

Praktische
Untersuchungen
Card to Card

Versichertenkarte nach
Art. 42a KVG

Teil 2 / 2

| Version | Autor | Datum | Kommentar |
|---------|---------------------------|-------------------|-----------|
| 1.3b | R. Eberhard S. Staible | 21. Dezember 2010 | |
| 1.4 | R. Eberhard S. Staible | 39. April 2011 | |

Inhaltsverzeichnis

| | | |
|-------|---|----|
| 1 | Abkürzungen..... | 3 |
| 1.1 | Definitionen | 3 |
| 1.2 | Referenzen..... | 4 |
| 2 | Einleitung..... | 5 |
| 2.1 | Ziele..... | 5 |
| 2.1.1 | Abgrenzung | 5 |
| 2.2 | Hilfsmittel und Durchführung | 5 |
| 2.2.1 | Praktische Untersuchungen ohne Card to Card Authentisierung | 5 |
| 2.2.2 | Praktische Untersuchungen mit Card to Card Authentisierung..... | 5 |
| 2.2.3 | Log-Dateien | 6 |
| 3 | Versuchsbeschreibung | 7 |
| 3.1 | Versuchsablauf..... | 7 |
| 3.2 | Versuchsaufbau | 9 |
| 3.2.1 | PDC Demonstrator | 9 |
| 3.2.2 | Übersicht über die Karten und ihre jeweiligen Zertifikate..... | 10 |
| 4 | Ergebnisse | 11 |
| 4.1 | Übersicht | 11 |
| 4.2 | Erläuterung zu Ergebnissen | 11 |
| 4.3 | Auslesen der Identifikations-Daten..... | 11 |
| 4.4 | Auslesen der administrativen Daten..... | 12 |
| 4.5 | Notfalldaten lesen/schreiben | 13 |
| 4.5.1 | Card-to-Card Authentisierung durchführen..... | 13 |
| 4.5.2 | Notfalldaten schreiben (EF.BGTD, transparent) | 13 |
| 4.5.3 | Notfalldaten lesen (EF.BGTD, transparent) | 13 |
| 4.5.4 | Notfalldaten schreiben (EF.ALLG, linear variable)..... | 14 |
| 4.5.5 | Notfalldaten lesen (EF.ALLG, linear variable)..... | 14 |
| 4.5.6 | Notfalldaten löschen (EF.BGTD, transparent) | 14 |
| 4.5.7 | Notfalldaten lesen (EF.BGTD, transparent) | 14 |
| 4.5.8 | Notfalldaten löschen (EF.ALLG, linear variable) | 15 |
| 4.5.9 | Notfalldaten lesen (EF.ALLG, linear variable)..... | 15 |
| 4.6 | PIN setzen/löschen..... | 16 |
| 4.6.1 | PIN-Schutz aktivieren und PIN erstmalig setzen | 16 |
| 4.6.2 | PIN-Schutz deaktivieren und PIN löschen | 17 |
| 4.6.3 | PIN-Schutz erneut aktivieren und PIN setzen..... | 17 |
| 4.6.4 | PIN-Schutz deaktivieren und PIN löschen | 17 |
| 4.7 | PIN-geschützte Notfalldaten lesen | 18 |
| 4.7.1 | PIN-Schutz aktivieren und PIN setzen..... | 18 |
| 4.7.2 | Card-to-Card Authentisierung durchführen..... | 18 |
| 4.7.3 | Notfalldaten lesen (EF.BGTD, transparent) ohne PIN | 18 |
| 4.7.4 | Freischalten der Notfalldaten durch Eingabe des PINs | 19 |
| | Freischalten der Notfalldaten durch Eingabe des PINs | 19 |
| 4.7.5 | Notfalldaten lesen (EF.BGTD, transparent) | 19 |
| 4.8 | Verifikation: Card-to-Card Authentication and Authorization | 20 |
| 4.9 | Verifikation: Stichproben der APDU-Kommandos | 22 |
| 4.9.1 | File-ID von EF.BGTD..... | 22 |
| 4.9.2 | Inhalt von EF.VERSION | 24 |
| 4.9.3 | APDU-Befehlssequenzen zur Validierung der LE-Zertifikate..... | 25 |

1 Abkürzungen

| Bezeichnung | Beschreibung |
|-------------|--|
| AID | Application Identifier |
| AM | Access Mode |
| APDU | Application Protocol Data Unit nach ISO 7816 |
| API | Application programming interface |
| CA | Certification Authority |
| CLA | Class-Byte of a command APDU |
| CVC | Card Verifiable Certificate |
| DO | Data Object |
| FID | File ID |
| HPC | Health Professional Card |
| INS | Instruction-Byte of a command APDU |
| LC | Length Command |
| LE | Length Expected |
| MF | Master File |
| P1 | Parameter P1 of a command APDU |
| P2 | Parameter P2 of a command APDU |
| SASIS | SASIS AG, beauftragte der santésuisse. |
| SC | Security Condition |
| SFID | Short File ID (implizite, interne Selektion) |
| VK | Versichertenkarte |

1.1 Definitionen

| Bezeichnung | Beschreibung |
|-------------|---|
| VK-Post | Versichertenkarte umgesetzt nach den Spezifikationen der Schweizerischen Post |
| VK-SASIS | Versichertenkarte umgesetzt nach den Spezifikationen der SASIS |

1.2 Referenzen

| Referenz | Beschreibung |
|----------------|--|
| [Expertise VK] | Expertise Versichertenkarte nach Art. 42a KVG, Teil 1 / 2, Version 2.5b |
| [Log VK POST] | Logdatei des Versuchsablaufs zur VK POST auf APDU-Basis. Erhältlich unter NDA von Albis Technologies AG. |
| [Log VK SASIS] | Logdatei des Versuchsablaufs zur VK SASIS auf APDU-Basis. Erhältlich unter NDA von Albis Technologies AG. |
| [eCH64] | eCH-0064 - Spezifikationen für das System Versichertenkarte, V1.0 vom 4. Februar 2008 |
| [SPEC-POST] | Implementierungsanleitung für die Versichertenkarte nach eCH-0064, V1.0.0 |
| [SPEC-SASIS] | SASIS - Versichertenkarte, Detailspezifikation, Version 1.4ech, Ausgabe: 09.08.2010 |
| [VVK] | Verordnung über die Versichertenkarte für die obligatorische Krankenpflegeversicherung vom 14. Februar 2007 (Stand am 1. Januar 2009), SR 832.105 |
| [VVK-EDI] | Verordnung des EDI über die technischen und grafischen Anforderungen an die Versichertenkarte für die obligatorische Krankenpflegeversicherung, vom 20. März 2008 (Stand am 1. April 2008), SR 832.105.1 |

2 Einleitung

2.1 Ziele

Der praktische Teil der Untersuchungen ergänzt die Erkenntnisse der [Expertise VK]. Die praktischen Untersuchungen wurden mit den folgenden Absichten durchgeführt:

- a) Die gemäss Art. 2 Abs. 2 VVK geforderte Kompatibilität der VK zu untersuchen.
- b) Technische Untersuchung, ob beide VK die in den jeweiligen Spezifikationen definierten Funktionalitäten grundsätzlich beherrschen. Dazu wurden Testabläufe definiert (siehe Kapitel 3.1), mit denen spezifische Funktionalitäten der VK untersucht wurden.
- c) Technische Untersuchung, ob sich beide Anbieter bezüglich Card-to-Card Authentisierung an ihre jeweiligen Spezifikationen halten. Abweichungen in Ablauf und Daten zu [eCH64] sind in [Expertise VK] bereits aufgeführt.
- d) Auf der Basis von Stichproben wurden spezifische Kommandos auf APDU-Ebene mit den jeweiligen Anbieterspezifikationen verglichen. Auf der Basis dieser Tests soll abgeschätzt werden können, ob die Anbieter der VK gemäss ihrer jeweiligen Spezifikation umgesetzt haben.

