eCH-0064 - Spezifikationen für das System Versichertenkarte

Name	Spezifikationen für das System Versichertenkarte
Standard-Nummer	eCH-0064
Kategorie	Standard
Reifegrad	Definiert
Version	1.0
Status	Genehmigt
Genehmigt am	2008-02-04
Ausgabedatum	2008-02-04
Ersetzt Standard	
Sprachen	Deutsch, Französisch
Antragsteller	Bundesamt für Gesundheit BAG
Autoren	Fachgruppe Versichertenkarte eCH Adrian Schmid, BAG, adrian.schmid@bag.admin.ch Jürg Burri, BAG, juerg.burri@bag.admin.ch Willy Müller, ISB, willy.mueller@isb.admin.ch Peter Stadlin, Arpage AG, stadlin@arpage.ch Martin Stingelin, Stingelin Informatik GmbH, info@stingelin-informatik.com
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, 8008 Zürich Tel: 044 / 388 74 64 Fax: 044 / 388 71 80 www.ech.ch/ info@ech.ch

Zusammenfassung

Das Dokument gilt als technischer Standard für die Versichertenkarte gemäss Art. 42a KVG und der Verordnung über die Versichertenkarte. Der Standard enthält technische Grundanforderungen an das Versichertenkartensystem unter Berücksichtigung international gültiger Normen.

Inhaltsverzeichnis

1 Status des Dokuments

Das vorliegende Dokument enthält den endgültigen Text, der vom Expertenausschuss am 4. Februar 2008 genehmigt wurde.

2 Einleitung

2.1 Überblick

Am 8. Oktober 2004 hat das Parlament die rechtliche Grundlage für die Einführung einer Versichertenkarte geschaffen. Der entsprechende **Artikel 42a im Krankenversicherungsgesetz KVG** ist seit dem 1. Januar 2005 in Kraft und lautet:

[1] Der Bundesrat kann bestimmen, dass jede versicherte Person für die Dauer ihrer Unterstellung unter die obligatorische Krankenpflegeversicherung eine Versichertenkarte erhält. Diese enthält den Namen der versicherten Person und eine vom Bund vergebene Sozialversicherungsnummer.

[2] Diese Karte mit Benutzerschnittstelle wird für die Rechnungsstellung der Leistungen nach diesem Gesetz verwendet.

[3] Der Bundesrat regelt nach Anhörung der interessierten Kreise die Einführung der Karte durch die Versicherer und die anzuwendenden technischen Standards.

[4] Die Karte enthält im Einverständnis mit der versicherten Person persönliche Daten, die von dazu befugten Personen abrufbar sind. Der Bundesrat legt nach Anhören der interessierten Kreise den Umfang der Daten fest, die auf der Karte gespeichert werden dürfen. Er regelt den Zugriff auf die Daten und deren Bearbeitung.

Die Ausführungsbestimmungen zum Gesetz sind in der Verordnung über die Versichertenkarte [VVK] festgelegt. Sie bestimmt u. a. in Artikel 17, dass die internationale Normung berücksichtigt werden muss und die technischen Standards nach Abs. 3 des Gesetzes in einer Departementsverordnung des EDI [VOEDI] festgehalten werden. Diese verlangt insbesondere, dass der vorliegende Standard bei der Umsetzung des Versichertenkartensystems angewendet werden muss.

Der vorliegende Standard definiert ein Minimalset an technologischen Vorgaben, um möglichst vielen Anbietern am Markt eine Umsetzung der Vorgaben zu ermöglichen.

2.2 Anwendungsgebiet

Der Standard enthält technische Anforderungen an die Karte nach Art. 2 der Verordnung [VVK], die Umsetzung der Sicherheitsanforderungen nach Art. 7 für die Daten auf der Karte sowie die Umsetzung der Sicherheitsbestimmungen für den Online-Informationsservice der Versicherungen nach Art. 15 [VVK].
Der vorliegende Standard ist kein Implementationsstandard, sondern ein Konzeptions-, Struktur- und Verfahrensstandard. Weitere Detailspezifikationen für das Versichertenkartensystem sind daher erforderlich. Der Standard ist in erster Linie für technische Spezialisten gedacht, welche mit der technischen Umsetzung der Kartenservices respektive der Online-Abfrage betraut sind.

2.3 Datenschutz und Datensicherheit

Beim Einsatz der Versichertenkarte werden Personendaten bearbeitet, wobei die medizinischen Informationen besonders schützenswerte Daten im Sinne des Datenschutzgesetzes DSG sind. Alle Stellen, welche die Daten bearbeiten, müssen die Grundsätze des DSG einhalten (Rechtmässigkeit, Verhältnismässigkeit, Transparenz, Zweckbindung). Im System „Versichertenkarte“ muss das Grundrecht jeder Person auf Selbstbestimmung im Informationsbereich gewahrt bleiben. Zudem sind die Daten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen. Bei richtiger Umsetzung der gesetzlichen Vorgaben ([VVK], [VOEDI], [DSG], [VDSG], werden Datenschutz und Datensicherheit gewährleistet durch

- Informationspflichten, welche Auskunfts- und Berichtigungsrechte der Versicherten ermöglichen und die Unterscheidung in obligatorische und freiwillige Kartenfunktionen klarstellen
- Sichere Identifikation der Zugriffsberechtigten
- Selektiver Datenzugang durch abgestufte Zugriffs- und Bearbeitungsrechte und Einwilligung des Versicherten bei freiwilligen Funktionen
- Ausreichend sichere Datenübermittlung der Online-Abfrage

Der vorliegende Standard regelt technische Massnahmen. Organisatorische Massnahmen liegen in der Verantwortung der Datenbearbeiter:

Datenschutz und Datensicherheit	**Massnahmen für administrative Daten nach Artikel 3 + 4 VVK**		**Massnahmen für persönliche Daten nach Artikel 6 VVK (freiwillige Kartenfunktion)**	
	Im Standard	**Ausserhalb des Standards**	**Im Standard**	**Ausserhalb des Standards**
Selbstbestimmung des Versicherten	- Keine technische Massnahme (Einsatz der Versichertenkarte ist Pflicht für KVG-Versicherte, die eine Leistung über die Krankenversicherung abrechnen wollen)	- Einverständnis des Versicherten für die Online-Abfrage (Art. 15 Abs. 3 VVK) - Recht zur Information und Veranlassung der Datenbearbeitung nach Art. 9 VVK - Aufklärung über Rechte und Pflichten nach Art. 12 und 13 VVK	- Möglichkeit für Versicherte, einzelne Kategorien der medizinischen Daten mit PIN zu schützen (Kapitel 3.5)	- Einwilligung des Versicherten für Aufnahme und Bearbeitung der Daten (Art. 7 Abs. 3 VVK) - Recht zur Information und zur Veranlassung der Datenbearbeitung nach Art. 9 VVK - Aufklärung über Rechte und Pflichten nach Art. 12 und 13 VVK

Datenschutz und Datensicherheit	**Massnahmen für administrative Daten nach Artikel 3 + 4 VVK**		**Massnahmen für persönliche Daten nach Artikel 6 VVK (freiwillige Kartenfunktion)**	
Klare Definition der Zugriffsrechte	- Sichere Datenübertragung und Zugangskontrolle zum Online-Verfahren durch die Versicherer mindestens über ID und Passwort (Kapitel 4);	- Zugriffsrechte generell für Leistungserbringer für das Online-Verfahren nach Art. 15 VVK - Erteilung des Zugriffsrechts im Einzelfall durch den Versicherten	- Card-to-Card-Authentisierung zwischen VK und elektronischem Leistungserbringernachweis (Kapitel 3.6); - Dateistruktur mit geregeltem Zugriff auf Files mit medizinischem Inhalt (Kapitel 3.4.2);	- Definition der generellen Zugriffsrechte nach Art. 7 VVK - Zugriffsrecht im Einzelfall nur mit Einwilligung des Versicherten (durch Kartenübergabe, Freischaltung bei PIN) - Authentisierung des LE mit einem elektronischen Leistungserbringernachweis nach Art. 8 VVK
Sicherheit bei der Datenbearbeitung	- Definierte Zugriffsabläufe beim Online-Verfahren (Kapitel 4.3 bis 4.5). - Anforderungen an die Kommunikation beim Online-Verfahren (Kapitel 4.2);	- Datenschutzgesetz und Verordnung	- Lokale Bearbeitung der Daten	- Datenschutzgesetz und Verordnung

2.4 Abgrenzung

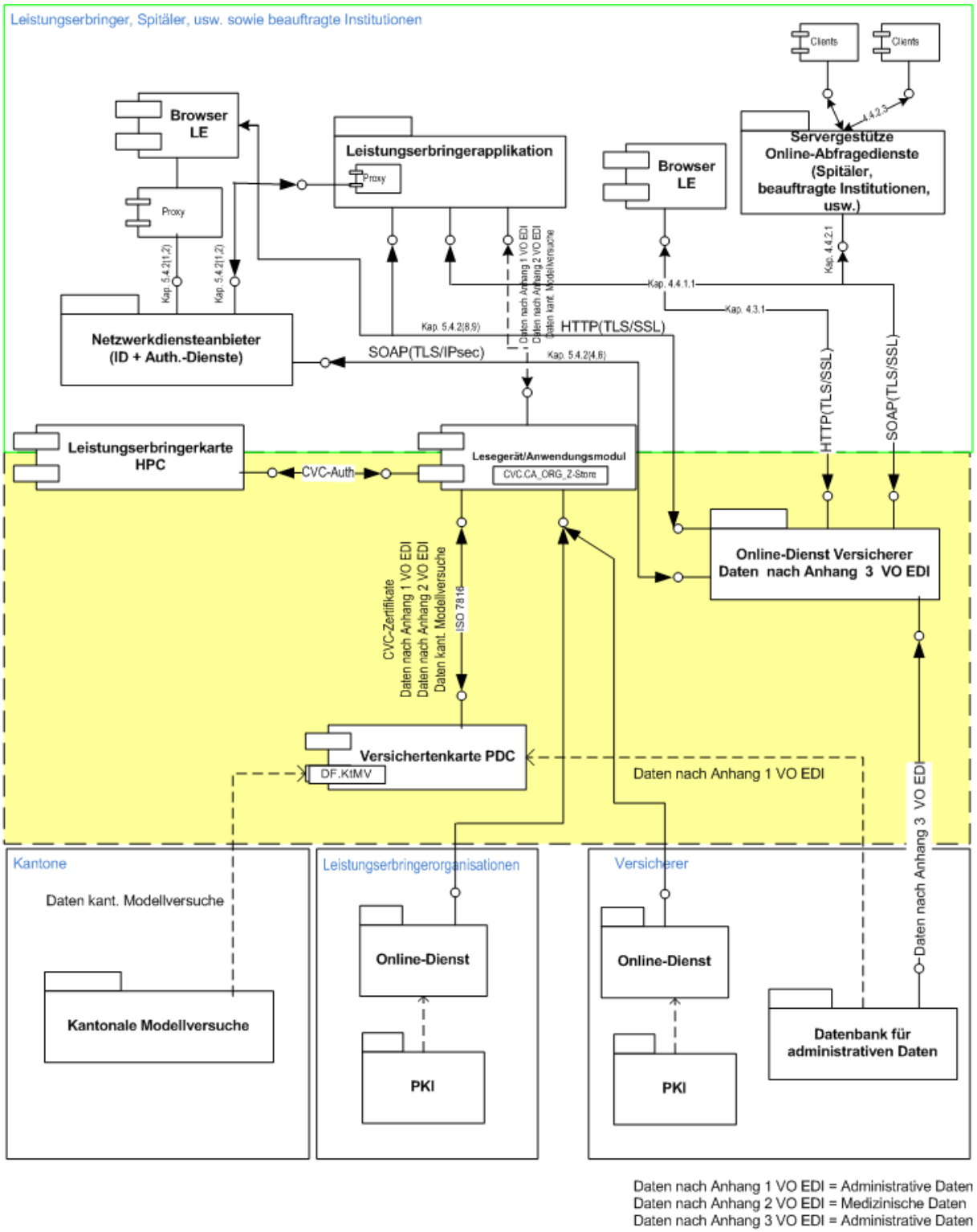
Sachverhalte, die bereits durch andere Standards beschrieben sind, werden im vorliegenden Standard nur durch eine entsprechende Referenz festgehalten. Im Falle von Abweichungen zu referenzierten Standards, sind diese im vorliegenden Standard explizit als solche gekennzeichnet.

Die nachfolgenden Sachverhalte sind nicht Bestandteil des vorliegenden Standards und separat zu regeln:

- Organisatorische Aspekte im Zusammenhang mit der Ausstellung respektive dem Einsatz der Versichertenkarte.
- Organisatorische Aspekte im Zusammenhang mit dem Online-Verfahren.

2.5 Komponentenschema

Das folgende Schema zeigt die Komponenten des Versichertenkartensystems und die wichtigsten Beziehungen zwischen ihnen. Der gelb markierte Bereich enthält die Komponenten, welche durch den vorliegenden Standard definiert werden. Für einzelne Komponenten wie die elektronische Leistungserbringerkarte HPC und das Kartenlesegerät enthält der Standard Teilspezifikationen, die für das Versichertenkartensystem erforderlich sind. Die ausserhalb des gelb markierten Bereichs liegenden Komponenten werden nur teilweise und spezifisch durch den Standard geregelt. Die Datensätze für die administrativen und medizinischen Daten sind in der [VOEDI] definiert.


Leistungserbringer, Spitäler, usw. sowie beauftragte Institutionen
Clients
Clients
Browser LE
Leistungserbringerapplikation
Proxy
Browser LE
Servergestützte Online-Abfragedienste (Spitäler, beauftragte Institutionen, usw.)
Proxy
Kap. 5.4.2(1,2)
Kap. 5.4.2(1,2)
Kap. 4.4.2.3
Kap. 4.4.2.1
Kap. 4.4.1.1
Kap. 4.3.1
Daten nach Anhang 1 VO EDI
Daten nach Anhang 2 VO EDI
Daten kant. Modellversuche
Netzwerkdiensteanbieter (ID + Auth.-Dienste)
Kap. 5.4.2(8,9)
HTTP(TLS/SSL)
SOAP(TLS/IPsec)
Kap. 5.4.2(4,6)
HTTP(TLS/SSL)
SOAP(TLS/SSL)
Leistungserbringerkarte HPC
CVC-Auth
Lesegerät/Anwendungsmodul
CVC.CA_ORG_Z-Store
Online-Dienst Versicherer Daten nach Anhang 3 VO EDI
CVC-Zertifikate
Daten nach Anhang 1 VO EDI
Daten nach Anhang 2 VO EDI
Daten kant. Modellversuche
ISO 7816
Versichertenkarte PDC
DF.KtMV
Daten nach Anhang 1 VO EDI
Daten nach Anhang 3 VO EDI
Kantone
Daten kant. Modellversuche
Kantonale Modellversuche
Leistungserbringerorganisationen
Online-Dienst
PKI
Versicherer
Online-Dienst
PKI
Datenbank für administrativen Daten
Daten nach Anhang 1 VO EDI = Administrative Daten
Daten nach Anhang 2 VO EDI = Medizinische Daten
Daten nach Anhang 3 VO EDI = Administrative Daten

2.6 Notation

Die Richtlinien in diesem Dokument werden gemäss der Terminologie aus [RFC2119] angegeben, dabei kommen die folgenden Ausdrücke zur Anwendung, die durch GROSSSCHREIBUNG als Wörter mit den folgenden Bedeutungen kenntlich gemacht werden:

ZWINGEND: Der Verantwortliche muss die Vorgabe umsetzen.

