T7 e.V.

AK Technik

24. Juli 2007

Rahmenspezifikation Kartenmanagement T7 - Nachladen qualifizierter Zertifikate

Version 1.0.1

Freigegeben

Version	Datum	Beschreibung	Bearbeiter
1.0	01.02.2007	Durch den technischen Arbeitskreis des T7 e.V. (TAT7) erarbeitete Rahmenspezifikation.	Hajo Bickenbach
1.0.1	24.07.2007	Fehlerkorrektur: In Tabelle 4 wird im Feld Common Name für Gütesiegelzertifikate der Eintrag „ICCSN“ ersetzt durch „ICSN“, die Seriennummer des Chips.	Hajo Bickenbach

Geschäftsstelle Bonn

Wilhelmstraße 40-42

53111 Bonn

Germany

www.t7-isis.org

info@t7-isis.org

1 Management Summary

Im Verlauf der aktuellen großen Bundesprojekte „elektronische Gesundheitskarte“ und „digitaler Personalausweis“ wird eine große Anzahl Chipkarten ausgegeben. Im Rahmen der e-Card-Initiative der Bundesregierung sollen diese mit der Funktion der qualifizierten Signatur versehen werden. Dazu dient die Signaturanwendung, die auf die eCard aufgebracht wird. Bei Ausgabe der eCard an den Karteninhaber kann diese Signaturanwendung bereits vollständig angelegt und sofort nutzbar sein, oder die eCard ist lediglich für die Erstellung von qualifizierten elektronischen Signaturen vorbereitet.

In dieser Spezifikation werden die technischen Voraussetzungen und Rahmenbedingungen beschrieben, die erfüllt sein müssen, um aus einer vorbereiteten eine nutzbare Signaturkarte zu erstellen, mit der qualifizierte elektronische Signaturen erzeugt werden können. Insbesondere werden bei der Produktion auf die eCard aufzubringende Merkmale beschrieben, mit deren Hilfe später, wenn sich die Chipkarte beim Karteninhaber befindet, ein qualifiziertes Zertifikat „nachgeladen“ werden kann. Auf Basis dieser Merkmale sind alle am Markt vertretenen Zertifizierungsdiensteanbieter (ZDA[1]) in der Lage, qualifizierte Zertifikate für jede so vorbereitete Chipkarte zu erzeugen. Durch das gewählte Vorgehen ist sichergestellt, dass die Zertifizierungsdiensteanbieter die Zertifikate weitgehend im Rahmen der bereits existierenden und erprobten Prozesse und damit kostengünstig erzeugen können.

[1] Unter einem Zertifizierungsdiensteanbieter (ZDA) wird in diesem Dokument immer eine Instanz verstanden, die laut Bundesnetzagentur dazu berichtigt ist, qualifizierte Signaturzertifikate auszustellen.

2 Beteiligte Unternehmen und Personen

Mitwirkende Personen, Unternehmen:

1.	Blick, Markus	T-Systems International GmbH
2.	Buchhalter, Sabine	Deutsche Post Com GmbH
3.	Byszio, Frank	D-TRUST GmbH
4.	Kirch, Stefan	T-Systems International GmbH
5.	Kux, Dr. Georg	Deutscher Sparkassen Verlag GmbH
6.	Lindemann, Rolf	TC TrustCenter GmbH
7.	Obermüller, Markus	Deutscher Sparkassen Verlag GmbH
8.	Pfeuffer, Dieter	Datev e.G.
9.	Ueberberg, Dr. Johannes	Deutscher Sparkassen Verlag GmbH

Editor (en):

	Bickenbach, Hajo	2B Advice GmbH

3 Zielsetzungen

Mit der elektronischen Gesundheitskarte, dem elektronischen Bundespersonalausweis, der Jobcard, dem Heilberufeausweis und anderen großen Kartenprojekten entsteht die Situation, dass in naher Zukunft große Stückzahlen von Chipkarten ausgegeben werden.

In der eCard-Initiative will die Bundesregierung die aktuellen Chipkarten-Projekte harmonisieren. Die Bundesregierung und die Wirtschaft streben im Rahmen der eCard Initiative u.a. an, dem Bürger die im Rahmen der genannten Projekte auszugebenden Karten und Ausweise für die Nutzung mit der qualifizierten elektronischen Signatur zur Verfügung zu stellen. Ziel ist es, in der Fläche für eine Vielzahl von Anwendungsszenarien die Nutzung der elektronischen Signatur zu ermöglichen und damit die IT-Sicherheit weiter zu verbessern.

Eine Ausprägung dieser Initiative besteht deshalb darin, dafür zu sorgen, dass ausgegebene Karten für den Einsatz als Signaturkarte zumindest vorbereitet sind. Die eCards sollen teilweise direkt mit den Schlüsseln und Zertifikaten nach einer Registrierung des Bürgers so ausgegeben werden, dass sie vom Bürger direkt als Signaturkarten einzusetzen sind. Teilweise werden die Karten aber auch nur so vorbereitet, dass die Identität der Bürger erst im Nachgang mit dem öffentlichen Schlüssel auf der Karte verknüpft wird, die Karte also bei Ausgabe nur „vorbereitet“ ist (vorbereitete bzw. schlafende Signaturkarte). Für diesen zweiten Fall fehlt es zum Zeitpunkt der Übergabe an den Karteninhaber noch an einer gemäß Signaturgesetz geforderten Verknüpfung der Identität des Karteninhabers mit dem öffentlichen Schlüssel auf der Karte und der Ausstellung eines Zertifikates über diese Verknüpfung.

Ziel dieser Spezifikation ist es, die technischen Voraussetzungen und Rahmenbedingungen darzustellen, die erfüllt sein müssen, um vorbereitete Signaturkarten signaturgesetzkonform zu komplettieren.

Dieser Vorgang wird als Nachladen bezeichnet, da aus Sicht des Karteninhabers eine weitere Funktion der bereits in seinem Besitz befindlichen Karte „nachgeladen“ wird, obwohl technisch in Wirklichkeit ein sehr viel komplexerer Vorgang zu beschreiben ist.

Diese Spezifikation bezieht sich allgemein auf eine eCard und ist unabhängig von einem speziellen Kartenprofil. Dabei werden auch erst in Zukunft verfügbare technische Umsetzungsmöglichkeiten, wie sie z.B. beim Personalausweis(dPA) zum Tragen kommen sollen, beschrieben und (teilweise zunächst optional) berücksichtigt. Im Hauptteil werden deshalb die Anforderungen an die Chipkarten, die Prozesse, etc. allgemein für beliebige Kartenprofile beschrieben.

Da die Anforderungen an die Chipkarten und an die Prozesse nicht unabhängig von dem konkreten Kartenprofil (also z.B. eGK oder dPA) festgelegt werden können, erfolgen die dafür notwendigen konkreten Festlegungen für jedes Kartenprofil gesondert in technischen Anhängen.

Zum Zeitpunkt der Version 1.0 dieses Dokumentes gibt es lediglich einen gesonderten Anhang für die eGK [QES eGK]. Eine Erstellung von technischen Anhängen für andere Kartenprofile ist erwünscht und erfolgt bei Vorliegen der Spezifikation dieser Kartenprofile.

4 Umfang der notwendigen Vereinbarungen

Die Herleitung des Umfangs der im Kontext des Nachladens qualifizierter Zertifikate notwendigen Verträge zwischen den beteiligten Rollen erfolgt in einem getrennten Dokument.

Dieses Dokument ist am 28.02.2006 vom Arbeitskreis Recht des T7 e.V. in der Version 1.0 herausgegeben und trägt den Titel

„Kurzgutachten notwendige Vertragsverhältnisse bei der Nachladbarkeit von Zertifikaten."

5 Rollenmodell und Ablaufbeschreibung

5.1 Beteiligte

Um den Prozess erläutern zu können, ist es zunächst hilfreich, die am Prozess beteiligten Instanzen und ihre Rollen im Prozess zu beschreiben.

Es wird zwischen den folgenden fünf Rollen unterschieden:

- Herausgeber der Chipkarte
- Produzent der Chipkarte
- ZDA-VP
- ZDA-NL
- Karteninhaber

Als Herausgeber einer Chipkarte wird nach dieser Spezifikation eine Institution verstanden, die die Chipkarte zu einem primären Zweck ausgibt, z.B. als elektronischer Personalausweis (dPA) oder als elektronische Gesundheitskarte (eGK).

Der Produzent produziert und personalisiert die Chipkarte im Sinne des primären Anwendungszwecks.

Die folgenden Schritte dienen der Personalisierung der Chipkarte in Bezug auf die Anwendung als qualifizierte elektronische Signaturkarte.

Der ZDA-VP ist im Rahmen der Kartenproduktion für das Aufbringen eines Sicherheitsankers, des Schlüsselpaares für das qualifizierte Zertifikat und weiterer Merkmale auf die Chipkarte verantwortlich. Diese Vorbereitung zur eigentlichen Personalisierung wird als Vorpersonalisierung bezeichnet.

Als Sicherheitsanker werden in dieser Spezifikation nur CV-Zertifikate (CVC) und Gütesiegel (GS) zugelassen.

Der ZDA-NL ist der Herausgeber des qualifizierten Zertifikats. Er bestimmt den Nachladeprozess und nutzt dabei den auf der Chipkarte im Rahmen der Vorpersonalisierung aufgebrachten Sicherheitsanker sowie den öffentlichen Schlüssel des Schlüsselpaares für das qualifizierte Zertifikat.

Der Karteninhaber erhält vom Herausgeber seine Chipkarte in einem vorpersonalisierten Transport-Zustand und kann diese nach erfolgreicher Ausführung des Nachladeverfahrens in nunmehr personalisierter Form als qualifizierte elektronische Signaturkarte nutzen.

5.2 Abläufe zwischen den Beteiligten

Wenn eine Chipkarte geeignet und dafür vorgesehen ist, nach der Ausgabe an den Chipkarteninhaber zusätzlich mit der Funktion einer qualifizierten elektronischen Signatur versehen zu werden, können die Verfahren dieser Spezifikation angewandt werden.

Der Herausgeber (z.B. die Bundesrepublik Deutschland für den dPA oder eine Krankenkasse für eine eGK) initiiert die Ausgabe und benötigt zu diesem Zweck einen **Produzenten** und

einen **ZDA-VP**. Der Produzent und der ZDA-VP werden typischerweise die Funktionen Produktion der Chipkarte, Personalisierung im Sinne des primären Anwendungszwecks und Vorpersonalisierung im Sinne dieser Spezifikation zusammen erledigen.

Um nach Übergabe der Chipkarte an den Inhaber den Nachladeprozess anstoßen zu können, müssen vor der Übergabe durch einen ZDA im Rahmen der Vorpersonalisierung (**ZDA-VP**) bereits Sicherheitsanker auf die Chipkarte aufgebracht werden sowie ggf. weitere Merkmale der Chipkarte gesetzt werden. Dazu gehört, dass Schlüssel für die Erzeugung qualifizierter elektronischer Signaturen vorab nur in der Verantwortung eines ZDA-VP generiert werden dürfen.

Die mit der Vorpersonalisierung verbundenen sicherheitsrelevanten Aktivitäten müssen deshalb im Rahmen des Sicherheitskonzepts des ZDA-VP ausgeführt werden. Hierzu werden typischerweise Teil-Sicherheitskonzepte durch die beteiligten Akteure erstellt und im Sicherheitskonzept des ZDA-VP referenziert.[2]

Als nächstes wird die Chipkarte an den **Karteninhaber** übergeben.

Nachdem der Karteninhaber die Chipkarte erhalten hat, kann er sie zunächst im Sinne des primären Zwecks nutzen, also z.B. als elektronische Gesundheitskarte. Wenn der Karteninhaber beschließt, die Chipkarte zusätzlich auch als elektronische Signaturkarte benutzen zu wollen, so wird er (typischerweise durch den Herausgeber gesteuert) Kontakt zu einem ZDA aufnehmen zum Zwecke des Nachladens (**ZDA-NL**) eines qualifizierten Zertifikats. Es kann sich dabei um denselben ZDA wie den ZDA-VP, aber auch um einen anderen ZDA handeln.

Im Rahmen des Nachladeprozesses werden beim ZDA grob vereinfacht drei Prozessschritte durchlaufen:

- Antragstellung
- Identifizierung und Registrierung des Karteninhabers
- Erstellung des qualifizierten Zertifikats und Setzen einer PIN und ggf. einer PUK

Oft sind das auch drei unterschiedene Prozessphasen, da die in der Mitte liegende Identifizierung in der Regel erfordert, dass der Karteninhaber eine dafür geeignete Stelle aufsucht, z.B. eine Postfiliale für das Postidentverfahren.

Nach Abschluss des Prozesses kann die Chipkarte vom Karteninhaber benutzt werden, um qualifizierte elektronische Signaturen zu erzeugen.

[2] Im Rahmen dieses Prozesses ist es möglich, aber keineswegs zwingend erforderlich, Chipkarten physikalisch zwischen den Akteuren auszutauschen.

5.3 Konzept zum Nachladen qualifizierter Zertifikate

Um die Implikationen der verschiedenen Aspekte besser darstellen zu können, werden die Schritte für die Produktion der evaluierten und bestätigten Signaturkarte im Folgenden vereinfacht in einem möglichen Prozess dargestellt:

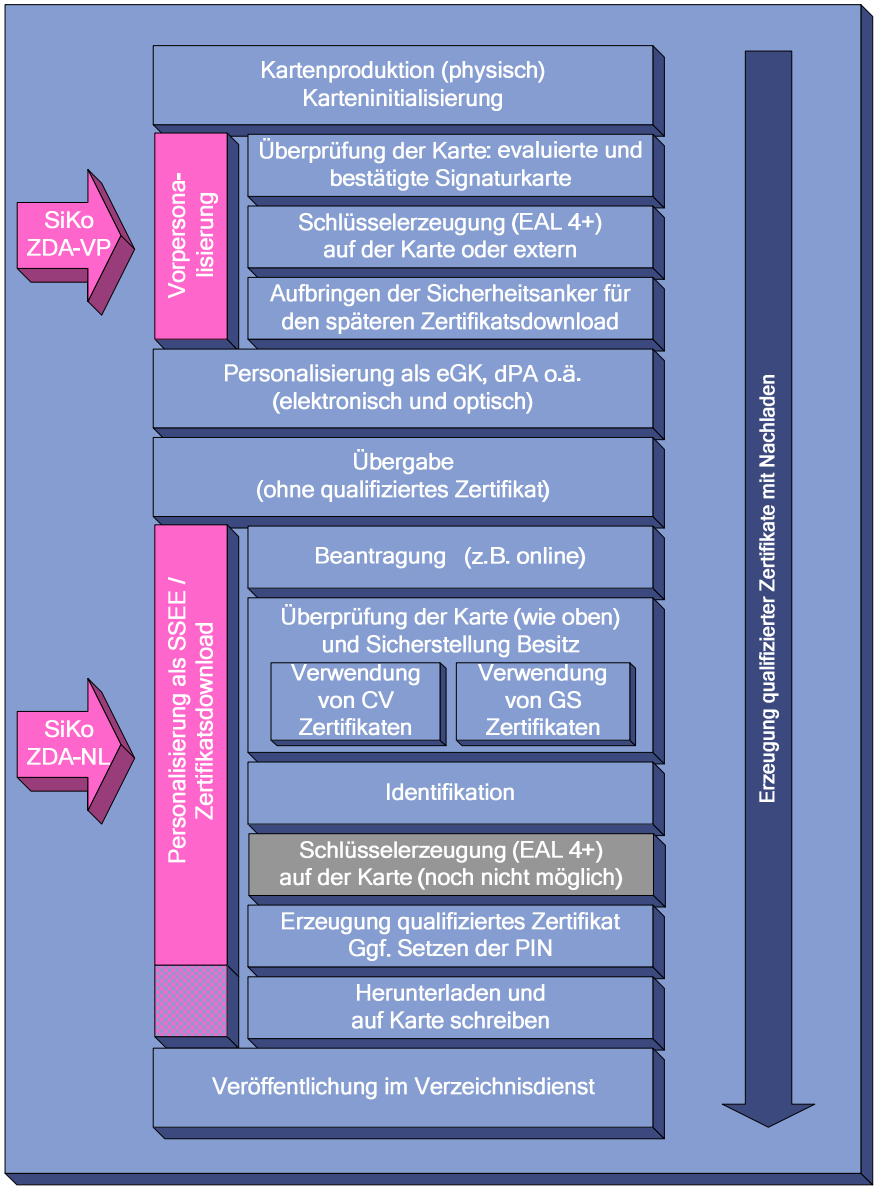

Abbildung 1: Prozessübersicht

Die in Abbildung 1 für den Nachladeprozess aufgeführten Blöcke sind als logische Trennung zu verstehen, nicht jedoch notwendig als zeitlich voneinander getrennt. Zudem ist die Reihenfolge nicht vorgegeben und obliegt dem jeweiligen ZDA-NL.

