden

Tabelle 270 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmier-fehler oder eine defekte Karte.	Fehleraus-gang »HPC defekt«
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

18.4 Verifizieren der SMC-bezogenen CV-Zertifikate (zweistufig)

Tabelle 271 – Verifizieren der SMC-bezogenen CV-Zertifikate (zweistufig)

Identifier	**UC_HPC_Verify_SMC_CVCs**
Name	Verifizieren der SMC-bezogenen CV-Zertifikate (zweistufig)
Beschreibung	Die SMC-bezogenen CV-Zertifikate sind zu prüfen und die darin enthaltenen öffentlichen Schlüssel in der HPC temporär zu speichern ([HPC-P2], 11.5), um im anschließenden Use Case der HPC / SMC-Authentisierung mit SM-Schlüsselvereinbarung die Authentizität der SMC prüfen zu können ([HPC-P2], 11.6). Das CHA-Feld des SMC-Authentisierungszertifikats wird ebenfalls temporär gespeichert (SMC mit Rollenkennung 00 im CHA-Feld haben jedoch keine Zugriffsrechte auf Daten / Funktionen der HPC; SMC für Nachladeoperationen haben aber eine von 00 verschiedene Rollenkennung).
Vorbedingungen	Selektion der Anwendung, die im Secure Messaging (SM)-Modus genutzt werden soll, z.B. die ESIGN oder QES-Anwendung
Nachbedingungen	Öffentlicher SMC-bezogener Schlüssel und CHA der SMC in der HPC für nachfolgendes Authentisierungsverfahren vorhanden
Standardablauf	1. Schritt: Kommando MANAGE SECURITY ENVIRONMENT (MSE) mit Option SET zur Selektion des öffentlichen Root-CA-Schlüssels der HPC 2. Schritt: Kommando VERIFY CERTIFICATE zum Prüfen des SMC-CA-Zertifikats und Speichern des öffentlichen SMC-CA-Schlüssels. 3. Schritt: Kommando MANAGE SECURITY ENVIRONMENT (MSE) mit Option SET zur Selektion des öffentlichen SMC-CA-Schlüssels 4. Schritt: Kommando VERIFY CERTIFICATE zum Prüfen des SMC-Authentisierungszertifikats und Speichern des öffentlichen SMC-Authentisierungsschlüssels und des CHA-Wertes.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Bei Anwendungswechsel ist das Authentisierungsverfahren erneut zu durchlaufen
Vorangegangene Use Cases	
Nachfolgende Use Cases	
Anmerkungen	Die öffentlichen Root-CA-Schlüssel einer SMC und der HPC können nach einem Wechsel des Root-CA-Schlüssels (oder später im europäischen Kontext) unterschiedlich sein. Dann ist das Abrufen und Prüfen eines Cross-Zertifikats erforderlich (siehe UC_HPC_Retrieve_Cross_CVC und UC_HPC_Verify_SMC_Cross_CVCs).
Festlegungen	

1. Schritt (von 4):
Tabelle 272 – Kommando: MSE Option SET ([HPC-P2], 5.6.3, Table 18)

CLA	INS	P1	P2	Lc	Daten (10 Bytes)	Le
0X	22	81	B6	0A	83 08 ... ([HPC-P2], 5.6.2, Figure 3)	-

- Die Referenz des öffentlichen Root-CA-Schlüssels PuK.RCS.CS ist im Wertefeld des Datenobjektes CAR des HPC-CA-Zertifikats im Klartext angeben und somit dem Primärsystem zugänglich.
- In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 273 – Korrekte Antworten ([HPC-P2], 5.6.3, Table 19 und [HPC-P1], Table A.17)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den öffentlichen Root-CA-Schlüssel erfolgreich registriert.	2. Schritt

Tabelle 274 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Öffentlicher Root-CA-Schlüssel der SMC ist auf der HPC nicht vorhanden. Das hätte das Primärsystem zuvor durch einen Vergleich der Root-CA-Referenz der SMC mit der im Primärsystem-Stack gespeicherten Root-CA-Referenz der HPC feststellen müssen (siehe Anwendungsfälle UC_HPC_Retrieve_Cross_CVC und UC_HPC_Verify_SMC_Cross_CVCs. Diese Return-Wert ist also ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehleraus-gang »HPC defekt«
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.	Diese Return-Wert ist ein Indiz für ein Programmierfehler oder eine defekte Karte.	

2. Schritt (von 4):
Tabelle 275 – Kommando: VERIFY CERTIFICATE ([HPC-P2], 5.6.3, Table 20)

CLA	INS	P1	P2	Lc	Daten (196 Bytes)	Le
0X	2A	00	AE	C4	5F37 8180 xx ... 5F38 3D xx ... ([HPC-P1], B.2, Table B.10, ohne DO CAR)	-
In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.						

Tabelle 276 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 21)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Prüfen des SMC-CA-Zertifikats erfolgreich	Schritt 3

Tabelle 277 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in den Kommandodaten	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

3. Schritt (von 4):
Tabelle 278 – Kommando: MSE Option SET ([HPC-P2], 5.6.3, Table 22)

CLA	INS	P1	P2	Lc	Daten (14 Bytes)	Le
0X	22	81	B6	0E	83 0C ... ([HPC-P2], 5.6.2, Figure 3)	-

- Als Referenz des öffentlichen SMC-CA-Schlüssels PuK.CA_NN.SMC (12 Bytes) dient der für das Primärsystem zugängliche Wert des Datenobjektes CAR (8 Bytes) des SMC-Authentisierungszertifikats mit vier vorangestellten Null-Bytes (d.h. insgesamt 12 Bytes).
- In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 279 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 23)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den öffentlichen SMC-CA-Schlüssel erfolgreich registriert.	4. Schritt

Tabelle 280 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

4. Schritt (von 4):
Tabelle 281 – Kommando: VERIFY CERTIFICATE ([HPC-P2], 5.6.3, Table 24)

CLA	INS	P1	P2	Lc	Daten (195 Bytes)	Le
0X	2A	00	AE	C3	5F37 8180 xx ... 5F38 3C xx ... ([HPC-P1], B.2, Table B.11, ohne DO CAR)	-

In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 282 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 25)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Prüfen des SMC-Authentisierungszertifikats erfolgreich	Use Case beenden

Tabelle 283 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in den Kommandodaten	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

18.5 Verifizieren der SMC-bezogenen CV-Zertifikate mit Cross-Zertifikat (dreistufig)

Tabelle 284 – Verifizieren der SMC-bezogenen CV-Zertifikate mit Cross-Zertifikat (dreistufig)

Identifier	UC_HPC_Verify_SMC_Cross_CVCs
Name	Verifizieren der SMC-bezogenen CV-Zertifikate mit Cross-Zertifikat (dreistufig)
Beschreibung	Prüfen eines Cross-CV-Zertifikats und temporäres Speichern des darin enthaltenen öffentlichen Root-CA-Schlüssel der SMC in der HPC. Anschließend Prüfen der SMC-bezogenen CV-Zertifikate und temporäres Speichern der darin enthaltenen öffentlichen Schlüssel in der HPC, damit die HPC bei einer anschließenden SMC / HPC-Authentisierung den öffentlichen SMC-Authentisierungsschlüssel kennt und die Authentizität der SMC prüfen kann. Das CHA-Feld des SMC-Authentisierungszertifikats wird ebenfalls temporär gespeichert (SMC mit Rollenkennung 00 im CHA-Feld haben jedoch keine Zugriffsrechte auf Daten / Funktionen der HPC; SMC für Nachladeoperationen haben aber eine von 00 verschiedene Rollenkennung).
Vorbedingungen	Selektion der Anwendung, die im Secure Messaging (SM)-Modus genutzt werden soll, z.B. die ESIGN oder QES-Anwendung. Cross-Zertifikat des Root-CA-Schlüssels der SMC im Primärsystem vorhanden.
Nachbedingungen	Öffentlicher SMC-bezogener Schlüssel und CHA der SMC in der HPC für nachfolgendes Authentisierungsverfahren vorhanden.
Standardablauf	1. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des öffentlichen Root-CA-Schlüssels der HPC 2. Schritt: Durchführung des Kommandos VERIFY CERTIFICATE zum Prüfen des Cross-CV-Zertifikats und zum temporären Speichern des öffentlichen Root-CA-Schlüssels der SMC. 3. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des öffentlichen Root-CA-Schlüssels der SMC 4. Schritt: Durchführung des Kommandos VERIFY CERTIFICATE zum Prüfen des CA-Zertifikats der SMC und zum temporären Speichern des öffentlichen CA-Schlüssels der SMC. 5. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des öffentlichen CA-Schlüssels der SMC 6. Schritt: Durchführung des Kommandos VERIFY CERTIFICATE zum Prüfen des SMC-Authentisierungszertifikats und zum temporären Speichern des öffentlichen Authentisierungsschlüssels der SMC.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Einmal pro SMC-Anwendungssession mit der HPC, wenn die Referenz des Root-CA-Schlüssels der SMC von dem der HPC abweicht. Ein Vergleich der Referenzen erfolgt auf Basis der Primärsystem-Stacks (siehe Anhang A.2).
Vorangegangene Use Cases	Falls nicht bereits im Primärsystem vorhanden: UC_HPC_Retrieve_Cross_CVC
Nachfolgende Use Cases	UC_HPC_Authenticate_SMC
Anmerkungen	Das Abrufen und Prüfen eines Cross-Zertifikats ist erforderlich, wenn der öffentliche Root-CA-Schlüssel der SMC und der HPC nach dem Wechsel eines Root-CA-Schlüssels (oder später zum Import eines Root-CA-Schlüssels im europäischen Kontext) unterschiedlich sind.
Festlegungen	-