2.1.1 Abgrenzung

- a) Die praktischen Untersuchungen konnten im Rahmen des Auftrages nur punktuell durchgeführt werden. Eine vollständige Untersuchung aller technischen Gegebenheiten war im Rahmen des Auftrages nicht möglich.
- b) Die praktischen Untersuchungen haben sich auf die funktionalen Anforderungen der VK bezogen. Sicherheitsspezifische Untersuchungen wie beispielsweise die Regelung des Zugriffs auf die Daten gem. Art. 7 VVK wurden nicht untersucht.

2.2 Hilfsmittel und Durchführung

2.2.1 Praktische Untersuchungen ohne Card to Card Authentisierung

Alle praktischen Untersuchungen, welche in der [Expertise VK] aufgeführt sind, wurden mit Hilfsmittel der Firma Keyon durchgeführt und analysiert. Diese Untersuchungen umfassten die technischen Gegebenheiten der VK, welche keine Card to Card Authentisierung voraussetzten.

2.2.2 Praktische Untersuchungen mit Card to Card Authentisierung

Alle praktischen Untersuchungen, welche eine Card to Card Authentisierung voraussetzen (und Bestandteil dieses Dokumentes sind), wurden mit einer Software der Firma Albis Technologies AG in den Räumlichkeiten der Albis Technologies AG durchgeführt.

Die Firma Albis Technologies AG konnte zum Zeitpunkt der praktischen Untersuchungen als einzige Firma eine Software bereitstellen, mit der die VK der Post und die VK der SASIS unter Verwendung einer einzigen HPC untersucht werden konnte. Die Software der Post oder die Software der SASIS war nur in der Lage, die jeweiligen VK anzusprechen.

| | |
|---------|--|
| Hinweis | Es kann davon ausgegangen werden, dass in Zukunft weitere Anbieter eine Middleware bereitstellen, die eine nahtlose Integration der Versichertenkarten und der HPC in Applikationen ermöglichen. |
|---------|--|

2.2.3 Log-Dateien

Die mit der Software der Firma Albis Technologies AG aufgezeichneten Log-Dateien beinhalten Informationen, welche die Firma Albis Technologies AG als schützenswert erachtet. Sie können unter Unterzeichnung einer Geheimhaltevereinbarung von der Firma Albis Technologies AG bezogen werden.

Albis Technologies AG
Herr August Kaelin
Head of Departement Technology, R&D T
Albisriederstrasse 199
CH-8047 Zürich
+41 58 252 4275 Phone
August.Kaelin@albistechnologies.com

3 Versuchsbeschreibung

Die praktischen Tests wurden mit der Software „PDC Demonstrator“ der Firma Albis Technologies AG durchgeführt. Dazu wurde mit je einer Test-Versichertenkarte der beiden Anbieter jeweils ein festgelegter Versuchsablauf ausgeführt. Für beide VK wurde dieselbe Test-HPC-Karte verwendet, welche je ein Leistungserbringerzertifikat für die VK POST und eines für die VK SASIS enthält.

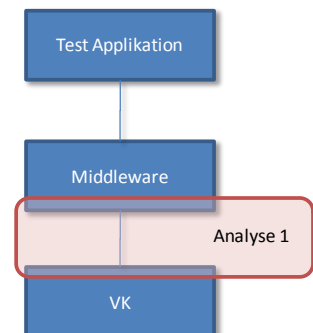
Die Kommunikation zwischen der PDC Demonstrator Software und den Versichertenkarten resp. der HPC Karte wurde mit dem integrierten APDU-Logger in eine Log-Datei aufgezeichnet.

3.1 Versuchsablauf

Die Untersuchungen umfassen die folgenden Anwendungsfälle.

1) Kommunikation zwischen der Applikation und der Versichertenkarte auf APDU Ebene

Es soll überprüft werden, ob die Versichertenkarte gemäss Spezifikation auf APDU Ebene umgesetzt wurde. Hierzu werden die folgenden Anwendungsfälle simuliert. Die Kommunikation zwischen der Applikation und der Versichertenkarte werden auf APDU Ebene aufgezeichnet.



a) Auslesen der Identifikations-Daten

Aus einer vorpersonalisierten Versichertenkarte sollen die Identifikations-Daten ausgelesen und angezeigt werden können.

b) Auslesen der administrativen Daten

Aus einer vorpersonalisierten Versichertenkarte sollen die administrativen Daten ausgelesen und angezeigt werden können.

c) Notfalldaten lesen/schreiben

Die Notfalldaten¹ sollen auf die Versichertenkarte geschrieben und wieder ausgelesen werden können. Zur Freischaltung dieser Funktionalität soll eine Card-to-Card-Authentisierung² mit einer HPC durchgeführt werden.

¹ Nur EF.BGTD (Transparent) und EF.ALLG (Linear variable)

² Die Sicherheitseigenschaften (Zugriffsregeln nach Artikel 42a Absatz 4 KVG) sind nicht Bestandteil der Untersuchungen. Die HPC soll mit einem Zertifikat eines Arztes personalisiert werden.

- 1) Schreiben der Notfalldaten mit einer HPC
- 2) Lesen der Notfalldaten mit einer HPC
- 3) Ändern (Löschen resp. Wiederbeschreiben) der Notfalldaten mit einer HPC

d) PIN-Schutz der Notfalldaten ein-/ausschalten

Der PIN-Schutz im Zusammenhang mit den Notfalldaten soll aktiviert und deaktiviert werden. Im Weiteren soll der PIN geändert werden.

| | |
|---------|---|
| Hinweis | Die beiden Abläufe unterscheiden sich, da das PIN Management der beiden VK unterschiedlich ist. |
|---------|---|

Ablauf bei der VK POST:

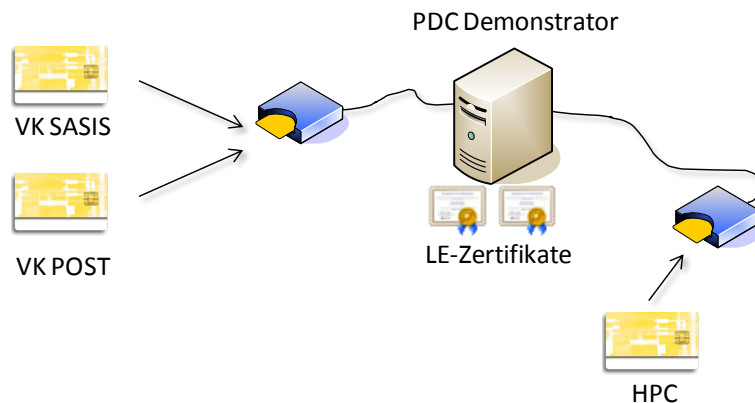
- 1) Erstmaliges Aktivieren des PIN-Schutzes und setzen des PIN
- 2) Deaktivieren des PIN-Schutzes
- 3) Erneutes Aktivieren des PIN-Schutzes und setzen des PIN
- 4) Deaktivieren des PIN-Schutzes
- 5) Erneutes Aktivieren des PIN-Schutzes und setzen des PIN
- 6) Lesen der Notfalldaten ohne vorherige PIN-Eingabe (analog Abschnitt c), Schritt 1 und 2 → muss fehlschlagen
- 7) Eingabe des PINs zum Schutz der Notfalldaten
- 8) Lesen der Notfalldaten (analog Abschnitt c), Schritt 1 und 2

Ablauf bei der VK SASIS:

- 1) Aktivieren des PIN-Schutzes für alle Notfalldatenfelder und setzen des PIN.
- 2) Lesen der Notfalldaten ohne vorherige PIN-Eingabe (analog Abschnitt c), Schritt 1 und 2 → muss fehlschlagen
- 3) Eingabe des PINs zum Schutz der Notfalldaten
- 4) Lesen der Notfalldaten (analog Abschnitt c), Schritt 1 und 2

3.2 Versuchsaufbau

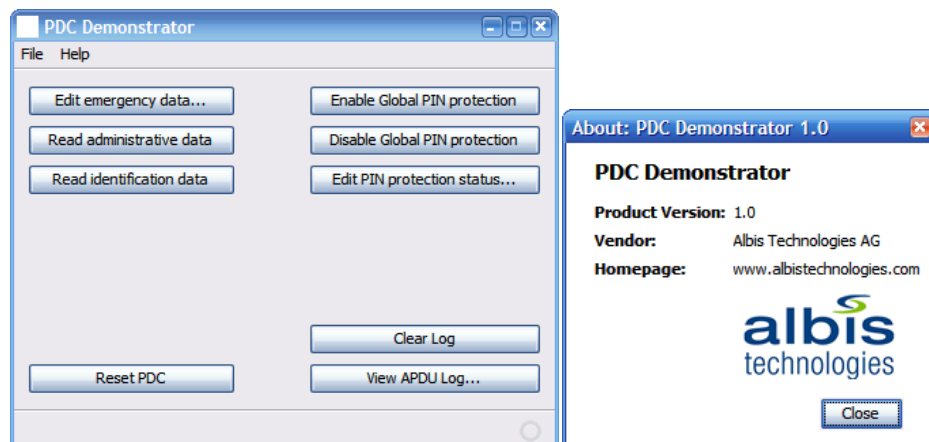
Der Versuchsaufbau besteht aus der Software "PDC Demonstrator", der mit den benötigten Leistungserbringer-Zertifikaten der beiden Anbieter ausgestattet ist, zwei Smartcard-Lesern, einer HPC und je einer VK der beiden Anbieter.



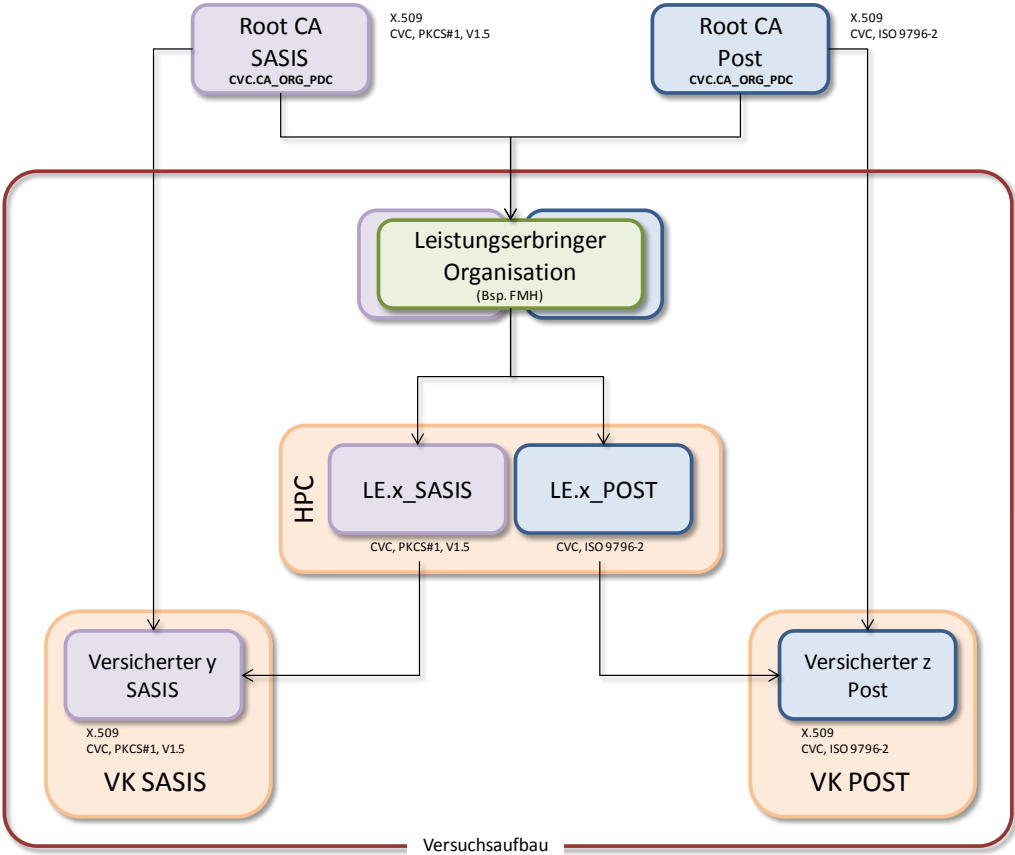
3.2.1 PDC Demonstrator

Mit dem PDC Demonstrator von der Firma Albis Technologies AG können folgende Funktionalitäten ausgeführt werden. Alle Funktionalitäten werden sowohl für die VK-POST wie auch für die VK-SASIS unterstützt:

- Lesen der Identifikations-Daten von der VK
- Lesen der administrativen Daten von der VK
- Durchführen der Card-to-Card-Authentisierung zwischen HPC und VK.
- Aktivieren und Deaktivieren des PIN-Schutzes der VK
- Lesen und Schreiben der Notfalldatenfelder auf der VK ohne Interpretation des Inhalts.



3.2.2 Übersicht über die Karten und ihre jeweiligen Zertifikate



Die beiden VK enthalten jeweils ein CA Zertifikat eines Anbieters (Post und SASIS). Die Test-HPC ist mit Leistungserbringer-Zertifikaten der jeweiligen Anbieter ausgestattet.

4 Ergebnisse

4.1 Übersicht

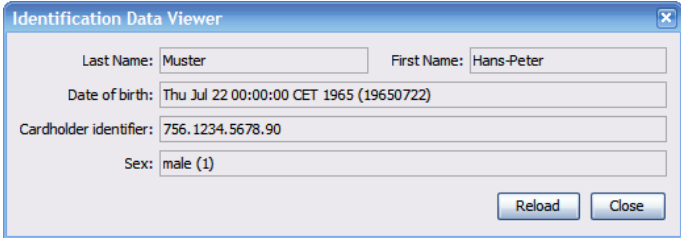
Die Durchführung der praktischen Tests hat folgendes gezeigt:

- Es konnte aufgezeigt werden, dass es mit einer entsprechenden Middleware und einer geeigneten HPC möglich ist, mit den VK beider Anbieter (Post und SASIS) umzugehen.
- Es konnte gezeigt werden, dass beide Karten die in den jeweiligen Spezifikationen definierten Funktionalitäten grundsätzlich beherrschen.
- Beide Anbieter halten sich bezüglich Card-to-Card Authentisierung an ihre jeweiligen Spezifikationen.
- Die Anbieter haben die Versichertenkarte gemäss ihren Spezifikationen umgesetzt.

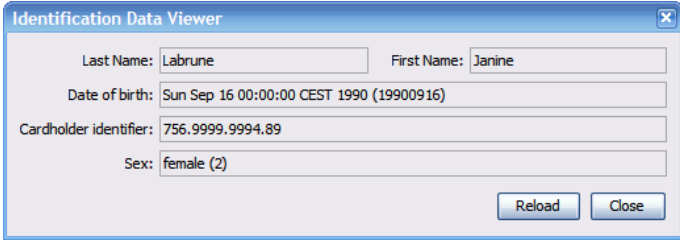
4.2 Erläuterung zu Ergebnissen

In den nachfolgenden Kapiteln werden die Ergebnisse der in Kapitel 3.1 definierten Versuchsabläufe aufgelistet. Dabei wird jeweils das zu beobachtende Verhalten der Karten im PDC Demonstrator beschrieben und es wird auf die entsprechenden Zeilen in den Log-Dateien verwiesen.