Das Leitprinzip dieser Spezifikation besteht darin, dass in der gesicherten Produktionsumgebung der Chipkarte eine minimale, aber ausreichende Menge an geeigneten Merkmalen auf der Chipkarte geschaffen wird, die einen ZDA in die Lage versetzen, nach SigG und SigV auch dann noch qualifizierte Zertifikate für den Karteninhaber auszustellen, wenn die Chipkarte bereits lange die gesicherte Produktionsumgebung verlassen hat und sich inzwischen beim Karteninhaber befindet. Diese minimale Menge an geeigneten Merkmalen bestimmt sich aus den gesetzlichen Anforderungen, die für einen ZDA erfüllt sein müssen, damit er ein qualifiziertes Zertifikat ausstellen darf.

Weiterhin sollen die Auswirkungen auf Produktion, Ausgabe und Nutzung der Chipkarte entsprechend ihrem primären Zweck auf ein notwendiges Minimum beschränkt sein.

Grundsätzliche Anforderungen an die Chipkarte:

1. Die Chipkarte ist eine evaluierte und nach SigG bestätigte Signaturkarte.
2. Der Schlüssel kommt aus einem evaluierten und nach SigG bestätigten Schlüsselgenerator (dies kann auch die Chipkarte selbst sein).
3. Die Chipkarte muss sich bei nachträglicher Beantragung eines qualifizierten Zertifikates im Besitz des Antragsstellers befinden.
4. Die Signaturanwendung auf der Chipkarte ist gegen unbemerktes Benutzen gesichert (z.B. durch eine Transport-PIN).
5. Die Signaturanwendung auf der Chipkarte befindet sich vor dem ersten Nachladen im Transportzustand, d.h. die SigG- Schlüssel und die PIN-Funktion sind unbenutzt.
6. Der Chipkarteninhaber hat die Möglichkeit, seine PIN zu ändern.
7. Der Bereich auf der Chipkarte, in dem das qualifizierte Zertifikat gespeichert wird, ist allen beteiligten ZDAs zugänglich.

1. Vorbereitung der Chipkarte zur Übergabe

Die folgenden Schritte müssen im Rahmen der Vorpersonalisierung durchgeführt werden. Die genaue Reihenfolge obliegt dabei dem ZDA-VP.

- Es muss sichergestellt sein, dass es sich bei der Chipkarte um eine evaluierte und bestätigte Signaturkarte handelt.
- Das Signaturschlüsselpaar muss erzeugt und, wenn es nicht auf der Chipkarte erzeugt wird, auf die Chipkarte aufgebracht werden. Bei der hier festgelegten Schlüsselerzeugung durch einen ZDA-VP (ggf. durch einen Kartenproduzenten in seinem Auftrag ausgeführt) spielt es keine Rolle, ob die Schlüssel auf der Chipkarte oder in einem geeigneten externen Schlüsselgenerator erzeugt werden.[3]

[3] Als Variante kann dieser Schritt theoretisch auch beim Nachladen in der Domäne des Karteninhabers auf der evaluierten und bestätigten Signaturkarte erfolgen, dann entfällt dieser Schritt hier. Dies ist aber erst für spätere Versionen dieser Spezifikation vorgesehen.

- Der Sicherheitsanker (Gütesiegel- oder CV-Zertifikat mit zugehörigem privatem Schlüssel) muss auf die Chipkarte geschrieben werden.

Für diese Schritte ist es zwingend notwendig, dass sie gemäß einem nach SigG bestätigten Sicherheitskonzept eines ZDA[4] durchgeführt werden.

Die Personalisierung der Chipkarte mit Daten, die unabhängig von der Signaturanwendung sind (weil sie z.B. zum primären Zweck der Chipkarte gehören), wird nicht durch SigG geregelt und muss somit auch nicht im Sicherheitskonzept des ZDA-VP verankert sein.

2. Ausgabe der Karte (ohne qualifiziertes Zertifikat)

Dies braucht in diesem Dokument nicht weiter betrachtet werden, der Prozess kann ohne ZDA durchgeführt werden.

3. Nachladen eines qualifizierten Zertifikats durch einen ZDA

Im Folgenden werden die erforderlichen Schritte für das Nachladen beschrieben. Die genaue Reihenfolge und Ausprägung obliegt dem ZDA-NL und wird in dieser Spezifikation nicht festgelegt. Aus technischer Sicht ist dies auch nicht erforderlich. Hier werden die Elemente allgemein beschrieben. Eine exemplarische Darstellung eines Prozesses im Zusammenhang folgt in Kap. 8.

- **Beantragung**

  Wenn der Chipkarteninhaber, um mit seiner Chipkarte qualifizierte elektronische Signaturen erstellen zu können, ein qualifiziertes Zertifikat bekommen möchte, muss er dieses zunächst beantragen, z.B. im Rahmen eines Online-Prozesses. Typischerweise wird der Kartenherausgeber den Karteninhaber an einen oder mehrere präferierte ZDA verweisen.

- **Überprüfung der Karte**

  Der ZDA-NL prüft zunächst, ob es sich um eine evaluierte und bestätigte Signaturkarte handelt und ob er sie nach seinem aktuellen Sicherheitskonzept[5] mit einem qualifizierten Zertifikat versehen kann. Hierfür werden die in Schritt 2 aufgebrachten Sicherheitsanker verwendet. Dies kann geschehen über

  - Gütesiegel (GS)

    Der öffentliche Schlüssel wird bei der Generierung mit einer elektronischen Signatur eines ZDAs in der Rolle des ZDA-VP als geeignet gekennzeichnet.

  - CV Zertifikate.

    Die Chipkarte ist im Nachladeprozess als geeignet erkennbar und der öffentliche Schlüssel wird von der Chipkarte authentisiert übergeben.

  Der private Schlüssel ist in jedem Fall durch die evaluierte und bestätigte Signaturkarte geschützt. Einzelheiten zu beiden Verfahren finden sich in Kap. 7.2 und 7.3.

[4] oder eines Dritten, der in einem vertraglichen Verhältnis zu einem ZDA gemäß § 4 Absatz 5 SigG steht (wie z.B. beim PostIdent Verfahren der Deutschen Post AG).
[5] Technische Komponenten müssen explizit im Sicherheitskonzept des ZDA-NL enthalten sein.

Beide Zertifikatstypen werden durch einen ZDA-VP nach §4 SigG erzeugt, es handelt sich aber natürlich nicht um qualifizierte Zertifikate. Nach erfolgreicher Prüfung beginnt die Erzeugung des qualifizierten Zertifikats.

Ein spezieller Aspekt der Nutzbarkeit von existierenden Schlüsseln für die Erzeugung von qualifizierten Zertifikaten ist die Übereinstimmung mit den Anforderungen des Algorithmenkatalogs der Bundesnetzagentur. In diesem Katalog ist für jeden Zeitpunkt festgehalten, welche Mindestanforderungen an verwendete Algorithmen und dafür notwendige Parameter gelten, also z.B. für Schlüssellängen der kryptografischen Schlüssel. Die Bestätigung einer Chipkarte ist an die Einhaltung dieser Bedingung gebunden, sie muss also mit überprüft werden.

Dieser Aspekt stellt im Zweifel einen begrenzenden Faktor für die Verwendbarkeit der Chipkarte zum gewählten Zeitpunkt dar. [6]

Beim digitalen Personalausweis muss besonders beachtet werden, dass dort nicht mehr der bisher weitgehend verwendete RSA-Algorithmus, sondern ein Algorithmus unter Verwendung von elliptischen Kurven vorgesehen ist.

- **Identifizierung**

  Vor Ausstellung eines qualifizierten Zertifikats muss der Antragsteller durch den ZDA zuverlässig identifiziert werden. Hier ist auch eine Identifizierung durch Dritte, also Vertragspartner des ZDA (z.B. PostIdent der Deutschen Post AG) möglich. Im Rahmen von Beantragung und/oder Identifizierung können mit dem Antragsteller Geheimnisse vereinbart werden, mit denen er sich im Prozess des Nachladens gegenüber dem Nachladesystem als der ursprüngliche Antragsteller ausweisen kann.

- **Sicherstellung, dass sich die Karte im Besitz des Beantragenden befindet**

  Vor der Erstellung des qualifizierten Zertifikates ist es notwendig, dass neben der Überprüfung, dass es sich bei der eingesetzten Chipkarte um eine evaluierte und bestätigte Signaturkarte handelt, auch zusätzlich der Chipkarteninhaber den Besitz der zugehörigen Chipkarte nachweist, z.B. durch eine Authentisierungssignatur, durch Eingabe eines zuvor im Prozess vereinbarten Geheimnisses oder auch durch eine organisatorische Regelung. Auch die erfolgreiche Entschlüsselung von übersandten Daten mit Hilfe eines auf der Chipkarte vorhandenen Verschlüsselungszertifikats ist möglich.

- **Zertifikatserzeugung, Schreiben des Zertifikats auf die Karte und ggf. Setzen der PIN**

  Der ZDA generiert ein qualifiziertes Zertifikat über den Signaturprüfschlüssel und übergibt dieses an den Chipkarteninhaber und/oder speichert das Zertifikat auf der evaluierten und bestätigten Signaturkarte. Neben dem Zertifikat kann der ZDA auf der Grundlage einer Vereinbarung mit dem Herausgeber weitere Daten in der Signaturapplikation auf der Chipkarte speichern. Bevor die Chipkarte genutzt werden kann, muss der Chipkarteninhaber die PIN setzen. Gleichzeitig wird geprüft, ob sich die Chipkarte

[6] Das gilt im Wesentlichen unabhängig davon, ob der Schlüssel vorab oder später generiert wird, weil bisher die verwendete Schlüssellänge für eine Chipkarte weitestgehend konstant die maximal mögliche Schlüssellänge ist.

noch im Transportzustand befindet und die PIN noch nicht geändert wurde. Dies wird sinnvollerweise in den Prozess des Nachladens integriert.

Der Prozess des Nachladens kann dann sofort in der Registrierungsstelle (je nach Prozessgestaltung) oder auch am Computer des Chipkarteninhabers erfolgen.

- **Veröffentlichung des Zertifikats im Verzeichnisdienst des ZDA**

  Da der Antrag gleichzeitig die Bestätigung über den Erhalt der Chipkarte beinhaltet, sollte hier zusätzlich eine Bestätigung über den Erhalt des qualifizierten Zertifikates erfolgen. Danach wird das qualifizierte Zertifikat nachprüfbar und auf Wunsch des Zertifikatsinhabers abrufbar gehalten.

Die verwendeten Gütesiegel- und CV-Zertifikate unterliegen, da es sich um technische Sicherheitsmechanismen und nicht um qualifizierte Zertifikate handelt, nicht den gleichen rechtlichen Anforderungen an dieselben. Sie können also z.B. auch unter Verwendung eines nicht nach SigG bestätigten HSM erzeugt werden. Allerdings ist angemessen hohe technische Sicherheit erforderlich, die Festlegung erfolgt in der Praxis im Rahmen des Bestätigungsverfahrens. Im Falle, dass ein solches Zertifikat als alleiniges Sicherheitsmerkmal fungiert, ist nach der Praxis der zugelassenen Bestätiger der Algorithmenkatalog der Bundesnetzagentur direkt anzuwenden.

4. „Späte“ Schlüsselgenerierung auf der Chipkarte

Sowohl für den dPA (als einzigen Fall) wie auch für die eGK (als Option) wird die Möglichkeit gefordert, eine „späte“ Schlüsselgenerierung auf der Chipkarte erst dann vorzusehen, wenn sie sich bereits im Feld befindet.

Eine späte Schlüsselgenerierung wird von den ZDA als gegenwärtig nicht geeignet für eine umsetzbare Spezifikation angesehen. Weder gibt es eine dafür geeignete bestätigte Chipkarte noch Erfahrung mit der Bestätigung eines darauf basierenden Prozesses. Würde diese Option unter den gegebenen Umständen aufgenommen, bestünde das Risiko, dass T7 als Herausgeber darauf festgelegt werden könnte, diese Option als umsetzbar deklariert zu haben.

Ein weiteres Problem in diesem Umfeld besteht darin, dass eine Schlüsselgenerierung auf der Chipkarte in einer ungesicherten Umgebung beim Karteninhaber nicht durch existierende Bestätigungen der Chipkarten abgedeckt wird. Als Ausweg wird hier gelegentlich die Schüsselgenerierung auf der Chipkarte in einer gesicherten Umgebung in einer RA vorgeschlagen. Solche RAs sind aber aktuell nicht existent und aus Kostengründen durch die ZDAs auch nicht realisierbar.

Damit ist die einzige Option in der aktuellen Version dieser Spezifikation die Schlüsselgenerierung vor der Ausgabe an den Karteninhaber.

Eine späte Schlüsselgenerierung soll in die Spezifikation aufgenommen werden, wenn die hier genannten Voraussetzungen gegeben sind oder zumindest als gegeben angenommen werden können. In dieser Version sind Hinweise enthalten, wie eine späte Schlüsselgenerierung zu einem späteren Zeitpunkt integriert werden kann.

Eine späte Schlüsselgenerierung schließt die Verwendung von Gütesiegeln in der in der Spezifikation beschriebenen Form aus.

6 Sicherheitsanker, PIN- und PUK-Verfahren

Die Karten können bei der Vorpersonalisierung gemäß dieser Spezifikation mit einem von zwei möglichen Sicherheitsankern, entweder einem CV-Zertifikat oder einem Gütesiegel-Zertifikat, versehen werden. Die Kombination beider Verfahren ist ebenfalls möglich, wird hier jedoch nicht weiter beschrieben. Es werden die drei Varianten

- Gütesiegelzertifikat mit Null-PIN
- Gütesiegelzertifikat mit abgeleiteter Transport-PIN und
- CV-Zertifikat mit abgeleiteter Transport-PIN

Zu jedem PIN-Verfahren ist optional ein PUK-Verfahren definiert. Der PUK dient dem Rücksetzen des Fehlbedienzählers der PIN. Ein Karteninhaber kann also bei abgelaufenem Fehlbedienzähler der PIN durch korrekte Eingabe der PUK diesen wieder auf den Wert bei Kartenausgabe zurücksetzen (in der Regel sind für die Eingabe der PIN 3 Fehlversuche zugelassen). Um Missbrauch vorzubeugen, wird die Anzahl der Verwendungen des PUK bei der Vorpersonalisierung auf einen festen Wert (z.B. 10) beschränkt. Beim Null-PIN-Verfahren wird zu diesem Zwecke, sofern diese Option unterstützt wird, anstelle des PUK eine zweite PIN verwendet. Da hier die Funktionalität der zweiten PIN benutzt wird, um den Fehlbedienzähler der ersten PIN zurückzusetzen, wird dieses Verfahren in diesem Dokument ebenfalls als PUK-Verfahren bezeichnet.