1. Schritt (von 6):
Tabelle 285 – Kommando: MSE Option SET ([HPC-P2], 5.6.3, Table 18)

CLA	INS	P1	P2	Lc	Daten (10 Bytes)	Le
0X	22	81	B6	0A	83 08 ... ([HPC-P2], 5.6.2, Figure 3)	-

- Die Referenz des öffentlichen Root-CA-Schlüssels PuK.RCA.CS ist im Wertefeld des Datenobjektes CAR des HPC-CA-Zertifikats im Klartext angeben und ist im HPC-Stack gespeichert (siehe Anhang A.2).
- In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 286 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 19 und [HPC-P1], Table A.17)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den öffentlichen Root-CA-Schlüssel der HPC erfolgreich registriert.	2. Schritt

Tabelle 287 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

2. Schritt (von 6):
Tabelle 288 – Kommando: VERIFY CERTIFICATE ([HPC-P2], 5.6.3, Table 20)

CLA	INS	P1	P2	Lc	Daten (196 Bytes)	Le
0X	2A	00	AE	C4	5F37 8180 xx ... 5F38 3D xx ... ([HPC-P1], B.2, Table B.10, ohne DO CAR)	-

In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 289 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 21)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Prüfen des Cross-Zertifikats erfolgreich	3. Schritt

Tabelle 290 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in den Kommandodaten	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

3. Schritt (von 6):
Tabelle 291 – Kommando: MSE Option SET ([HPC-P2], 5.6.3, Table 22)

CLA	INS	P1	P2	Lc	Daten (12 Bytes)	Le
0X	22	81	B6	0E	83 0C ... ([HPC-P2], 5.6.2, Figure 3)	-

- Als Referenz des öffentlichen Root-CA-Schlüssels PuK.RCA_SMC.CS (12 Bytes) dient der Wert des Datenobjektes CAR (8 Bytes) des Cross-Zertifikats mit vier vorangestellten Null-Bytes (d.h. insgesamt 12 Bytes).
- In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 292 – Korrekte Antworten ([HPC-P2], 5.6.3, Table 23 und [HPC-P1], Table A.17)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den öffentlichen Root-CA-Schlüssel der SMC erfolgreich registriert.	4. Schritt

Tabelle 293 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Dieser Return-Werte sollten bei einer HPC-konformen Karte nicht auftreten.	Fehlerausgang »HPC defekt«
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

4. Schritt (von 6):
Tabelle 294 – Kommando: VERIFY CERTIFICATE ([HPC-P2], 5.6.3, Table 24)

CLA	INS	P1	P2	Lc	Daten (196 Bytes)	Le
0X	2A	00	AE	C4	5F37 8180 xx ... 5F38 3D xx ... ([HPC-P1], B.2, Table B.10, ohne DO CAR)	-

In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 295 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 25)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Prüfen des SMC-CA-Zertifikats erfolgreich	5. Schritt

Tabelle 296 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in den Kommandodaten	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

5. Schritt (von 6):
Tabelle 297 – Kommando: MSE Option SET ([HPC-P2], 5.6.3, Table 22)

CLA	INS	P1	P2	Lc	Daten (14 Bytes)	Le
0X	22	81	B6	0E	83 0C ... ([HPC-P2], 5.6.2, Figure 3)	-

- Als Referenz des öffentlichen SMC-CA-Schlüssels PuK.CA_NN_SMC (12 Bytes) dient der für das Primärsystem zugängliche Wert des Datenobjektes CAR (8 Bytes) des SMC-Authentisierungszertifikats mit vier vorangestellten Null-Bytes (d.h. insgesamt 12 Bytes).
- In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 298 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 23)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenz für den öffentlichen SMC-CA-Schlüssel erfolgreich registriert.	6. Schritt

Tabelle 299 – Abweichende Antworten ([HPC-P1], Table A.17)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

6. Schritt (von 6):
Tabelle 300 – Kommando: VERIFY CERTIFICATE ([HPC-P2], 5.6.3, Table 24)

CLA	INS	P1	P2	Lc	Daten (195 Bytes)	Le
0X	2A	00	AE	C3	5F37 8180 xx ... 5F38 3C xx ... ([HPC-P1], B.2, Table B.11, ohne DO CAR)	-

In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt) CLA = 00 Basiskanal. CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.

Tabelle 301 – Korrekte Antwort ([HPC-P2], 5.6.3, Table 25)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Prüfen des SMC-Authentisierungszertifikats erfolgreich	Use Case beenden

Tabelle 302 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 80	Formatfehler in den Kommando-daten	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
6A 88	Referenzdaten nicht gefunden		
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

18.6 Durchführen der HPC / SMC Authentisierung mit SM-Schlüsselvereinbarung

Tabelle 303 – Durchführen der HPC / SMC Authentisierung mit SM-Schlüsselvereinbarung

Identifier	**UC_HPC_Authenticate_SMC**
Name	Durchführen der HPC / SMC Authentisierung mit SM-Schlüsselvereinbarung
Beschreibung	• Nachweis der Authentizität der SMC durch das Anwenden des privaten Authentisierungsschlüssels der SMC gegenüber der HPC. • Nachweis der Zugriffsrechte der HPC (d.h. das bei der Verifikation des HPC-Authentisierungszertifikats der SMC präsentierte Zugriffsprofil der HPC) durch das Anwenden des privaten Authentisierungsschlüssels der HPC gegenüber der SMC. • Vereinbarung von SM-Schlüsseln zur nachfolgenden Nutzung innerhalb eines Trusted Channel zwischen der stationären HPC und einer SMC an einem Arbeitsplatz
Vorbedingungen	HPC ist betriebsbereit, das SMC-Authentisierungszertifikat ist verifiziert, d.h. der öffentliche Authentisierungsschlüssel der SMC ist in der HPC vorhanden.
Nachbedingungen	Die SMC und die HPC sind gegenseitig authentisiert, die Secure Messaging-Schlüssel sind vereinbart.
Standardablauf	1. Schritt: Durchführung des Kommandos MANAGE SECURITY ENVIRONMENT (MSE) SET zur Selektion des öffentlichen SMC-Authentisierungsschlüssels und des privaten HPC-Authentisierungsschlüssels 2. Schritt: Durchführung des Kommandos GET CHALLENGE zum Abrufen einer Zufallszahl (Challenge) von der HPC 3. Schritt: Durchführung des Kommandos EXTERNAL AUTHENTICATE zum Prüfen der SMC-Authentisierungsdaten und zur Berechnung der SM-Schlüssel in der HPC gemäß [HPC-P1], Annex E.3. 4. Schritt: Durchführung des Kommandos INTERNAL AUTHENTICATE zum Abrufen der HPC-Authentisierungsdaten gemäß [HPC-P1], Annex E.3.
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Einmal pro QES-Anwendungssession oder ESIGN-Anwendungssession auf einer stationären HPC mit einer SMC an einem Arbeitsplatz.
Vorangegangene Use Cases	UC_HPC_Open_Remote_Application, UC_HPC_Verify_SMC_CVCs (bzw. UC_HPC_Verify_SMC_Cross_CVCs)
Nachfolgende Use Cases	UC_HPC_Read_DM und UC_HPC_Use_Stationary_HPC
Anmerkungen	Nach der SMC / HPC-Authentisierung mit SM-Schlüsselvereinbarung ist in der SMC der Sicherheitsstatus »CHA.x mit Rollenkennung / Zugriffsprofil x wurde erfolgreich präsentiert« gesetzt, d.h. der HPC-Inhaber hat seine Zugriffsberechtigung gegenüber der SMC nachgewiesen.
Festlegungen	-