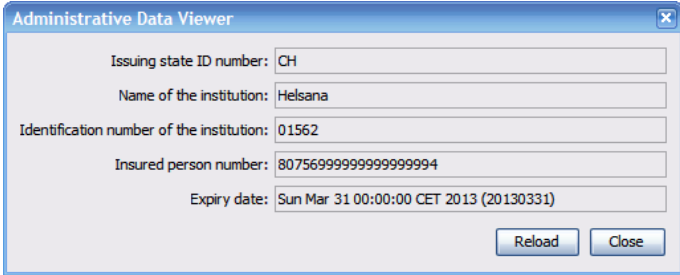
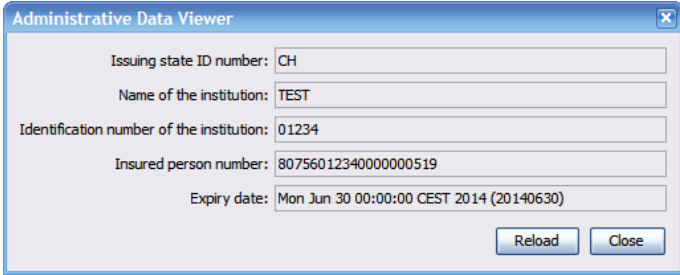
4.3 Auslesen der Identifikations-Daten

| A1. | Auslesen der Identifikations-Daten |
|------------------|---|
| [VK-POST] | Ergebnis |
| Zeilen 344 - 403 | <p>Die Identifikationsdaten können gelesen und angezeigt werden:</p>  |



| | |
|------------------|---|
| [Log VK-SASIS] | Ergebnis |
| Zeilen 204 - 249 | Die Identifikationsdaten können gelesen und angezeigt werden:  |

4.4 Auslesen der administrativen Daten

| | |
|------------------|---|
| A2. | Auslesen der administrativen Daten |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 406 - 465 | Die administrativen Daten werden gelesen und angezeigt:  |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 252 - 297 | Die administrativen Daten werden gelesen und angezeigt:  |



4.5 Notfalldaten lesen/schreiben

4.5.1 Card-to-Card Authentisierung durchführen

| | |
|-------------------|--|
| A3. | Card-to-Card Authentisierung durchführen |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 468 - 1112 | Die Card-to-Card-Authentisierung mit der HPC wurde erfolgreich durchgeführt. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 300 - 916 | Die Card-to-Card-Authentisierung mit der HPC wurde erfolgreich durchgeführt. |

4.5.2 Notfalldaten schreiben (EF.BGTD, transparent)

| | |
|--------------------|--|
| A4. | Notfalldaten schreiben (EF.BGTD, transparent) |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 1143 - 1215 | Es wurde der Text ‚Blutgruppe A‘ in EF.BGTD geschrieben. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 947 - 1003 | Es wurde der Text ‚Blutgruppe A‘ in EF.BGTD geschrieben. |

4.5.3 Notfalldaten lesen (EF.BGTD, transparent)

| | |
|--------------------|---|
| A5. | Notfalldaten lesen (EF.BGTD, transparent) |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 1218 - 1277 | Es wurde der Text ‚Blutgruppe A‘ aus EF.BGTD gelesen. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 1006 - 1093 | Es wurde der Text ‚Blutgruppe A‘ aus EF.BGTD gelesen. |

4.5.4 Notfalldaten schreiben (EF.ALLG, linear variable)

| | |
|--------------------|--|
| A6. | Notfalldaten schreiben (EF.ALLG, linear variable) |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 1308 - 1367 | Es wurde der Text ‚Heuschnupfen‘ in EF.ALLG geschrieben. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 1124 - 1168 | Es wurde der Text ‚Heuschnupfen‘ in EF.ALLG geschrieben. |

4.5.5 Notfalldaten lesen (EF.ALLG, linear variable)

| | |
|--------------------|---|
| A7. | Notfalldaten lesen (EF.ALLG, linear variable) |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 1370 - 1429 | Es wurde der Text ‚Heuschnupfen‘ aus EF.ALLG gelesen. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 1171 - 1230 | Es wurde der Text ‚Heuschnupfen‘ aus EF.ALLG gelesen. |

4.5.6 Notfalldaten löschen (EF.BGTD, transparent)

| | | | |
|--------------------|---|---------|---|
| A8. | Notfalldaten löschen (EF.BGTD, transparent) | | |
| [Log VK-POST] | Ergebnis VK POST | | |
| Zeilen 1460 - 1519 | Der zuvor geschriebene Inhalt ‚Blutgruppe A‘ wurde gelöscht. <table border="1" data-bbox="488 1364 1426 1462"> <tr> <td>Hinweis</td> <td>Gemäss Aussage von der Firma Albis Technologies AG kann die Dateigrösse von EF.BGTD nicht verändert werden. Beim Löschen werden die gespeicherten Daten mit Nullen (0x00) überschrieben</td> </tr> </table> | Hinweis | Gemäss Aussage von der Firma Albis Technologies AG kann die Dateigrösse von EF.BGTD nicht verändert werden. Beim Löschen werden die gespeicherten Daten mit Nullen (0x00) überschrieben |
| Hinweis | Gemäss Aussage von der Firma Albis Technologies AG kann die Dateigrösse von EF.BGTD nicht verändert werden. Beim Löschen werden die gespeicherten Daten mit Nullen (0x00) überschrieben | | |
| [Log VK-SASIS] | Ergebnis VK SASIS | | |
| Zeilen 1261 - 1317 | Der zuvor geschriebene Inhalt ‚Blutgruppe A‘ wurde gelöscht. | | |

4.5.7 Notfalldaten lesen (EF.BGTD, transparent)

| | |
|--------------------|--|
| A9. | Notfalldaten lesen (EF.BGTD, transparent) |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 1522 - 1581 | Es wurde ein leerer Text (alles Nullen) aus EF.BGTD gelesen. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 1320 - 1407 | Es wurde ein leerer Text (alles Nullen) aus EF.BGTD gelesen. |