Bei Verwendung eines PUK-Verfahren gibt es demnach die folgenden Kombinationen

- Gütesiegelzertifikat mit Null-PIN und zweiter PIN
- Gütesiegelzertifikat mit abgeleiteter Transport-PIN und PUK
- CV-Zertifikat mit abgeleiteter Transport-PIN und PUK[7]

Der Einsatz der PUK-Verfahren ist abhängig von der Bestätigungsfähigkeit derselben.

Der ZDA-VP wählt Sicherheitsanker und PIN- bzw PUK-Verfahren aus. Ein ZDA-NL kann demnach nicht das Vorhandensein einer bestimmten der obigen Kombinationen aus Sicherheitsanker und PIN- oder PUK-Verfahren verlangen. Er muss somit alle oben aufgeführten Varianten unterstützen können, um das Nachladen für alle vorpersonalisierten eCards zu ermöglichen.

Hierfür werden die folgenden normativen technischen Festlegungen getroffen:

- Der Transportzustand der Chipkarte wird für die kombinierten Merkmale Sicherheitsanker und PIN-Verfahren auf einer vom Kartenprofil unabhängigen Ebene spezifiziert.
- Die Merkmale und Geheimnisse, die bei der Vorpersonalisierung des ZDA-VP für jede der Kombinationen verwendet werden, werden in dieser Spezifikation festgelegt.

[7] In diesem Fall kann die PUK entweder selbst abgeleitet oder über CVC gesichert auslesbar sein. S.u. Kapitel 7.1.3.3

- Die Merkmale und Geheimnisse, die auf seiten des ZDA-NL erforderlich sind, um auf alle Kombinationen qualifizierte Zertifikate nachladen zu können, werden in dieser Spezifikation festgelegt.
- Ein teilnehmender ZDA-VP muss nach dieser Spezifikation die verwendeten Merkmale und Geheimnisse den anderen ZDAs zur Verfügung stellen, ein teilnehmender ZDA-NL muss in der Lage sein, mit ihrer Hilfe und nach den erforderlichen Prüfungen qualifizierte Zertifikate zu erzeugen.
- Der Kreis der ZDA ist jederzeit erweiterbar.

6.1 Konkrete Zugriffsregeln als Anhang erforderlich

In dieser Spezifikation werden normative Festlegungen getroffen. Um Konfliktfreiheit zu gewährleisten, muss in einem Anhang zu dieser Spezifikation die konkrete Ausprägung für ein konkretes Chipkartenprofil in Übereinstimmung mit den Festlegungen dieser Spezifikation aufgeführt werden.

Kartenprofile, die zu dieser Spezifikation konform sein sollen, müssen mindestens eine gültige Beschreibung auf dieser konkreten Ebene liefern können, die alle genannten Anforderungen eindeutig umsetzt. Solche Beschreibungen können in dieses Dokument als Anhang aufgenommen oder unabhängig von diesem Dokument veröffentlicht werden.

7 Anforderungen an Komponenten

In diesem Kapitel werden Anforderungen an die am Prozess beteiligten Komponenten beschrieben. Dazu gehören die Chipkarte, die Zertifikatshierarchien für CV- und Gütesiegel-Zertifikate sowie die Vorpersonalisierungs- und Nachlade-Anwendung.

7.1 Chipkarte

7.1.1 Allgemeine Anforderungen an die Chipkarte

- Evaluierte und bestätigte Signaturkarte

  Die Evaluation einer Signaturkarte bezieht sich auf die Chipkarten-Hardware sowie auf die darauf initialisierte Software, das Chipkarten Betriebsyystem (COS). Für beides muss im Zusammenwirken eine Evaluierung der nach SigV geforderten Stufe[8] als sichere Signaturerstellungseinheit vorliegen.

  Die Bestätigung umfasst dagegen das Vorgenannte zusammen mit einer auf der Karte befindlichen Chipkartenapplikation für die Erzeugung von qualifizierten Signaturen, zunächst im Zustand, in dem sie an den Karteninhaber übergeben wird, dann im Nutzungszustand. Zusätzlich wird i.d.R. der Mechanismus bestätigt, mittels dessen die Chipkarte vom Karteninhaber in Betrieb genommen werden kann, also v.a. Aktivieren oder Setzen einer PIN.

  Wenn also in dieser Spezifikation von einer evaluierten und bestätigten Signaturkarte[9] die Rede ist, so ist damit gemeint, dass für diese Chipkarte eine Evaluation sowie eine Bestätigung nach SigG und SigV vorliegen und dass die Karte sich zum beschriebenen Zeitpunkt in einem Zustand befindet, der im Einklang mit dieser Bestätigung ist und ggf. eine valide Vorform des Transport- oder Nutzungszustands darstellt.

- Identifikation des genauen Kartentyps
  - Ein ZDA darf nur dann ein qualifiziertes Zertifikat ausstellen, wenn er in seinem Sicherheitskonzept genau dieses Kartenprodukt (neben ggf. anderen) beschrieben hat. Das genaue Kartenprodukt muss deshalb anhand der Chipkarte selbst feststellbar sein.

    Hinweis: Für die in dem vorliegenden Dokument betrachteten Chipkarten wird es grundsätzlich eine sogenannte ICCSN geben, die als "Kartennummer" jede Chipkarte eindeutig identifiziert. Die Struktur und der genaue Aufbau der ICCSN werden in den entsprechenden Spezifikationen festgelegt.

[8] EAL 4+ nach Common Criteria bzw. E3 hoch nach ITSEC

[9] An dieser Stelle wurde bewusst der Begriff „sichere Signaturerstellungseinheit“ (SSEE) vermieden. Einerseits ist das die Formulierung in Gesetz und Verordnung, andererseits ist aber auch das Protection Profile so benannt, auf dem die Evalution der Chipkarte fußt. Eine „nur“ evaluierte Chipkarte, für die keine Bestätigung vorliegt, darf aber nicht verwendet werden. Eine evaluierte und bestätigte Signaturkarte umfasst dagegen immer die Bestätigung nach SigG und SigV.

- Einer der folgenden Sicherheitsanker muss in der in dieser Spezifikation beschriebenen Form unterstützt werden:
    - Gütesiegel
        - Lesen:

          Das Gütesiegelzertifikat über den öffentlichen Signaturschlüssel kann ohne Einhaltung von Zugriffsbedingungen aus der Chipkarte gelesen werden.
        - Schreiben:

          Das qualifizierte Zertifikat kann entweder frei oder per Secure-Messaging über MAC-gesicherte Kommandos auf die Chipkarte geschrieben werden. Zur MAC-Sicherung werden abgeleitete kartenindividuelle symmetrische Schlüssel verwendet. .
    - CV-Zertifikate
        - Lesen:

          Der öffentliche Signaturschlüssel muss durch gegenseitige Komponenten-Authentifikation z.B. über CV-Zertifikate gesichert aus der Chipkarte gelesen werden können.
        - Schreiben:

          Das qualifizierte Zertifikat darf nur nach gegenseitiger Komponenten-Authentifikation z.B. über CV-Zertifikate gesichert auf die Chipkarte geschrieben werden können.
- Eines der folgenden Verfahren zum PIN-Handling muss unterstützt werden, ggf. mit dem zugehörigen PUK-Verfahren:
    - Für Gütesiegel:
        - Transport-PIN abgeleitet oder
        - Null-PIN
    - Für CV-Zertifikate:
        - Transport-PIN abgeleitet

7.1.2 Allgemeine Definition Transportzustand

Die Chipkarte im Transportzustand ist die Schnittstelle zwischen der Vorpersonalisierung durch einen ZDA-VP und dem Nachladevorgang durch einen ZDA-NL.

Der Transportzustand ist der Zustand der Chipkarte zu dem Zeitpunkt, wenn die Vorpersonalisierung des ZDA-VP abgeschlossen ist, der Nachladeprozess jedoch noch nicht initiiert wurde. Er hat die besondere Bedeutung, dass über ihn die Interoperabilität der ZDAs beim

Nachladen hergestellt wird. Außerdem beschreibt er die Sicherheitseigenschaften, die es erlauben, dass die Karte bis zum Nachladen in unsicheren Umgebungen genutzt werden kann, ohne diesen Transportzustand zu gefährden. Er wird deshalb in dieser Spezifikation normativ festgeschrieben.

Der Nutzungszustand ist der Zustand nach erfolgreichem Nachladen eines qualifizierten Zertifikats. Er unterliegt dem Sicherheitskonzept des ZDA-NL, zusätzlich können sich aus der Erst-Identität der Chipkarte als eGK, DPA o.ä. weitere Anforderungen ergeben.

Die Zustände vor und nach dem Transportzustand sowie die Kartenkommandos, mit denen diese Zustände hergestellt werden, sind nicht Gegenstand dieser Spezifikation.

Es muss möglich sein, dass auch fortfolgende Nachladevorgänge im Nutzungszustand erfolgen können, um auch lange Gültigkeitszeiträume der Chipkarte wie z.B. beim Deutschen Personalausweis (10 Jahre) zu unterstützen.

7.1.3 Transportzustände der Chipkarte

Im Folgenden werden die Transportzustände der Chipkarte generisch beschrieben. Eine konkrete Ausprägung für konkrete Kartenprofile findet sich im jeweiligen technischen Anhang für das konkrete Kartenprofil.

Welche der erlaubten Kombinationen verwendet wird, obliegt dem ZDA-VP.

Kommandos sollen nur ausgeführt werden, wenn die Sicherheitsbedingungen entsprechend der Zugriffsregel für diese Operationen sind oder das Kommando durch eine implizite Konvention immer erlaubt ist.

Es sei darauf hingewiesen, dass nicht alle Objekte, die mit dem Kürzel EF versehen sind, auch in allen COS tatsächlich als Elementary File kodiert sind, wie z.B. bei der Repräsentation der eigentlichen PIN in der Chipkarte.

7.1.3.1 Transportzustand bei Sicherheitsanker Gütesiegel mit Null-PIN[10]

Der Transportzustand der Chipkarte, wenn diese als Sicherheitsanker ein Gütesiegel-Zertifikat enthält und als PIN-Verfahren das Null-PIN-Verfahren unterstützt, ist in Bezug auf Objekte und Access Rules folgendermaßen festgelegt:

Tabelle 1: Transportzustand GS mit Null-PIN

Nr	Titel	Definition	Erläuterung
1	EF Private Key	Funktion: Compute DS SC: Der Benutzer muss sich mit der PIN (EF PIN1 oder EF PIN2) erfolgreich authentisieren	Privater Schlüssel zur Erzeugung qualifizierter elektronischer Signaturen COS-spezifisch, es muss sichergestellt sein, dass der PrK nur PIN-verifiziert verwendet werden kann.
2	EF Certificate	Funktion: Read Binary SC: Always	
		Funktion: Update Binary SC: Always *oder* SC: nur mit MAC-gesicherten Kommandos	Das Schreiben des Zertifikats muss aus rechtlicher Sicht nicht authentisiert erfolgen. Um ggf. das unberechtigte Beschreiben dieses EF trotzdem verhindern zu können, kann das EF dadurch geschützt werden, dass ein Beschreiben nur mit MAC-gesicherten Kommandos auf Basis eines von kartenindividuellen Merkmalen abgeleiteten symmetrischen Schlüssels möglich ist. Inhalt: • Im Transportzustand befindet sich hier der öffentliche Schlüssel in der Form eines GS • Nach erfolgreichem Nachladeprozess befindet sich hier das qualifizierte Zertifikat.
3	EF Public Key	*Zugriff erfolgt ausschließlich im Rahmen der Vorpersonalisierung zum Zwecke der Erzeugung eines Gütesiegels, wird daher hier nicht weiter betrachtet.*	Öffentlicher Schlüssel zu 1
4	EF Card Capability Description (CCD)	Funktion: Read Record SC: Always	Das EF muss ohne Einhaltung von Zugriffsbedingungen gelesen werden können. Die Kodierung wird im konkreten Anhang zu einem Kartenprofil festgelegt.

[10] Zu diesem Verfahren ist bekannt, dass es durch ein Patent der Deutschen Telekom AG geschützt ist.

Nr	Titel	Definition	Erläuterung
5	EF PIN1	Funktion: Activate File SC: nur mit MAC-gesichertem Kommando vor der erstmaligen Nutzung	Im Transportzustand ist das EF PIN1 deaktiviert. Es wird durch ein MAC-gesichertes Kommando aktiviert und kann dann geändert werden.
		Funktion: Verify, Change RD SC: Always *Hierbei handelt es sich um die im Zusammenhang mit dem Anlegen eines PIN-Objekts COS-spezifisch gespeicherte PIN.*	EF PIN1 ist noch nicht für den Wirkbetrieb gesetzt. Inhalt: • Im Transportzustand ein nicht für die Erzeugung von Signaturen geeigneter Wert • Nach erfolgreichem Nachladevorgang ein für die Erzeugung von Signaturen geeigneter Wert, den nur der Karteninhaber kennt.
6	EF PIN2 (optional)	Funktion: Reset RC, Change RD SC: Der Benutzer muss sich mit der PIN1 erfolgreich authentisieren	EF PIN2 ist noch nicht für den Wirkbetrieb gesetzt. Inhalt: • Im Transportzustand ist die PIN2 mit einem Zufallswert gesetzt, der vor der ersten Benutzung geändert werden muss. Zur Änderung muss sich der Benutzer mit der PIN1 erfolgreich authentisieren.
		Funktion: Verify, Change RD SC: Always	• Nach erfolgreichem Nachladevorgang ein für die Erzeugung von Signaturen geeigneter Wert, den nur der Karteninhaber kennt.

Lässt sich der Wert der PIN1 durch ChangeRD auf einen nutzbaren Wert ändern, so befand sich die Chipkarte bis zu diesem Zeitpunkt noch im Transportzustand. Bei Misserfolg muss der Transportzustand als gebrochen angesehen werden, es darf kein qualifiziertes Zertifikat erzeugt werden.

7.1.3.2 Transportzustand bei Sicherheitsanker Gütesiegel mit abgeleiteter PIN

Das EF PIN sowie das EF PUK enthalten einen (typischerweise 5-stelligen) PIN- bzw. PUK-Wert, der nicht für die Erzeugung von Signaturen bzw. zum Zurücksetzen des Fehlbedienugnszählers benutzt werden kann. Der Wert kann mit ChangeRD auf einen nutzbaren Wert gesetzt werden.

Der Wert von Transport-PIN und -PUK wird kryptografisch aus Kartenmerkmalen hergeleitet. Die dazu verwendeten beiden MasterKeys muss vom ZDA-VP an den ZDA-NL übergeben werden.