1. Schritt (von 4):
Tabelle 304 – Kommando: MSE Option SET ([HPC-P2], 11.6, Table 93)

CLA	INS	P1	P2	Lc	Daten (17 Bytes)	Le
0X	22	C1	A4	11	83 0C ... (Referenz des öffentl. SMC-Authentisierungsschlüssels, PuK.SMC.AUT) 84 01 11 ... (Referenz des privaten HPC-Authentisierungsschlüssels PrK.HPC.AUT für SMC / HPC-Authentisierung, [HPC-P2], 5.2.8, Table 2)	-
• Lc in [HPC-P2], Table 93, ist fälschlicherweise mit 14 angegeben. • In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.						

Tabelle 305 – Korrekte Antwort ([HPC-P2], 11.6, Table 94)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	Schlüsselreferenzen erfolgreich registriert.	2. Schritt

Tabelle 306 – Abweichende Antworten ([HPC-P2], Annex A, Table A.17)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

2. Schritt (von 4):
Tabelle 307 – Kommando: GET CHALLENGE ([HPC-P2], 11.6, Table 95)

CLA	INS	P1	P2	Lc	Daten	Le
0X	84	00	00	-	-	08
In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.						

Tabelle 308 – Korrekte Antwort ([HPC-P2], 11.6, Table 96)

Daten (8 Bytes)	SW1 SW2	Ursache	Aktion
XX XX XX XX XX XX XX XX ([HPC-P1], Annex E.3, Figure E.2)	90 00	Zufallszahl erzeugt und ausgegeben	3. Schritt

Tabelle 309 – Abweichende Antworten

SW1 SW2	Fehlerbedingung	Ursache	Aktion
-	-	-	-

3. Schritt (von 4):
Tabelle 310 – Kommando: EXTERNAL AUTHENTICATE ([HPC-P2], 11.6, Table 97)

CLA	INS	P1	P2	Lc	Daten (128 Bytes)	Le
0X	82	00	00	80	XX ... ([HPC-P1], Annex E.3, Figure E.2)	-
In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert. Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.						

Tabelle 311 – Korrekte Antwort ([HPC-P2], 11.6, Table 98)

Daten	SW1 SW2	Ursache	Aktion
-	90 00	SMC-Authentisierungsdaten erfolgreich verifiziert	4. Schritt

Tabelle 312 – Abweichende Antworten ([HPC-P1], Annex A, Table A.12)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

4. Schritt (von 4):
Tabelle 313 – Kommando: INTERNAL AUTHENTICATE ([HPC-P2], 11.6, Table 99)

CLA	INS	P1	P2	Lc	Daten (128 Bytes)	Le
0X	82	00	00	80	XX ...	-
In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert; Bits b4-b3 sind 0, d.h. das Kommando wird im Plaintext-Modus gesandt. CLA = 00 Basiskanal, CLA = 01 Logischer Kanal 1, CLA = 02 Logischer Kanal 2, CLA = 03 Logischer Kanal 3.						

Tabelle 314 – Korrekte Antwort ([HPC-P2], 11.6, Table 100)

Daten (128 Bytes)	SW1 SW2	Ursache	Aktion
XX ... ([HPC-P1], Annex E.3, Figure E.2)	90 00	HPC-Authentisierungsdaten erfolgreich erzeugt und ausgegeben	Use Case beenden

Tabelle 315 – Abweichende Antworten ([HPC-P1], Annex A, Table A.11)

SW1 SW2	Fehlerbedingung	Ursache	Aktion
6A 88	Referenzdaten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		

18.7 Lesen der Display Message

Tabelle 316 – Lesen der Display Message

Identifier	**UC_HPC_Read_DM**
Name	Lesen der Display Message
Beschreibung	Lesen der Display Message in der transparenten Datei EF.DM der QES-Anwendung ([HPC-P2], 8.1.4) bzw. in der transparenten Datei Datei EF.DM der ESIGN-Anwendung ([HPC-P2], 9.1.3) zum Informieren des Heilberuflers, dass für die geöffnete Anwendung ein Trusted Channel erfolgreich aufgebaut wurde.
Vorbedingungen	Die QES-Anwendung bzw. ESIGN-Anwendung ist in der Sicherheitsumgebung 2 (Security Environment 2, SE # 2) geöffnet und, falls notwendig, wurde ein weiterer logischer Kanal zur HPC geöffnet. Ein Trusted Channel zu einer SMC ist aufgebaut.
Nachbedingungen	Die QES-Anwendung bzw. ESIGN-Anwendung ist im SE # 2 geöffnet. Ein Trusted Channel zu einer SMC ist aufgebaut.
Standardablauf	1. Schritt: Durchführung des Kommandos READ BINARY mit SFID mit Secure Messaging
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Immer dann wenn ein Trusted Channel aufgebaut worden ist, d.h. auch nach einem Anwendungswechsel zwischen DF.ESIGN und DF.QES und dem erneuten Aufbau eines Trusted Channel für die Remote-Nutzung der geöffneten Anwendung.
Vorangegangene Use Cases	UC_Open_Channel und UC_HPC_Authenticate_SMC
Nachfolgende Use Cases	Im Kontext der QES-Anwendung: • UC_HPC_Verify_QES_PIN und UC_HPC_SIGN im Trusted Channel (mit Secure Messaging) Im Kontext der ESIGN-Anwendung: • UC_HPC_Verify_PIN und UC_HPC_AUT oder UC_HPC_DEC im Trusted Channel (mit Secure Messaging)
Anmerkungen	Das Kommando zum Lesen der Display Message ist nur im Modus Secure Messaging zugelassen. In [HPC-P2], 11.7, Table 101, ist das Kommando allerdings im Plaintext-Modus beschrieben.
Festlegungen	-

1. Schritt (von 1):
Tabelle 317 – Kommando: READ BINARY ([HPC-P2], 11.7, Table 101)

CLA	INS	P1	P2	Lc	Daten	Le
0X	B0	84	00	0D	97 01 08 (DO Le) 8E 08 XX XX XX XX XX XX XX XX (DO Prüfsumme)	00
In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert, in den Bits b4 = 1 und b3 = 1 wird Secure Messaging mit Integration des Kommando-Headers angezeigt. Zur Konstruktion des Secure Messaging-Kommandos mittels SMC siehe [HPC-P1], Annex D, Figure D.1. CLA = 0C SM im Basiskanal, CLA = 0D SM im Logischen Kanal 1, CLA = 0E SM im Logischen Kanal 2, CLA = 0F SM im Logischen Kanal 3.						

Tabelle 318 – Korrekte Antworten ([HPC-P2], 11.7, Table 102)

Daten (29 Bytes)	SW1 SW2	Ursache	Aktion
87 11 01 XX XX ... (adding Indicator mit Kryptogramm der Display Message) 8E 08 XX XX XX XX XX XX XX XX (DO Prüfsumme)	90 00	Lesen der QES-Display Message erfolgreich	Use Case beenden
Zur Verarbeitung der Secure Messaging-Antwort mittels SMC siehe [HPC-P1], Annex D, Figure D.2.			