4.5.8 Notfalldaten löschen (EF.ALLG, linear variable)

| | | | |
|--------------------|---|---------|---|
| A10. | Notfalldaten schreiben (EF.ALLG, linear variable) | | |
| [Log VK-POST] | Ergebnis VK POST | | |
| Zeilen 1612 - 1823 | <p>Der zuvor geschriebene Inhalt ‚Heuschnupfen‘ wird gelöscht.</p> <table border="1"> <tr> <td>Hinweis</td> <td>Gemäss Aussage von der Firma Albis Technologies AG kann auf der VK POST kein leerer Record geschrieben werden. Es muss mindestens ein (Null-) Byte geschrieben werden. (Siehe Zeilen 1612 – 1671).</td> </tr> </table> | Hinweis | Gemäss Aussage von der Firma Albis Technologies AG kann auf der VK POST kein leerer Record geschrieben werden. Es muss mindestens ein (Null-) Byte geschrieben werden. (Siehe Zeilen 1612 – 1671). |
| Hinweis | Gemäss Aussage von der Firma Albis Technologies AG kann auf der VK POST kein leerer Record geschrieben werden. Es muss mindestens ein (Null-) Byte geschrieben werden. (Siehe Zeilen 1612 – 1671). | | |
| [Log VK-SASIS] | Ergebnis VK SASIS | | |
| Zeilen 1438 - 1482 | <p>Der zuvor geschriebene Inhalt ‚Heuschnupfen‘ wird gelöscht.</p> <table border="1"> <tr> <td>Hinweis</td> <td>Gemäss Aussage von der Firma Albis Technologies AG können auf der VK SASIS einmal angelegte Record-basierte Datenfelder in ihrer Länge nicht geändert werden. Eine Applikation oder eine Middleware sollte daher immer die jeweilige Maximallänge eines Records anlegen, um ein allfälliges Überschreiben eines bestehenden Datensatzes mit einem grösseren Datensatz zu ermöglichen.</td> </tr> </table> | Hinweis | Gemäss Aussage von der Firma Albis Technologies AG können auf der VK SASIS einmal angelegte Record-basierte Datenfelder in ihrer Länge nicht geändert werden. Eine Applikation oder eine Middleware sollte daher immer die jeweilige Maximallänge eines Records anlegen, um ein allfälliges Überschreiben eines bestehenden Datensatzes mit einem grösseren Datensatz zu ermöglichen. |
| Hinweis | Gemäss Aussage von der Firma Albis Technologies AG können auf der VK SASIS einmal angelegte Record-basierte Datenfelder in ihrer Länge nicht geändert werden. Eine Applikation oder eine Middleware sollte daher immer die jeweilige Maximallänge eines Records anlegen, um ein allfälliges Überschreiben eines bestehenden Datensatzes mit einem grösseren Datensatz zu ermöglichen. | | |

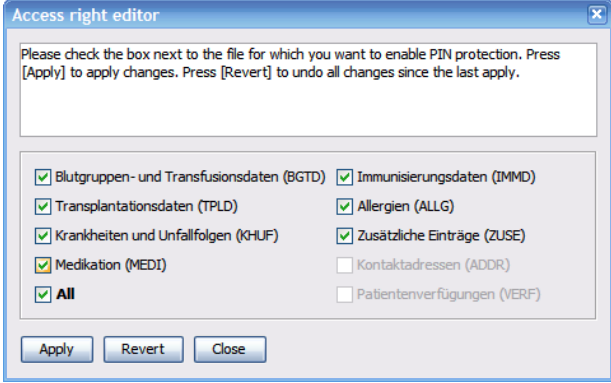
4.5.9 Notfalldaten lesen (EF.ALLG, linear variable)

| | |
|--------------------|--|
| A11. | Notfalldaten lesen (EF.ALLG, linear variable) |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 1826 - 1885 | Es wurde ein leerer Text aus EF.ALLG gelesen. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 1485 - 1544 | Es wurde ein leerer Text aus EF.ALLG gelesen. |



4.6 PIN setzen/löschen

4.6.1 PIN-Schutz aktivieren und PIN erstmalig setzen

| A12. | PIN-Schutz aktivieren und PIN erstmalig setzen |
|--------------------|---|
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 1888 -1995 | <p>Der PIN zum Schutz der Notfalldaten wurde aktiviert und auf ‚12345678‘ gesetzt.</p> <p>Bei der VK POST läuft das erstmalige Setzen des PINs leicht anders ab, als alle späteren PIN-Wechsel. Der Grund ist, dass die VK bei Auslieferung keinen PIN gesetzt hat. Der PIN kann jedoch nicht wieder gelöscht werden. Er kann nur geändert werden. Zum Löschen wird er in den Tests auf ‚00000000‘ gesetzt.</p> |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 1547 - 2502 | <p>Der PIN zum Schutz der Notfalldaten wurde aktiviert und auf ‚12345678‘ gesetzt.</p> <p>Die VK SASIS erlaubt ebenfalls wie die VK POST kein Löschen des PINs. Zum Löschen wird er in den Tests auf ‚00000000‘ gesetzt.</p> <p>Für den Test wurde zudem auf der VK SASIS der PIN-Schutz sämtlicher Notfall-Datenfelder explizit aktiviert. Zeilen 2136 - 2370</p>  |



4.6.2 PIN-Schutz deaktivieren und PIN löschen

| | |
|--------------------|---|
| A13. | PIN-Schutz deaktivieren und PIN löschen |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 1998 - 2105 | Der PIN zum Schutz der Notfalldaten wurde deaktiviert und gelöscht (auf ,00000000' gesetzt). |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 3385 - 3673 | Der PIN zum Schutz der Notfalldaten wurde deaktiviert und gelöscht (auf ,00000000' gesetzt). Weiter löscht der PDC Demonstrator den individuellen PIN-Schutz der einzelnen Notfall-Datenfelder wieder. |

4.6.3 PIN-Schutz erneut aktivieren und PIN setzen

| | |
|--------------------|---|
| A14. | PIN-Schutz aktivieren und PIN erneut setzen |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 2108 - 2215 | Der PIN zum Schutz der Notfalldaten wurde aktiviert und auf ,12345678' gesetzt. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 1547 - 2502 | Identisch mit Kapitel 4.6.1 |

4.6.4 PIN-Schutz deaktivieren und PIN löschen

| | |
|--------------------|--|
| A15. | PIN-Schutz deaktivieren und PIN löschen |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 2218 - 2325 | Der PIN zum Schutz der Notfalldaten wurde gelöscht (auf ,00000000' gesetzt). |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 3385 - 3673 | Analog zu Kapitel 4.6.1 |

4.7 PIN-geschützte Notfalldaten lesen

Die Karte wurde kurzzeitig aus dem Lesegerät entfernt. Sie befindet sich somit nicht mehr im authentisierten Zustand.

4.7.1 PIN-Schutz aktivieren und PIN setzen

| | |
|--------------------|---|
| A16. | PIN-Schutz aktivieren und PIN setzen |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 2328 - 2435 | Der PIN zum Schutz der Notfalldaten wurde aktiviert und auf ‚12345678‘ gesetzt. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 1547 - 2502 | Der PIN zum Schutz der Notfalldaten wurde aktiviert und auf ‚12345678‘ gesetzt. (Für den Test wurde zudem auf der VK SASIS der PIN-Schutz sämtlicher Notfall-Datenfelder explizit aktiviert. Zeilen 2136 - 2370) |

4.7.2 Card-to-Card Authentisierung durchführen

| | |
|--------------------|--|
| A17. | Card-to-Card Authentisierung durchführen |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 2505 - 3163 | Die Card-to-Card-Authentisierung wurde erfolgreich durchgeführt. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 2505 - 3163 | Die Card-to-Card-Authentisierung wurde erfolgreich durchgeführt. |

4.7.3 Notfalldaten lesen (EF.BGTD, transparent) ohne PIN

| | |
|--------------------|--|
| A18. | Notfalldaten lesen (EF.BGTD, transparent) |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 3267 - 3326 | Der Zugriff auf die Datei wird von der Karte verweigert. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 3166 - 3239 | Der Zugriff auf die Datei wird von der Karte verweigert. |



4.7.4 Freischalten der Notfalldaten durch Eingabe des PINs

| | |
|--------------------|---|
| A19. | Freischalten der Notfalldaten durch Eingabe des PINs |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 3357 - 3374 | Der PIN wurde von der Karte akzeptiert. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 3256 - 3272 | Der PIN wurde von der Karte akzeptiert. |

4.7.5 Notfalldaten lesen (EF.BGTD, transparent)

| | |
|--------------------|---|
| A20. | Notfalldaten lesen (EF.BGTD, transparent) |
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 2277 - 3436 | Der Zugriff auf die Datei ist freigeschaltet. Es wurde der zuletzt in Kapitel 4.5.6 gespeicherte leere Text aus EF.BGTD gelesen. |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 3275 - 3362 | Der Zugriff auf die Datei ist freigeschaltet. Es wurde der zuletzt in Kapitel 4.5.6 gespeicherte leere Text aus EF.BGTD gelesen. |

4.8 Verifikation: Card-to-Card Authentication and Authorization

In diesem Kapitel wird die Card-to-Card Authentisierung zwischen der HPC und der VK aufgeschlüsselt.