EMPFOHLEN: Der Verantwortliche kann aus wichtigen Gründen auf eine Umsetzung der Vorgabe verzichten.

OPTIONAL: Es ist dem Verantwortlichen überlassen, ob er die Vorgabe umsetzen will.

3 Spezifikationen für das System Versichertenkarte nach Artikel 2 und 6 [VVK]

3.1 Allgemeine Anforderungen

3.1.1 Technische Spezifikation

Begründung: Die Anforderungen berücksichtigen die internationale Normung nach Artikel 17 [VVK] und werden von möglichst vielen Kartenanbietern erfüllt.

ZWINGEND: Die technischen Spezifikationen der Versichertenkarte richten sich nach dem Standard ISO/IEC 7816. Die in diesem Kapitel verwendeten Fachausdrücke sind im erwähnten Standard definiert.

3.1.2 Physikalische Anforderungen

Begründung: Die Anforderungen werden von möglichst vielen Kartenanbietern erfüllt.

ZWINGEND: Die Versichertenkarte muss den Anforderungen folgender Normen genügen:

- ISO/IEC 7816-1 (Physical Characteristics of Integrated Circuit Cards)
- ISO/IEC 7816-2 (Dimensions and Locations of Contacts)

3.1.3 Kommunikations-Anforderungen

Begründung: Die folgenden Minimalanforderungen auf der Basis von ISO/IEC 7816 sind so bestimmt, dass sie von möglichst vielen Kartenanbietern erfüllt werden können.

ZWINGEND: Das Übertragungsverfahren zwischen der Versichertenkarte und dem Lesegerät ist gemäss ISO/IEC 7816-3 zu implementieren und muss folgende Funktionalitäten unterstützen:

- **ZWINGEND:**, Übertragungsprotokoll T = 1, wobei die Fähigkeit der Verkettung (Chaining) zwingend ist
- **ZWINGEND:** Wird ein Übertragungsblock zur Karte gesendet, muss das NAD-Byte den Wert '00' haben; d.h. keine Knotenadressierung
- **EMPFOHLEN:** S-Block ABORT [PCB] nicht verwenden, kann aber von der Karte optional zum Abbruch einer zu langen Kette bei Nicht-Beachtung der I/O- Puffergrössen eingesetzt werden
- **ZWINGEND:** Grösse der Informationsfelder: IFSC = 128 Byte (mindestens) , IFSD = 254 Byte
- **ZWINGEND:** Protokoll-Parameter-Auswahl (PPS) mit Unterstützung des aushandelbaren Modus, sonst Teiler (CRFC) auf die Werte 372 oder 512 fest eingestellt, so dass mindestens eine Übertragungsrate von 38 kbps oder höher gewährleistet werden kann.
- **ZWINGEND:** ATR-Kodierung in Übereinstimmung mit ISO/IEC 7816-3

3.1.4 Elektronischer Leistungserbringernachweis

Begründung: Der elektronische Leistungserbringernachweis muss als universelles Token mit international geregelten Funktionen, Kommandos und physikalischen Schnittstellen ausgestaltet sein, so dass eine optimale, einfache Einbindung in eine Vielfalt von Leistungserbringeranwendungen ermöglicht wird - insbesondere auch im Zusammenhang und Anwendung mit der Versichertenkarte.

ZWINGEND: Der elektronische Leistungserbringernachweis beruht als HPC-Chipkarte auf den Spezifikationen nach ISO/IEC 7816-1, 2, 3, 4, 5, 6, 8, 9 und muss im ID-1 Format nach ISO 7810 ausgegeben werden. Sie kann bei Bedarf aus dem ID-1 Format vom Leistungserbringer durch Ausbrechen in das ID-000 Format überführt werden. Alle Funktionen und Datenstrukturen sind öffentlich definiert.

3.2 Chipkarte und Betriebssystem

3.2.1 Befehlssatz

Begründung: Der folgende minimale Befehlssatz nach ISO/IEC 7816 ermöglicht die Umsetzung der in Kapitel 3.6 geforderten Funktionalitäten und wird von möglichst vielen Kartenanbietern und Kartenbetriebssystemen angeboten.

ZWINGEND: Das Betriebssystem der Versichertenkarte muss mindestens folgenden Befehlssatz gemäss dem Standard ISO/IEC 7816-4 unterstützen. Eine Reduktion des untenstehenden Befehlssatzes ist möglich, wenn durch Substitution eines Basiskommandos mittels spezifischer Anwendung von der in dieser Liste enthaltenen Kommandos die geforderte Funktionalität, Performance und die Interoperabilität der Versichertenkarte nicht eingeschränkt wird.

- APPEND RECORD
- CHANGE REFERENCE DATA
- DISABLE VERIFICATION REQUIREMENT
- ENABLE VERIFICATION REQUIREMENT
- ENVELOPE
- ERASE BINARY
- ERASE RECORD (S)
- EXTERNAL AUTHENTICATE
- GET CHALLENGE
- GET DATA
- GET RESPONSE
- INTERNAL AUTHENTICATE
- MANAGE CHANNEL
- MANAGE SECURITY ENVIRONMENT
- PUT DATA
- READ BINARY
- READ RECORD (S)
- RESET RETRY COUNTER
- SEARCH BINARY
- SEARCH RECORD
- SELECT

- UPDATE BINARY
- UPDATE RECORD
- VERIFY
- WRITE BINARY
- WRITE RECORD

3.2.2 Operationen für Verschlüsselung

Begründung: Mit dem folgenden, minimalen Befehlssatz auf der Basis von ISO/IEC 7816 können die geforderten Anforderungen an kryptologische Operationen auf kostengünstigen Chipkarten erfüllt werden.

ZWINGEND: Für die kryptologischen Operationen muss das Betriebssystem der Chipkarte (Versichertenkarte) mindestens folgenden Befehlssatz gemäss dem Standard ISO/IEC 7816-8 unterstützen:

- ***GENERATE ASYMMETRIC KEY PAIR***

- ***'7F49' INTERINDUSTRY TEMPLATE***
  - 06' Object identifier of the algorithm
  - '80' Algorithm reference as used in control reference data objects for secure messaging (ev. für kant. Modellversuche)
  - Set of public key data objects for RSA
    - '81' Modulus
    - '82' Public exponent

- ***PERFORM SECURITY OPERATION***
  - Computation of a digital signature;
  - Calculation of a hash-code;
  - Verification of a digital signature;
  - Verification of a certificate;
  - Encipherment;
  - Decipherment.

3.2.3 EEPROM Speicher

Begründung: Die Anforderung wird für die Speicherung der in [VOEDI] definierten Daten benötigt und von Standardkarten mit niedrigen Lieferfristen erfüllt.

ZWINGEND: Der EEPROM Speicherbereich der Chipkarte muss über mindestens 32 KByte verfügen.

Hinweis: Die Anhänge 1 bis 3 der [VOEDI] spezifizieren Datenkataloge für die administrativen und persönlichen, medizinischen Daten im Umfang von ca. 2 bzw. 70 KByte. Die effektiv auf der Versichertenkarte gespeicherten Daten umfassen nur einen Teil davon, der von der versicherten Person für sich als relevant und wünschbar erachtet wird.

3.2.4 Initialisierung und Personalisierung der Chipkarte

Begründung: Der folgende Befehlssatz ist notwendig für die Spezifikation der Personalisierung und Initialisierung der Karte.

ZWINGEND: Die Chipkarte muss mindestens folgenden Befehlssatz gemäss den Standard ISO/IEC 7816-9 unterstützen:

- CREATE FILE
- DELETE FILE
- DEACTIVATE FILE
- ACTIVATE FILE
- TERMINATE DF
- TERMINATE EF
- TERMINATE CARD USAGE

ZWINGEND: Die Zustände und Zustandsübergänge eines vollständigen Lebenszyklus von Dateien sind gemäss dem Standard ISO/IEC 7816-9 geregelt.

ZWINGEND: Die Initialisierung und Personalisierung ist so durchzuführen, dass nach Abschluss dieser Prozesse und der abschliessenden Aktivierung der Versichertenkarte der Kartenherausgeber keine Möglichkeit mehr hat, auf die Dateien der Notfalldaten ohne einen berechtigten Leistungserbringernachweis zuzugreifen.

3.3 Authentisierung

3.3.1 Card Verifiable Certificates (CVC)

Begründung: Karten nach ISO/IEC 7816 benötigen CVC-Zertifikate für eine sichere asymmetrische Card-to-Card-Authentisierung.

ZWINGEND: Für die Authentisierung und Autorisierung müssen sogenannte Card Verifiable Certificates eingesetzt werden, welche wie folgt definiert sind:

Interindustry DO's for CV Certificates		
Tag	**Data element**	**Definiert in**
'7F21'	CV certificate	ISO/IEC 7816-6
'5F4E'	Certificate content	ISO/IEC 7816-8
'5F29'	Interchange profile descriptor, z.B. Certificate profile Identifier (CPI)	ISO/IEC 7816-6
'42'	Certification authority reference (CAR), Referenzattribut der herausgebenden CA (analog Authority Key Identifier, RFC 3280)	ISO/IEC 7816-6/8
'5F20'	Certificate holder reference (CHR), z.B. Name des Karteninhabers oder ICCSN	ISO/IEC 7816-6/8
'5F49'	Certificate holder public key (primitive DataObject)	ISO/IEC 7816-6/8
'7F49'	Certificate holder public key, (constructed DataObject, vorzugsweise)	ISO/IEC 7816-8
'06'	Object Identifier (OID) für Signaturalgorithmus oder Zertifikatsbesitzer	ISO/IEC 7816-6
'5F4A'	Public Key of CA or its reference	ISO/IEC 7816-6
'5F4C'	Certificate holder authorisation (CHA), hier sind die Zugriffsrollen definiert	ISO/IEC 7816-8/9
'5F37'	Signature of a certificate, Signatur der herausgebenden CA	ISO/IEC 7816-6/8
'5F38'	Public Key-Remainder (Rest des Modulus, gefolgt von einem Exponent)	ISO/IEC 7816-6

3.3.2 Authentisierung

Begründung: RSA stellt das gängigste asymmetrische Verfahren dar.

ZWINGEND: Die Authentisierung beruht auf einem asymmetrischen Verfahren nach ISO/IEC 9798-3, welches auf der Anwendung von öffentlichen und privaten Schlüssel beruht.

ZWINGEND: Als Algorithmus muss RSA verwendet werden, wobei die Schlüssellänge 1024 Bit beträgt.

ZWINGEND: Als Hashfunktion muss SHA1 verwendet werden, wobei der Hashwert 160 Bit beträgt.

3.4 Dateisystem

3.4.1 Dateiverwaltung nach ISO/IEC 7816-4

Begründung: Die folgenden Minimalanforderungen auf der Basis von ISO/IEC 7816 sind so bestimmt, dass sie von möglichst vielen Kartenanbietern erfüllt werden können.

ZWINGEND: Die Dateiverwaltung muss dem Standard ISO/IEC 7816-4 genügen und die folgenden Funktionalitäten umfassen:

- Schachtelungstiefe mindestens: MF-Ebene und DF-Ebene
- EF's mit transparenten Strukturen
- EF's mit linearer Struktur und Records festgelegter Länge
- EF's mit linearer Struktur und Records variabler Länge
- EF's mit zyklischer Struktur
- Records mit einer maximalen Länge bis zu 511 Byte
- Anzahl von Records in einem File: Maximal 254
- EF's mit Short EF Identifier (nutzbar nur im zugehörigen DF oder der zugehörigen Anwendung)
- DF mit Application Identifier

3.4.2 Dateistruktur der Versichertenkarte

Begründung: Die folgenden Anforderungen an die Dateistruktur nach ISO/IEC 7816 sind notwendig für die Umsetzung der Vorgaben der [VOEDI].

ZWINGEND: Die Dateien in der Versichertenkarte müssen gemäß ISO/IEC 7816-4 organisiert sein. Die folgende Abbildung zeigt die Dateistruktur. Die einzelnen Files werden in den folgenden Abschnitten beschrieben.

Die mit (*) bezeichneten Dateien enthalten medizinische Daten nach dem Anhang 2 der [VOEDI].

ZWINGEND: Zugriffe des Kartenherausgebers auf die medizinischen Daten sind durch technische Massnahmen zu verhindern.

ZWINGEND: Ein Zugriff auf die mit (*) gekennzeichneten Dateien ist nur mit vorangehender Authentisierung und Autorisierung der entsprechenden Leistungserbringergruppe möglich.

ZWINGEND: Zudem können die mit (*) gekennzeichneten Dateien zusätzlich mit einem persönlichen PIN vor sämtlichen Zugriffen geschützt werden.

ZWINGEND: Die folgenden Vorgaben zu den EF's auf MF-Ebene sind zwingend.

MF	**Masterfile**	**Working**
Root-Verzeichnis, welches implizit nach einem Reset der Chipkarte selektiert wird. In ihm befinden sich alle andern Verzeichnisse und Dateien. Es muss in jeder Chipkarte vorhanden sein.		

DF.NOT	**Dedicated File**	**Working**
Wirkt als Verzeichnisdatei und fasst alle Dateien mit Nutzdaten, die zu einer Anwendung gehören, zusammen. Chipkarten mit mehreren Anwendungen können über mehrere entsprechende DF's, in denen die zugehörigen EF's eingerichtet sind, verfügen (z.B. bei kantonalen Modellversuchen). Die Verzeichnisdatei DF.NOT beinhaltet alle Dateien, welche für den Zugriff und die Abspeicherung der medizinischen Daten der Versichertenkarte notwendig sind.		

$EF.ARR_1$	**Access Rule Reference file**		**Internal**
Structure: Linear variable	**Type:** Record	**AM:** R	**SC:**
Wird für die Speicherung von Zugriffsregeln auf der MF-Ebene verwendet.			

Datei	**Dateiname**	**Lesen**	**Schreiben/Löschen**
Cardholder Verification File	EF.PIN	Aktivierungs-byte+Statusbyte+PIN	Aktivierungs-byte+Statusbyte+PIN
Notfalldaten	DF.NOT	Authentisierung ok	Authentisierung ok
Optional: Kantonaler Modellversuch	n.n.	n.n.	n.n.
Weitere Zugangsregelungen	n.n.	n.n.	n.n.