Tabelle 319 – Abweichende Antworten ([HPC-P1], Table A.4)

Daten	SW1 SW2	Beschreibung	Ursache	Aktion
99 02 62 82 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	62 82	EOF vor Le erreicht	Diese Return-Werte sind ein Indiz für ein Programmier-fehler oder eine defekte Karte.	Fehleraus-gang »HPC defekt«
99 02 69 81 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	69 81	Datei nicht transparent		
99 02 69 86 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	69 86	Kommando ohne SFID; keine Datei selektiert		
99 02 6A 82 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	6A 82	Datei mit SFID nicht gefunden		
99 02 6B 00 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	6B 00	Offset größer oder gleich Dateigröße		
99 02 68 81 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	68 81	Im CLA-Byte angezeigter logischer Kanal nicht un-terstützt bzw. nicht ge-öffnet.		
-	69 87	Erwartetes SM DO fehlt		
-	69 88	SM DO inkorrekt		

18.8 Aktualisieren der Display Message

Tabelle 320 – Aktualisieren der Display Message

Identifier	**UC_HPC_Update_DM**
Name	Aktualisieren der Display Message
Beschreibung	Aktualisieren der Display Message in der transparenten Datei EF.DM der QES-Anwendung ([HPC-P2], 8.1.4) bzw. in der transparenten Datei EF.DM der ESIGN-Anwendung ([HPC-P2], 9.1.3).
Vorbedingungen	Die Karteninhaber-PIN ist erfolgreich präsentiert und DF.QES bzw. DF.ESIGN geöffnet.
Nachbedingungen	Die Karteninhaber-PIN wurde erfolgreich präsentiert, die QES-Anwendung bzw. die ESIGN-Anwendung ist geöffnet und die entsprechende Display Message aktualisiert.
Standardablauf	1. Schritt: Durchführung des Kommandos UPDATE BINARY mit SFID und neuer vom Heilberufler eingegebener Display Message
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Auf Wunsch des Heilberuflers.
Vorangegangene Use Cases	UC_Verify_PIN und UC_HPC_Open_QES bzw. UC_HPC_Open_ESIGN
Nachfolgende Use Cases	Je nach Anwendungskontext, z.B. UC_HPC_Open_Remote_Application
Anmerkungen	Der Schritt des Use Case ist im Basiskanal ohne Trusted Channel dargestellt, da im Gegensatz zum Lesen der Display Message kein Trusted Channel erforderlich ist (siehe Vorbedingungen). Der Befehl kann aber auch im Trusted Channel und einem logischen Kanal ungleich dem Basiskanal durchgeführt werden.
Festlegungen	-

1. Schritt (von 1):
Tabelle 321 – Kommando: UPDATE BINARY ([HPC-P2], 11.7, Table 103)

CLA	**INS**	**P1**	**P2**	**Lc**	**Daten (8 Bytes)**	**Le**
00	D6	84	00	08	XX XX XX XX XX XX XX XX (Vom Heilberufler eingegebene neue Display Message)	-

Tabelle 322 – Korrekte Antworten ([HPC-P2], 11.7, Table 102)

Daten	**SW1 SW2**	**Ursache**	**Aktion**
-	90 00	Aktualisieren der Display Message erfolgreich	Use Case beenden

Tabelle 323 – Abweichende Antworten ([HPC-P1], Table A.5)

SW1 SW2	**Beschreibung**	**Ursache**	**Aktion**
62 81	Datei nicht transparent EOF erreicht, bevor Le ungleich 0 gelesen	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
69 86	Kommando-Option ohne SFID, keine Datei selektiert		
69 82	Mit SFID referenzierte Datei nicht gefunden		
6A 87	Offset + Lc größer Dateigröße		
6B 00	Offset größer oder gleich Dateigröße		

18.9 Erzeugen einer qualifizierten elektronischen Signatur in der stationären HPC

Tabelle 324 – Erzeugen einer qualifizierten elektronischen Signatur in der stationären HPC

Identifier	UC_HPC_SIGN_With_Stationary_HPC
Name	Erzeugen einer qualifizierten elektronischen Signatur in der stationären HPC
Beschreibung	Nutzen der QES-Anwendung der HPC an einem Arbeitsplatz mit SMC mittels Trusted Channel, d.h. mit Kommandos und Antworten im SM-Mode in einem logischen Kanal.
Vorbedingungen	Der in den Befehlen anzuzeigende logische Kanal ist geöffnet. Die gewünschte Anwendung der HPC ist im SE # 2 geöffnet und eine HPC / SMC-Authentisierung mit SM-Schlüsselvereinbarung hat erfolgreich stattgefunden.
Nachbedingungen	Der in den Befehlen anzuzeigende logische Kanal ist geöffnet. Die gewünschte Anwendung der HPC ist im SE # 2 geöffnet und eine HPC / SMC-Authentisierung mit SM-Schlüsselvereinbarung hat erfolgreich stattgefunden.
Standardablauf	Beispiel: Erstellen einer qualifizierten elektronischen Signatur (hashen außerhalb des HPC) in der stationären HPC von einem der verteilten Arbeitsplätze aus. 1. Schritt: Durchführung des Kommandos VERIFY zum Prüfen der QES-PIN mit Secure Messaging 2. Schritt: Durchführung des Kommando MANAGE SECURITY ENVIRONMENT (MSE) mit Option SET zur Selektion des privaten Signatursschlüssels und des Algorithmus mit Secure Messaging 3. Schritt: Durchführung des Kommando PSO:COMPUTE DS mit DigestInfo ohne Padding im Datenfeld mit Secure Messaging
Ablauf im Fehlerfall	Siehe »Abweichende Antworten«.
Häufigkeit	Bei jeder SMC-Anwendungssession zur Nutzung einer Anwendung der stationären HPC (z.B. QES-Anwendung) in einem bestimmten logischen Kanal.
Vorangegangene Use Cases	UC_HPC_Open_Remote_Application, UC_HPC_Verify_SMC_CVCs, UC_HPC_Authenticate_SMC
Nachfolgende Use Cases	Je nach Anwendungskontext
Anmerkungen	Jeder logische Kanal hat seinen eigenen Sicherheitsstatus, d.h. eine erfolgreiche HPC / SMC-Authentisierung mit SM-Schlüsselvereinbarung gilt nur in dem logischen Kanal, in dem sie durchgeführt wurde (siehe ISO 7816-4, 5.1.1.2).
Festlegungen	-

1. Schritt (von 3):
Tabelle 325 – Kommando: VERIFY ([HPC-P2], 8.5.1, Table 52)

CLA	INS	P1	P2	Lc	Daten (29 Bytes)	Le
0X	20	00	81	1D	87 11 01 XX XX ... (DO Padding Indicator mit 16 Byte-Kryptogramm der eingegebenen QES-PIN im Format 2 PIN Block) 8E 08 XX XX XX XX XX XX XX XX (DO Prüfsumme)	-
In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert, in den Bits b4 = 1 und b3 = 1 wird Secure Messaging mit Integration des Kommando-Headers angezeigt. Zur Konstruktion des Secure Messaging-Kommandos mittels SMC siehe [HPC-P1], Annex D, Figure D.1. CLA = 0C SM im Basiskanal, CLA = 0D SM im Logischen Kanal 1, CLA = 0E SM im Logischen Kanal 2, CLA = 0F SM im Logischen Kanal 3.						

Tabelle 326 – Korrekte Antworten ([HPC-P2], 8.5.1, Table 53 und [HPC-P1], Table A.14)

Daten	SW1 SW2	Ursache	Aktion
99 02 90 00 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	90 00	QES-PIN-Verifikation erfolgreich	2. Schritt
99 02 63 83 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	63 83	QES-PIN-Verifikationsmethode blockiert	UC_HPC_Reset_RC_QES_PIN in SM-Modus
99 02 63 CX (DO SW1 SW2) 8E 08 XX ...(DO Prüfsumme)	63 CX (X > 0)	QES-PIN-Verifikation nicht erfolgreich, d.h. QES-PIN falsch eingegeben, X weitere Versuche möglich	UC_HPC_Verify_QES_PIN im SM-Modus
99 02 63 C0 (DO SW1 SW2) 8E 08 XX ...(DO Prüfsumme)	63 C0	QES-PIN-Verifikation nicht erfolgreich erfolgreich, keine weitere Versuche mehr möglich	UC_HPC_Reset_RC_QES_PIN im SM-Modus
Zur Verarbeitung der Secure Messaging-Antwort mittels SMC siehe [HPC-P1], Annex D, Figure D.2.			