Es konnte verifiziert werden, dass sowohl mit der VK POST als auch mit der VK SASIS eine Card-to-Card Authentisierung und Autorisierung mit einer geeigneten HPC gemäss der Spezifikation des Anbieters erfolgreich durchgeführt werden kann.

| # | [eCH64] | [Log VK Post] | [Log VK SASIS] |
|----|--|--|------------------------|
| 1 | Selektieren und Auslesen des Chipcard Identifier Files | Zeilen 186 – 212 (ICCSN wird für Signatur auf HPC benötigt, Abweichung von [eCH64]) | n.a. |
| 2 | Übertragung des Chipcard Identifier Files der Versichertenkarte | | |
| 3 | Selektieren und Auslesen des CV Personenzertifikats des Versicherten | Nicht Teil des Tests | Nicht Teil des Tests |
| 4 | Übertragung des CV Personenzertifikats des Versicherten | | |
| 5 | Setzen des öffentlichen Root-Schlüssels der Versichererorganisation des Versicherten | | |
| 6 | Prüfen des CV Personenzertifikats des Versicherten | | |
| 6a | Überprüfung der Chipkartenseriennummer durch Vergleich der Nummern auf der Karte und im CV Personenzertifikat | | |
| 7 | Selektieren und Auslesen des Chipcard Identifier Files der Leistungserbringerkarte | | |
| 8 | Übertragung des Chipcard Identifier Files der Leistungserbringerkarte | | |
| 9 | Selektieren und Auslesen des CV Leistungserbringerzertifikats | Zeilen 817 - 867 (HPC) | Zeilen 635 – 722 (HPC) |
| 10 | Übertragung des CV Leistungserbringerzertifikat | | |
| 11 | Auslesen und Speichern der notwendigen Leistungserbringer-Attribute aus dem CV Leistungserbringerzertifikat | n.a. (Terminal) | n.a. (Terminal) |
| 12 | Anhand der Leistungserbringer-Attribute wird das entsprechende Leistungserbringerorganisationszertifikat selektiert. | n.a. (Terminal) | n.a. (Terminal) |
| 13 | Der Container für das ausgewählte Leistungserbringerorganisationszertifikat wird ausgewählt und soll beschrieben werden. | n.a. | n.a. |
| 14 | Übertragung und Speicherung des Leistungserbringerorganisationszertifikats | Zeilen 922 - 933 | Zeilen 740 - 751 |
| 15 | Das CV Leistungserbringerzertifikat wird der Versichertenkarte zur Verifikation bereitgestellt | Zeilen 948 - 959 | Zeilen 766 - 777 |
| 16 | Setzen des Root-Schlüssels der Versichererorganisation des Versicherten | Zeilen 909 - 920 | Zeilen 727 -738 |

| | | | |
|----|--|--------------------------|------------------------|
| 17 | Prüfen des CV Zertifikats der entsprechenden Leistungserbringerorganisation | Zeilen 922 - 933 | Zeilen 740 - 751 |
| 18 | Setzen des öffentlichen CA-Schlüssels der entsprechenden Leistungserbringerorganisation | Zeilen 935 - 946 | Zeilen 753 - 764 |
| 19 | Prüfen des CV Leistungserbringerzertifikats | Zeilen 948 - 959 | Zeilen 766 - 777 |
| 20 | Zwischenspeicherung des Karteninhaberautorisierungsmerkmalswertes CHAn , welches im Leistungserbringerzertifikat eingebunden ist | Zeilen 967 - 978 | Zeilen 785 - 796 |
| 21 | Zufallszahl erzeugen | Zeilen 994 - 1006 | Zeilen 798 - 810 |
| 22 | Zufallszahl übermitteln | Zeilen 1075 - 1087 (HPC) | Zeilen 835 - 894 (HPC) |
| 23 | Zufallszahl signieren | | |
| 24 | Signierte Zufallszahl übermitteln | Zeilen 1095 - 1106 | Zeilen 897 - 913 |
| 25 | Verifikation der Signatur der signierten Zufallszahl | | |
| 26 | Der Karteninhaberautorisierungsmerkmalswert CHAn wird freigeschaltet | | |
| 27 | Datenaustausch zwischen dem Lesegerät/Anwendungsmodul und der Versichertenkarte | Zeilen 1106 ff. | Zeilen 913 ff. |

4.9 Verifikation: Stichproben der APDU-Kommandos

Es wird Stichprobenweise untersucht, ob die Karten sich an die anbieterspezifische Spezifikationen [SPEC-POST] und [SPEC-SASIS] halten.

4.9.1 File-ID von EF.BGTD

| A21. | Kontrolle der File-ID von EF.BGTD |
|--------------------|---|
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 1159 - 1185 | <p>Ergebnis gemäss Spezifikation (Kapitel 2.16.1)</p> <pre> Date: Fri Dec 03 11:03:41 CET 2010 Card: PDC Helsana Command: SELECT FILE CLA: 0x00 INS: 0xa4 P1: 0x01 P2: 0x00 Le: 0x0100 Sent data: DF01 Sent data length: 2 Received data: 6F0A8406D75683210500A500 Received data length: 12 SW: Command executed correctly (0x9000) Date: Fri Dec 03 11:03:41 CET 2010 Card: PDC Helsana Command: SELECT FILE CLA: 0x00 INS: 0xa4 P1: 0x02 P2: 0x04 Le: 0x0100 Sent data: 1F01 Sent data length: 2 Received data: 62198002012EC502000C82010183021F0188008A0105A1038B0106 Received data length: 27 SW: Command executed correctly (0x9000) </pre> |



| [Log VK-SASIS] | Ergebnis VK SASIS |
|------------------|---|
| Zeilen 918 - 961 | <p>Ergebnis gemäss Spezifikation (Kapitel 2.16.1)</p> <p>Date: Fri Dec 03 11:27:51 CET 2010 Card: PDC SASIS Command: SELECT FILE CLA: 0x00 INS: 0xa4 P1: 0x01 P2: 0x00 Le: 0x0100 Sent data: DF01 Sent data length: 2 Received data: 6225820238418A01078302DF0181025C3F8406D75683210500860CA4000000FFF FE0008000FFFF Received data length: 39 SW: Command executed correctly (0x9000)</p> <p>Date: Fri Dec 03 11:27:51 CET 2010 Card: PDC SASIS Command: SELECT FILE CLA: 0x00 INS: 0xa4 P1: 0x02 P2: 0x00 Le: 0x0100 Sent data: 1F01 Sent data length: 2 Received data: 62408202014180040000012E8A010783021F018102012E8624B0100100FFFFCA1 00100FFFA4000000FFFFD6100200FFFF26000000FFFF28000000FFFA5038901 10 Received data length: 66 SW: Command executed correctly (0x9000)</p> |