EF.ATR	Answer to Reset File		Working
Structure: transparent	**Type:** BER-TLV	**AM:** R	**SC:**
Nach dem Anlegen der Spannungsversorgung, des Taktes und des Resetsignals sendet die Chipkarte am I/O-Pin einen Answer to Reset (ATR) aus. Dieser maximal 33 Byte lange Datenstring wird gemäss ISO/IEC 7816-3 immer mit dem Teilerverhältnis 372 gesendet und enthält Datenobjekte zur Identifizierung der Betriebsmerkmale der Karte (Parametrisierung des Übertragungsverfahrens, Identifizierung, usw.). Diese Datenobjekte sind in der Datei EF.ATR mit Lesezugriff unveränderbar abgelegt.			

EF.DIR	Directory File		Working
Structure: linear variable	**Type:** Record	**AM:** R	**SC:**
EF.DIR enthält die Anwendungsvorlagen gemäss ISO/IEC 7816-4 für die in der Versichertenkarte vorhandenen Anwendungen. Diese Datei ist für die Selektion der Anwendungen von kantonalen Modellversuchen besonders geeignet. EF.DIR weist eine Rekordstruktur auf, die in den Historical Bytes angezeigt werden muss.			

EF.ICCSN	Chipcard Identifier File [ICCSNF]		Working
Structure: linear variable	**Type:** Record	**AM:** R	**SC:**
In EF.ICCSN wird das DO ICCSN (Identifier (tag) ‘5A’) gespeichert. Die ICCSN entspricht der Kennnummer der Versichertenkarte.			
Record 1: SIMPE-TLV: DO ICCSN (Identifier (tag) ‘5A’)			
Record 2: Reference Number (Binär 8 Byte)			
Record 3: generalTime (GeneralizedTime[15 BCD]:= YYYYMMDDHHMMSSZ)			

EF.PIN	Cardholder Verification File		Internal
Structure: entweder/oder - transparent - linear variable	**Type:** entweder/oder - Bit-String - Record	**AM:** R/UP	**SC:**

Bei der Kartenausgabe wird das Aktivierungsbyte auf 0 gesetzt, d.h. auf die Notfalldaten kann ohne PIN-Schutz zugegriffen werden. Wenn eine Person eine mit (*) bezeichnete Datei (siehe Dateien-Struktur) durch einen PIN-Code schützen will, wird das Aktivierungsbyte auf 1 gesetzt.

Aktivierungs-Byte	PIN-Identifier	PIN-Value	Pre-set attempt value	Unblocking PIN Value	Number of unblocking mechanisms
0/1; no / yes	Referenz ←	6-8 Ziffern	5 Versuche	8 Ziffern	10 Versuche

EF.StatusPIN	Status PIN-Eingabe auf Notfalldaten		Internal
Structure: linear fixed	**Type:** Record	**AM:** R/UP	**SC:**
- Der Status bezüglich der Aktivierung einer PIN- Eingabe wird hier festgehalten. - Der Status des PIN bezüglich Zugangssperrung oder Freigabe auf die einzelnen Notfalldateien (EF's) wird hier festgehalten (siehe EF.PIN). - Die Zugriffsregelungen werden in den entsprechenden Dateien $EF.ARR_2$ bzw. $EF.ARR_1$ festgelegt.			

EF.ID	Identification Data		Working
Structure: transparent	**Type:** BER-TLV	**AM:** R	**SC:**
Identifikationsdaten des Karteninhabers nach Anhang 1 der [VOEDI]			

EF.AD	Administrative Data		Working
Structure: transparent	**Type:** BER-TLV	**AM:** R	**SC:**
Administrative Daten des Karteninhabers nach Anhang 1 der [VOEDI]			

EF.LOG	Protokolldatei		Working
Structure: linear cyclic	**Type:** record (z.B.50 records)	**AM:** R/UP	**SC:**
Diese Datei ist eine anwendungsspezifische Protokolldatei für technische Statusinformationen zum Sitzungsablauf. Damit kann eine Fehlerbehebungsfunktion (error recovery) und eine Zustandswiederherstellungsfunktion (roll back) ermöglicht werden.			

$EF.S_B$	Private Key für asymmetrische Authentisierung		Internal
Structure: - linear variable - Transparent	**Type:** - Record - Bit-String	**AM:** R	**SC:**
Für das Card-to-Card-Authentisierungsverfahren auf der Basis von CV-Zertifikaten wird ein globaler privater Schlüssel S_B benötigt, der in einer Schlüssel-Datei unterhalb des MF abgelegt ist. Der zugehörige öffentliche Schlüssel ist im Zertifikat CVC.PDC integriert, welches sich im Container EF.CVC.PDC befindet.			

EF.CVC.PDC	Datei für CVC-Zertifikat		Working
Structure: transparent	**Type:** Binary	**AM:** R	**SC:**
Die Datei EF.CVC.PDC enthält das CVC-Zertifikat der Versichertenkarte.			

EF.PK.CA_ORG_PDC	Public Root Key für asymmetrische Authentisierung		Internal
Structure: **-** linear variable - Transparent	**Type:** - Record - Bit-String	**AM:** R	**SC:**
Für das C2C-Authentisierungsverfahren auf der Basis von CV-Zertifikaten wird ein globaler öffentlicher Root-Schlüssel PK.CA_ORG_PDC benötigt; welcher auf der entsprechenden Offline-CVC-PKI erzeugt wurde und in einer Schlüssel-Datei unterhalb des MF abgelegt ist. Der zugehörige öffentliche Schlüssel ist im Zertifikat CVC.CA_ORG_PDC integriert, welches im Container EF.CVC.CA_ORG_PDC auslesbar und unveränderbar gespeichert ist. Dieser Root-Schlüssel wird zur dynamischen Zertifikatsüberprüfung der Leistungserbringerorganisationszertifikate benötigt. Die Leistungserbringerorganisationszertifikate werden vom Lesegerät/Anwendungs-modul in den Container EF.CVC.CA_ORG_HPC geladen und mit dem öffentlichen Root-Schlüssel bezüglich korrekter Signatur verifiziert.			

EF.CVC.CA_ORG_PDC	Datei für CVC-Zertifikat		Working
Structure: transparent	**Type:** Binary	**AM:** R	**SC:**
Zur Vervollständigung wird das Root-Zertifikat der Versicherer CVC.CA_ORG_PDC in diesem Container gespeichert. Ein CVC-Zertifikat belegt ca. 220 Byte			

EF.CVC.CA_ORG_HPC	Datei für CVC-Zertifikat		Working
Structure: transparent	**Type:** Binary	**AM:** R/W	**SC:**
Dies ist ein Container zur dynamischen Überprüfung der Leistungserbringer und der Leistungserbringerorganisationszertifikate. Die Leistungserbringerorganisationszertifikate, welche auf dem Lesegerät/Anwendungsmodul gespeichert sind werden entsprechend selektiert in diesen Container gespeichert. Durch eine 2-fache, hierarchische Zertifikatsverifikation wird die Vertrauenshierarchie bezüglich Integrität sichergestellt. Dieses Zertifikat wird im Rahmen des Card-to-Card-Authentisierungsverfahrens für die Zertifikatsverifikation verwendet. Ein CVC-Zertifikat belegt ca. 220 Byte			

ZWINGEND: Die folgenden Vorgaben für EF‘s auf der DF.NOT-Ebene sind zwingend.

EF.ARR$_2$	**Access Rule Reference file**		**Internal**
Structure: Linear variable	**Type:** Record	**AM:** R	**SC:**
Wird für die Speicherung von Zugriffsregeln innerhalb des DF.NOT- Verzeichnisses verwendet.			

Datei	**Dateiname**	**Lesen**	**Schreiben/Löschen**
Blutgruppen- und Transfusionsdaten	EF.BGTD	Schlüssel_1 + PIN	Schlüssel_2 + PIN
Immunisierungsdaten	EF.IMMD	Schlüssel_1 + PIN	Schlüssel_2 + PIN
Transplantationsdaten	EF.TPLD	Schlüssel_1 + PIN	Schlüssel_2 + PIN
Allergien	EF.ALLG	Schlüssel_1 + PIN	Schlüssel_2 + PIN
Krankheiten und Unfallfolgen	EF.KHUF	Schlüssel_1 + PIN	Schlüssel_2 + PIN
Zusätzliche Einträge	EF.ZUSE	Schlüssel_1 + PIN	Schlüssel_2 + PIN
Medikation	EF.MEDI	Schlüssel_1 + PIN	Schlüssel_2 + PIN oder Schlüssel_3 + PIN
Kontaktadressen	EF.ADDR	Schlüssel_1	Schlüssel_1
Patientenverfügungen	EF.VERF	Schlüssel_1	Schlüssel_1

EF.AUT	Authorization Reference file		Internal
Structure: Linear fixed	**Type:** Record	**AM:** R	**SC:**
Wird für die Zuordnung der Zugriffsregeln anhand des Autorisierungskodes verwendet.			

Leistungserbringer	Autorisierungskode	Schlüssel_1	Schlüssel_2	Schlüssel_3
Ärzte	CHA_1	x	x	
Apotheker	CHA_2	x		x
Zahnärzte	CHA_3	x	x	
Chiropraktoren	CHA_4	x	x	
Hebammen	CHA_5	x		
Physiotherapeuten	CHA_6	x		
Ergotherapeuten	CHA_7	x		
Pflegefachleute	CHA_8	x		
Logopäden	CHA_9	x		
Ernährungsberater	CHA_{10}	x		

EF.BGTD	Blutgruppen- und Transfusionsdaten		Working
Structure: Transparent	**Type:** BER-TLV	**AM:** R/UP/W	**SC:** $EF.ARR_2$
Der Inhalt des strukturierten Datenobjekts ist im Anhang 2 [VOEDI] definiert.			

EF.IMMD	Immunisierungsdaten		Working
Structure: Linear variable	**Type:** Record(SIMPLE-TLV)	**AM:** R/UP/W	**SC:** EF.ARR2
Diese Datei muss als Rekordstruktur angelegt sein. Der einzelne Rekord beinhaltet ein Datenobjekt, welches in SIMPLE-TLV kodiert ist. Die Inhalte der einzelnen Rekords und ihre strukturierten Datenobjekte sind im Anhang 2 der [VOEDI] definiert.			
Aufzeichnungsfolge:			
Rekord [1 .. 50]	Impfungen		

EF.TPLD	Transplantationsdaten		Working
Structure: Linear variable	**Type:** Record(SIMPLE-TLV)	**AM:** R/UP/W	**SC:** EF.ARR$_2$
Diese Datei muss als Rekordstruktur angelegt sein. Der einzelne Rekord beinhaltet ein Datenobjekt, welches in SIMPLE-TLV kodiert ist. Die Inhalte der einzelnen Rekords und ihre strukturierten Datenobjekte sind im Anhang 2 der [VOEDI] definiert.			
Aufzeichnungsfolge:			
Rekord [1 .. 10]	Zur Transplantation angemeldet		
Rekord [11 .. 20]	Bereits durchgeführte Transplantationen		

EF.KHUF	Krankheiten und Unfallfolgen		Working
Structure: Linear variable	**Type:** Record(SIMPLE-TLV)	**AM:** R/UP/W	**SC:** EF.ARR$_2$
Diese Datei muss als Rekordstruktur angelegt sein. Der einzelne Rekord beinhaltet ein Datenobjekt, welches in SIMPLE-TLV kodiert ist. Die Inhalte der einzelnen Rekords und ihre strukturierten Datenobjekte sind im Anhang 2 der [VOEDI] definiert.			
Aufzeichnungsfolge:			
Rekord [1 .. 50]	Krankheiten und Unfallfolgen		

EF.ZUSE	Zusätzliche Einträge		Working
Structure: Linear variable	**Type:** Record(SIMPLE-TLV)	**AM:** R/UP/W	**SC:** EF.ARR$_2$
Diese Datei muss als Rekordstruktur angelegt sein. Der einzelne Rekord beinhaltet ein Datenobjekt, welches in SIMPLE-TLV kodiert ist. Die Inhalte der einzelnen Rekords und ihre strukturierten Datenobjekte sind im Anhang 2 der [VOEDI] definiert.			
Aufzeichnungsfolge:			
Rekord [1 .. 10]	Hinweise auf verfügbare medizinische und pharmazeutische Dossiers		
Rekord [11 .. 35]	weitere medizinische und pharmazeutische Einträge		

EF.MEDI	Medikation		Working
Structure: Linear variable	**Type:** Record(SIMPLE-TLV)	**AM:** R/UP/W	**SC:** EF.ARR$_2$
Diese Datei muss als Rekordstruktur angelegt sein. Der einzelne Rekord beinhaltet ein Datenobjekt, welches in SIMPLE-TLV kodiert ist. Die Inhalte der einzelnen Rekords und ihre strukturierten Datenobjekte sind im Anhang 2 der [VOEDI] definiert.			
Aufzeichnungsfolge:			
Rekord [1 .. 50]	Dauermedikation		

EF.ALLG	Allergien		Working
Structure: Linear variable	**Type:** Record(SIMPLE-TLV)	**AM:** R/UP/W	**SC:** EF.ARR$_2$
Diese Datei muss als Rekordstruktur angelegt sein. Der einzelne Rekord beinhaltet ein Datenobjekt, welches in SIMPLE-TLV kodiert ist. Die Inhalte der einzelnen Rekords und ihre strukturierten Datenobjekte sind im Anhang 2 der [VOEDI] definiert.			
Aufzeichnungsfolge:			
Rekord [1 .. 25]	Soforttypreaktionen		
Rekord [26 .. 50]	Spättypreaktionen		

EF.ADDR	Kontaktadressen		Working
Structure: Linear variable	**Type:** Record(SIMPLE-TLV)	**AM:** R/UP/W	**SC:** EF.ARR$_2$
Diese Datei muss als Rekordstruktur angelegt sein. Der einzelne Rekord beinhaltet ein Datenobjekt, welches in SIMPLE-TLV kodiert ist. Die Inhalte der einzelnen Rekords und ihre strukturierten Datenobjekte sind im Anhang 2 der [VOEDI] definiert.			
Aufzeichnungsfolge:			
Rekord [1 .. 10]	Kontaktadressen für den Notfall		

EF.VERF	Patientenverfügungen und Organspende-ausweise		Working
Structure: Linear variable	**Type:** Record(SIMPLE-TLV)	**AM:** R/UP/W	**SC:** EF.ARR$_2$
Diese Datei muss als Rekordstruktur angelegt sein. Der einzelne Rekord beinhaltet ein Datenobjekt, welches in SIMPLE-TLV kodiert ist. Die Inhalte der einzelnen Rekords und ihre strukturierten Datenobjekte sind im Anhang 2 der [VOEDI] definiert.			
Aufzeichnungsfolge:			
Rekord [1 .. 10]	Hinweise auf bestehende Patientenverfügungen und Organspende-ausweise		

DF.KtMV	Dedicated File	Working
Wirkt als Verzeichnisdatei und fasst alle Dateien mit Nutzdaten, die zu einer Anwendung gehören, zusammen. Chipkarten mit mehreren Anwendungen können über mehrere entsprechende DF's, in denen die zugehörigen EF's eingerichtet sind, verfügen. Die Verzeichnisdatei DF.KtMV beinhaltet alle Dateien, welche für den Zugriff und die Abspeicherung in einem kantonalen Modellversuch notwendig sind.		