Tabelle 327 – Abweichende Antworten ([HPC-P1], Table A.14)

Daten	SW1 SW2	Fehlerbedingung	Ursache	Aktion
99 02 6A 80 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	6A 80	Formatfehler in Format 2 PIN Block	Diese Return-Werte sind ein Indiz für ein Programmierfehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
99 02 6A 88 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	6A 88	Referenzdaten nicht gefunden		
99 02 68 81 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		
-	69 87	Erwartetes SM DO fehlt		
-	69 88	SM DO inkorrekt		

2. Schritt (von 3):
Tabelle 328 – Kommando: MSE Option SET ([HPC-P2], 8.6.2, Table 66)

CLA	INS	P1	P2	Lc	Daten (21 Bytes)	Le
0X	22	41	B6	15	87 09 01 XX XX XX ... (DO Padding Indicator mit Kryptogramm der Referenz des privaten Signaturschlüssels PrK.HP.QES, siehe [HPC-P2], 8.1.2, Table 48, und der Referenz des Algorithmus: entweder '12' oder '42', siehe [HPC-P2], Table E.1) 8E 08 XX XX XX XX XX XX XX XX (DO Prüfsumme)	-
In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert, in den Bits b4 = 1 und b3 = 1 wird Secure Messaging mit Integration des Kommando-Headers angezeigt. Zur Konstruktion des Secure Messaging-Kommandos mittels SMC siehe [HPC-P1], Annex D, Figure D.1. CLA = 0C SM im Basiskanal, CLA = 0D SM im Logischen Kanal 1, CLA = 0E SM im Logischen Kanal 2, CLA = 0F SM im Logischen Kanal 3.						

Tabelle 329 – Korrekte Antworten ([HPC-P2], 8.6.2, Table 67)

Daten	SW1 SW2	Ursache	Aktion
99 02 90 00 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	90 00	Schlüsselreferenz und Algorithmusreferenz erfolgreich registriert.	3. Schritt
Zur Verarbeitung der Secure Messaging-Antwort mittels SMC siehe [HPC-P1], Annex D, Figure D.2.			

Tabelle 330 – Abweichende Antworten ([HPC-P1], Table A.17)

Daten	SW1 SW2	Fehlerbedingung	Ursache	Aktion
99 02 6A 88 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	6A 88	Referenzierte Daten nicht gefunden	Diese Return-Werte sind ein Indiz für ein Programmier-fehler oder eine defekte Karte.	Fehlerausgang »HPC defekt«
99 02 68 81 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		
-	69 87	Erwartetes SM DO fehlt		
-	69 88	SM DO inkorrekt		

3. Schritt (von 3):
Tabelle 331 – Kommando: PSO: COMPUTE DS ([HPC-P2], 8.6.2, Table 66)

CLA	INS	P1	P2	Lc	Daten	Le
0X	2A	9E	9A	xx	81 xx XX XX ... (DO Plaintext mit DigestInfo, [HPC-P2], Table E.1.2) 97 01 00 (DO Le) 8E 08 XX XX XX XX XX XX XX XX (DO Prüfsumme)	00
In den Bits b2-b1 des CLA-Byte ist die Kanal-Nr. codiert, in den Bits b4 = 1 und b3 = 1 wird Secure Messaging mit Integration des Kommando-Headers angezeigt. Zur Konstruktion des Secure Messaging-Kommandos mittels SMC siehe [HPC-P1], Annex D, Figure D.1. CLA = 0C SM im Basiskanal, CLA = 0D SM im Logischen Kanal 1, CLA = 0E SM im Logischen Kanal 2, CLA = 0F SM im Logischen Kanal 3.						

Tabelle 332 – Korrekte Antwort ([HPC-P2], 8.6.2, Table 67)

Daten	SW1 SW2	Ursache	Aktion
81 80 XX XX ... (DO Plaintext mit Signatur) 8E 08 XX ... (DO Prüfsumme)	90 00	Signatur erfolgreich berechnet	Use Case beenden

Tabelle 333 – Abweichende Antworten ([HPC-P1], Table A.17)

Daten	SW1 SW2	Bedeutung	Ursache	Aktion
99 02 6A 88 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	6A 88	Referenzierte Daten nicht gefunden	Dieser Return-Wert ist ein Indiz für ein Programmier-fehler oder eine defekte Karte.	Fehleraus-gang »HPC defekt«
99 02 68 81 (DO SW1 SW2) 8E 08 XX ... (DO Prüfsumme)	68 81	Im CLA-Byte angezeigter logischer Kanal nicht unterstützt bzw. nicht geöffnet.		
-	69 87	Erwartetes SM DO fehlt		
-	69 88	SM DO inkorrekt		

Literatur

[ALGCAT] Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, Algorithmenkatalog 2005 vom 02.01.2005, 30. März 2005, Bundesanzeiger Nr. 59, S. 4695-4696 , siehe www.bundesnetzagentur.de

[eGK-P1] Die Spezifikation der elektronischen Gesundheitskarte
Teil 1 – Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform;
V1.1.0, 07.02.2006

[eGK-P2] Die Spezifikation der elektronischen Gesundheitskarte
Teil 2 – Anwendungen und anwendungsspezifische Strukturen
V1.1.1, 23.03.2006

[HPC-P1] German Health Professional Card and Security Module Card
Part 1: Commands, Algorithms and Functions of the COS Platform
V2.1.0 21.02.2006

[HPC-P2] German Health Professional Card and Security Module Card
Part 2: HPC Applications and Functions
V2.1.0 21.02.2006

[HPC-P3] German Health Professional Card and Security Module Card
Part 3: SMC Applications and Functions
V2.1.0 21.02.2006

[ISO7816-3] ISO/IEC 7816-3: FCD2 2005 (2nd edition)
Identification cards - Integrated circuit cards with contacts -
Part 3: Electrical interface and transmission protocols

[ISO7816-4] ISO/IEC 7816-4: 2005 (2nd edition)
Identification cards - Integrated circuit cards -
Part 4: Organization, security and commands for interchange

[ISO7816-15] ISO/IEC 7816-15: 2004
Identification cards - Integrated circuit cards -
Part 15: Cryptographic information application

Anhang A

A.1 Abkürzungsverzeichnis

AC = Attribute Certificate
AID = Application Identifier
AM = Access Mode
AOD = Authentication Object Directory
ARR = Access Rule Reference
ASN.1 = Abstract Syntax Notation One
AT = Authentication Template
ATR = Answer-to-Reset
AUT = Authentication
AVS = Apothekenverwaltungssystem
BÄK = Bundesärztekammer
BCD = Binary Coded Decimal
BER = Basic Encoding Rules
BNA = BundesNetzAgentur
BS = Buffer Size
C = Certificate (X.509-Zertifikat)
CA = Certification Authority
CAMS = Card Application Management System
CAR = Certification Authority Reference
CBC = Cipher Block Chaining
CC = Cryptographic Checksum
CD = Certificate Directory
CE = Certificate Extensions
CG = Cryptogram
CH = Cardholder
CHA = Certificate Holder Authorization
CHR = Certificate Holder Reference
CIA = Cryptographic Inform. Application
CIO = Cryptographic Inform. Objects
CLA = Class byte of a command
COS = Card Operating System
CPI = Certificate Profile Identifier
CRT = Control Reference Template
CS = CertSign (Schlüsselverwendungszweck)
CT = Confidentiality Template
C2C = Card-to-Card
CV = Card Verifiable
CVC = Card Verifiable Certificate
CWA = CEN Working Agreement
D, DIR = Directory
DE = Data Element
DER = Distinguished Encoding Rules
DES = Data Encryption Standard
DF = Dedicated File
DO = Data Object
DI = Baud rate adjustment factor
DSI = Digital Signature Input
DST = Digital Signature Template
E = Evaluation
EAL = Evaluation Assurance Level
EF = Elementary File
eGK = elektronische GesundheitsKarte
EHIC = European Health Insurance Card
ENC = Encipherment
EOF = End-of-File
FCI = File Control Information
FI = Clock rate conversion factor
FID = File Identifier
FM = File Management
GDO = Global Data Objects