Der Transportzustand der Chipkarte, wenn diese als Sicherheitsanker ein Gütesiegel-Zertifikat enthält und als PIN-Verfahren das Verfahren mit abgeleiteter PIN unterstützt, ist in Bezug auf Objekte und Access Rules folgendermaßen festgelegt:

Tabelle 2: Transportzustand GS mit abgeleiteter PIN

Nr	Titel	Definition	Erläuterung
1	EF Private Key	Funktion: Compute DS SC: Der Benutzer muss sich mit der PIN (EF PIN1 oder EF PIN2) erfolgreich authentisieren	Privater Schlüssel zur Erzeugung qualifizierter elektronischer Signaturen COS-spezifisch, es muss sichergestellt sein, dass der PrK nur PIN-verifiziert verwendet werden kann.
2	EF Certificate	Funktion: Read Binary SC: Always	
		Funktion: Update Binary SC: Always *oder* SC: nur mit MAC-gesicherten Kommandos	Das Schreiben des Zertifikats muss aus rechtlicher Sicht nicht authentisiert erfolgen. Um ggf. das unberechtigte Beschreiben dieses EF trotzdem verhindern zu können, kann das EF dadurch geschützt werden, dass ein Beschreiben nur mit MAC-gesicherten Kommandos auf Basis eines von kartenindividuellen Merkmalen abgeleiteten symmetrischen Schlüssels möglich ist. Inhalt: • Im Transportzustand befindet sich hier der öffentliche Schlüssel in der Form eines GS • Nach erfolgreichem Nachladeprozess befindet sich hier das qualifizierte Zertifikat.
3	EF Public Key	*Zugriff erfolgt ausschließlich im Rahmen der Vorpersonalisierung zum Zwecke der Erzeugung eines Gütesiegels, wird daher hier nicht weiter betrachtet.*	Öffentlicher Schlüssel zu 1
4	EF Card Capability Description (CCD)	Funktion: Read Record SC: Always	Das EF muss ohne Einhaltung von Zugriffsbedingungen gelesen werden können. Die Kodierung wird im konkreten Anhang zu einem Kartenprofil festgelegt.

Nr	Titel	Definition	Erläuterung
5	EF PIN	Funktion: Verify, Change RD, Reset RC SC: Always Hierbei handelt es sich um die im Zusammenhang mit dem Anlegen eines PIN-Objekts COS-spezifisch gespeicherte PIN.	Im Transportzustand befindet sich im EF PIN ein nicht für die Erzeugung von Signaturen geeigneter Wert, z.B. eine fünfstellige PIN. Er kann von einem ZDA, der die dazu benötigten Geheimnisse (einen symmetrischen Masterkey und das zugehörige Ableitungsverfahren der Transport-PIN aus diesem) kennt, errechnet und dem Karteninhaber mitgeteilt werden. Nach erfolgreichem Nachladen enthält das EF PIN einen für die Erzeugung qualifizierter elektronischer Signaturen geeigneten Wert, den nur der Karteninhaber kennt.
6	EF PUK (optional)	Funktion: Verify, Change RD, Reset RC SC: Always Hierbei handelt es sich um die im Zusammenhang mit dem Anlegen eines PIN-Objekts COS-spezifisch gespeicherte PUK.	Im Transportzustand befindet sich im EF PUK ein dem Karteninhaber unbekannter Wert. Dieser kann von einem ZDA-NL mittels der dazu benötigten Geheimnisse (eines symmetrischen Masterkeys und des zugehörigen Ableitungsverfahrens der Transport-PUK aus diesem) errechnet und dem Karteninhaber mitgeteilt werden. Nach erfolgreichem Nachladen enthält das EF PUK einen für die Erzeugung qualifizierter elektronsicher Signaturen geeigneten Wert, den nur der Karteninhaber kennt.

7.1.3.3 Transportzustand bei Sicherheitsanker CV-Zertifkate

Das EF PIN enthält einen (typischerweise 5-stelligen) PIN-Wert, der nicht für die Erzeugung von Signaturen benutzt werden kann. Der Wert kann mit ChangeRD auf einen nutzbaren Wert gesetzt werden.
Das EF PUK enthält einen Wert zum Zurücksetzen des Fehlbedienzählers der PIN. Die Anzahl, wie oft der Fehlbedienzähler zurückgesetzt werden darf, legt der ZDA-VP fest.
.
Der Wert von Transport-PIN und -PUK wird kryptografisch aus Kartenmerkmalen hergeleitet. Die dazu verwendeten beiden MasterKeys muss vom ZDA-VP an den ZDA-NL übergeben werden.

Der Transportzustand der Chipkarte, wenn diese als Sicherheitsanker ein CV-Zertifikat enthält und als PIN-Verfahren das Verfahren mit abgeleiteter PIN unterstützt, ist in Bezug auf Objekte und Access Rules folgendermaßen festgelegt:

Tabelle 3: Transportzustand CVC mit abgeleiteter PIN

Nr	Titel	Definition	Erläuterung
1	EF CV-Zertifikat	Funktion: Read Binary SC: Always	Die CV-Zertifikate müssen ohne Einhaltung von Zugriffsbedingungen gelesen werden können. Inhalt: CV-Zertifikat der Chipkarte, das vom ZDA-VP ausgestellt wird
2	EF Private CV Key	Funktion: Signaturberechnung im Rahmen von INTERNAL AUTHENTICATE	Inhalt: Globaler privater Schlüssel, der zur gegenseitigen Authentifikation auf Basis der CV-Zertifikate genutzt wird
3	EF Public CV Keys	Funktion: VERIFY CERTIFICATE SC: Always	Die öffentlichen Schlüssel müssen zur Verfikation von CV-Zertifkaten ohne Einhaltung von Zugriffsbedingungen genutzt werden können. Inhalt: Öffentliche Schlüssel, die zur Prüfung von CV-Zertifikaten durch die Chipkarte genutzt werden
4	EF Private Key	Funktion: Compute DS SC: Der Benutzer muss sich mit der PIN (EF PIN) erfolgreich authentisieren	COS-spezifisch, es muss sichergestellt sein, dass auf den PrK nur PIN-verifiziert zugegriffen werden kann.
5	EF Certificate	Funktion: Read Binary SC: Always	
		Funktion: Update Binary SC: Ext. Auth. Chipkarte-ZDA (mit Etablierung TC) (asym.)	Das Überschreiben des Zertifikats wird nur ZDAs mit entsprechend kodiertem CV-Zertifikat ermöglicht und erst nach Aufbau eines Trusted Channels zwischen ZDA und Chipkarte nach gegenseitiger Komponentenauthentifikation z.B. auf Basis CVC. Inhalt: Nach erfolgreichem Nachladeprozess befindet sich hier das qualfizierte Zertifikat.

Nr	Titel	Definition	Erläuterung
6	EF Public Key	Funktion: GENERATE ASYMMETRIC KEY PAIR SC: Ext. Auth. Chipkarte – ZDA (mit Etablierung TC) (asym.)	Das Auslesen des öffentlichen Signaturschlüssels ist nur ZDAs mit dem entsprechenden Recht erlaubt und erst nach Aufbau eines Trusted Channels zwischen ZDA und Chipkarte. Inhalt (Rückgabewert): Im Rahmen der Vorpersonalisierung (oder später) erzeugter öffentlicher Schlüssel Das Speichern des Schlüssels erfolgt betriebssystem-spezifisch
7	EF Card Capability Description (CCD)	Funktion: Read Record SC: Always	Das EF muss ohne Einhaltung von Zugriffsbedingungen gelesen werden können. Die Kodierung wird im konkreten Anhang zu einem Kartenprofil festgelegt.
8	EF PIN	Funktion: Verify, Change RD, Reset RC SC: Always Hierbei handelt es sich um die im Zusammenhang mit dem Anlegen eines PIN-Objekts COS-spezifisch gespeicherte PIN.	EF PIN ist noch nicht für den Wirkbetrieb gesetzt. Inhalt: • Im Transportzustand ein nicht für die Erzeugung von Signaturen geeigneter Wert, z.B. eine fünfstellige PIN Er kann von einem ZDA, der die dazu notwendigen Geheimnisse kennt, errechnet und dem Karteninhaber mitgeteilt werden. • Nach erfolgtem Nachladen ein für die Erzeugung von Signaturen geeigneter Wert, den nur der Karteninhaber kennt.

Nr	Titel	Definition	Erläuterung
9a	EF PUK (optional)	Funktion: Reset RC SC: Always Hierbei handelt es sich um die im Zusammenhang mit dem Anlegen eines PIN-Objekts COS-spezifisch gespeicherte PUK.	Der Karteninhaber kann mittels Eingabe der PUK den Fehlbedienzähler der PIN zurücksetzen. Die Anzahl, wie oft der PIN-Fehlbedienzähler mittels der PUK zurückgesetzt werden darf, legt der ZDA-VP fest. Inhalt: • Im Transportzustand ein fester dem Karteninhaber unbekannter Wert. Er kann von einem ZDA, der die dazu notwendigen Geheimnisse kennt, errechnet und dem Karteninhaber mitgeteilt werden. • Nach Änderung der Transport-PIN in eine 6-stellige PIN kann dieser Wert zum Rücksetzen des Fehlbedienzählers der PIN genutzt werden.
oder alternativ			
9b	EF PUK Info	Funktion: Read Binary SC: Ext. Auth. Chipkarte-ZDA (mit Etablierung TC) *Hierbei handelt es sich nicht um die im Zusammenhang mit dem Anlegen eines PUK-Objekts COS-spezifisch gespeicherte PUK, sondern um den gleichen separat noch einmal gespeicherten Wert.*	Der Wert der PUK ist auslesbar durch einen ZDA nach vorheriger gegenseitiger Komponentenauthentifikation auf Basis von CV Zertifikaten. Dieses Verfahren steht unter dem Vorbehalt einer Bestätigung nach SigG und SigV.

Lässt sich der Inhalt von EF PIN durch ChangeRD auf einen nutzbaren Wert ändern mit dem abgeleiteten Wert als „alter PIN“, so befand sich die Chipkarte bis zu diesem Zeitpunkt noch im Transportzustand. Bei Misserfolg muss der Transportzustand als gebrochen angesehen werden, es darf kein qualifiziertes Zertifikat erzeugt werden.

7.1.4 Zustand nach erfolgreichem Nachladen

Der Nutzungszustand unterscheidet sich vom Transportzustand in folgenden Punkten:

- Im EF Certificate befindet sich ein qualifiziertes Zertifikat,
- die PIN im EF.PIN ist auf eine nutzbare und nur dem Karteninhaber bekannte PIN geändert und
- der Karteninhaber ist in die Lage versetzt, die PUK in einen betriebsbereiten Zustand zu überführen, wenn sie sich nicht bereits in einem solchen befindet.

Ist der Nutzungszustand erreicht, so darf auf seiner Grundlage ebenfalls ein erneutes Nachladen initiiert werden. Erneutes Nachladen auf Basis des Nutzungszustandes unterscheidet sich vom erstmaligen Nachladen in den folgenden Punkten:

- Der Schlüssel wird direkt dem bereits existierenden qualifizierten Zertifikat entnommen. Gegenwärtig kann gemäß dieser Spezifikation nur dieser Schlüssel re-zertifiziert werden. Die Verwendbarkeit des „alten“ Schlüssels fällt unter die gleichen Bedingungen wie bei der erstmaligen Zertifizierung. Es ist der Algorithmenkatalog der Bundesnetzagentur zu beachten.
- PIN und PUK sind bereits erfolgreich in Betrieb genommen worden, sie müssen nicht erneut betrachtet werden.
- Die Ausstellung eines Folge-Zertifikats kann auf der Basis eines mit dem „alten“ Zertifikat elektronisch signierten Antrags erfolgen.

7.2 Zertifikatshierarchie Gütesiegel-Zertifikate

Ein Gütesiegel im Sinne dieser Spezifikation kann im Rahmen des folgenden Konzepts als Sicherheitsanker benutzt werden:

- Ein ZDA-VP erklärt mit Hilfe einer elektronischen Signatur,
  - dass in seiner Verantwortung in eine bestimmte Chipkarte (referenziert über die Seriennummer) ein Schlüsselpaar eingebracht wurde, das aus einem nach SigG bestätigten Schlüsselgenerator kommt,
  - dass für die Chipkarte eine Bestätigung nach SigG vorliegt,
  - dass die Chipkarte in einem Prozess unter einem nach SigG bestätigten Sicherheitskonzept in diesen Transportzustand gebracht wurde.
- Dies wird technisch dadurch realisiert, dass über den öffentlichen Schlüssel des o.g. Schlüsselpaares ein X.509-Zertifikat erstellt wird, in dem als Subject die Zertifikatsseriennummer und weitere Merkmale zur Identifikation des ZDA und der Chipkartenbestätigung eingetragen sind.
- Die o.g. Signatur ist die Signatur unter diesem Zertifikat.
- Ein ZDA-NL kann basierend auf dieser Erklärung des ZDA-VP ein qualifiziertes Zertifikat im Rahmen seines nach SigG bestätigten Sicherheitskonzepts erzeugen

.

Zur Ausstellung von Gütsiegel-Zertifikaten betreibt jeder ZDA eine eigene PKI mit einer eigenen Root-CA sowie optional einer oder mehrerer Transport-CAs. Zur Erstellung von Gütesiegeln wird ein Transport-CA-Zertifikat verwendet.

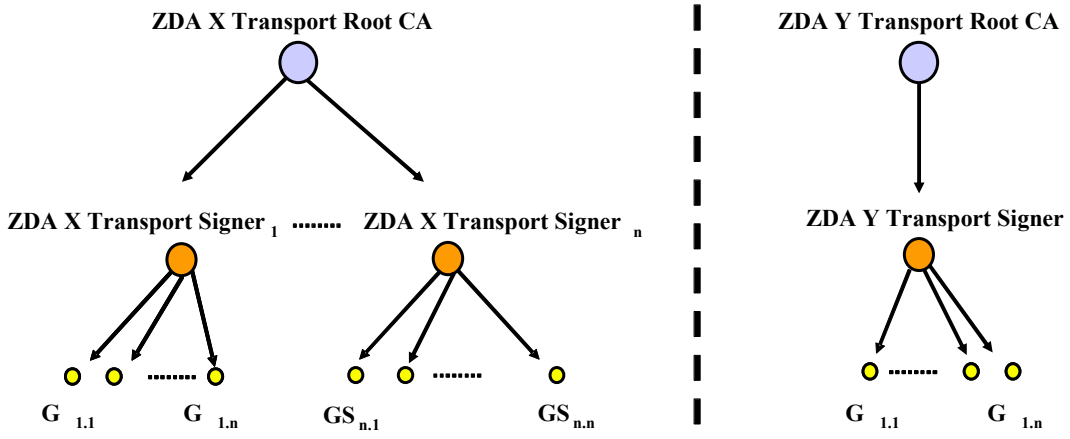

Abbildung 2: Zertifikatshierarchie Gütesiegel-Zertifikate

Eine Transport-CA bietet den Vorteil, dass ein einfaches Sperrmanagement von ganzen Mengen von GS möglich wird, indem eine solche CA ggf. ganz gesperrt werden kann. Eine solche Transport-CA kann z.B. auch im Auftrag eines ZDA bei einem Kartenproduzenten stehen und dann bei Missbrauch vollständig abgeschaltet werden.

Diese Struktur bietet den Vorteil, dass die gegenseitige Anerkennung verschiedener ZDAs flexibel gehandhabt werden kann. So kann z.B. ein ZDA anhand der Root eines anderen ZDAs die gesamte Transport-PKI-Hierarchie dieses ZDAs in sein Sicherheitskonzept integrieren, während ein weiterer ZDA ggf. nur eine bestimmte Transport-Signer-CA integriert.