EF.X509-1	Container für X.509-Zertifikat	Working	
Structure: transparent	**Type:** Binary	**AM:** One-time write	**SC:**
Leerer Container für mögliche Datei, welche ein X.509-Zertifikat im Rahmen eines kantonalen Modellversuchs enthalten kann. Die Zertifikatsdatei in DER-Kodierung kann genau einmal abgespeichert werden und immer ausgelesen werden.			

EF.X509-2	Container für X.509-Zertifikat	Working	
Structure: transparent	**Type:** Binary	**AM:** R/W	**SC:**
Leerer Container für mögliche Datei, welche ein X.509-Zertifikat im Rahmen eines kantonalen Modellversuchs enthalten kann. Die Zertifikatsdatei in DER-Kodierung kann mehrfach abgespeichert, überschrieben und immer ausgelesen werden.			

EF.PuK$_{X509}$	**Public Root Key für asymmetrische Authentisierung**		**Working**
Structure: **-** linear variable - Transparent	**Type:** **-** Record - Bit-String	**AM:** R	**SC:**
Ein öffentlicher Schlüssel, welcher im Rahmen der Initialisierung und Personalisierung durch die Herausgeberorganisation der Versichertenkarte generiert und in diesem Container abgespeichert wurde. Dieser öffentliche Schlüssel kann für einen Pilotbetrieb im Rahmen eines kantonalen Modellversuchs verwendet und immer ausgelesen werden. Der dazugehörende private Schlüssel wird im Container EF.PrK$_{X509}$ nicht auslesbar abgespeichert.			

EF.PrK$_{X509}$	**Private Key für asymmetrische Verfahren**		**Internal**
Structure: **-** linear variable - Transparent	**Type:** - Record - Bit-String	**AM:** R	**SC:**
Ein privater Schlüssel, welcher im Rahmen der Initialisierung und Personalisierung durch die Herausgeberorganisation der Versichertenkarte generiert und in diesem Container abgespeichert wurde. Dieser private Schlüssel kann für einen Pilotbetrieb im Rahmen eines kantonalen Modellversuchs verwendet und nicht ausgelesen werden. Der dazugehörende öffentliche Schlüssel wird im Container EF.PuK$_{X509}$ auslesbar abgespeichert.			

3.5 PIN-Management

Begründung: Die Anforderungen für das PIN-Management nach ISO/IEC 7816 sind notwendig für die Umsetzung der Vorgaben der [VVK].

3.5.1 Befehlssatz

ZWINGEND: Für das PIN-Management wird folgender Befehlssatz gemäss ISO/IEC 7816-4 angewandt:

- VERIFY
- CHANGE REFERENCE DATA
- RESET RETRY COUNTER
- ENABLE VERIFICATION REQUIREMENT
- DISABLE VERIFICATION REQUIREMENT
- TERMINATE CARD USAGE

3.5.2 PIN-Aktivierung / Deaktivierung und Eingabe

Für das PIN-Management ist keine Card-to-Card-Authentisierung und Autorisierung notwendig.
Die Aktivierung kann auf einem Lesegerät/Anwendungsmodul mit Tastatur bei einem Leistungserbringer oder auf einem dedizierten Lesegerät mit Tastatur beim Versicherten selber, oder bei einem andern Dienstanbieter erfolgen.
Eine Aktivierung / Deaktivierung oder PIN-Eingabe alleine erlaubt keinen Zugriff auf die Notfalldaten.

3.5.3 PIN-Schutzzustände

ZWINGEND: Sämtliche Prozesse zur Festlegung der PIN-Schutzzustände erfolgen einzeln, sequentiell und können nicht kombiniert werden.

3.5.3.1 Versichertenkarte nach Auslieferung durch den Versicherer

ZWINGEND: Der PIN-Mechanismus ist deaktiviert. Damit ist grundsätzlich ein freier, geregelter Zugriff auf alle Notfalldaten möglich, sofern Card-to-Card-Authentisierung und Autorisierung erfolgreich durchgeführt worden sind.

3.5.3.2 Aktivierung des PIN-Mechanismus

ZWINGEND: Folgende Prozessschritte müssen durchgeführt werden:

1. Aktivierung des PIN-Mechanismus
2. Auswahl der Kategorien der Notfalldaten (EF.Dateien), welche mit einem PIN-Schutz belegt werden sollen, mittels Tastatur durch den Versicherten.
3. Eingabe des neuen PIN-Kodes mittels Tastatur durch den Versicherten

3.5.3.3 Änderung des PIN-Schutzes auf Kategorien der Notfalldaten

ZWINGEND: Folgende Prozessschritte müssen durchgeführt werden:

1. Eingabe des PIN-Kodes mittels Tastatur durch den Versicherten
2. Auswahl der Kategorien der Notfalldaten (EF.Dateien), welche mit einem PIN-Schutz belegt oder wieder freigegeben werden sollen, mittels Tastatur durch den Versicherten.
3. Eingabe des PIN-Kodes mittels Tastatur durch den Versicherten

3.5.3.4 Änderung des PIN-Kodes (PIN-Mechanismus aktiviert)

ZWINGEND: Folgende Prozessschritte müssen durchgeführt werden:

1. Eingabe des PIN-Kodes mittels Tastatur durch den Versicherten
2. Eingabe des Änderungsbegehrens mittels Tastatur durch den Versicherten
3. Eingabe des geänderten PIN-Kodes mittels Tastatur durch den Versicherten
4. Nochmalige Eingabe des geänderten PIN-Kodes mittels Tastatur durch den Versicherten

3.5.3.5 Deaktivierung des PIN-Mechanismus

ZWINGEND: Folgende Prozessschritte müssen durchgeführt werden:

1. Eingabe des PIN-Kodes mittels Tastatur durch den Versicherten
2. Eingabe des Deaktivierungsbegehrens mittels Tastatur durch den Versicherten

Bei einer allfälligen Reaktivierung werden die letzten PIN-Schutzbelegungen wieder wirksam.

3.5.3.6 PIN-Sperrmechanismen

ZWINGEND: Nach 5 fehlerhaften Versuchen wird die PIN-Eingabe gesperrt. Diese kann mit einem PUK von 8 Ziffern und einer Zulassung von maximal 10 Fehlversuchen wieder entsperrt werden. Werden die 10 Fehlversuche bei der PUK-Eingabe überschritten, bleibt die Versichertenkarte gesperrt und kann nicht mehr reaktiviert werden. Der zufällige PUK-Kode wird von den Versicherern bei der Kartenausgabe initialisiert und ist auf der Karte enthalten.

3.6 Card-to-Card-Authentisierung und Autorisierung

Begründung: Die Anforderungen sind notwendig für die Umsetzung der Vorgaben zur Card-to-Card-Authentisierung der [VVK], siehe auch Begründung zu Kapitel 3.3.1.

3.6.1 Prinzip

Der Authentisierungsprozess zwischen der VK (Versichertenkarte) und der HPC (Health Professional Card) beruht auf einem asymmetrischen Verfahren gemäss ISO/IEC 9798-3. Dazu enthalten die VK und die HPC CVC-Zertifikate nach den Vorgaben des Kapitels 3.6.2. Die Zertifikate der Leistungserbringer enthalten insbesondere den Autorisierungsmerkmalswert CHA, welcher das Mitglied einer Leistungserbringergruppe ausweist und zuordnet, siehe Kapitel 3.3.1. Weil beide Organisationen (Leistungserbringer, Versicherer) über keine gemeinsamen, zentralen Geheimnisse verfügen und die Authentisierung und Autorisierung alleine auf einem asymmetrischen Verfahren mit je eigenen individuellen Geheimnissen beruhen, sind Verifikationen von Zertifikaten notwendig. Dabei vertraut die VK auf den unveränderbar abgespeicherten öffentlichen Root-Schlüssel des CVC-Zertifikats der Versichererorganisationen(en). Mit dem privaten Root-Schlüssel der Versichererorganisationen(en) wurden alle Leistungserbringerorganisationszertifikate unterschrieben. Damit ist es möglich, durch eine 2-stufige Zertifikatsverifikation das Leistungserbringerzertifikat auch bei nachgeladenem, zwischengespeicherten Leistungserbringerorganisationszertifikat sicher zu überprüfen, weil die überprüfte Zertifikatshierarchie lückenlos auf dem unveränderbar abgespeicherten öffentlichen Root-Schlüssel des CVC-Zertifikats der Versichererorganisationen(en) beruht. Mit Hilfe des Lesegerätes/Anwendungsmoduls ist es möglich, die Personenzertifikate der Versicherten sowie der beteiligten Organisationen online oder offline zu überprüfen.

Für die Authentisierung erzeugt die Versichertenkarte zuerst eine Zufallszahl R_B und sendet diese an die Leistungserbringerkarte. Die Leistungserbringerkarte signiert diese Zufallszahl

mit ihrem individuellen privaten Schlüssel und sendet das signierte Datenpaket an die Versichertenkarte zurück. Die Versichertenkarte kann nun mit dem öffentlichen Schlüssel der Leistungserbringerkarte, welcher in dem CVC-Zertifikat der Leistungserbringerkarte enthalten ist, die zur Zufallszahl gehörende Signatur überprüfen. Für die Versichertenkarte hat sich damit die Leistungserbringerkarte authentisiert. Eine gegenseitige Authentisierung der Versichertenkarte bei der Leistungserbringerkarte ist nicht notwendig, weil die Versichertenkarte keinen Zugriff auf die Leistungserbringerkarte vornimmt. Falls der beschriebene Authentisierungsprozess erfolgreich abgeschlossen ist, gibt die Versichertenkarte den Zugriff gemäss dem im CVC-Zertifikat der Leistungserbringerkarte unveränderbar eingebetteten Autorisierungsmerkmalswert CHA (Rolle) frei. Damit sind grundsätzlich nur 2 individuelle Geheimnisse (private Schlüssel S_A und S_B) für den ganzen Authentisierungs- und Autorisierungsprozess notwendig. Diese Geheimnisse sind auf verschiedene Inhaber aufgeteilt. Authentisierung und Autorisierung stellen keine Anforderungen an das Vertrauen gegenüber dem Lesegerät/Anwendungsmodul.

3.6.2 Schlüssel und Zertifikate in Entitäten

Um eine wirksame Card-to-Card-Authentisierung und Autorisierung mittels asymmetrischen Verfahren zu implementieren, müssen Zertifikate, welchen den öffentlichen Schlüssel enthalten und die relevanten privaten Schlüssel in entsprechenden Speicherumgebungen abgelegt werden. Dabei sind die Dateien und Parameter im privaten Teil auf einer Chipkarte von aussen nicht auslesbar und können nur vom Chipkartenbetriebssystem für bestimmte Verfahren benutzt werden. Für ein gesichertes Card-to-Card-Authentisierung und Autorisierungsverfahren, welche Card Verifiable Certificates (CVC) erfordern, müssen mindestens Root-Zertifikate nur auslesbar und unveränderbar im öffentlichen Teil der jeweiligen Chipkarte abgelegt werden. Das Lesegerät/Anwendungsmodul spielt bei dieser Authentisierung und Autorisierung lediglich die Rolle eines Moderators und stellt gegebenenfalls eine Online-Verbindung zu den Herausgeberentitäten her. Da das Lesegerät/Anwendungsmodul auch offline betrieben werden soll, können die aktuellen, notwendigen Zertifikate vorgängig über das Internet heruntergeladen und auf dem Lesegerät/Anwendungsmodul im sogenannten öffentlichen Teil gespeichert werden. Um den Schutz der persönlichen, medizinischen Daten des Versicherten zu gewährleisten, braucht an das Lesegerät/Anwendungsmodul kein besonderer Schutzbedarf gestellt werden.

ZWINGEND: Die folgenden Schlüssel und Zertifikate sind auf der HPC, dem Lesegerät/Anwendungsmodul und der VK aufzubringen:

A: HPC-Karte

Öffentlicher Teil	Privater Teil
- CVC.HPC[P_A]	- S_A

T: Lesegerät/Anwendungsmodul

Öffentlicher Teil	Privater Teil
- X509.CA_Pub_{x1} - X509.CA_Pub_{x2} - X509.CA_ORG_PDC_m - X509.CA_ORG_HPC_m - CVC.CA_ORG_PDC_m[PK.CA_ORG_PDC_m] - CVC.CA_ORG_HPC_m[PK.CA_ORG_HPC_m]	

B: Versichertenkarte

Öffentlicher Teil	Privater Teil
- CVC.CA_ORG_HPC_m[PK.CA_ORG_HPC_m] - CVC.CA_ORG_PDC_m[PK.CA_ORG_PDC_m] - CVC.PDC[P_B]	- PK.CA_ORG_PDC_m - S_B

Bezeichnungen Versichertenkarte [B]	
S_B	Privater Schlüssel, welcher dem öffentlichen Schlüssel P_B im Personenzertifikat zugeordnet ist
CVC.PDC[P_B]	CVC-Personenzertifikat mit in ihm enthaltenen öffentlichen Schlüssel P_B
PK.CA_ORG_PDC$_m$	Öffentlicher Root-Schlüssel des CVC-Zertifikats der Versicherer-organisation(en)
CVC.CA_ORG_HPC$_m$[PK.CA_ORG_HPC$_m$]	CVC-Zertifikate der Leistungserbringerorganisation(en), wobei m:= 1 .. n ; z.B. 10 Leistungserbringerorganisationszertifikate.
CVC.CA_ORG_PDC$_m$[PK.CA_ORG_PDC$_m$]	CVC-Zertifikat der Versichererorganisation(en)

Bezeichnungen Leistungserbringerkarte [A]	
CVC.HPC[P_A]	CVC-Leistungserbringerzertifikat mit in ihm enthaltenen öffentlichen Schlüssel P_A
S_A	Privater Schlüssel, welcher dem öffentlichen Schlüssel P_A im Leistungserbringerzertifikat zugeordnet ist
Weitere Zertifikate möglich	Sind nicht Gegenstand der Regelungen bezüglich der Versichertenkarte