HB = Historical Bytes
HBK = Heilberufler-Kennung
HF2 = Hash Function ISO 10118-2
HI = Health Institution
HP = Health Professional
HPA = Health Professional Application
HPC = Health Professional Card
ICC = Integrated Circuit Card
ICCSN = ICC Serial Number
ICM = Integrated Circuit Manufacturer
ID = Identifier
IFD = Interface Device
IFSC = Information Field Size Card
IFSD = Information Field Size Device
IIN = Issuer Identification Number
IK = Individual Key
I/O = Input/Output
INS = Instruction byte of a command
IV = Initial Value
KD = Key Derivation data
KE = Key Encipherment
KEI = Key Encipherment Input
KID = Key Identifier
KIS = Krankenhaus-Informations-System
KN = KeyName
KT = Kartenterminal
Lc = Length field for coding the length of command data field
LC = Logical Channel
Le = Length field for coding the length of expected response data field
LSB = Least Significant Byte(s)
MF = Master File
MII = Major Industry Identifier
MSE = MANAGE SECURITY ENVIRONMENT
OID = Object Identifier
P = Patient
P1 = Parameter 1 byte of a command
P2 = Parameter 2 byte of a command
PHAR = Pharmacist
PHYS = Physician
PK,PuK = Public Key
PI = Padding Indicator
PIN = Personal Identification Number
PIX = Proprietary Appl. Prov. Extension
PP = Protection Profile
PPS = Protocol Parameter Selection
PrK = Private Key
PRND = Padding Random Number
PSO = PERFORM SECURITY OPERATION
PUK = Personal Unblocking Key (= Resetting Code)
PVS = Praxis-Verwaltungssystem
QES = Qualified Electronic Signature
R = Role ID
RC = Retry Counter
RCA = Root CA
RD = Reference Data
RFC = Request for Comment
RID = Registered Application Provider ID
RND = Random Number
ROM = Read Only Memory
RSA = Algorithm of Rivest, Shamir, Adleman
S = Server
SC = Security Condition
SFID = Short EF Identifier
SIG = Signature
SigG = Signaturgesetz
SigV = Signaturverordnung
SK = Secret Key

SM = Secure Messaging
SMA = Security Module Application
SMC = Security Module Card
SMK = SM Key
SSC = Send Sequence Counter
SSCD = Secure Signature Creation Device
SSEC = Security Status Evaluation Counter
SSL = Security Sockets Layer
SN = Serial Number
TC = Trusted Channel
TLS = Transport Layer Security
UC = Use Case
UID = User Identification
UQ = Usage Qualifier
VD = Verification Data
ZGW = Zertifizierungsstelle Gesundheitswesen

A.2 Stacks im Primärsystem

Abb. A.1 zeigt den HPC Stack und den CVC Stack. Im HPC Stack werden unter der HPC-spezifischen ICCSN alle Daten abgelegt, die nur einmal ermittelt, aber immer wieder gebraucht werden. Im CVC-Stack werden die Cross CV-Zertifikate abgelegt. Dieser Stack ist zunächst leer, füllt sich aber in der Zeitachse. Die max. Anzahl der Cross-CV-Zertifikatspaare hängt von der HPC-Laufzeit ab. Beträgt diese 3 Jahre, dann werden insgesamt 6 Cross-CVCs benötigt.

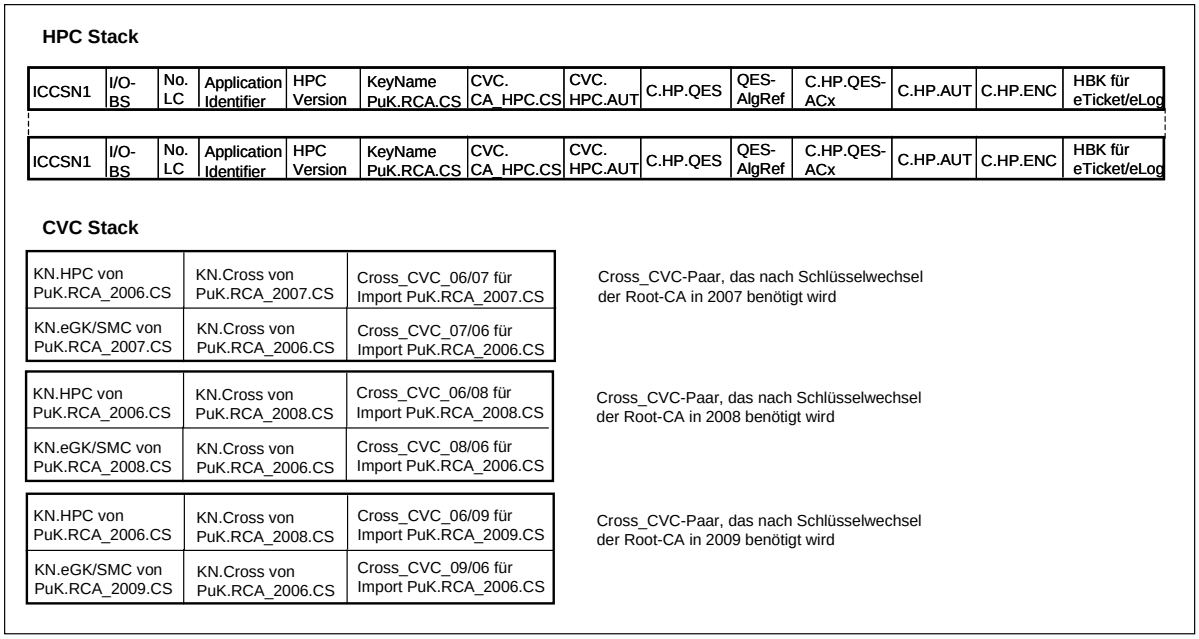

Abbildung 2 – PVS / KIS Stacks

A.3 Initialisierungsphase der HPC-Session (informativ)