Auf eine gemeinsame Root wird aus praktischen Gründen verzichtet. Jeder ZDA-NL integriert im Rahmen der Bestätigung seines Sicherheitskonzeptes die Roots der darin aufgenommenen ZDA-VPs. Die Bekanntgabe wird im Rahmen des für die Integration ins Sicherheitskonzept notwendigen Vertrages zwischen ZDA-VP und ZDA-NL geregelt.

7.2.1 Zertifikatsprofile

Für Root- und Signer-Zertifikate werden übliche Zertifikatsprofile zu [X.509V3] ohne besondere Anforderungen verwendet. Signer-Zertifikate ersetzten in diesem Zusammenhang die sonst üblichen CA-Zertifikate. Zur Kennzeichnung, dass es sich um eine PKI zur Ausgabe von X509-Gütesiegel-Zertifikaten handelt, sollen die „CommonNames“ (CN) folgendem Schema folgen:

- Root-CA-Zertifikate: CN = [ZDA] Transport Root [Jahr]
  - Bsp. „XY-ZDA Transport Root 05“
- CA-Zertifikate: CN = [ZDA] Transport Signer [Jahr]
  - Bsp. „XY-ZDA Transport Signer 05“

Für die Gütesiegel-Zertifikate soll ein Zertifikatsprofil zu [X.509V3] mit folgenden Merkmalen verwendet werden:

Tabelle 4: X.509 Zertifikatsprofil Gütesiegelzertifikat

Attribute	Inhalt	Kommentar
Version	2	V3
SerialNumber	<Seriennummer>	
SignatureAlgorithm Identifier	z.B. 1 2 840 113549 1 1 5	sha1withRSAEncryption
Issuer		
Country	<Länderkürzel>	
Organisation	<ZDA>	
Organisational Unit	<ZDA>	optionales Attribut für weitere Beschreibung des ZDA
Common Name	<Name d. Transport Signer>	Format: CN = [ZDA] Transport Signer [Personalisierer xyz] [Jahr], z.B. „ZDA XY Transport Signer 06“
Validity		
Not Before	<Datum Erstellung>	Die Gültigkeit wird durch den ZDA festgelegt, es

Attribute	Inhalt	Kommentar
Not After	<Datum Erstellung + Gültigkeitsdauer>	werden keine Vorgaben gemacht. Eine Gültigkeitsdauer wird gesetzt, um die Verarbeitung mit Standardsoftware zu ermöglichen, sie hat aber keine Bedeutung für die tatsächliche Dauer der Verwendbarkeit des enthaltenen öffentlichen Schlüssels. Diese richtet sich z.B. nach dem Algorithmenkatalog oder anderen Anforderungen an Schlüssel für qualifizierte Zertifikate
Subject		
Country	<Länderkürzel>	
Organisation Name	<ZDA>	
Organisational Unit	<ZDA>	
Common Name	<ICSN>	eindeutige Seriennummer des Chips
SubjectPublicKeyInfo	1 2 840 113549 1 1 1	rsaEncryption
	<Public key des Signaturschlüssels>	Da es sich bei einem GS um ein Zertifikat über den Public Key des später zu erzeugenden qualifizierten Zertifikats handelt, steht hier der öffentliche Schlüssel des Signatur-Schlüsselpaares
CertificatePolicies	1 3 6 1 4 1 25564 1 1	Es wird eine für alle ZDAs[11] einheitliche OID gesetzt, welche als Kennzeichnung, dass es sich um ein GS handelt, wie folgt definiert ist: • Die OID beschreibt, dass der Schlüssel geeignet ist, d.h. dass der Schlüssel aus einem evaluierten und nach SigG bestätigten Schlüsselgenerator stammt. • Die OID beschreibt, dass es sich bei der Karte um eine evaluierte und nach SigG bestätigte Signaturkarte handelt.
AuthorityKeyID	<ID>	
SubjectKeyIdentifier	<ID>	

Die Belegung von weiteren Standard-Feldern aus [X.509V3] ist erlaubt, darf aber nicht dazu führen, dass eine Verwendung nur basierend auf der Auswertung dieser zusätzlichen Felder möglich ist. Es dürfen keine zusätzlichen privaten Extensionen eingefügt werden, insbesondere keine als kritisch markierten.

7.3 CV-Zertifikatshierarchie

Ein CV-Zertifikat kann im Rahmen des folgenden Konzepts als Sicherheitsanker benutzt werden:

- Ein ZDA-VP
  - bringt in seiner Verantwortung in eine bestimmte Chipkarte ein CV-Zertifikat ein, das über die dahinterliegende Zertifikatshierarchie auf diesen ZDA-VP zurückgeführt werden kann.

[11] 1 3 6 1 4 1 25564 ist die für T7 reservierte private enterprise OID

- Er bringt solche CV-Zertifikate ausschließlich in Chipkarten ein, für die eine Bestätigung nach SigG vorliegt.
- Der öffentliche Schlüssel des Signatur-Schlüsselpaares kann basierend auf dem CV-Zertifikat authentisiert aus der Chipkarte ausgelesen werden (Trusted Channel nach gegenseitiger Komponentenauthentisierung).

- Ein ZDA-NL kann basierend auf der Verfikation eines solchen CV-Zertifikats des ZDA-VP ein qualifiziertes Zertifikat im Rahmen seines nach SigG bestätigten Sicherheitskonzepts erzeugen.

.

Für die Verwendung von CV-Zertifikaten als Sicherheitsanker muss eine getrennte PK-Infrastruktur bereitgestellt werden. Sofern im Rahmen der primären Anwendung bereits ein CV-Zertifikat auf der Chipkarte aufgebracht ist, besteht im Einzelfall die Möglichkeit, dieses und damit das hierzu erzeugte Schlüsselpaar zu nutzen. Voraussetzung ist jedoch, dass ein ZDA-VP dieses CV-Zertifikat für die Chipkarte erzeugt oder im Auftrag erzeugen lässt.

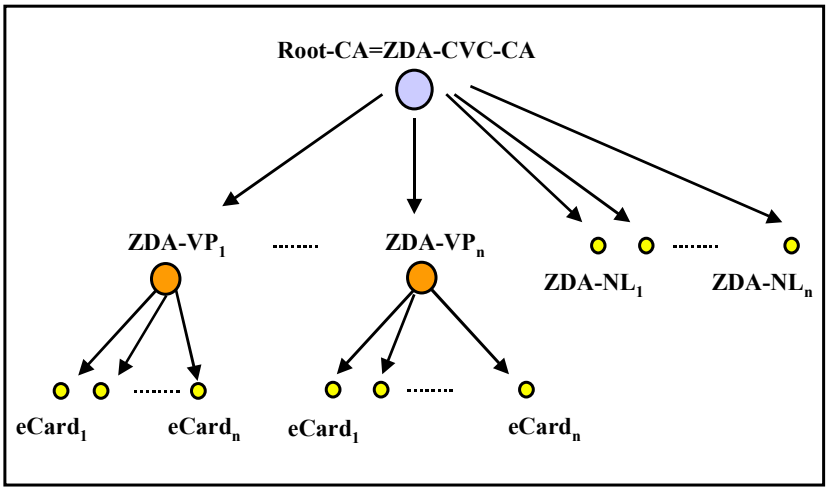

Abbildung 3: Zertifikatshierarchie CVC

Zunächst wird eine Root-CA festgelegt. Diese erstellt sowohl die CV-Zertifikate für die einzelnen ZDA-VP als auch für die ZDA-NL.

Schlüsselmanagement:

Jeder ZDA-VP erzeugt und verwaltet die Schlüssel für die CV-Zertifikate der Karte selbst. Die Schlüssel für das CV-Zertifikat als CV-CA erzeugt er ebenfalls selbst und läßt sich von der Root-CA ein CV-Zertifikat darüber erstellen.

Die ZDA-CVC-CA erzeugt und verwaltet die Schlüssel für das ZDA-CVC-CA CV-Zertifikat selbst und läßt sich von der Root-CA ein CV-Zertifikat darüber erstellen.
Ein ZDA-NL erzeugt die Schlüssel für sein CV-Zertifikat selbst und läßt sich von der ZDA-CVC-CA ein CV-Zertifikat darüber erstellen.

Unterscheidung der ZDA-VPs:

Um die für die Vorpersonalisierung zugelassenen ZDA-VP unterscheiden zu können, wird für jeden ein eindeutiges 3 ASCII Zeichen langes Akronym vergeben. Dieses wird an geeigneter Stelle auf der Chipkarte gespeichert (z.B. innerhalb des EF CCD) sowie in die CHR des CV-Zertifikats des ZDA-VP geschrieben.

Tabelle 5: Akronyme der ZDA für CVC

ZDA-VP	Akronym
Datev	DTV
Deutsche Post Com	DPC
DSV	DSV
D-Trust	DTR
T-Systems	TSI
TC TrustCenter	TCT

Für das Akronym der ZDA-CV-CA wird ASCII kodiert 'ZCA' festgelegt. Dieses wird in den CA-Namen der CAR der CV-Zertifikate des HSM der ZDA-NL und in den CA-Namen der CAR des CV-Zertifikats der ZDA-VP geschrieben.

7.4 PIN/PUK-Ableitungsverfahren

Falls die Transport-PIN bzw. die PUK abgeleitet werden, dann ist das nachstehende Ableitungsverfahren zu verwenden.

7.4.1 Überblick über das Ableitungsverfahren

Zur Berechnung wird ein geheimer 16 Byte langer Masterkey MK herangezogen. Dieser wird vom ZDA-VP allen ZDA-NL zur Verfügung gestellt. Für die Berechnung der Transport-PIN wird ein anderer Masterkey als zur Berechnung der PUK verwandt.
Das Verfahren zur Ableitung unterteilt sich in drei Schritte und unterscheidet sich geringfügig, je nachdem, ob eine Transport PIN oder eine PUK berechnet wird:

Transport-PIN

- Erzeugung eines kartenindividuellen Datenblocks DBL_1.
- Ableitung eines Zwischenwerts ZW_1 aus dem kartenindividuellen Datenblock DBL_1 und dem Masterkey MK.
- Ableitung der Transport-PIN aus dem Zwischenwert ZW_1.

PUK

- Erzeugung von zwei kartenindividuellen Datenblöcken DBL_1 und DBL_2.
- Ableitung von zwei Zwischenwerten ZW_1 und ZW_2 aus den kartenindividuellen Datenblöcken DBL_1 und DBL_2 und dem Masterkey MK.
- Ableitung der PUK aus den Zwischenwerten ZW_1 und ZW_2.

7.4.2 Erzeugung der kartenindividuellen Datenblöcke

Die kartenindividuellen Datenblöcke bestehen aus 12 Byte

- ICCSN aus dem CV-Zertifikat, Gütesiegel oder EF.BVD (10 Byte)
- ID der evaluierten und bestätigten Signaturkarte aus EF.ASD (2 Byte)

und sind wie folgt aufgebaut:

DBL_1 = ICCSN | ID

DBL_2 = ID | ICCSN

7.4.3 Ableitung der Zwischenwerte aus einem Masterkey

Zur Ableitung eines Zwischenwerts ZW aus einem kartenindividuellen Datenblock DBL und einem Masterkey MK wird der folgende Algorithmus verwendet:
Dabei wird für die Zwischenwerte ZW_1 bzw. ZW_2 der Datenblock DBL_1 bzw. DBL_2 verwandt.
Der 16 Byte lange Zwischenwert ZW (= ZW_1 oder ZW_2) wird aus den Daten

- MK (16 Byte)
- DBL (= DBL_1 oder DBL_2), Datenblock mit '00' auf eine Länge eines Vielfachen von 8 Byte gepaddet, wobei die Mindestlänge 16 Byte ist
- der öffentliche Initialwert

  I='52 52 52 52 52 52 52 52 25 25 25 25 25 25 25 25' (16 Byte)

als

ZW = d*MK(H(I,DBL))

berechnet.
Hierbei ist

- d*MK die Triple-DES Entschlüsselung mit dem Schlüssel MK, wobei die beiden 8 Byte langen Blöcke H1 und H2 von H(I,DBL) = H1 | H2 separat entschlüsselt werden (ECB-Mode)

- H die in [ISO HF2] definierte Hash-Funktion, die Werte X mit einer Länge, die ein Vielfaches von 8 Byte ist, mittels des Startwertes I (gemäß Anhang A von [ISO HF2]) auf einen Wert von 16 Byte Länge abbildet. Es werden die um das Parity Adjustment P erweiterten Transformationen u (Ad10) und u' (Ad 01) aus Anhang A von [ISO HF2] verwendet. H ist rekursiv definiert:

- Sei X = x1|...|xn die Zerlegung des Wertes X in 8 Byte lange Blöcke und L0|R0 die Zerlegung des vorgegebenen Startwerts I in zwei 8 Byte Blöcke.

- eK(X) ist die DES-Verschlüsselung eines 8 Byte Wertes mit einem 8 Byte Schlüssel.

- $\oplus$ sei die bitweise Addition modulo 2 (XOR).

- Die Transformationen Ad10 und Ad01 transformieren 8 Byte Werte K wie folgt:

  Sei $K = k_1,...,k_{64}$ die Darstellung von K als Folge von 64 Bit. Dann ist

  $Ad10(K) = [P](k_1,1,0,k_4,...,k_{64})$

  $Ad01(K) = [P](k_1,0,1,k_4,...,k_{64})$

  [P]: Das Parity Adjustment in Ad10 und Ad01 ist optional. Wenn vor der DES-Verschlüsselung eK(X) keine Paritätsprüfung des Schlüssels K erfolgt, kann P entfallen.

- Dann errechnet sich $L_i|R_i$ aus $L_{i-1}|R_{i-1}$ und x_i wie folgt:

  L_{i-1} bestehe aus den Bits $l_1,...,l_{64}$ und R_{i-1} bestehe aus den Bits $r_1,...,r_{64}$,

  Schritt 1: $L'_i := Ad10(L_{i-1}) = [P](l_1,1,0,l_4,...,l_{64})$

  $R'_i := Ad01(R_{i-1}) = [P](r_1,0,1,r_4,...,r_{64})$

  Schritt 2: $A_i = A_{i[links]}|A_{i[rechts]} = eL'_i(x_i) \oplus x_i$.

  $B_i = B_{i[links]}|B_{i[rechts]} = eR'_i(x_i) \oplus x_i$.

  Schritt 3: $L_i = A_{i[links]}|B_{i[rechts]}$

  $R_i = B_{i[links]}|A_{i[rechts]}$

- $L_n|R_n$ ist dann der Hash-Wert von X unter H:

  $H(I,X) = L_n|R_n$

7.4.4 Ableitung der Transport-PIN aus dem Zwischenwert ZW_1

Zur Ableitung der 5-stelligen Transport-PIN aus dem Zwischenwert ZW_1 wird der folgende Algorithmus benutzt:
Der Zwischenwert ZW_1 besteht aus 32 Halb-Bytes, die ihrerseits jeweils eine Ziffer zwischen 0 und 15 darstellen. In diesem Sinne besteht ZW_1 aus 32 Ziffern.

1. Setze n = Anzahl der Ziffern aus ZW_1, die im Bereich '0' – '9' liegen.
2. Falls n >= 5 gehe zu Schritt 7.
3. Suche von links nach rechts die erste Ziffer im Bereich 'A' - 'F'.
4. Falls n gerade ist, ersetze die in Schritt 3 gefundene Ziffer gemäß folgender Abbildung: 'A' durch '0', 'B' durch '1', ... und 'F' durch '5'.
5. Falls n ungerade ist, ersetze die in Schritt 3 gefundene Ziffer gemäß folgender Abbildung: 'A' durch '4', 'B' durch '5', ... und 'F' durch '9'.
6. Erhöhe n um eins und gehe zu Schritt 2.
7. Die Transport-PIN besteht aus der Konkatenation der ersten 5 Ziffern von links nach rechts in dem Bereich '0' – '9' von ZW_1.