Bezeichnungen Lesegerät/Anwendungsmodul [T]	
CVC.CA_ORG_PDC$_m$[PK.CA_ORG_PDC$_m$]	CVC-Zertifikate der Versichererorganisation(en)
CVC.CA_ORG_HPC$_m$[PK.CA_ORG_HPC$_m$]	CVC-Zertifikate der Leistungserbringerorganisation(en), wobei m:= 1 .. n; z.B. 10 Leistungserbringerorganisationszertifikate.
X509.CA_ORG_PDC$_m$	Serverzertifikat nach X.509 (RFC 3280) der Versichererorganisation(en)
X509.CA_ORG_HPC$_m$	Serverzertifikat nach X.509 (RFC 3280) der Leistungserbringerorganisation(en), wobei m:= 1 .. n; z.B. 10 Leistungserbringerserverzertifikate
X509.CA_Pub$_x$	Ausstellerzertifikate nach X.509 (RFC 3280) der anerkannten Zertifizierungsdienstanbieter, wobei x:= 1 ..n sein kann

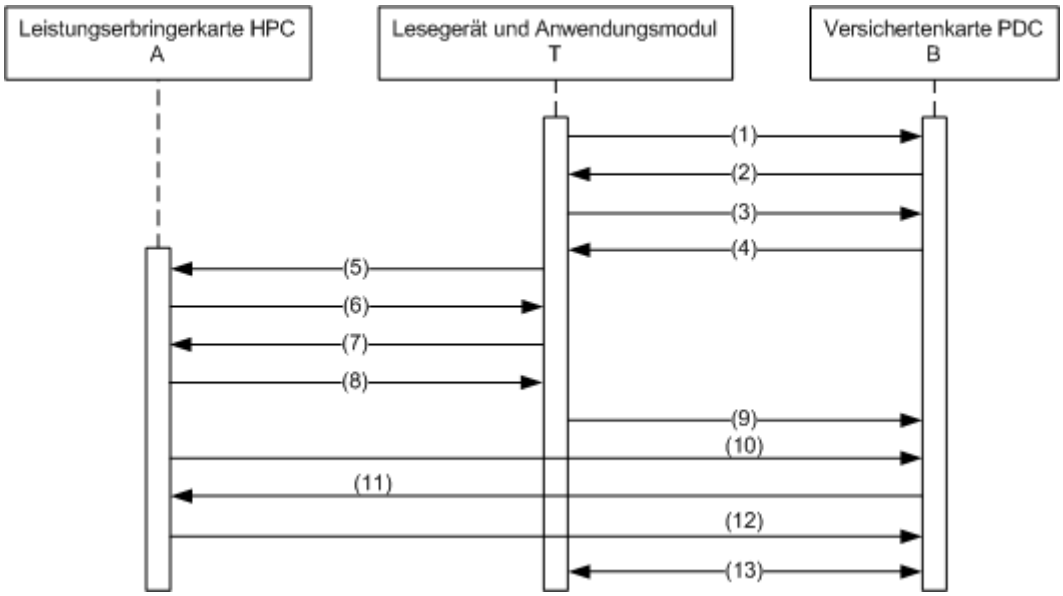
3.6.3 Begriffe und Abkürzungen

	Erläuterungen
CHA_1	Ärzte
CHA_2	Apotheker
CHA_3	Zahnärzte
CHA_4	Chiropraktoren
CHA_5	Hebammen
CHA_6	Physiotherapeuten
CHA_7	Ergotherapeuten
CHA_8	Pflegefachleute
CHA_9	Logopäden
CHA_{10}	Ernährungsberater
CHA_m	Card Holder Autorisierung, im signierten CVC-Zertifikat integriert
R_X	Zufallszahl, welche von der Entität X erzeugt wurde.
sS_X	Signieren mit privatem, geheimen Schlüssel der Entität X
sP_X	Signaturverifikation mit öffentlichem Schlüssel der Entität X
CVC	Card Verifiable Certificate
X509	Zertifikat basierend auf dem Standard RFC 3280, DER-kodiert
PK.A	Öffentlicher Schlüssel von A
{ ... }	Datenpaket
ICCSNF	Chipcard Identifier File
A[B]	B enthalten in A
‖	Zusammensetzungsoperator
$A \subset B$	A in B enthalten
< .. >	Zeiger auf Objekt
$A \leftarrow B$	Zeiger innerhalb Objekt
A(B;C;..)	Operator, A angewandt auf B und C, usw.

3.6.4 Verfahren

3.6.4.1 Offline Card-to-Card-Authentication and Authorization

ZWINGEND: Der Zugriff erfolgt gemäss nachfolgendem Schema



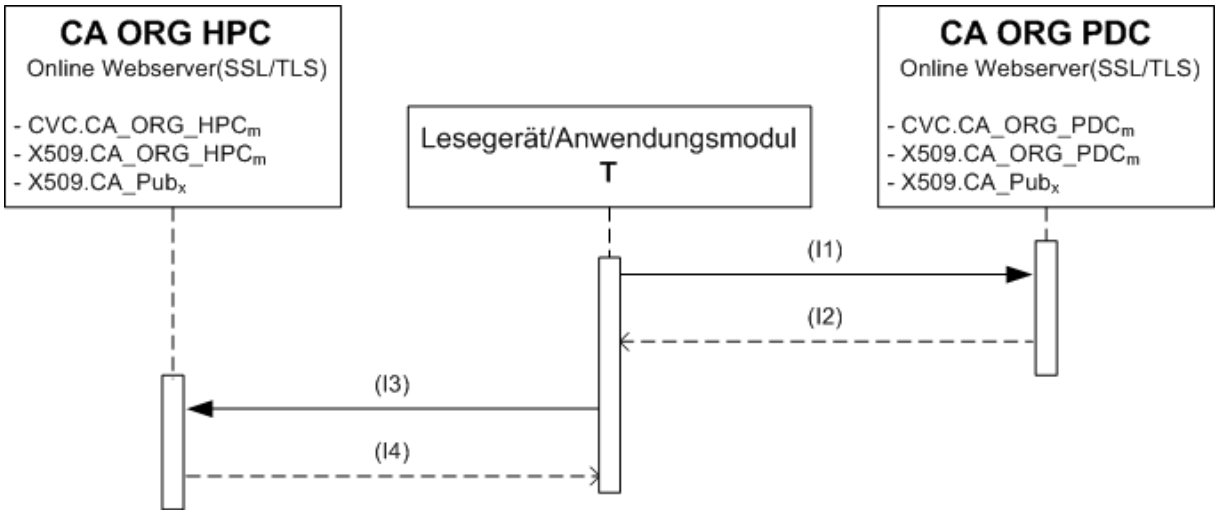
1	(1)	SelectFile‖ReadRecord (ICCSNF$_B$)
	REM	Selektieren und Auslesen des Chipcard Identifier Files
2	(2)	{ICCSNF$_B$}
	REM	Übertragung des Chipcard Identifier Files der Versichertenkarte
3	(3)	SelectFile‖ReadBinary (EF.CVC.PDC)
	REM	Selektieren und Auslesen des CVC-Personenzertifikats des Versicherten
4	(4)	{CVC.PDC}
	REM	Übertragung des CVC-Personenzertifikats des Versicherten
5	(T)	MSE SET<PK.CA_ORG_PDC$_m$←(CVC. CA_ORG_PDC$_m$)>
	REM	Setzen des öffentlichen Root-Schlüssels der Versichererorganisation des Versicherten
6	(T)	PSO VERIFY CERTIFICATE(CVC.PDC) → nok→break; ok→continue; Store (CHR$_B$); Extract (ICCSN$_B$)
	REM	Prüfen des CVC-Personenzertifikats des Versicherten
6a	(T)	optional: Compare(ICCSNF$_B$[ICCSN$_B$]; EF.CVC.PDC[ICCSN$_B$])
	REM	Überprüfung der Chipkartenseriennummer durch Vergleich der Nummern auf der Karte und im CVC-Personenzertifikat

7	(5)	SelectFile‖ReadRecord (ICCSNF$_A$)
	REM	Selektieren und Auslesen des Chipcard Identifier Files
8	(6)	{ICCSNF$_A$}
	REM	Übertragung des Chipcard Identifier Files der Leistungserbringerkarte
9	(7)	SelectFile‖ReadBinary (EF.CVC.HPC)
	REM	Selektieren und Auslesen des CVC-Leistungserbringerzertifikats
10	(8)	{CVC.HPC}
	REM	Übertragung des CVC-Leistungserbringerzertifikat
11	(T)	Read‖Extract(CVC.HPC) -> (CPI = 04, CAR, CHR, CHA) -> Store
	REM	Auslesen und Speichern der notwendigen Leistungserbringer-Attribute aus dem CVC-Leistungserbringerzertifikat
12	(T)	Search((CPI = 04, CAR, CHR, CHA), (CVC.CA_ORG_HPC$_m$))$_m$; -> Select(CVC.CA_ORG_HPC$_m$)
	REM	Anhand der Leistungserbringer-Attribute wird das entsprechende Leistungs-erbringerorganisationszertifikat selektiert.
13	(T)	SelectFile‖WriteBinary(CVC.CA_ORG_HPC$_m$) ->
	REM	Der Container für das ausgewählte Leistungserbringerorganisationszertifikat wird ausgewählt und soll beschrieben werden.
14	(9)	{CVC.CA_ORG_HPC$_m$} -> EF.CVC.CA_ORG_HPC
	REM	Übertragung und Speicherung des Leistungserbringerorganisationszertifi-kats
15	(10)	{CVC.HPC[P$_A$]}
	REM	Das CVC-Leistungserbringerzertifikat wird der Versichertenkarte zur Verifi-kation bereitgestellt
16	(B)	MSE SET<PK.CA_ORG_PDC$_m$>
	REM	Setzen des öffentlichen Root-Schlüssels der Versichererorganisation des Versicherten
17	(B)	PSO VERIFY CERTIFICATE(CVC.CA_ORG_HPC$_m$) → nok→break; ok→continue; Store (PK.CA_ORG_HPC$_m$)
	REM	Prüfen des CVC-Zertifikats der entsprechenden Herausgeberorganisation
18	(B)	MSE SET<PK.CA_ORG_HPC$_m$←(CVC.CA_ORG_HPC$_m$)>
	REM	Setzen des öffentlichen CA-Schlüssels der entsprechenden Leistungserbrin-gerorganisation

19	(B)	PSO VERIFY CERTIFICATE(CVC.HPC) → nok→break; ok→continue;
	REM	Prüfen des CVC-Leistungserbringerzertifikats
20	(B)	Store (CHA_n)
	REM	Zwischenspeicherung des Karteninhaberautorisierungsmerkmalswertes CHA_n , welches im Leistungserbringerzertifikat eingebunden ist
21	(B)	Generate (R_B)
	REM	Zufallszahl erzeugen
22	(11)	{R_B}
	REM	Zufallszahl übermitteln
23	(A)	$sS_A(R_B)$
	REM	Zufallszahl signieren
24	(12)	{$sS_A(R_B)$}
	REM	Signierte Zufallszahl übermitteln
25	(B)	$sP_A(sS_A(R_B))$; $R_B = R_B$ → ok→continue; nok→break
	REM	Verifikation der Signatur der signierten Zufallszahl
26	(B)	(CHA_n); Autorisation ok!
	REM	Der Karteninhaberautorisierungsmerkmalswert CHA_n wird freigeschaltet
27	(13)	Lesegerät/Anwendungsmodul kann erst jetzt mittels dem Karteninhaberautorisierungsmerkmalswert (CHA_n) auf die Versichertenkarte zugreifen
	REM	Datenaustausch zwischen dem Lesegerät/Anwendungsmodul und der Versichertenkarte

3.6.4.2 Optionale Online/Offline Certificate Verification

OPTIONAL: Zertifikate können optional durch das Lesegerät/Anwendungsmodul heruntergeladen und geprüft und online/offline werden.



1	(i1)	Get Certificates ⊂ $CA\_ORG\_PDC_m$: - $CVC.CA\_ORG\_PDC_m$ - $X509.CA\_ORG\_PDC_m$ - $X509.CA\_Pub_x$
2	(i2)	Download Certficates ⊂ $CA\_ORG\_PDC_m$: - $CVC.CA\_ORG\_PDC_m$ - $X509.CA\_ORG\_PDC_m$ - $X509.CA\_Pub_x$
3	(i3)	Get Certificates ⊂ $CA\_ORG\_HPC_m$: - $CVC.CA\_ORG\_HPC_m$ - $X509.CA\_ORG\_HPC_m$ - $X509.CA\_Pub_x$
4	(i4)	Download Certficates ⊂ $CA\_ORG\_HPC_m$: - $CVC.CA\_ORG\_HPC_m$ - $X509.CA\_ORG\_HPC_m$ - $X509.CA\_Pub_x$

3.6.4.3 Offline-PKI der Herausgeberorganisationen zur Erstellung von CVC-Zertifikaten

Begründung: Die Anforderungen sind hinreichend für eine Definition der Offline-CVC-PKI der Herausgeberorganisationen. Die Anforderungen müssen von den Herausgeber-organisationen zwingend umgesetzt werden, damit eine optionale Überprüfung der Zertifikate und deren Zertifikatskette möglich ist.

ZWINGEND: Die Offline-CVC-PKI muss in einem Sicherheitsbereich untergebracht sein, welcher durch festgelegte Sicherheitszonen mit angemessenen Sicherheitsbarrieren und Zugangskontrollen geschützt ist.

Zur sicheren Signaturerstellung muss durch geeignete Technik und Verfahren zumindest gewährleistet werden, dass

a) **ZWINGEND:** die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten nur einmal auftreten können und dass ihre Geheimhaltung hinreichend gewährleistet ist

b) **ZWINGEND:** die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur vor Fälschungen bei Verwendung der jeweils verfügbaren Technologie geschützt ist

c) **ZWINGEND:** die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten von dem rechtmäßigen Unterzeichner vor der Verwendung durch andere verlässlich geschützt werden können

d) **EMPFOHLEN:** zum verbesserten Schutz des privaten Schlüssels sollen sogenannte HSM's (Hardware Security Module) eingesetzt werden, welche den Anforderungen nach FIPS 140 Level 3 genügen.

ZWINGEND: Die öffentlichen Schlüssel der Offline-CVC-PKIs ($PK.CA\_ORG\_PDC_m$, $PK.CA\_ORG\_HPC_m$) der entsprechenden Herausgeberorganisationen sind in den entsprechenden Zertifikaten ($CVC.CA\_ORG\_PDC_m$, $CVC.CA\_ORG\_HPC_m$) im CVC-Format nach ISO/IEC 7816-8 in den durch die Tags '7F49' und '5F38' referenzierten Datenelementen normgerecht einzubinden: Siehe Kapitel 6.1. Diese Zertifikate müssen mittels einem Onlinedienst auf einem Webserver unter der Anwendung eines öffentlichen Serverzertifikats (siehe Kapitel 6.2), welches von einem anerkannten Zertifizierungsdienstanbieter nach ZertES ausgestellt wurde, als Datei in der Kodierung nach ISO/IEC 7816-8 bereitgestellt werden und vom Lesegerät/Anwendungsmodul zur Verifikation der Zertifikatskette bzw. zur Verifikation der CVC- Personenzertifikate auf der Versichertenkarte mittels der Protokolle SSL/TLS über das Internet heruntergeladen werden können (Prozessschritte (i1, i2) bzw. (i3, i4)).