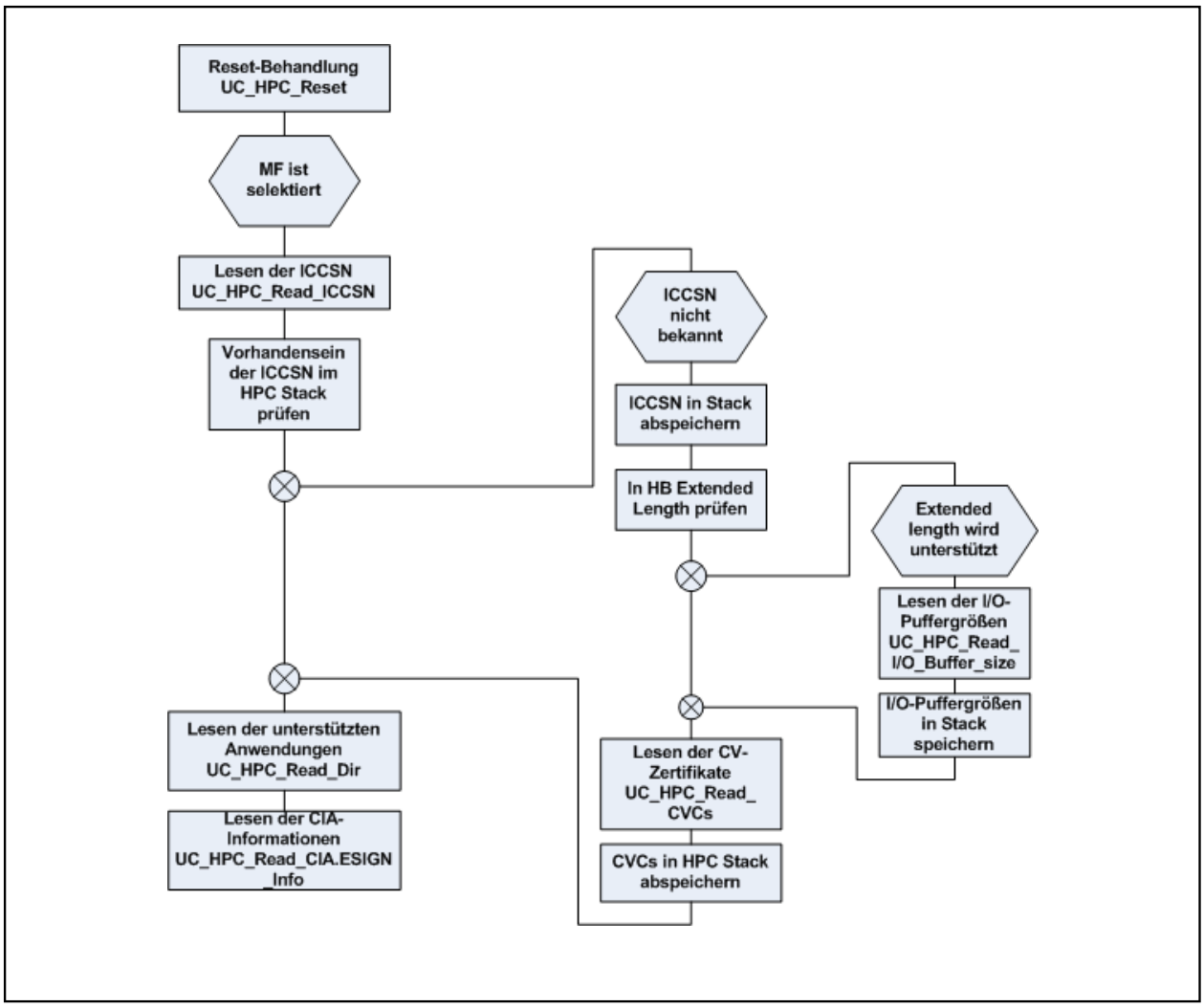

Abbildung 3 – Initialisierungsphase der HPC-Session

Es wird empfohlen, alle karten-spezifischen Daten, die nur einmal ausgelesen werden müssen, unter der ICCSN persistent zu speichern. In der Sessionaufbauphase sind dies folgende:

- I/O Puffergröße
- Anzahl LC
- CVC.CA_HPC.CS
- CVC.HPC.AUT

Das Lesen von EF.DIR und der CIA-Datenfiles ist anwendungsabhängig.

A.4 Asymetrisches Authentisierungsverfahren ohne SM-Schlüsselvereinbarung

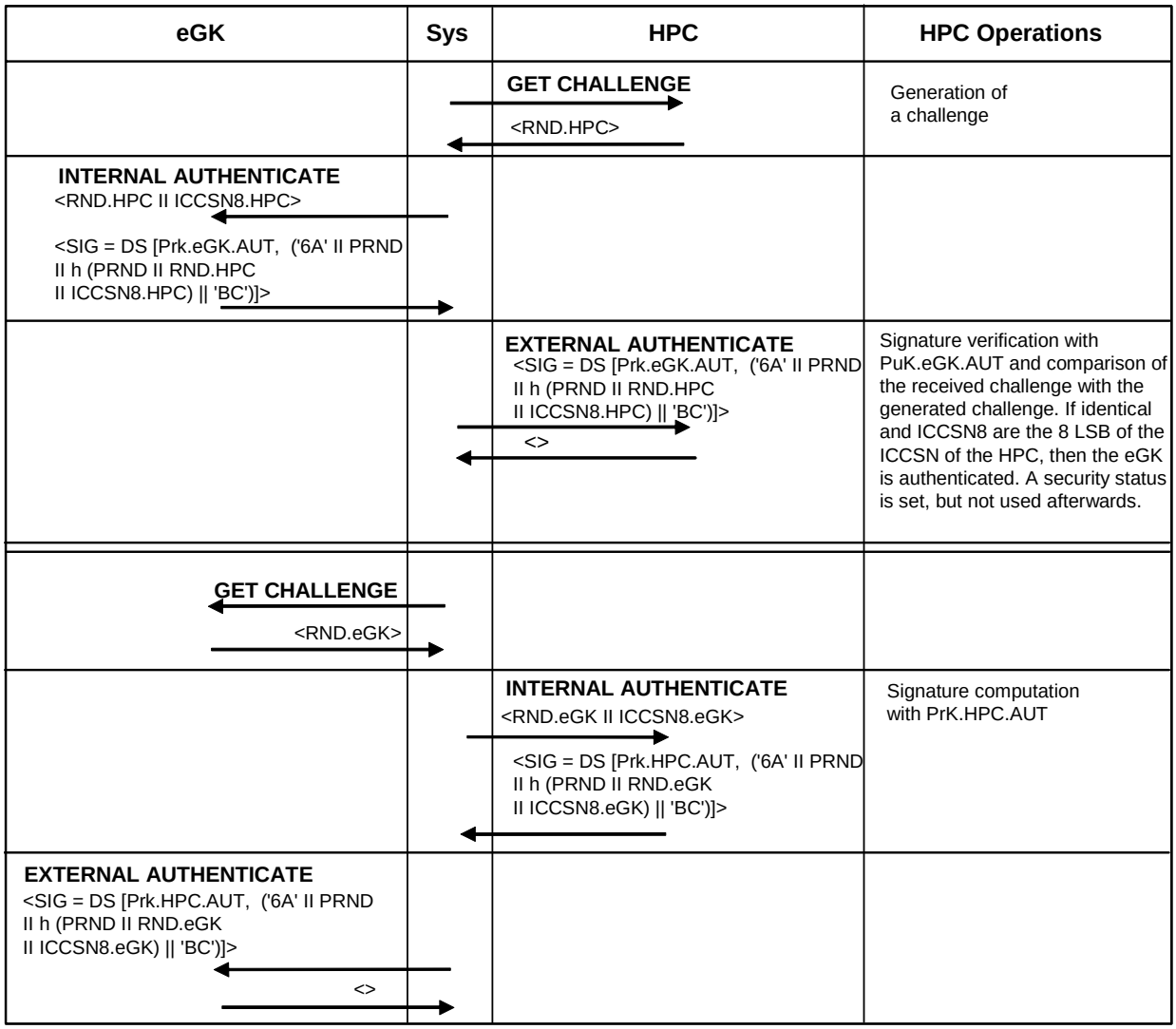

Abbildung 4 – Asymetrisches Authentisierungsverfahren ohne SM-Schlüsselvereinbarung