Bemerkung: In dem Fall, dass es in den 32 Halb-Bytes keine fünf Ziffern im Bereich '0 – 9' gibt, werden die Ziffern '0 – 9' der Transport-PIN nicht exakt gleichverteilt. Dieser Fall kann aber vernachlässigt werden, da er nur mit der Wahrscheinlichkeit

$$\sum_{i=0}^{4}\binom{32}{i}\left(\frac{10}{16}\right)^{i}\left(\frac{6}{16}\right)^{32-i} \approx 7\cdot 10^{-9}$$

auftritt (Bernoulli-Experiment).

7.4.5 Ableitung einer PUK aus den Zwischenwerten ZW_1 und ZW_2

Für die kryptographische Ableitung der 8-stelligen PUK wird ein eigener Masterkey verwendet, der vom ZDA-VP an den ZDA-NL zu übergeben ist.
Zur Ableitung der PUK werden aus den Zwischenwerten ZW_1 und ZW_2 jeweils eine Halb-PUK HP_1 und HP_2 von je vier Ziffern berechnet. Die beiden Halb-PUKs HP_1 und HP_2 werden dann zu der PUK zusammengefügt. Jede der Halb-PUKs wird analog zu der Ableitung der Transport-PIN berechnet.
Der Zwischenwert ZW_i (i = 1, 2) besteht aus 32 Halb-Bytes, die ihrerseits jeweils eine Ziffer zwischen 0 und 15 darstellen. In diesem Sinne besteht ZW_i aus 32 Ziffern.

1. Setze n = Anzahl der Ziffern aus K, die im Bereich '0' – '9' liegen.
2. Falls n >= 4 gehe zu Schritt 7.
3. Suche von links nach rechts die erste Ziffer im Bereich 'A' - 'F'.

4. Falls n gerade ist, ersetze die in Schritt 3 gefundene Ziffer gemäß folgender Abbildung: 'A' durch '0', 'B' durch '1', ... und 'F' durch '5'.

5. Falls n ungerade ist, ersetze die in Schritt 3 gefundene Ziffer gemäß folgender Abbildung: 'A' durch '4', 'B' durch '5', ... und 'F' durch '9'.

6. Erhöhe n um eins und gehe zu Schritt 2.

7. Die Halb-PUK HP_i (i = 1, 2) besteht aus der Konkatenation der ersten 4 Ziffern von links nach rechts in dem Bereich '0' – '9' von ZW_i.

Bemerkung: In dem Fall, dass es in den 32 Halb-Bytes keine vier Ziffern im Bereich '0 – 9' gibt, werden die Ziffern '0 – 9' der Transport-PIN nicht exakt gleichverteilt. Dieser Fall kann aber vernachlässigt werden, da er nur mit der Wahrscheinlichkeit

$$\sum_{i=0}^{3}\binom{32}{i}\left(\frac{10}{16}\right)^{i}\left(\frac{6}{16}\right)^{32-i} \approx 8\cdot 10^{-10}$$

auftritt (Bernoulli-Experiment).
Die PUK ergibt sich aus den beiden Halb-PUKs: PUK = HP_1 | HP_2.

7.5 Anforderungen Vorpersonalisierungs-Anwendung

Die Vorpersonalisierungsanwendung muss folgende funktionale Anforderungen erfüllen:

- Verwendet folgende Mittel, um
  - Gütesiegel aufzubringen
    1. Bei Erzeugung des Schlüsselpaares auf der Karte: Möglichkeit zum Auslesen des öffentlichen Schlüssels (aus EF Public Key)
    2. Signierkomponente, mit der der öffentliche Schlüssel in Form eines GS signiert werden kann.
       - Verwendet dafür das nach Kap. 7.2 für die Signatur von öffentlichen Schlüsseln entsprechend dieser Spezifikation geeignete Zertifikat des ZDA
    3. Möglichkeit zum Einbringen des GS in die Karte, ins EF Certificate

  oder

  - CV-Zertifikate aufzubringen
    1. Schlüsselgenerator für die für das CV-Zertifikat benötigten Schlüssel
    2. Signierkomponente, mit der der öffentliche CV-Schlüssel signiert werden kann.
       - Verwendet dafür das Zertifikat des ZDA-VP nach Kap. 7.3

3. Möglichkeit zum Einbringen des CV-Zertifikats, des zugehörigen privaten Schlüssels sowie des öffentlichen Schlüssels der ZDA-CVC-CA

- Falls eine von Kartenmerkmalen abgeleitete Transport-PIN verwendet wird, muss folgende Information dem ZDA-NL zur Verfügung gestellt werden:
  - MasterKey, von dem abgeleitet wird
- Falls eine von Kartenmerkmalen abgeleitete Transport-PUK verwendet wird, muss folgende Information dem ZDA-NL zur Verfügung gestellt werden:
  - MasterKey, von dem abgeleitet wird
- Falls eine von Kartenmerkmalen abgeleiteter symmetrischer Schlüssel zum authentisierten Schreiben des Zertifikats in die Chipkarte und zum authentisierten Aktivieren des PIN-Objektes verwendet wird, muss folgende Information dem ZDA-NL zur Verfügung gestellt werden:
  - MasterKey, von dem abgeleitet wird
- Ein ZDA-VP kann Verschlüsselungs- oder Authentisierungszertifikate als Zuordnungsmerkmal zur Chipkarte mitteilen:
  - Die Übergabe dieses Merkmals muss zwischen ZDA-VP und ZDA-NL gesondert geregelt werden.

Die verwendeten Elemente müssen allen ZDA-NL vom ZDA-VP zur Verfügung gestellt werden.

7.6 Anforderungen Nachlade-Anwendung

Die Nachlade-Anwendung, mit deren Hilfe das Nachladen entsprechend dieser Spezifikation bewerkstelligt wird, muss folgende Anforderungen erfüllen:

- Die Nachlade-Anwendung verwendet folgende Elemente, um CVC nutzen zu können:
  - Besitzt CV-Zertifikat mit Rollen-ID der ZDA
  - öffentl. Schlüssel der CA, die eCard-CV-Zertifikate ausstellt
  - Die aufgeführten Elemente müssen entweder vom ZDA-VP oder dem Betreiber der ZDA-CVC-CA zur Verfügung gestellt werden.

- Die Nachlade-Anwendung verwendet folgende Elemente, um GS nutzen zu können:
  - Prüfmöglichkeit des GS
    1. Root-CA-Zertifikat für Gütesiegel (auf vertrauenswürdige Weise)
    2. CA-Zertifikate
    3. Zugehörige Sperrlisten (optional)

  - Masterkey für die Ableitung des symmetrischen Schlüssels für das Mac-gesicherte Lesen und Schreiben gegen die Chipkarte
  - Elemente, die verwendet werden, müssen zusätzlich zum Sicherheitskonzept des ZDA-VP auch im Sicherheitskonzept des ZDA-NL beschrieben werden.
- Falls eine von Kartenmerkmalen abgeleitete Transport-PIN verwendet wird, verwendet die Nachlade-Anwendung das folgende Element, das vom ZDA-VP zur Verfügung gestellt wird:
  - MasterKey, von dem abgeleitet wird
- Falls eine von Kartenmerkmalen abgeleitete Transport-PUK verwendet wird, verwendet die Nachlade-Anwendung das folgende Element, das vom ZDA-VP zur Verfügung gestellt wird:
  - MasterKey, von dem abgeleitet wird

Die aufgeführten Elemente müssen allen ZDA-NL vom ZDA-VP zur Verfügung gestellt werden.

8 Prototypischer Beispiel-Prozess

In diesem Kapitel werden die Teilprozesse Vorpersonalisierung und Nachladeprozess beschrieben. Diese Prozessbeschreibungen sind nicht normativ, sondern belegen die Möglichkeit (im Sinne eines Proof-of-Concept), auf der Grundlage der hier spezifizierten Transportzustände eine Bestätigung nach SigG und SigV für einen Nachladeprozess zu erlangen.

Die drei Varianten von Sicherheitsankern kombiniert mit PIN-Verfahren (s.o. 7.1.1), die bei der Vorpersonalisierung existieren, werden im Prozess abgeprüft und die entsprechende Bearbeitung wird angestoßen. Die Varianten seien hier noch einmal aufgeführt:

- Gütesiegelzertifikat mit Null-PIN
- Gütesiegelzertifikat mit abgeleiteter Transport-PIN
- CV-Zertifikat mit abgeleiteter Transport-PIN

8.1 Prozessübersichten

Eine Gesamtübersicht über den Prozess befindet sich in Kap. 5.2. Hier folgen detailliertere Darstellungen in Form von Flussdiagrammen, aus denen die unterschiedliche Verfahrensweise bei den verschiedenen Varianten ersichtlich wird.

8.1.1 Vorpersonalisierung

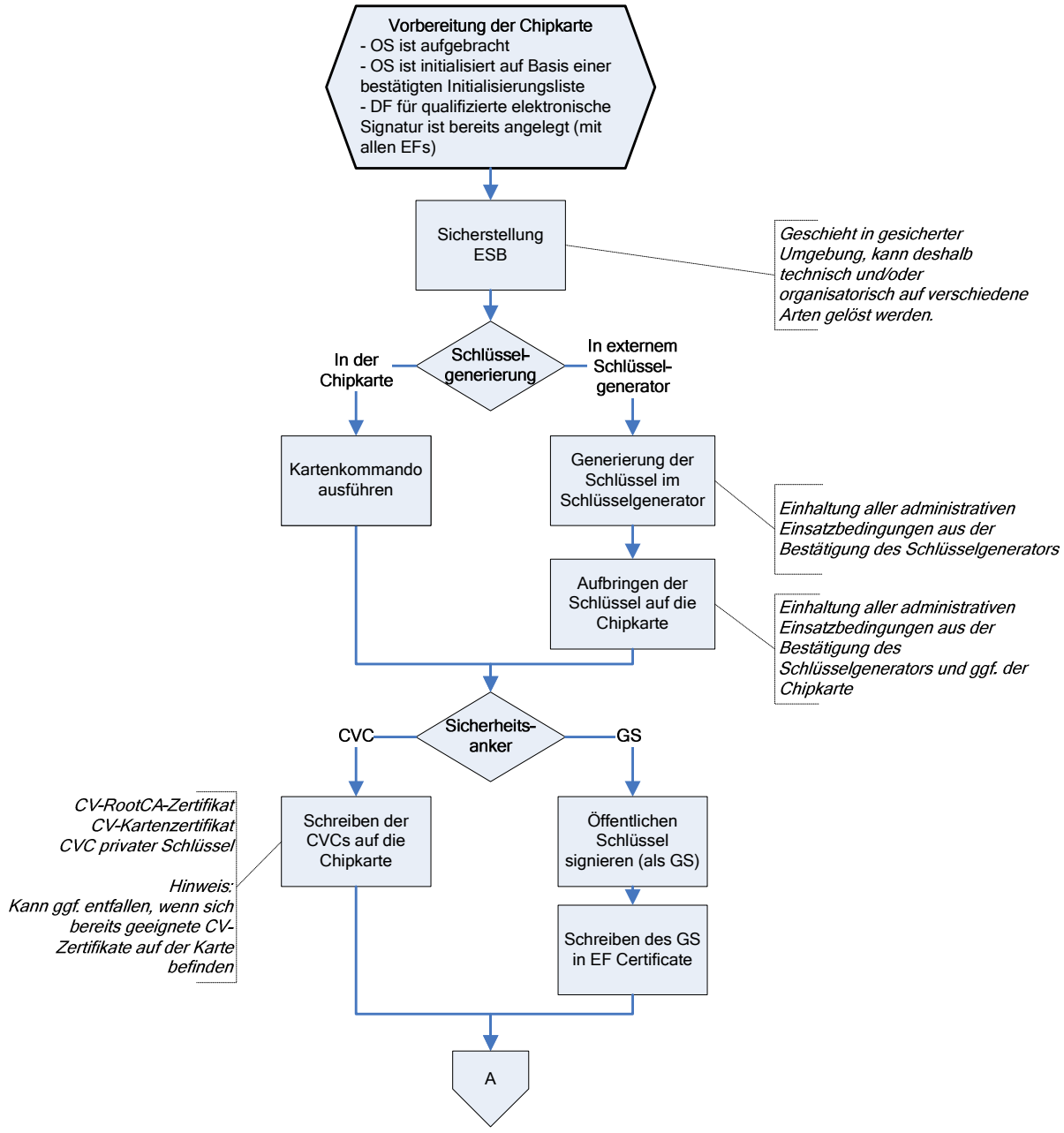

Abbildung 4: Vorpersonalisierung 1

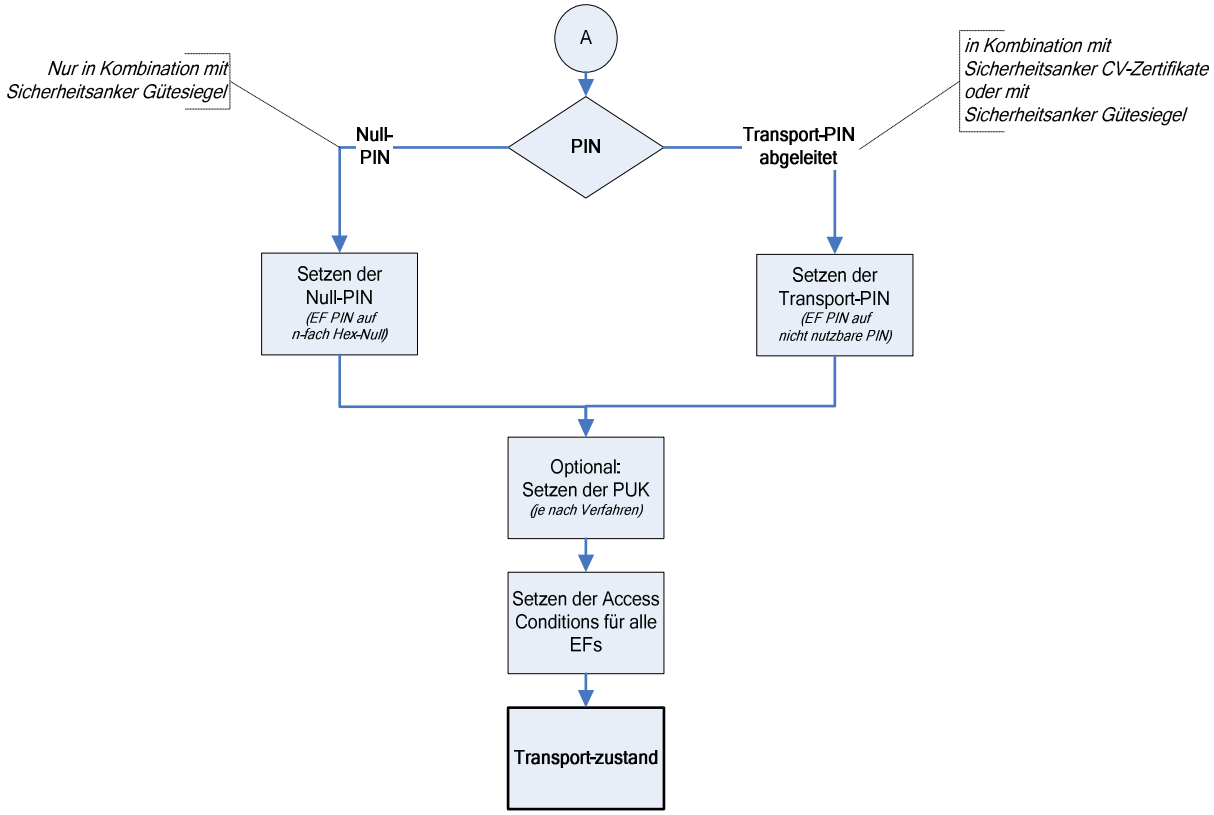

Abbildung 5: Vorpersonalisierung 2 (Fortsetzung)

Der Prozess der Vorpersonalisierung setzt sich aus den bereits genannten (Kap. 5.2) Elementen zusammen. Sie sind hier im Rahmen eines Teilprozesses Vorpersonalisierung in einer typischen Reihenfolge zusammengestellt. Insbesondere die zeitliche Reihenfolge ist abhängig von den Bedingungen der Produktionsumgebung beim Chipkartenproduzent. Z.B. kann die Initialisierung der PIN- und ggf. PUK-Objekte je nach Umgebung auch sehr viel früher im Prozess erfolgen. In dieser allgemeinen Beschreibung sind alle durch die verschiedenen Möglichkeiten der Vorpersonalisierung gegebenen Varianten als Zweig vorhanden. Im konkreten Fall einer bestimmten Vorpersonalisierung, die ZDA-VP/Kartenproduzent festgelegt haben, wird jeweils nur ein Zweig durchlaufen.