ZWINGEND: Die Serverzertifikate ($X509.CA\_ORG\_HPC_m$, $X509.CA\_ORG\_PDC_m$) der erforderlichen Onlinedienste der Herausgeberorganisationen müssen ebenfalls auf dem Webserver als Datei in der gebräuchlichen DER-Kodierung nach X.690 (ISO/IEC 8825-1) so bereitgestellt werden, dass diese mittels SSL/TLS über das Internet in das Lesegerät/Anwen-dungsmodul heruntergeladen werden können. Diese Zertifikate können dazu verwendet werden, um auf dem Lesegerät/Anwendungsmodul eine Vertrauensbeziehung zwischen dem öffentlichen Serverzertifikat der entsprechenden Herausgeberorganisation

und dem dazugehörenden CVC- Herausgeberorganisationszertifikat elektronisch nachzuweisen (Prozessschritte (i1, i2) bzw. (i3, i4)).

ZWINGEND: Die Herausgeberorganisationen müssen zusätzlich noch das Ausstellerzertifikat (X509.CA_Pub$_x$) des anerkannten Zertifizierungsdienstanbieters nach ZertES auf ihrem online Webserver als Datei in der gebräuchlichen DER-Kodierung nach X.690 (ISO/IEC 8825-1) bereitstellen, so dass dieses mittels SSL/TLS über das Internet in das Lesegerät/Anwendungsmodul heruntergeladen werden kann. Damit kann die Zertifikatsvetrauenskette bezüglich den ausgestellten Serverzertifikaten der online Webserver der Herausgeberorganisationen und den CA-Ausstellerzertifikaten der nach ZertES anerkannten Zertifizierungsdienstanbieter vom Lesegerät/Anwendungsmodul elektronisch überprüft werden. (i1,i2) bzw. (i3,i4)).

3.6.4.4 Online/Offline- Überprüfung der Zertifikate

EMPFOHLEN: Auf dem Lesegerät/Anwendungsmodul sollten folgende Verifikationen durchgeführt werden:

1. Überprüfung der Beziehung der Serverzertifikate (X509.CA_ORG_HPC$_m$, X509.CA_ORG_PDC$_m$) der erforderlichen online Webdienste der Herausgeberorganisationen zu den entsprechenden CVC-Herausgeberorganisationszertifikaten (CVC.CA_ORG_PDC$_m$, CVC.CA_ORG_HPC$_m$): Durch einen Vergleich des Description Attribute im Subjet-Feld des Serverzertifikats der Herausgeberorganisation und dem CAR-Datenelement plus den Datenelementen, welche im CVC- Herausgeberorganisationszertifikat den öffentlichen Schlüssel enthalten, kann auf dem Lesegerät/Anwendungsmodul durch entsprechende Transformation eine Vertrauensbeziehung und Zuordnung zwischen den beiden Zertifikaten und deren Organisationen elektronisch nachgewiesen werden: Siehe auch Kap. 6.2.2.
2. Überprüfung der Signaturen der Serverzertifikate (X509.CA_ORG_HPC$_m$, X509.CA_ORG_PDC$_m$) mit den Ausstellerzertifikaten (X509.CA_Pubx) auf dem Lesegerät/Anwendungsmodul.
3. Überprüfung der Zertifikatskette mittels den Attributen (AuthorityKeyIdentifier, SubjectKeyIdentifier) in den entsprechenden Zertifikaten (X509.CA_ORG_HPC$_m$, X509.CA_ORG_PDC$_m$, -> X509.CA_Pub$_x$) auf dem Lesegerät/Anwendungsmodul.

Die CVC- und X.509-Zertifikate sind im Kapitel 6 spezifiziert.

3.6.4.5 Anforderung an die Detailspezifikation

ZWINGEND: In den Detailspezifikationen sollen alle Basiskommandos, Grundfunktionen des Betriebssystems, grundlegende Sicherheitsfunktionen und -algorithmen, Detailspezifikationen für die Dateistrukturen und der zugehörigen Datenelemente, die bei der Initialisierung und Personalisierung in die Versichertenkarte geladen werden, detailliert beschrieben werden, sofern sie für eine Sicherstellung der Interoperablität für die Kommunikation und den Zugriff relevant sind.

ZWINGEND: Die Detailspezifikationen enthalten einheitlich vorgegebene Fehlermeldungen.

EMPFOHLEN: Der Kartenherausgeber stellt ein Application Programming Interface zur Verfügung.

4 Online-Verfahren nach Artikel 15 [VVK]

4.1 Grundsatz

Der Versicherer bietet zur Abfrage der Daten nach Anhang 3 der [VOEDI] die folgenden drei Möglichkeiten an:

ZWINGEND: Manueller Zugang mit marktüblichen Internet-Browser mittels HTTP v1.1 über SSL v3.0 oder TLS v1.0

ZWINGEND: Zugang über einen Webservice auf Basis von SOAP. Das SOAP- Protokoll muss an HTTP v1.1 über SSL v3.0 oder TLS v1.0 gebunden werden.

ZWINGEND: Direkter Zugang mit Web-Redirection mittels HTTP/1.1 über SSL v3.0 oder TLS v1.0

4.2 Anforderungen an die Kommunikation

ZWINGEND: Die Datenübertragung geschieht verschlüsselt mittels der nachfolgend aufgeführten Protokolle, welche von den aktuellen Internet-Browsern unterstützt werden.

- Secure Socket Layer SSL v3.0 (Netscape 1996); SSL v2.0 ist untersagt
- Transport Layer Security TLS v1.0 [RFC 2246, RFC 3546] (Bei Wahlfreiheit ist dieses SSL v3.0 vorzuziehen)

ZWINGEND: Die Schlüssellänge für das asymmetrische Verschlüsselungsverfahren sollte mindestens 1024 Bit, diejenige für das symmetrischen Verfahren 3DES mindestens 168 Bit und für das symmetrischen Verfahren AES mindestens 256 Bit betragen.

ZWINGEND: Für die Umsetzung der Online-Abfrage sind folgende Protokolle und Standards zu verwenden:

- HTTP-Protokoll (Version 1.1, RFC 2616)
- SOAP-Nachrichtenübertragungsprotokoll (ab Version 1.2)
- XML
- WSDL ab Version 1.2

4.3 Direkter Online-Zugang mittels HTTP über SSL/TLS

4.3.1 Internet-Browser auf Desktop-Rechner des Leistungserbringers

ZWINGEND: Online-Abfrageverfahren dürfen nur marktübliche Internet-Browser – ohne produktspezifische Funktionalitäten - voraussetzen, wobei diese folgende Spezifikationen und Protokolle unterstützen müssen:

- HTTP- Protokoll (Version 1.1, RFC 2616)
- Einseitige, serverzertifikatsbasierte Verschlüsselung mit den Protokollen SSL v3.0 oder TLS v1.0

4.3.2 Zugriffskontrolle

ZWINGEND:
- Die Zugriffskontrolle muss über ID und Passwort erfolgen.
- Bei maximal 5 Passwortfehleingaben wird der Zugriff gesperrt
- Der Zugriff erfolgt über eine einseitige, serverzertifikatsbasierte Verschlüsselung.

OPTIONAL: Zur Erhöhung der Zugriffssicherheit und zur Verminderung von missbräuchlichen Abfragen können zusätzliche Verfahren angewandt werden. Zum Beispiel: Challenge-Response-Verfahren (Grid, SMS, usw.), HIP-Verfahren (Human Interactive Proof).

4.4 Direkter Online-Zugang mittels SOAP/HTTP über SSL/TLS

4.4.1 Online-Abfrageverfahren aus Anwendungen beim Leistungserbringer

4.4.1.1 Zugangsprotokolle

ZWINGEND: Folgende Spezifikationen und Protokolle müssen unterstützt werden:

- HTTP- Protokoll (Version 1.1, RFC 2616)
- SOAP- Nachrichtenprotokoll (ab Version 1.2) für den direkten Lesezugriff auf die administrativen Daten, welches an HTTP v1.1 gebunden ist.
- Mindestens einseitige, zertifikatsbasierte Verschlüsselung mit den Protokollen SSL v3.0 oder TLS v1.0

HINWEIS: XML-Schemata und WSDL-Schnittstellendefinition werden vom BAG zur Verfügung gestellt.

4.4.1.2 Zugriffskontrolle

ZWINGEND: Die Zugriffskontrolle muss über ID und Passwort erfolgen. Dabei können ID und Passwort in der Leistungserbringeranwendung gespeichert werden, wobei ein Zugriffs- und Ausleseschutz so implementiert werden muss, dass ein Missbrauch mit grosser Wahrscheinlichkeit ausgeschlossen werden kann. Bei maximal 5 Passwortfehlübertragungen wird der Zugang gesperrt.

OPTIONAL: Die Versicherer können für Leistungserbringerzugänge mit hohem Abfragevolumen eine zweiseitige, zertifikatsbasierte Verschlüsselung mittels den Protokollen SSL v3.0 oder TLS v1.0 verlangen. Dabei liefern die Versicherer eine Datei mit einem passwortgeschützten Container in PKCS#12-Format, in welchem der private Schlüssel mit dem entsprechenden X.509-Zertifikat nach dem Standard RFC 3280 enthalten ist. Diese sind in der Leistungserbringeranwendung unter einem geeigneten Zugriffs- und Ausleseschutz so abzuspeichern, dass ein Missbrauch mit grosser Wahrscheinlichkeit ausgeschlossen werden kann.

4.4.2 Servergestützte, direkte Online-Abfrageverfahren für Dienste bei Leistungserbringern oder den von ihnen beauftragten Institutionen

4.4.2.1 Zugangsprotokolle

ZWINGEND: Folgende Spezifikationen und Protokolle müssen unterstützt werden:

- HTTP- Protokoll (Version 1.1, RFC 2616)
- SOAP- Nachrichtenprotokoll (ab Version 1.2) für den direkten Lesezugriff auf die administrativen Daten, welches an HTTP v1.1 gebunden ist.
- Zweiseitige, zertifikatsbasierte Verschlüsselung mit den Protokollen SSL v3.0 oder TLS v1.0

HINWEIS: XML-Schemata und WSDL-Schnittstellendefinition werden vom BAG zur Verfügung gestellt.

4.4.2.2 Zugriffskontrolle

ZWINGEND: Die Versicherer definieren für diese Kategorie von Diensten die notwendigen Zugriffsmerkmalswerte und gegebenenfalls eine Erweiterung der vom BAG bereitgestellten Schnittstellendefinition in WSDL. Der Zugriff beruht fallweise aus einem oder einer Kombination der folgenden Merkmalswerte:

- ID und Passwort der jeweilig zugeordneten Leistungserbringer, welche durch die Weitergabe ihrer Merkmalswerte an einen Dienstanbieter ihre Zugriffsrechte damit delegiert haben
- Dedizierte Zugangs-ID
- Weitere Merkmalswerte (z.B. Gruppen-ID, ZSR-Nummer)

Alle Merkmalswerte müssen in einer Datenbank im Server des Dienstanbieters beim Leistungserbringers oder bei der von ihm beauftragten Institution unter einem geeigneten Zugangs- und Ausleseschutz so gespeichert werden, dass ein Missbrauch ausgeschlossen werden kann. Bei maximal 5 fehlerhaften Zugriffsversuchen wird der Zugang gesperrt.

OPTIONAL: Die Versicherer können bei solchen Diensten mit hohem Abfragevolumen für den Datenzugang über einen geschützten Kommunikationskanal eine zweiseitige, zertifikatsbasierte Verschlüsselung mittels den Protokollen SSL v3.0 oder TLS v1.0 verlangen.

Begründung: Das Missbrauchsrisiko ist durch die veränderten Zugriffsmöglichkeiten sehr viel höher und verlangt höhere Sicherheitsmassnahmen.

Es müssen zum verbesserten Schutz des privaten Schlüssels und der gesicherten Anbindung der Identität an den Server des Dienstanbieters sogenannte HSM's (Hardware Security Module) eingesetzt werden, welche den Anforderungen nach FIPS 140 Level 3 genügen. Das dazugehörende X.509-Zertifikat nach RFC 3280 muss mit einer Zertifikatsanfrage, welche im PKCS#10-Format (RFC 2986) an den entsprechenden Dienst der Versicherer übermittelt wird, angefordert werden. Der Zertifizierungsdienst der Versicherer erstellt unter der Berücksichtigung einer genauen Abklärung der Identität des Antragstellers ein entsprechend signiertes Zertifikat auf seiner Offline-X.509-PKI und sendet dieses anschliessend als Datei

in DER- oder PEM-Kodierung (X.690/ISO 8825-1 bzw. RFC 1421-RFC 1424) an den Antragsteller. Die Versicherer definieren den dazu notwendig gesicherten Datenaustausch sowie die Identitätsüberprüfung.

ZWINGEND: Die Versicherer legen ein Service Level Agreement (SLA) fest, welches als Grundlage für diese Kategorie von Online-Abfragediensten dient und zwischen Versicherer und Dienstanbieter abgeschlossen werden muss.

4.4.2.3 Client-Server-Anbindung

Die Anbindung der Clients an den Dienstserver beim Leistungserbringer oder bei der von ihm beauftragten Institution muss mindestens folgende technische Anforderungen erfüllen:

ZWINGEND: Verschlüsselte Ende-zu-Ende-Verbindung, wobei die Anforderungen bezüglich Verschlüsselung mindestens den Anforderungen, wie unter Kapitel 4.2 definiert, genügen müssen.

ZWINGEND: Die Zugangskontrolle muss mindestens über ID und Passwort erfolgen

4.4.2.4 Zertifizierungsdienst der Versicherer für Zertifikate nach X.509 (RFC 3280)

ZWINGEND: Es genügt, dass die Versicherer zur Bereitstellung der geforderten Zertifikate und Zertifizierungsdienste eine angemessen gesicherte Offline-X.509-PKI ohne einen öffentlichen Verzeichnisdienst betreiben oder betreiben lassen.

4.5 Authentisierter Zugang mittels Netzwerkdiensteanbieter (Authentisierungsdienst)

Bei dieser Anwendung werden die Identifikation und die Authentisierung durch den Netzwerkdiensteanbieter mittels entsprechenden Diensten durchgeführt. Die Zuweisung eines authentisierten und identifizierten Benutzers zu einer ZSR-Nummer, gegebenenfalls zu einem Gruppennamen sowie einer Mitglieder-ID erfolgt direkt durch den Authentisierungsserver des Netzwerkdiensteanbieters. Da diese ID's über eine gesicherte, vertrauensvolle Verbindung vom Authentisierungsserver des Netzwerkdiensteanbieters an den Dienstserver der Versicherer übermittelt werden, ist die Zugangsfreigabe für die Abfrage der Daten vom Leistungserbringer mittels Internet-Browser oder Leistungserbringeranwendungen direkt ohne weitere Authentisierungsstufen möglich - eine zertifikatsbasierte Authentisierungslösung seitens der Leistungserbringeranwendung ist hier nicht mehr notwendig.