A.5 Asymetrisches Authentisierungsverfahren mit SM-Schlüsselvereinbarung

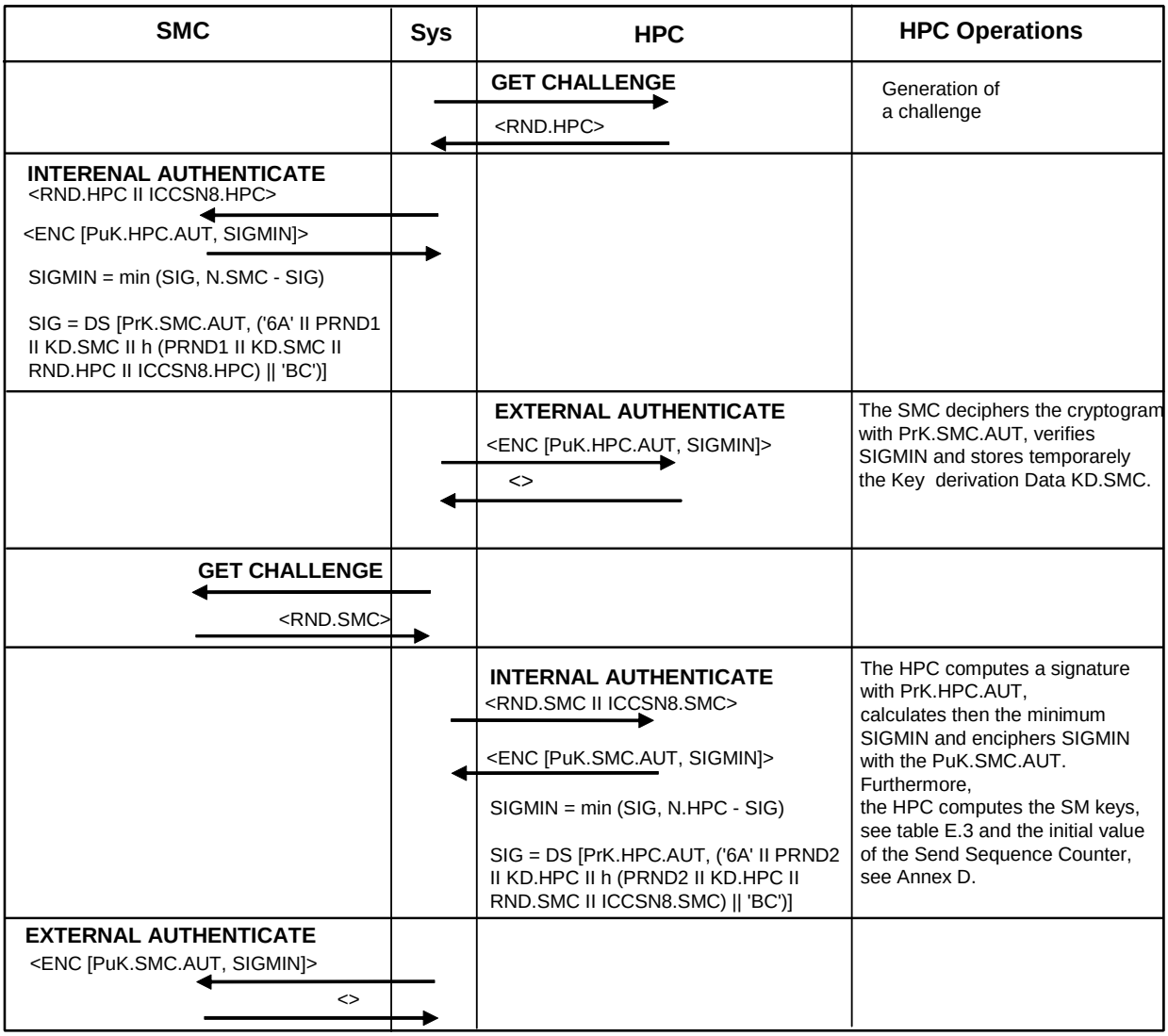

Abbildung 5 – Asymetrisches Authentisierungsverfahren mit SM-Schlüsselvereinbarung

A.6 Generierung von SM-Kommandos und Verarbeitung von SM-Antworten

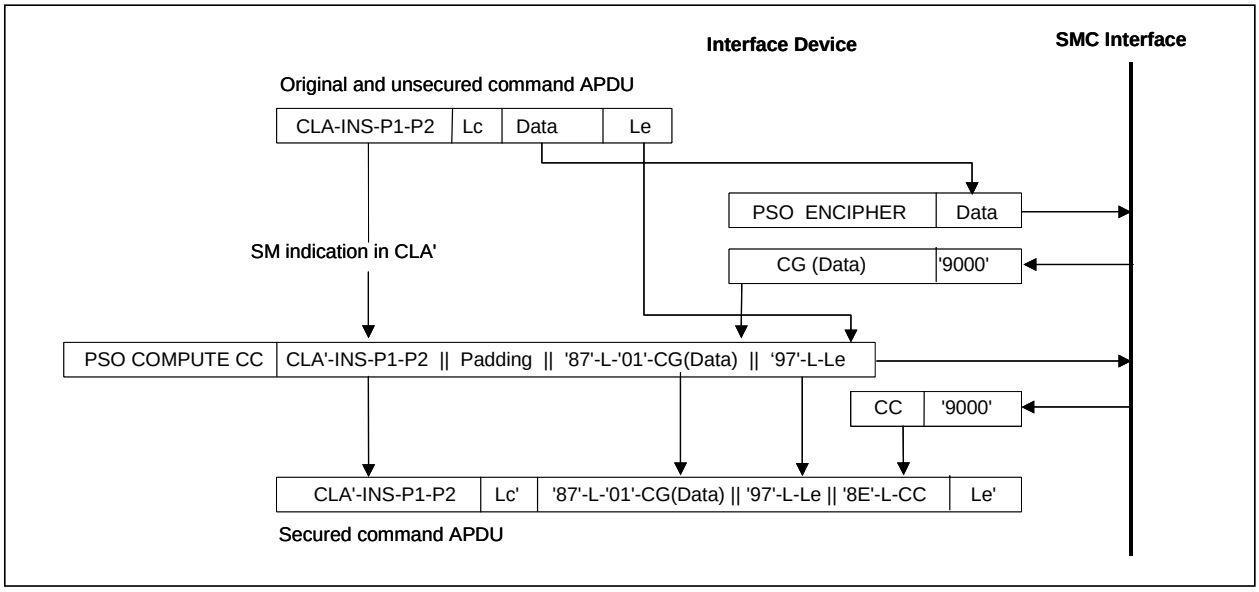

Abbildung 6 – Beispiel der Generierung eines SM-Kommandos

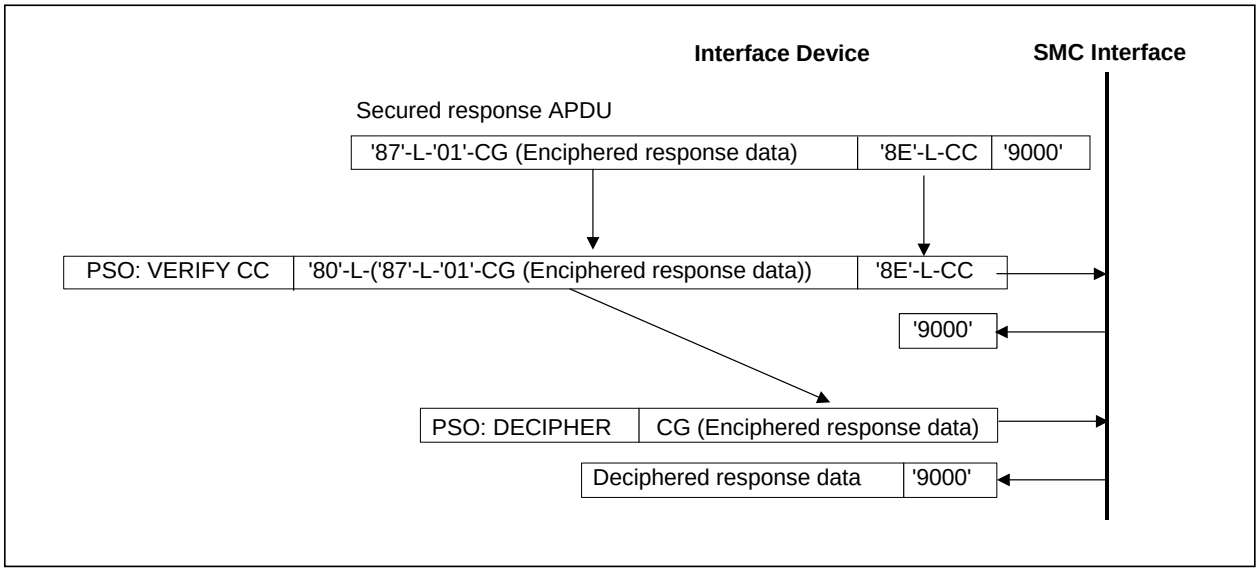

Abbildung 7 – Beispiel der Verarbeitung einer SM-Antwort

A.7 Beispielscript für das Anwendungszenario „Qualifizierte elektronische Signatur erzeugen"

Das Folgende Beispielscript fasst die einzelnen UseCases zusammen, die für das Anwendungszenario „Qualifizierte elektronische Signatur erzeugen" durchzuführen sind. Das Auslesen der Attributszertifikate und des Signaturzertifikats wird hier nicht weiter betrachtet.

:SELECT QES
CLA: 00 INS: A4 P1: 04 P2: 0C LC: 06
Data: d2 76 00 00 66 01

:VERIFY PIN.QES
CLA: 00 INS: 20 P1: 00 P2: 81 LC: 08
Data: 26 12 34 56 ff ff ff ff

:MSE SET
CLA: 00 INS: 22 P!: 41 P": b6 LC: 06
Data: 84 01 84 80 01 12

:COMPUTE DS
CLA: 00 INS: 2a P1: 9e P2: 9a LC: 23 LE: 00
Data: 30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 54
85 41 36 19 43 69 64 29 46 92 46 29 78 64 89 45 18 38 38

Der Dateninput (DigestInfo) für das Kommando COMPUTE DS ist wie folgt zu interpretieren (Hexdezimal DER-encoding):

```
30 21                                   // Tag und Länge einer ASN.1-Sequenz
    30 09                               // Tag und Länge einer ASN.1-Sequenz
        06 05                           // Tag und Länge eines ASN.1 kodierten Object Identifier
            2b 0e 03 02 1a              // OID
        05 00                           // Tag und Länge einer ASN.1-Null (d.h. keine Parameter)
        04 14                           // Tag und Länge eines ASN.1-Oktett-Strings
            54 85 41 36 19 43 69 64 29 46 92 46 29 78 64 89 45 18 38 38  // 20 Byte fiktiver Hash-
                                                                            Wert
```