4.9.2 Inhalt von EF.VERSION

| A22. | Kontrolle des Inhalts von EF.VERSION |
|------------------|---|
| [Log VK-POST] | Ergebnis VK POST |
| Zeilen 689 - 701 | <p>Entspricht Spezifikation (Kapitel 2.11)</p> <p>Date: Fri Dec 03 11:03:11 CET 2010 Card: PDC Helsana Command: READ BINARY CLA: 0x00 INS: 0xb0 P1: 0x00 P2: 0x00 Le: 0x0100 Sent data: Sent data length: 0 Received data: 44535080 Received data length: 4 SW: Command executed correctly (0x9000)</p> |
| [Log VK-SASIS] | Ergebnis VK SASIS |
| Zeilen 507 - 519 | <p>Entspricht Spezifikation (Kapitel 4.10)</p> <p>Date: Fri Dec 03 11:27:22 CET 2010 Card: PDC SASIS Command: READ BINARY CLA: 0x00 INS: 0xb0 P1: 0x00 P2: 0x00 Le: 0x0100 Sent data: Sent data length: 0 Received data: 53415380 Received data length: 4 SW: Command executed correctly (0x9000)</p> |

4.9.3 APDU-Befehlssequenzen zur Validierung der LE-Zertifikate

| A23. | Kontrolle der APDU-Befehlssequenzen zur Validierung der LE-Zertifikate | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------------|--|------|------|------|---|----|--------------|----|------|------|------|------|------|---|---|-----|-----|----|----|----|--------------|----|------|------|------|------|------|---|---|
| [Log VK-POST] | Ergebnis VK POST | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Zeilen 909 - 959 | <p>Entspricht Spezifikation (Kapitel 3.4.1)</p> <p>16 (B) MSE SET PK.CA_ORG_PDC_m</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>CLA</th> <th>INS</th> <th>P1</th> <th>P2</th> <th>Lc</th> <th>Command Data</th> <th>Le</th> </tr> </thead> <tbody> <tr> <td style="background-color: #ffff00;">,00'</td> <td style="background-color: #ffff00;">,22'</td> <td style="background-color: #ffff00;">,81'</td> <td style="background-color: #ffff00;">,B6'</td> <td style="background-color: #ffff00;">,12'</td> <td style="background-color: #90ee90;">,83 10' CHR(PK.CA_ORG_PDC_m)</td> <td style="background-color: #d9d9d9;">-</td> </tr> </tbody> </table> <p>Date: Fri Dec 03 11:03:13 CET 2010 Card: PDC Helsana Command: MANAGE SECURITY ENVIRONMENT (MSE)</p> <p>CLA: 0x00 INS: 0x22 P1: 0x81 P2: 0xb6</p> <p>Sent data: 831000000000000000000000000000004348445350600109 Sent data length: 18 Received data: Received data length: 0 SW: Command executed correctly (0x9000)</p> <p>17 (B) PSO Verify Certificate CVC.CA_ORG_HPC_m</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>CLA</th> <th>INS</th> <th>P1</th> <th>P2</th> <th>Lc</th> <th>Command Data</th> <th>Le</th> </tr> </thead> <tbody> <tr> <td style="background-color: #ffff00;">,00'</td> <td style="background-color: #ffff00;">,2A'</td> <td style="background-color: #ffff00;">,00'</td> <td style="background-color: #ffff00;">,AE'</td> <td style="background-color: #ffff00;">,CB'</td> <td style="background-color: #90ee90;">,5F37 8180' Signatur ,5F38 44' PK_Part2 PK_exp⁷</td> <td style="background-color: #d9d9d9;">-</td> </tr> </tbody> </table> <p>Date: Fri Dec 03 11:03:13 CET 2010 Card: PDC Helsana Command: PERFORM SECURITY OPERATION (PSO)</p> <p>CLA: 0x00 INS: 0x2a P1: 0x00 P2: 0xae</p> <p>Sent data: 5F3781801B5E1394CD7905FB69F8960BB51CE407C2549EC76AF8AD40BCEEEB67A AB2D42686C48A7865E7AEC05D42642FE5FEC9D00AFE32422728152E492EC09297 EAA8E8553BFC7C940C37F52CAF37084FD27950282AEF6497938BD4778C3A36A64 C97CFEDA1C93281476A3924798D447DFFB11C3E4594E3AE21EC133A0021F4F34E 02BF5F3844757A346264CDB5CC4E3237F1538AB1E4BD1129FA86A818838CD1E9</p> | CLA | INS | P1 | P2 | Lc | Command Data | Le | ,00' | ,22' | ,81' | ,B6' | ,12' | ,83 10' CHR(PK.CA_ORG_PDC _m) | - | CLA | INS | P1 | P2 | Lc | Command Data | Le | ,00' | ,2A' | ,00' | ,AE' | ,CB' | ,5F37 8180' Signatur ,5F38 44' PK_Part2 PK_exp ⁷ | - |
| CLA | INS | P1 | P2 | Lc | Command Data | Le | | | | | | | | | | | | | | | | | | | | | | | |
| ,00' | ,22' | ,81' | ,B6' | ,12' | ,83 10' CHR(PK.CA_ORG_PDC _m) | - | | | | | | | | | | | | | | | | | | | | | | | |
| CLA | INS | P1 | P2 | Lc | Command Data | Le | | | | | | | | | | | | | | | | | | | | | | | |
| ,00' | ,2A' | ,00' | ,AE' | ,CB' | ,5F37 8180' Signatur ,5F38 44' PK_Part2 PK_exp ⁷ | - | | | | | | | | | | | | | | | | | | | | | | | |