4.5.1 Identitätsverwaltung - und Zugriffsautorisierung

ZWINGEND: Die Versicherer stellen den Netzwerkdienstanbietern ein Verfahren zur Zugriffsautorisierung zur Verfügung, welches ihren Mitglieder einen direkten Zugang ohne weitere Authentisierung für eine Online-Abfrage auf dem Dienstserver der Versicherer erlaubt.

ZWINGEND: Die Versicherer stellen mittels geeigneten Verfahren sicher, dass nur berechtige Mitglieder eines Netzwerkdiensteanbieters direkten Zugang aus einem Heimnetz auf den

Dienstserver der Versicherer erhalten. Die Autorisierung für die Online-Abfrage untersteht den Versicherern.

ZWINGEND: Die Übermittlung der notwendigen Zugangsdaten vom Authentisierungsserver des Netzwerkdiensteanbieters an den Dienstserver der Versicherer geschieht mittels einer SOAP-Nachricht (Zugangsnachrichtenprotokoll) über ein sicheres Transportprotokoll.

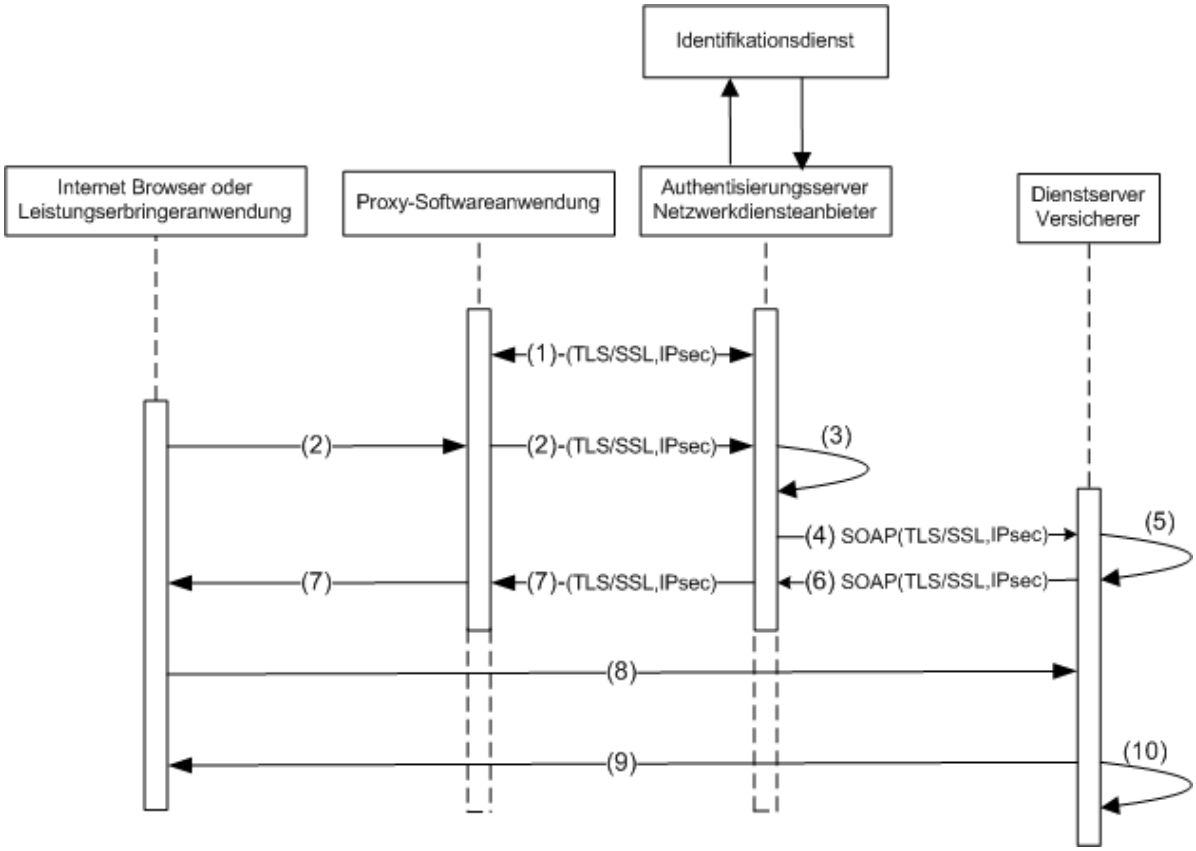
ZWINGEND: Die Versicherer definieren ein Zugangsnachrichtenprotokoll auf der Basis von SOAP mit folgenden Merkmalswerten:

- Dedizierte Zugangs-ID
- Weitere Merkmalswerte (z.B. Gruppen-ID, ZSR-Nummer)

ZWINGEND: Die Versicherer definieren Verfahren unter der Verwendung von geeigneten elektronischen Mitteln, welche sowohl den Netzwerkdienstanbietern wie auch den Versicherern eine sichere, zurechenbare Zugriffsverwaltung mit geringem administrativen Aufwand ermöglichen, um so einen Zugang eines authentisierten Mitglieds im Heimnetz eines Netzwerkdienstanbieters für die Online-Abfrage auf dem Dienstserver der Versicherer ohne weitere Authentisierung und Autorisierung zu realisieren.

4.5.2 Zugriffsverfahren

ZWINGEND: Das nachfolgend beschriebene Verfahren ist einzuhalten. Der Einsatz eines Proxys ist allerdings optional.



(1) Der Leistungserbringer authentisiert sich im Heimnetz auf dem Authentisierungsserver des Netzwerkdiensteanbieters mittels einer dedizierten Proxy-Softwareanwendung unter der Anwendung einer gegenseitigen starken Client/Server-Authentisierung. Bei erfolgreicher Authentisierung wird zwischen dem Proxydienst auf der Leistungserbringerplattform und dem Kommunikationsdienst des Netzwerkdiensteanbieters ein sicherer verschlüsselter Datenkanal aufgebaut.

(2) Der Leistungserbringer fordert nun mit dem Internet-Browser (http, SSL/TLS) oder einer Leistungserbringeranwendung (SOAP/http, SSL/TLS) mittels einer dedizierten Adresse (URL) auf dem Authentisierungsserver des Netzwerkdiensteanbieters den Online-Abfragedienst der Versicherer an.

(3) Der Authentisierungsserver des Netzwerkdiensteanbieters bindet die dedizierten ID's und Merkmalswerte für den Zugang auf den Dienstserver der Versicherer für den entsprechend registrierten Benutzer anhand seiner Identifikationsdaten, welche vom Identifikationsdienst des Netzwerkdiensteanbieters geliefert werden, in das definierte SOAP- Zugangsnachrichtenprotokoll ein.

(4) Der Authentisierungsserver des Netzwerkdiensteanbieters sendet die SOAP- Zugangsnachricht über ein sicheres Transportprotokoll an den Dienstserver der Versicherer.

(5) Der Dienstserver der Versicherer empfängt und verarbeitet die SOAP- Zugangsnachricht, überprüft die dedizierten ID's und Merkmalswerte, generiert eine zufällige Session-ID, erzeugt und autorisiert die spezifische Zugriffsberechtigung (URI, Session-ID, Timeout) und verpackt die URI und die Session-ID für die HTTP-Redirection in die neu erzeugte SOAP- Zugangsnachricht.
(6) Der Dienstserver der Versicherer sendet nun diese SOAP- Zugangsnachricht an den Authentisierungsserver des Netzwerkdiensteanbieters
(7) Der Authentisierungsserver des Netzwerkdiensteanbieters erzeugt aus den Daten in der SOAP- Zugangsnachricht die dedizierte HTTP-Redirection und sendet diese im verschlüsselten Datenkanal über den identifizierten Proxydienst dem Internet-Browser bzw. der Leistungserbringeranwendung.
(8) Der Internet-Browser bzw. die Leistungserbringeranwendung baut nun eine Verbindung mittels HTTP-Redirection (URI, Session-ID) zum dedizierten Abfrageportal des Dienstservers der Versicherer so auf, dass eine durchgehende, einseitig zertifikatsbasierte Ende-zu-Ende-Verschlüsselung mittels dem sicheren Transportprotokoll (SSL 3.0/TLS 1.0) gewährleistet werden kann. Dabei kann der verschlüsselte Datenkanal (SSL/TLS) vom Internet-Browser bzw. der Leistungserbringeranwendung auf den Dienstserver der Versicherer entweder innerhalb des Datenkanals der Netzwerkdienstanbieter oder ausserhalb über das Internet geführt werden.
(9) Beim ordnungsmässigen Ausloggen wird die Session geschlossen und gegebenenfalls mittels HTTP-Redirection der Adressvektor auf den Netzwerkdiensteanbieter dem Internet-Browser bzw. der Leistungserbringeranwendung zurückgegeben.
(10) Bei keinem oder nicht ordnungsgemässen Ausloggen wird die Session mittels einem definierten Timeout automatisch geschlossen.

ZWINGEND: Die Versicherer legen ein Service Level Agreement (SLA) fest, welches als Grundlage für diese Kategorie von Online-Abfragediensten dient und zwischen Versicherer und Dienstanbieter abgeschlossen werden muss.

5 Kantonale Modellversuche nach Artikel 16 [VVK]

- **ZWINGEND:** Für kantonale Modellversuche enthält die Versichertenkarte ein dediziertes Verzeichnis (Verzeichnisdatei DF).
- **ZWINGEND:** Nutzdateien, Logikdateien, Schlüsseldateien und Dateien mit Zertifikaten (CVC, X.509) sind strikte innerhalb eines solchen dedizierten Verzeichnisses (DF) für kantonale Modellversuche abzulegen.
- **ZWINGEND:** Bei kantonalen Modellversuchen ist sicherzustellen, dass die in diesem technischen Standard festgelegten Verfahren, Applikationen, Daten- und Logikdateien für die Versichertenkarte ohne kantonale Modellversuche weder eingeschränkt noch beeinträchtigt werden.
- **ZWINGEND:** Das anlässlich der Initialisierung und Personalisierung der Versichertenkarte erzeugte Schlüsselpaar für Pilotversuche im Rahmen von kantonalen Modellversuchen wird von den Versicherern und/oder deren Herausgeberorganisationen weder gespeichert noch administrativ verwaltet.
- **ZWINGEND:** Das anlässlich der Initialisierung und Personalisierung der Versichertenkarte erzeugte Schlüsselpaar für Pilotversuche im Rahmen von kantonalen Modellversuchen unterliegt ausschliesslich dem Lebenszyklus, welcher von den Versicherern definiert wird.
- **ZWINGEND:** Die Versicherer haften nicht für Verluste und Schäden jeglicher Art, welche im Zusammenhang mit der Verwendung des Schlüsselpaars für Pilotversuche im Rahmen von kantonalen Modellversuchen entstanden sind oder entstehen könnten.

6 Definition Zertifikate

ZWINGEND: Alle in diesem Kapitel 6 aufgeführten Definitionen sind einzuhalten.

6.1 Spezifikation CVC-Zertifikate nach ISO/EC 7816-8 mit message recovery nach ISO/IEC 9796-2

Tag	Tag	Tag	Bez.	Beschreibung	Length
'7F21'	**CVC-Zertifikat**				[Bytes]
	'5F37'	**Signatur**			M
		'6A'	**Padding**	Padding entsprechend [ISO 9796-2]	
		'5F29'	**CPI**	Certificate Profile Identifier	1
		'42'	**CAR**	Certification Authority Reference	8
		'5F20'	**CHR**	Certificate Holder Reference	16
		'5F4C'	**CHA**	Certificate Holder Authorisation	7
		'06'	**OID**	Object Identifier:= OID-Kodierung	8
		'7F49'	**PK_Part1**	= 'xx..xx' (MSB ⇒LSB); $N_{1/2}$	$N_{1/2}$
			Hash	'xx..xx' = Hash (20 byte)	20
		'BC'	**Trailer**	Digitale Signatur wird über den Datenblock, begrenzt durch '6A..'BC', gebildet	
	'5F38'	**PK_Part2** = 'xx..xx' (MSB ⇒LSB); $N_{2/2}$ **PK_exp** = '00 01 00 01'; e= 64 bit			$N_{2/2}$+ e
	'42'	**CAR:** Certification Authority Reference			8

Tag of Data element	Length
'5F37'	M = 128 Byte, [1024 Bit]
'7F49'	$N_{1/2}$ = 64 Byte, [512 Bit]
'5F38'	$N_{2/2}$+ e = 72 Byte, wobei $N_{2/2}$ = 64 Byte [512 Bit]

6.1.1 CVC-Zertifikate ['7F21']

Inhaber	CVC-Zertifikat ['7F21']
Versicherter (Personenzertifikat)	CVC.PDC
Leistungserbringer (Personenzertifikat)	CVC.HPC
Versichererherausgeberorganisation	$CVC.CA\_ORG\_PDC_m$
Leistungserbringerherausgeberorganisation	$CVC.CA\_ORG\_HPC_m$

6.1.2 Signatur ['5F37']

Inhaber	Signatur ['5F37']
Versicherter: CVC.PDC	Sig(CA_ORG_PDC$_m$);n= 1024 Bit
Leistungserbringer: CVC.HPC	Sig(CA_ORG_HPC$_m$);n= 1024 Bit
Versichererherausgeberorganisation: CVC.CA_ORG_PDC$_m$	Sig(CA_ORG_PDC$_1$)*;n= 1024 Bit
Leistungserbringerherausgeberorganisation: CVC.CA_ORG_HPC$_m$	Sig(CA_ORG_PDC$_1$)*;n= 1024 Bit

(*): erste, in Betrieb genommene Offline-CVC-PKI der Versicherer

6.1.3 CPI - Certificate Profile Identifier ['5F29']

Der “Certificate Profile Identifier (CPI)” hat den Zweck, die genaue Struktur eines CVC- Zertifikates anzuzeigen. Hier wird unterschieden, ob es sich um ein Benutzerzertifikat ('04') oder um ein CA-Zertifikat (Herausgeberorganisationszertifikat) ('03') handelt

CPI - Certificate Profile Identifier ['5F29']	CPI Kodierung: ['01'..'7E']
Versichertenkarte: PDC	'04'
Leistungserbringerkarte: HPC	'04'
Versichererherausgeberorganisation: CA_ORG_PDC	'03'
Leistungserbringerherausgeberorganisation: CA_ORG_HPC	'03'

6.1.4 CAR- Certification Authority Reference (Authority Key Identifier)

Dieses Element wird zur Identifizierung der Zertifikatsausgabestelle (CA) benutzt.