Hinweis: Da es sich sowohl bei den Gütesiegeln wie auch bei den CV-Zertifikaten nicht um qualifizierte Zertifikate im Sinne des Signaturgesetzes handelt, sondern um Maßnahmen der technischen Sicherheit zum Zwecke der Erzeugung von qualifizierten Zertifikaten, können für ihre Erzeugung HSMs eingesetzt werden, für die keine Evaluierung und Bestätigung nach dem Signaturgesetz vorliegt.

8.1.2 Nachladeprozess

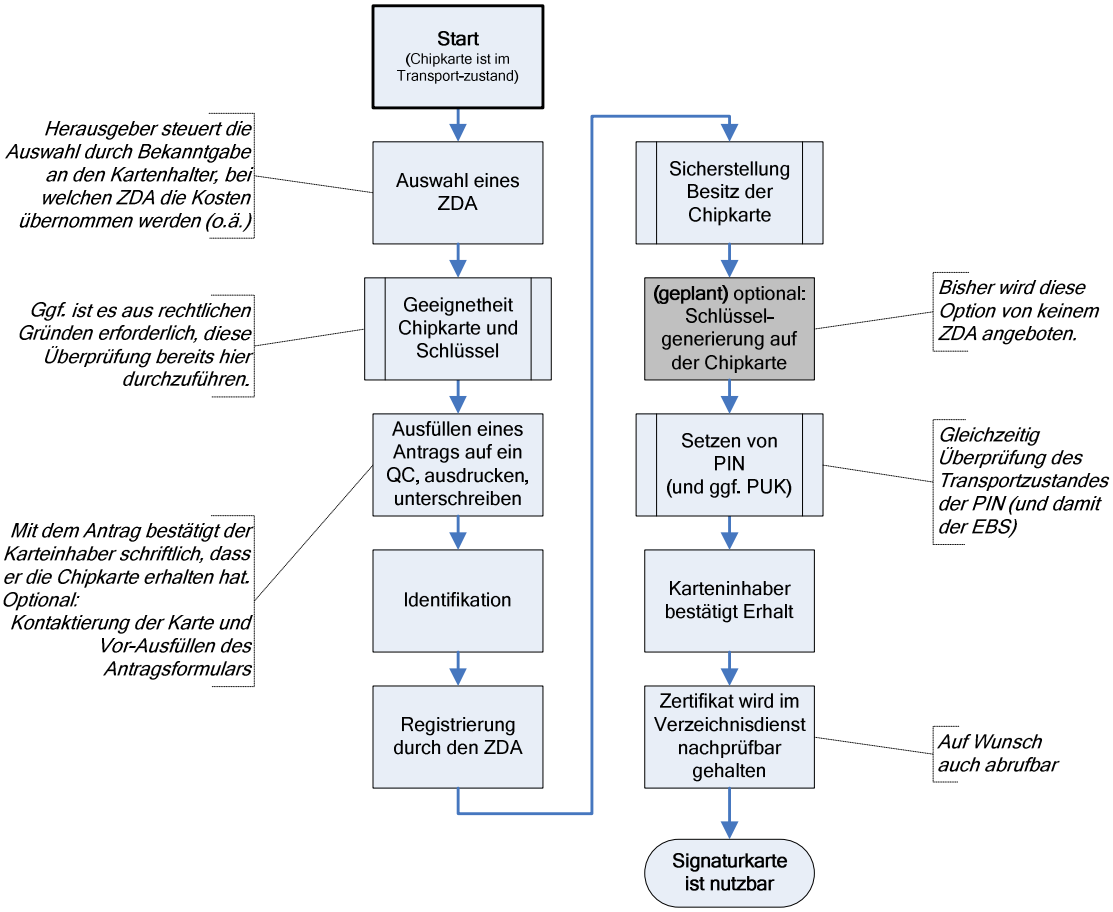

Abbildung 6: Nachladeprozess - Gesamtsicht

Der Nachladeprozess basiert auf den durch die Vorpersonalisierung geschaffenen Voraussetzungen, insbesondere auf der Art des Vertrauensankers und auf der Art der Absicherung der durch den Benutzer zu setzenden PIN und ggf. PUK. Im Unterschied zum Vorpersonalisierungsprozess besteht hier keine Wahlfreiheit mehr in Bezug auf diese Merkmale. Sie sind bei der Vorpersonalisierung gesetzt und müssen hier angemessen ausgewertet werden.

Aus Gründen der Übersichtlichkeit sind Teilprozesse aus dieser Grafik in Einzelsichten ausgelagert, die auf den folgenden Seiten dargestellt werden. Je nach Lösung der Anforderungen (s. Kap. 5.2) können sich aber auch hier völlig unterschiedliche Reihenfolgen der Prozessschritte ergeben.

Ein Abgleich der grundsätzlichen Erfüllbarkeit der gesetzlichen Anforderungen mit der Bundesnetzagentur erfolgt auf der Basis der hier niedergelegten Reihenfolge. Die rechtliche Herleitung dieser Reihenfolge ist in einem externen Dokument niedergelegt.

Im Folgenden werden Teilprozesse des Nachladens genauer beschrieben.

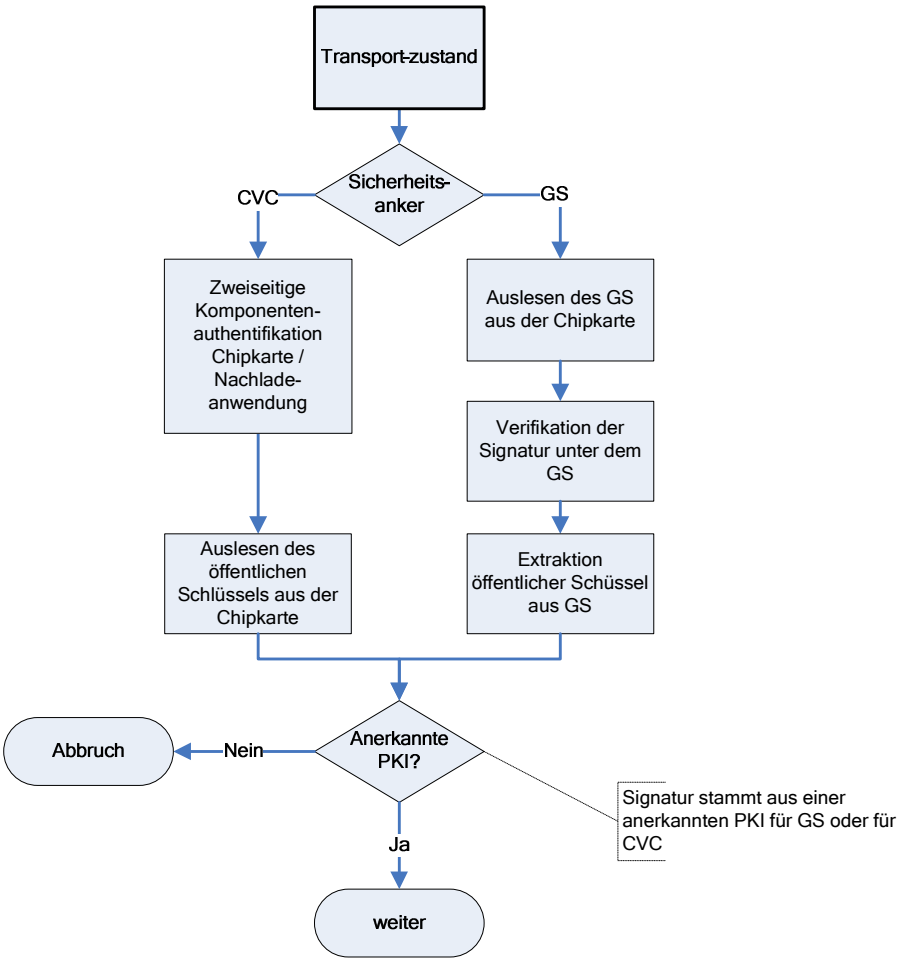

Abbildung 7: Nachladen Teilprozess - Geeignetheit Chipkarte und Schlüssel

Abhängig von der Art des bei der Vorpersonalisierung verwendeten Sicherheitsankers ist im Positivfall das Ergebnis dieses Teilprozesses die Vergewisserung auf seiten des ZDA, dass der jeweilige öffentliche Schlüssel verwendet werden darf und dass sich der zugehörige private Schlüssel geschützt auf einer evaluierten und bestätigten Signaturkarte befindet.

Eine „anerkannte PKI“ ist eine solche, die durch Vertrag zwischen ZDA-VP und ZDA-NL (s. Kap. 4) als PKI zu diesem Zweck vereinbart wurde, sowohl für CVC als auch für GS.

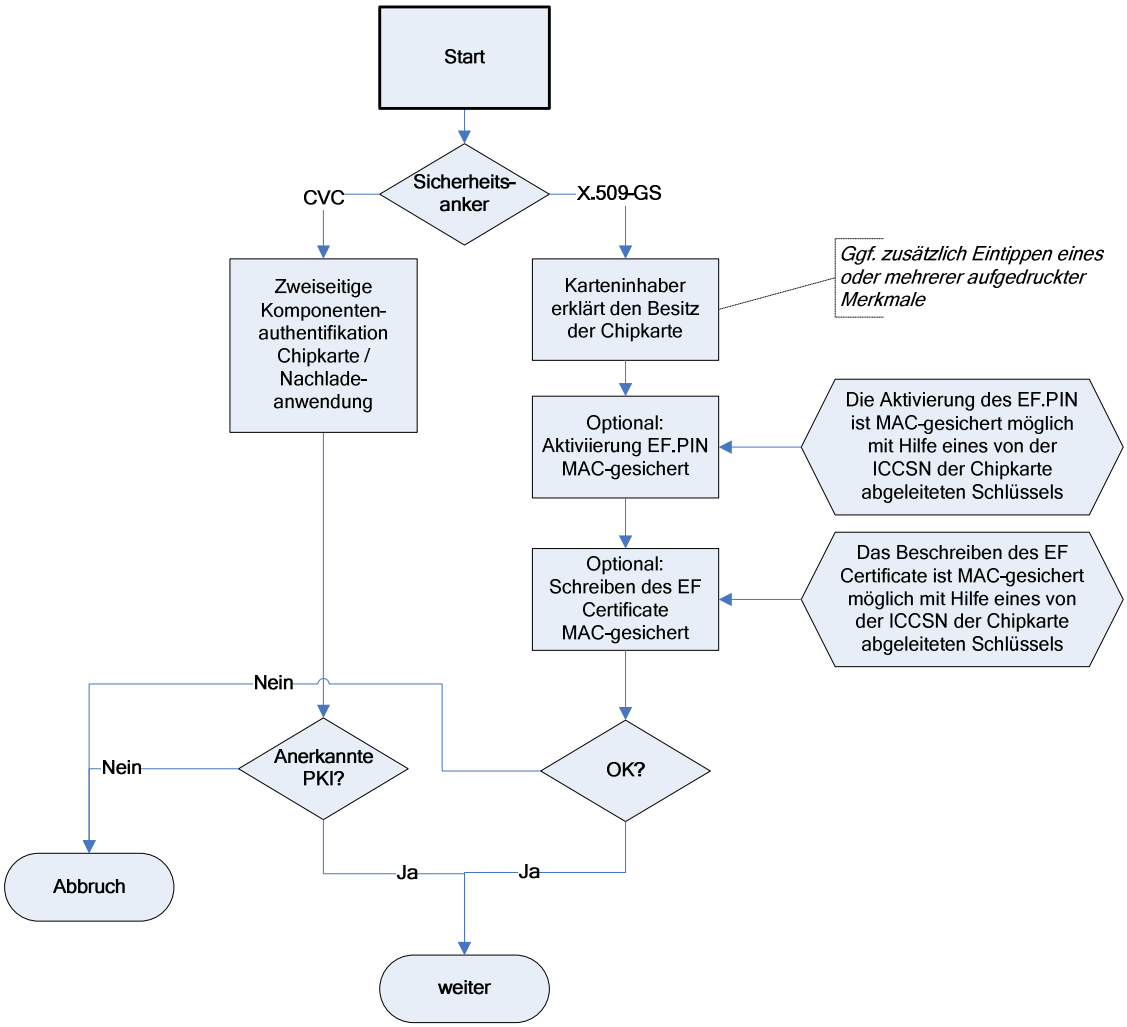

Abbildung 8: Nachladen Teilprozess - Sicherstellung Besitz Chipkarte

Die Sicherstellung auf seiten des ZDA, dass sich die Chipkarte im Besitz des Antragstellers befindet, hängt ebenfalls von der Art des bei der Vorpersonalisierung verwendeten Sicherheitsankers ab. Im Falle von GS werden neben dem Vertrauensanker selbst für die Erfüllung dieser Anforderungen typischerweise weitere technische Verfahren wie Verschlüsselung oder Authentisierung verwendet, die stärker sind als eine reine Erklärung des Antragstellers. Im Falle von CVC wird die Karte im Verlauf der Überprüfung direkt authentifiziert und damit als im Besitz der den Antrag stellenden Person verifiziert.

In jedem Falle müssen diese Informationen noch mit der Identifikation des Antragstellers alsEs ist aber zusätzlich zu berücksichtigen, dass sich der ZDA die Übergabe der Signaturschlüssel und der Identifikationsdaten von dem Karteninhaber schriftlich oder durch eine qualifizierte elektronische Signatur bestätigen lassen muss und dass durch weitere Merkmale (wie z.B. bei Beantragung vereinbarte Einmalpassworte) sichergestellt werden kann, dass die Person, die den Antrag gestellt hat und die Person, die die Karte zum Nachladen vorlegt, identisch sind.