| | <p>DECA2B8B00010001</p> <p>Sent data length: 203</p> <p>Received data:</p> <p>Received data length: 0</p> <p>SW: Command executed correctly (0x9000)</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------|--|---|-----|---|---|----|--|--|--|-----|-----|----|----|----|------|----|-----|-----|-----|-----|----|---------------------------------------|---|---------|--|---|--|--|--|--|--|-----|-----|----|----|----|------|----|-----|-----|-----|-----|-------|---|---|
| [Log VK-SASIS] | <p>Ergebnis VK SASIS</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Zeilen 2974 - 3024 | <p>Entspricht Spezifikation (Kapitel 6.2.16 – 6.2.19)</p> <p>6.2.16 Setzen des öffentlichen Root-Schlüssels der neutralen CA_ROOT_VK</p> <table border="1" data-bbox="499 815 1406 920"> <thead> <tr> <th colspan="2">PDC</th> <th colspan="6">MSE SET <PuK.CA_ROOT_VK> ← (CVC.CA_ROOT_VK)</th> </tr> <tr> <th>CLA</th> <th>INS</th> <th>P1</th> <th>P2</th> <th>Lc</th> <th>Data</th> <th>Le</th> </tr> </thead> <tbody> <tr> <td>00h</td> <td>22h</td> <td>81h</td> <td>B6h</td> <td>12</td> <td>{'83' '10' CHR(CVC.CA_ROOT_VK)}</td> <td>-</td> </tr> </tbody> </table> <p>Date: Fri Dec 03 11:29:50 CET 2010</p> <p>Card: PDC SASIS</p> <p>Command: MANAGE SECURITY ENVIRONMENT (MSE)</p> <p>CLA: 0x00</p> <p>INS: 0x22</p> <p>P1: 0x81</p> <p>P2: 0xb6</p> <p>Sent data: 8310434852564B6030313233343536373839</p> <p>Sent data length: 18</p> <p>Received data:</p> <p>Received data length: 0</p> <p>SW: Command executed correctly (0x9000)</p> <p>6.2.17 Prüfen des CVC-Zertifikats der entsprechenden Leistungserbringer-Herausgeberorganisation</p> <table border="1" data-bbox="499 1496 1406 1601"> <thead> <tr> <th colspan="2">PDC (9)</th> <th colspan="6">PSO VERIFY CERTIFICATE (CVC.CA_ORG_HPC_m)</th> </tr> <tr> <th>CLA</th> <th>INS</th> <th>P1</th> <th>P2</th> <th>Lc</th> <th>Data</th> <th>Le</th> </tr> </thead> <tbody> <tr> <td>00h</td> <td>2Ah</td> <td>00h</td> <td>BEh</td> <td>026Bh</td> <td>7F4E{Certificate Body} 5F37{Signature}</td> <td>-</td> </tr> </tbody> </table> <p>Date: Fri Dec 03 11:29:51 CET 2010</p> <p>Card: PDC SASIS</p> <p>Command: PERFORM SECURITY OPERATION (PSO)</p> <p>CLA: 0x00</p> <p>INS: 0x2a</p> <p>P1: 0x00</p> <p>P2: 0xbe</p> <p>Sent data: 7F4E8201615F2901024210434852564B60303132333435363738397F498201120</p> | PDC | | MSE SET <PuK.CA_ROOT_VK> ← (CVC.CA_ROOT_VK) | | | | | | CLA | INS | P1 | P2 | Lc | Data | Le | 00h | 22h | 81h | B6h | 12 | {'83' '10' CHR(CVC.CA_ROOT_VK)} | - | PDC (9) | | PSO VERIFY CERTIFICATE (CVC.CA_ORG_HPC _m) | | | | | | CLA | INS | P1 | P2 | Lc | Data | Le | 00h | 2Ah | 00h | BEh | 026Bh | 7F4E{Certificate Body} 5F37{Signature} | - |
| PDC | | MSE SET <PuK.CA_ROOT_VK> ← (CVC.CA_ROOT_VK) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CLA | INS | P1 | P2 | Lc | Data | Le | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 00h | 22h | 81h | B6h | 12 | {'83' '10' CHR(CVC.CA_ROOT_VK)} | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PDC (9) | | PSO VERIFY CERTIFICATE (CVC.CA_ORG_HPC _m) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CLA | INS | P1 | P2 | Lc | Data | Le | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 00h | 2Ah | 00h | BEh | 026Bh | 7F4E{Certificate Body} 5F37{Signature} | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |



```

6076085740522020181820100C5E22C3771986674F55638A7A68B1DB42B32C1E9
C763E9330E8F8E9A93788946994ABC3D875EE794A76CF94B6F8FDA23EDFF2B82
7DF0D9011EA343B561730D029D022686E3D4BD373C0E129C5291F5373AD769E00
8387FB374482E58BBBF52C5684CC33CAC4C8004F031C70D094688D2D31C0EDF9D
A0126B01C09DCD86B8AA1ED8025EF214B1ACF2864B15FD1959F905B2DE4F1B3D0
BA83A300B4131DCA156E5FCBE8B472971AA1A349846D0E74A0DFFB80746647178
2AF8F585932C154898B87F2A0FDD834F98C7D3F98C702E44FF50A3A9E7B6E6504
8042099CE68D1C84742E870E504358B3508BF3979DEEB2352EF3D42B62F71DF08
6DAB052611D72D5FD82030100015F201043484850546139383736353433323130
7F4C0C0607608574052201015301005F25060001000100015F240601020102010
25F378201007CABF21DEC3F46BEF1C0CEBFB9ED25E3DA04BAD02610F98CE4710B
214B6B466C12B7236E0E4805A4E872D5D11D451A8D3372C46EB5B974424E4D6DF
AB7627810D824710AAA19E76607245F77AE7166B21EC09BAEB72CB0064D82C399
1C1E6001DF7EB0357382B7788B6E94E5E1B26FC85DE669C616F3692979275D2C9
ADC7BAE9332381CC4C231743B7FB86B4C984B7B34399E30DA8DCA196878B58C8E
1642EFA454FCA29E2D686367F1D70D66E18A67504D3D1D6E130AA2F33330953A7
D1551DCC1AE5C31F4DDCB3B94ED0C22E2EB683A90BBC232EB9D54F816EC830D41
E5975FE294B50BF15D8390844E12F3D908012BDBD42AB8F7E7605D37DFB0BE6FA
07A
Sent data length: 619
Received data:
Received data length: 0
SW: Command executed correctly (0x9000)

```

6.2.18 Setzen des CA-Schlüssels der entsprechenden Leistungserbringer-Herausgeberorganisation

| PDC | | MSE SET <PuK.CA_ORG_HPC _m <← (CVC.CA_ORG_HPC _m)> | | | | | | |
|-----|-----|---|-----|-----|--------------|-----------------------------------|----|---|
| CLA | INS | P1 | P2 | Lc | Data | | Le | |
| 00h | 22h | 81h | B6h | 12h | {'83' '10' | CHR(CVC.CA_ORG_HPC _m) | | - |

```

Date: Fri Dec 03 11:29:51 CET 2010
Card: PDC SASIS
Command: MANAGE SECURITY ENVIRONMENT (MSE)
CLA: 0x00
INS: 0x22
P1: 0x81
P2: 0xb6
Sent data: 831043484850546139383736353433323130
Sent data length: 18
Received data:
Received data length: 0
SW: Command executed correctly (0x9000)

```



6.2.19 Prüfen des CVC-Leistungserbringerzertifikats

| PDC (10) | | PSO VERIFY CERTIFICATE (CVC.HPC) | | | | | |
|----------|-----|----------------------------------|-----|-------|---|--|----|
| CLA | INS | P1 | P2 | Lc | Data | | Le |
| 00h | 2Ah | 00h | BEh | 026Dh | 7F4E{Certificate Body} 5F37{Signature} | | - |

Date: Fri Dec 03 11:29:51 CET 2010

Card: PDC SASIS

Command: PERFORM SECURITY OPERATION (PSQ)

CLA: 0x00

INS: 0x2a

P1: 0x00

P2: 0xbe

Sent data:

7F4E8201635F2901034210434848505461393837363534333231307F498201120
6076085740522020181820100D16002CEBD0C2FF51F7786AEB4D0AF9E288C2BC1
97190B4EC75A3EAE8C680C94C934966D4ACF6A8531A6F5A26B1405A289D8B5DE1
C3B28DE398759041F54752AE4F9D2372296030B12A33B2BEBCCF71F0F7399B77D
50DD456C93CA6066B43A6C16A8170E72D87A74D09252DC3CECBB4447D166A276E
89D43710C76461358FC64D114B1EFA46FEBA1A74C756ED02E6B10FAE6CA3A49FC
2F5F3EC16CE8138A6687F6726D6EC274FD16E3726507D1F33564ECD797CC85D2
58832D7A3AB084604AFEB48D22F06B0C49D1C32F29D589A81261979F92EF5B089
377F6347D25F0BC85F0A3DF8A89466A4F090BAB235C23F0DC9CF07E643E9DE4F5
1D74D134FA6A43B9B82030100015F201201020304050607000001020304050607
08097F4C0C0607608574052201015301015F25060009000302075F24060104000
302075F378201006D5C7E3E4E9DCA39FF5E31385BB24FBEDAD7EF00702F7EA354
D162304A6AC245E10B3E43B0658B868934367DB8B2B1EE59B15F4A4C4D78BB083
F3A54BBBF18041425A14FB01485735756104383D9CF8877774CD93B9C61851169
6349F9B1405454A78C6BC3AD2AC5148874D1F63CBF7C216A9C21FBE8EA2D2D9D5
BF4FC1A0438B45680FF60DF16E4636B406BFF8EE2140508C15B72DD100EB7EC3C
90AA334BE00893C41CF0159AE23A043D5432BF078DA8F98195CD2B0484EA8FE7D
5A8FFCED231A3C35A518979B4EE6CAF8E0BC418A2211E52DAB370EE92211D14FF
2E66F669C79C08633E4F8DE411363ACB032F829B56CEFAFC5CF9E7A24AFFD88A7
7B8AD07

Sent data length: 621

Received data:

Received data length: 0

SW: Command executed correctly (0x9000)