CAR ['42']	CA Name [5 Bytes]		Erweiterung für Schlüsselreferenzierung			
	Land	Name	Service-Indikator	CA - spezifische Information	Algorithmen-Referenz	Datum CA-Schlüssel-erzeugung
Länge	[2 Byte]	[3 Byte]	[1 BCD]	[1 BCD]	[2 BCD]	[2 BCD]
PDC	'CH'	NNN	'1'	'0'	'01'	'YY'
HPC	'CH'	NNN	'1'	'1'	'01'	'YY'
CA_ORG_PDC	'CH'	NNN	'6'	'0'	'01'	'YY'
CA_ORG_HPC	'CH'	NNN	'6'	'1'	'01'	'YY'

Land:	Ländercode entsprechend ISO 3166 (2 Bytes CH = Schweiz)
Datum der CA- Schlüsselerzeugung:	Enthält die letzten Ziffern des Jahres, in welchem das Schlüsselpaar zur Signierung der Zertifikate generiert wurde.
Algorithmenreferenz	- [01]: SHA1 with RSA signature algorithm using padding rules according to ISO 9796-2
CA- spezifische Information	- [0]: Zertifikat ausgestellt durch CA der Versichererherausgeberorganisation - [1]: Zertifikat ausgestellt durch CA der Leistungserbringerherausgeberorganisation

Service Indikator:	**[1 BCD]**	**Name: NNN**	**[3 Byte]**
Digital Signature	'0'	z.B. VeKa-Center	VKC
Entity Authentication	'1'	z.B. FMH	FMH
Key Encipherment	'2'	z.B. OFAC	OFC
Data Encipherment	'3'	z.B. Pflegefachleute	SBK
Key Agreement	'4'	usw.	.....
Entity Authentication(C)	'5'		
CertSign (no service indicated)	'6		
CertSign for Authentication and Key Encipherment	'7'		
CertSign for Authentication and Key Agreement	'8'		

6.1.5 CHR- Certificate Holder Reference (Subject Key Identifier)

Dieses Element wird zur Identifizierung des Zertifikatinhabers benutzt. Es weist eine Länge von 16 Byte auf.

Herausgeberzertifikate:

CHR ['5F20']		**CA Name [5 Bytes]**		**Erweiterung für Schlüsselreferenzierung**			
	Füller	**Land**	**Name**	**Service-Indikator**	**CA - spezifische Information**	**Algorithmen-Referenz**	**Datum CA-Schlüsselerzeugung**
Länge	[8 Byte]	[2 Byte]	[3 Byte]	[1 BCD]	[1 BCD]	[2 BCD]	[2 BCD]
CA_ORG_PDC	'00000000'	'CH'	NNN	'6'	'0'	'01'	'YY'
CA_ORG_HPC	'00000000'	'CH'	NNN	'6'	'1'	'01'	'YY'

Vergleiche Kap. 6.1.4 Certification Authority Reference

Versichertenzertifikate:

CHR ['5F20']		
	Füller	**ICCSN**
Länge	[6 Byte]	[10 Byte]
PDC	'000000'	'xxxxxxxxxx'

Leistungserbringerzertifikate, LE-Zertifikate:

CHR ['5F20']				
	LE-Kennziffer	**Besitzer**	**Trenner**	**ICCSN**
Länge	[4 Byte] binär	[2 BCD]	[2 BCD]	10 Byte
HPC Inhaber	'.....' B	'00'	'00'	'aaaaaaaaaa'
HPC delegiert_1	dito LE-Kennziffer	'01'	'00'	'bbbbbbbbbb'
HPC delegiert_n	dito LE-Kennziffer	'99'	'00'	'zzzzzzzzzz'

6.1.6 CHA- Certificate Holder Authorisation

Die "Certificate Holder Authorisation" (CHA) hat den Zweck, die Zugriffsrechte des Karteninhabers in Bezug auf Daten, die in einer anderen Karte gespeichert sind, festzulegen.

Karte / Zertifikat	CHA Profil-ID	CHA ['5F4C']	Beschrieb
PDC	CHA_0 = 00	AID(DF.NOT) ‖ '00'	Kein Zugriff auf Daten
HPC	CHA_1 = 01	AID(DF.NOT) ‖ '01'	Zugriff auf Notfalldaten
HPC	CHA_2 = 02	AID(DF.NOT) ‖ '02'	Zugriff auf Notfalldaten
HPC	CHA_3 = 03	AID(DF.NOT) ‖ '03'	Zugriff auf Notfalldaten
HPC	CHA_4 = 04	AID(DF.NOT) ‖ '04'	Zugriff auf Notfalldaten
HPC	CHA_5 = 05	AID(DF.NOT) ‖ '05'	Zugriff auf Notfalldaten
HPC	CHA_6 = 06	AID(DF.NOT) ‖ '06'	Zugriff auf Notfalldaten
HPC	CHA_7 = 07	AID(DF.NOT) ‖ '07'	Zugriff auf Notfalldaten
HPC	CHA_8 = 08	AID(DF.NOT) ‖ '08'	Zugriff auf Notfalldaten
HPC	CHA_9 = 09	AID(DF.NOT) ‖ '09'	Zugriff auf Notfalldaten
HPC	CHA_{10} = 10	AID(DF.NOT) ‖ '10'	Zugriff auf Notfalldaten

Karte / Zertifikat	CHA Profil-ID	CHA ['5F4C']	Beschrieb
CA_ORG_PDC	CHA_0 = 00	AID(DF.NOT) ‖ '00'	Kein Zugriff auf Daten
CA_ORG_HPC	CHA_0 = 00	AID(DF.NOT) ‖ '00'	Kein Zugriff auf Daten

6.1.7 OID- Kodierung

Karte / Zertifikat	OID-Kodierung ['06'] nach ISO 8825	OID-Nummer	OID-Name	Registration Authority
PDC	2B 0E 03 02 0F	1.3.14.3.2.15	SHA with RSA signature algorithm using padding rules according to ISO 9796-2	OIW
HPC	2B 0E 03 02 0F	1.3.14.3.2.15	SHA with RSA signature algorithm using padding rules according to ISO 9796-2	OIW
CA_ORG_PDC	2B 0E 03 02 0F	1.3.14.3.2.15	SHA with RSA signature algorithm using padding rules according to ISO 9796-2	OIW
CA_ORG_HPC	2B 0E 03 02 0F	1.3.14.3.2.15	SHA with RSA signature algorithm using padding rules according to 9796-2	OIW

Öffentlicher Schlüssel RSA	
Tag '81'	Modulus
Tag'82'	Public exponent

6.2 Serverzertifikate nach X.509 (RFC 3280) für den Onlinedienst

6.2.1 Zertifikatsdefinition

Zertifikate	**$X509.CA\_ORG\_PDC_m$ $X509.CA\_ORG\_HPC_m$**	
Attribute	**Werte**	**Hinweise**
Version	Version 3	
serialNumber	eindeutiger Integer	Serienummer
signature	{1 2 840 113549 1 1 5}	sha1WithRSAsignature
issuer	Distinguished Name des anerkannten Zertifizierungsdienstanbieters nach ZertES	z.B. Swisscom, SwissSign, QuoVadis, BIT
validity	- not before: - not after:	UTCTime, ETSI TS 102 280
subject	Distinguished Name der Herausgeberorganisation: { DESCRIPTION=carpukcvc, CN=, OU=, O=, L= , C= }	- OU: Herausgeberorganisation - O: Betreiberorganisation - OID(description) = {2.5.4.13} - carpukcvc-> siehe 6.2.2 z.B. O=Swisscom, OU=FMH z.B. O=Veka-C, OU=Veka-C
subjectPublicKeyInfo	- Algorithm: 1 2 840 113549 1 1 1 - subjectPublicKey: 1024 Bit	rsaEncryption
authorityKeyIdentifier	- keyIdentifier: sha1(subjectPublicKey) - authorityCertIssuer - authorityCertSerialNumber	von anerkannten Zertifizierungsdienstanbieters nach ZertES
subjectKeyIdentifier	sha1 (subjectPublicKey)	Identifiziert den Schlüssel des Inhabers
keyUsage	- critical = TRUE - digitalSignature - keyEncipherment	Schlüsselverwendung für Serverauthentisierung für den Onlinedienst
certificatePolicies	OID der Zertifikatsrichtlinie für dieses Zertifikat vom anerkannten Zertifizierungsdienstanbieter	- Richtlinienkennung - Richtlinienqualifierinformationen
crlDistributionPoints	uRI des anerkannten Zertifizierungsdienstanbieters	Sperrlistenverteilungspunkt vom anerkannten Zertifizierungsdienstanbieter
extKeyUsage	serverAuth: 1 3 6 1 5 5 7 3 1	Server Authentication
AuthorityInfoAccess	- accessMethod: id-ad-caIssuers - accessLocation: [uRI]	Stelleninformationszugriff mit weiteren Information vom Zertifizierungsdienstanbieter [http], ev. URL(OCSP)
signatureAlgorithm	- Algorithm: 1 2 840 113549 1 1 5 - signature: mindestens 2048 Bit	sha1WithRSAsignarure

6.2.2 DESCRIPTION (2.5.4.13): carpukcvc

Dieses Beschreibungsattribut dient zur Referenzierung und Identifizierung der Merkmalswerte der Offline-CVC-PKI der in diesem Serverzertifikat aufgeführten Herausgeberorganisation.

Variable: carpukcvc [40 Byte]						**Format: DirectoryString{printableString}**
CAR- Certification Authority Reference						- **PK.CA_ORG_PDC$_m$** - **PK.CA_ORG_HPC$_m$**
Land [2 Byte]	**Name** [3 Byte]	**Service** [1 BCD]	**CA-Info** [1 BCD]	**AlgoRe** [2 BCD]	**Datum KeyCA** [2 BCD]	**Public Key in HEX-Code-Darstellung** [64 BCD]

6.3 Ausstellerzertifikate nach X.509 (RFC 3280) [X509.CA_Pub$_x$]

Diese öffentlichen Ausstellerzertifikate müssen von Zertifizierungsdienstanbietern ausgestellt werden, welche im Verzeichnis der anerkannten Anbieterinnen nach Artikel 5 ZertES mindestens nach allen Normen von ZertES, VZertES und TAV-ZertES eingetragen sind. Für die Ausgabe von solchen Zertifikaten muss der Zertifizierungsdienstanbieter die gleichen organisatorischen und technischen Verfahren anwenden sowie die gleiche oder eine gleichwertige technische Infrastruktur nutzen wie für die Ausgabe von qualifizierten Zertifikaten nach ZertES.

7 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellt, oder welche **eCH** referenziert, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

8 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Glossar und Abkürzungen

Die im Standard verwendeten Fachausdrücke und Abkürzungen sind in den referenzierten Standards und RFC's dokumentiert.

AM	Chipkarte: Access Mode
CVC	Card Verifiable Certificates, Zertifikate für die Card-to-Card-Authentisierung
HPC	Health Professional Card, elektronische Leistungserbringerkarte
Internal	Files auf der VK, auf welche nur das Kartenbetriebssystem selbst Zugriff hat
LE	(medizinischer) Leistungserbringer
PDC	Patient Data Card, Versichertenkarte
RFC	Remote Function Call
SC	Chipkarte: Security Condition
Structure	Chipkarte: Elementary File Structure
Type	Chipkarte: Elementary File Type
VK	Versichertenkarte
Working	Files auf der VK, auf welche von aussen zugegriffen werden kann
ZSR	Zahlstellenregister, wird von santésuisse geführt
ZSR-Nummer	Nummer des ZSR für Leistungserbringer, welche unter dem Krankenversicherungsgesetz abrechnen

Anhang B – Referenzen und Bibliographie

[VVK]	Verordnung über die Versichertenkarte für die obligatorische Krankenpflegeversicherung (SR 832.105)
[VOEDI]	Verordnung des EDI über die technischen und grafischen Anforderungen an die Versichertenkarte für die obligatorische Krankenpflegeversicherung (SR 832.105.1)
[DSG]	Bundesgesetz über den Datenschutz (SR 235.1)
[VDSG]	Verordnung zum Bundesgesetz über den Datenschutz (SR 235.11)
[EU-Beschluss Nr. 190]	Beschluss Nr. 190 der Verwaltungskommission der europäischen Gemeinschaften für die soziale Sicherheit der Wanderarbeitnehmer vom 18. Juni 2003 betreffend die technischen Merkmale der europäischen Krankenversicherungskarte.
[ISO8601: 2004]	Datumsformate im internationalen Kontext
[RFC 2119: 1997]	Key words for use in RFCs to Indicate Requirement Levels
[RFC 3280: 2002]	Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile
[RFC 2246: 1999]	TLS Protocol Version 1.0
[RFC 2616: 1999]	Hypertext Transfer Protocol, HTTP 1.1
[RFC 3546: 2003]	Transport Layer Security (TLS) Extensions
[ISO 3166-1: 2006]	Codes for the representation of names of countries and their subdivisions, Part 1: Country Codes
[ISO7810: 2003]	Identification cards -- Physical characteristics
[ISO7816-1: 1998]	Physical Characteristics of Integrated Circuit Cards
[ISO7816-2: 1999]	Dimensions and Locations of Contacts
[ISO7816-3: 2006]	Electronic Signals and Transmission Protocols
[ISO7816-4: 2005]	Interindustry Commands for Interchange
[ISO7816-6: 2004]	Interindustry data elements for interchange
[ISO7816-8: 2004]	Commands for security operations
[ISO7816-9: 2004]	Commands for card management
[ISO8825-1: 2002] [ITU-T: X.690:2002]	Specification of BER, CER, DER - Encoding Rules
[ISO9796-2: 2002]	Digital signatures schemes giving message recovery (Integer factorization)

[ISO9798-1: 1997] Part 1: General (Definitions and Notations)

[ISO9798-3: 1998] Part 3: Mechanisms using digital signature techniques

Anhang C – Mitarbeit und Überprüfung

Hannes Bösch, (Arpage AG)
Marc Defalque (Swisscom IT Services)
Marzio Della Santa (GDK)
Martin Denz
Nguyen Don (Telekurs)
Hänsenberger Stephan (H+)
Christian Hausammann (Accarda)
Simon Hölzer (H+)
Siegfried Isele (Hp)
Michèle Kathriner (PwC)
Birgit Lang (SUVA)
Hansjörg Looser (Kt. SG)
Christian Lovis (Hôpital Univ. Genève)
Andreas Lux (Debold&Lux)
Jérome Magnin (ZAS)
Urs Mathis (Trüb AG)
René Meier (Intercard)
Daniel Muscionico (OFAC)
Beat Nussbaumer (Swisscom)
Rolf Oppliger (ISB)
Bernhard Ostertag (Intercard AG)
Thomas Räber (CSS)
Serge Reichlin (Siemens MED Solutions)
Xavier Rossmanith (BSV)
Stefano Salvadè (Kt. TI)
Rolf Schmidiger (SUVA)
Hans-Peter Schönenberger (santésuisse)
Christoph Schöni (H+)
Burkhard Schwalm (EDOEB)
Pawel Silberring (Celsi)
Urs Stromer (Schweizerische Post)
Urs Suter (Siemens)
Michael Vetterli (Signpool)
David Voltz (Ofac)
Judith Wagner (FMH)
Michael Ziegler (H-Net)