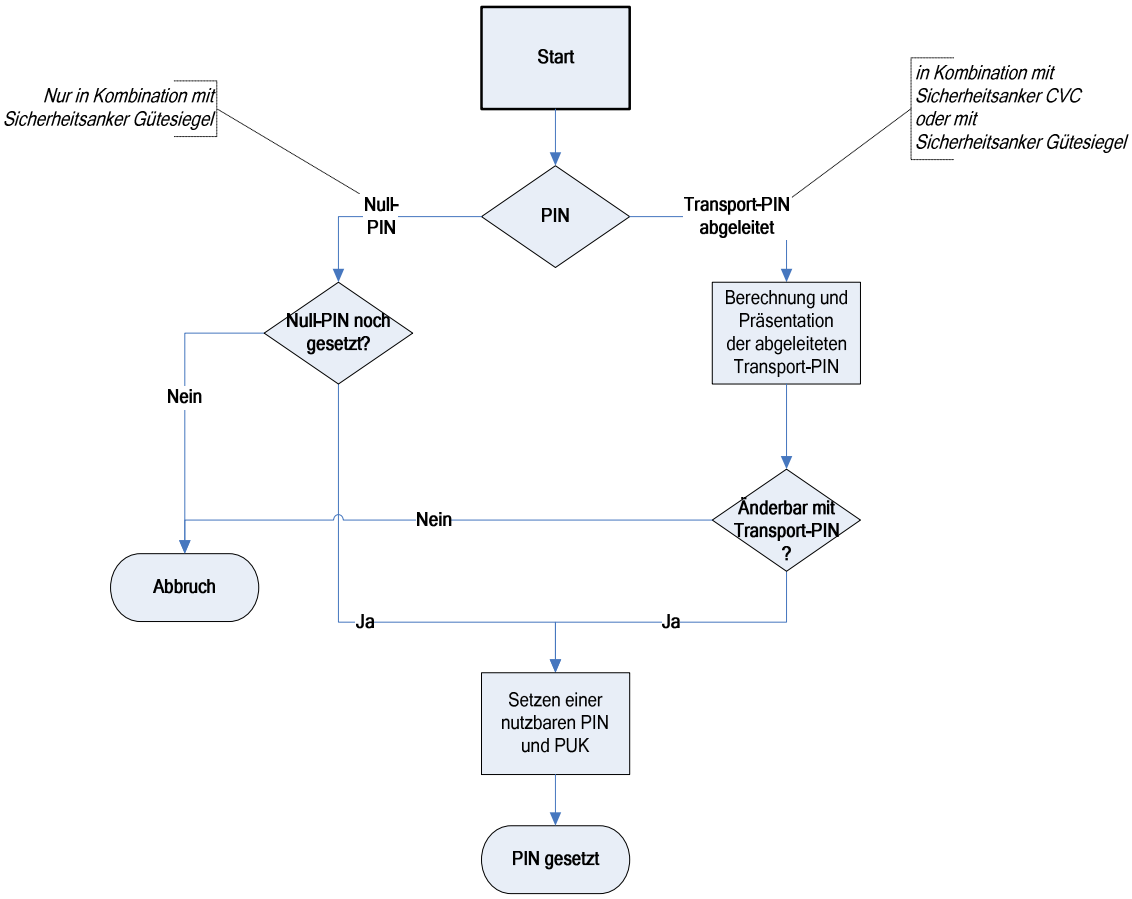

Abbildung 9: Nachladen Teilprozess - Setzen von PIN und ggf. PUK

Der Teilprozess „Setzen einer PIN“ hat die beiden Funktionen

- Verifikation des Transportzustandes[12]
- Inbetriebnahme der Chipkarte durch Setzen einer gebrauchsfähigen PIN

Ist die PIN (und ggf. die PUK) einmal gesetzt, ist der Transportzustand der Karte verlassen und kann nicht wiederhergestellt werden.

[12] Die Verifikation des Transportzustandes kann im Fall der abgeleiteten Transport-PIN auch indirekt erfolgen, z.B. indem die Transport-PIN fünfstellig ist und nach Setzen der nutzbaren sechsstelligen PIN nicht mehr in eine fünfstellige PIN geändert werden kann. Somit ist sichergestellt, dass sich die PIN im Transportzustand befand, wenn sie mit der fünfstelligen abgeleiteten Transport-PIN geändert werden konnte.

8.2 Sonderfall elektronischer Personalausweis

Im Falle des Nachladens auf einen elektronischen Personalausweis sind nach bisheriger Kenntnis wahrscheinlich folgende Besonderheiten gegeben:

- Eine **Identifizierung** hängt in diesem besonderen Fall an der Chipkarte selbst, die ja den bei der Identifizierung zu nutzenden Ausweis darstellt. Vorausgesetzt, es gibt eine sichere und bestätigte Möglichkeit, die im elektronischen Teil des Personalausweises gespeicherten Merkmale in den Beantragungsprozess zu übernehmen und so sicherzustellen, dass zu einem Ausweis immer ein Zertifikat mit genau den richtigen Daten aus dem Ausweis erstellt wird, könnte eine physisch durchzuführende Identifizierung überflüssig werden. Natürlich bleibt die Anforderung bestehen, dass der ZDA-NL sicherstellen muss, dass sich die Chipkarte noch im Besitz des Original-Karteninhabers befindet.
- Die geplante **Authentisierung** gegenüber der Anwendung auf der Chipkarte wird wahrscheinlich ähnlich der Verwendung von CV-Zertifikaten sein. Insofern muss zum gegenwärtigen Zeitpunkt davon ausgegangen werden, dass die aufgeführten Prozessmerkmale auch für den dPA Gültigkeit haben. Das ist natürlich nach Vorliegen entsprechenden Informationen zu überprüfen. Das aus dem dPA-Projekt dazu genannte Stichwort lautet „extended Access Control“.
- Die beim dPA eingesetzte **RFID-Technologie** erfordert zusätzlich zu den oben beschriebenen Authentisierungsschritten zwischen Ausweis und Nachladeanwendung auch Authentisierungsschritte zwischen Ausweis und Kartenterminal. Ein ausschließlich über RFID zu erreichender Ausweis erfordert beim Anwender ein entsprechendes Kartenterminal. Solange von dessen Existenz nicht sicher ausgegangen werden kann, sollten mindestens für eine Übergangszeit über den Einsatz von dual interface Chipkarten nachgedacht werden.
- Ob es sich beim dPA um eine Chipkarte im gleichen Format wie die bisher am Markt vertretenen Signaturkarten handeln wird, ist noch nicht festgelegt.
- Es ist auf jeden Fall eine **„späte“ Schlüsselgenerierung** vorgesehen. Die dafür notwendigen Voraussetzungen in Bezug auf Durchführung der Schlüsselgenerierung beim Karteninhaber (oder ggf. in einer gesicherten RA-Umgebung) müssen im Rahmen der Spezifikation des dPA geschaffen werden.
- In diesem Kontext soll auf einen ZDA-VP verzichtet werden, und als Sicherheitsanker sollen CV-Zertifikate verwendet werden, die bei der Produktion des Ausweises im Rahmen der für den Ausweis selbst geschaffenen Hintergrund-PKIs in den Ausweis eingebracht werden. Diese Elemente können erst nach abschließender Klärung der Umsetzbarkeit mit den Bestätigungsstellen und mit der Bundesnetzagentur in eine konkreten technischen Anhang für den dPA zu dieser Nachlade-Spezifikation eingeführt werden.

9 Anhang A: Gesetzliche Grundlagen

SigG

- SigG §4 Abs.5: Der Zertifizierungsdiensteanbieter kann unter Einbeziehung in sein Sicherheitskonzept nach Absatz 2 Satz 4 Aufgaben nach diesem Gesetz und der Rechtsverordnung nach § 24 an Dritte übertragen.
- SigG §5 Abs.4: Der Zertifzierungsdiensteanbieter hat Vorkehrungen zu treffen, damit Daten für qualifizierte Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Er hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der Signaturschlüssel zu gewährleisten. Eine Speicherung von Signaturschlüsseln außerhalb der sicheren Signaturerstellungseinheit ist unzulässig.
- SigG §5 Abs.6: Der Zertifizierungsdiensteanbieter hat sich in geeigneter Weise zu überzeugen, dass der Antragsteller die zugehörige sichere Signaturerstellungseinheit besitzt.
- SigG §11 Abs.4: Der Zertifizierungsdiensteanbieter haftet für beauftragte Dritte nach § 4 Abs. 5 und beim Einstehen für ausländische Zertifikate nach § 23 Abs. 1 Nr. 2 wie für eigenes Handeln. § 831 Abs. 1 Satz 2 des Bürgerlichen Gesetzbuchs findet keine Anwendung.
- SigG §15 Abs.7: Bei Produkten für qualifizierte elektronische Signaturen muss die Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 und der Rechtsverordnung nach § 24 nach dem Stand von Wissenschaft und Technik hinreichend geprüft und durch eine Stelle nach § 18 bestätigt worden sein; Absatz 1 Satz 3 findet entsprechende Anwendung. Der akkreditierte Zertifizierungsdiensteanbieter hat
  1. für seine Zertifizierungstätigkeit nur nach Satz 1 geprüfte und bestätigte Produkte für qualifizierte elektronische Signaturen einzusetzen,
  2. qualifizierte Zertifikate nur für Personen auszustellen, die nachweislich nach Satz 1 geprüfte und bestätigte sichere Signaturerstellungseinheiten besitzen, und
  3. die Signaturschlüssel-Inhaber im Rahmen des Abs. 1 über nach Satz 1 geprüfte und bestätigte Signaturanwendungskomponenten zu unterrichten.

- SigG §17 Abs.4: Die Erfüllung der Anforderungen nach den Absätzen 1 und 3 Nr. 1 sowie der Rechtsverordnung nach § 24 ist durch eine Stelle nach § 18 zu bestätigen. Zur Erfüllung der Anforderungen nach den Absätzen 2 und 3 Nr. 2 und 3 genügt eine Erklärung durch den Hersteller des Produkts für qualifizierte elektronische Signaturen.

SigV

- SigV §2: Das Sicherheitskonzept nach § 4 Abs. 2 Satz 4 des Signaturgesetzes hat u.a. folgendes zu enthalten: eine Übersicht über die eingesetzten Produkte für qualifizierte elektronische Signatu-ren mit Herstellererklärungen nach § 17 Abs. 4 Satz 2 oder Bestätigungen nach § 17 Abs. 4 Satz 1 oder nach § 15 Abs. 7 Satz 1 des Signaturgesetzes
- SigV §5 Abs.1: § 5 Einzelne Sicherheitsvorkehrungen des Zertifizierungsdiensteanbieters

  (1) Der Zertifizierungsdiensteanbieter hat durch geeignete Maßnahmen sicherzustellen, dass Signaturschlüssel nur auf der jeweiligen sicheren Signaturerstellungseinheit oder bei ihm oder einem anderen Zertifizierungsdiensteanbieter unter Nutzung von technischen Komponenten nach § 17 Abs. 3 Nr. 1 des Signaturgesetzes erzeugt und auf sichere Signaturerstellungseinheiten übertragen werden. Soweit er auch Wissensdaten zur Identifikation des Signaturschlüssel-Inhabers gegenüber einer sicheren Signaturerstellungseinheit oder technische Komponenten zur Erfassung biometrischer Merkmale und Übertragung von Referenzdaten auf die sichere Signaturerstellungseinheit bereit-stellt, hat er auch Vorkehrungen zu treffen, um die Geheimhaltung der Identifikationsdaten zu gewährleisten und deren Speicherung außerhalb der jeweiligen sicheren Signaturerstellungseinheit nach Einbringen in dieselbe auszuschließen.
- SigV §5 Abs.2: Der Zertifizierungsdiensteanbieter hat von ihm bereitgestellte Signaturschlüssel und Identifikationsdaten dem Signaturschlüssel-Inhaber auf der sicheren Signaturerstellungseinheit persönlich zu übergeben und die Übergabe von diesem schriftlich oder als mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenes elektronisches Dokument bestätigen zu lassen, es sei denn, es wird eine andere Übergabe vereinbart. Erst nachdem der Signaturschlüssel-Inhaber den Erhalt der sicheren Signaturerstellungseinheit gegenüber dem Zertifizierungsdiensteanbieter bestätigt hat, darf das zugehörige qualifizierte Zertifikat nach § 5 Abs. 1 Satz 2 und 3 des Signa-turgesetzes nachprüfbar und, soweit vereinbart, abrufbar gehalten werden.
- SigV §8 Abs.2: 9. die Übergabebestätigungen für Signaturschlüssel und Identifikationsdaten nach § 5 Abs. 2 Satz 1 oder die Erklärung des Signaturschlüssel-Inhabers, wenn er eine andere Übergabe verlangt hat, und gegebenenfalls einen anderen Nachweis.

Anlage zur Verordnung zur elektronischen Signatur

Anlage 1

- Die Prüfung muss bei sicheren Signaturerstellungseinheiten nach § 2 Nr. 10 des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen,
- Sicherheitsbestätigungen für Signaturprodukte
  - Eine Ausfertigung des Prüfberichtes, der Bewertung durch die Bestätigungsstelle und der Bestätigung ist bei der zuständigen Behörde zu hinterlegen. Auf Anforderung sind dieser auch alle weiteren Prüfunterlagen vorzulegen. Sie

kann bei Anhaltspunkten für Mängel bei Prüfungen oder bei bestätigten Produkten sowie stichprobenweise Gutachten eines unabhängigen Dritten darüber einholen, ob die Produkte gemäß dieser Anlage geprüft wurden und ob diese die Anforderungen des Signaturgesetzes und der Signaturverordnung erfüllen. Betroffene Hersteller, Vertreiber und Prüfstellen haben die dafür erforderliche Unterstützung zu gewähren.

10 Verzeichnisse und Glossar

10.1 Tabellenverzeichnis

10.2 Abbildungsverzeichnis

10.3 Glossar und Abkürzungen

CCD	Card Capability Description, ein EF, das in die QES-Anwendung auf der Chipkarte eingefügt wird, um dem ZDA-NL Daten zur Verfügung zu stellen, die nicht aus anderen Quellen auf der Chipkarte (ATR etc.) entnommen werden können.
COS	(Smart-)Card Operating System, das Betriebssystem einer Chipkarte
CV-Zertifikat	„Card-Verifiable“ Zertifikat: Ein Zertifikat, das mit den begrenzten Möglichkeiten einer Chipkarte von derselben verwendet werden kann, um eine elektronische Signatur zu verifizieren.
CVC	CV-Zertifikat
dPA	Digitaler Personalausweis
eGK	Elektronische Gesundheitskarte
ICCSN	Für die in dem vorliegenden Dokument betrachteten Chipkarten wird es grundsätzlich eine sogenannte ICCSN geben, die als "Kartennummer" jede Chipkarte eindeutig identifiziert. Die Struktur und der genaue Aufbau der ICCSN werden in den entsprechenden Spezifikationen festgelegt.
GS	Gütesiegelzertifikat im Format X.509, d.h. im Standard-Zertifikatsformat. Ein Zertifikatsprofil findet sich in Kap. 7.2.1
Personalisierung	die vertrauenswürdige Zuordnung der Identität einer Person zu den kryptografisch einmaligen Merkmalen einer Chipkarte durch Ausstellung eines Zertifikats, im Falle dieser Spezifikation eines qualifizierten Zertifikats nach dem Signaturgesetz. (Im weiteren Sinne wird auch der gesamte Vorgang der Erstellung einer Chipkarte z.B. als Ausweis oder Bankkarte für eine Person als Personalisierung bezeichnet, in dieser Spezifikation wird aber nur die engere Bedeutung benutzt.)
Sicherheitsanker	Es gibt zwei Typen von Sicherheitsankern, „Gütesiegel“ und CV-Zertifikate. Der im Rahmen dieser Spezifikation festgelegte Begriff Sicherheitsanker bezeichnet ein technisch spezifiertes Merkmal einer Chipkarte, mit dessen Hilfe sich ein ZDA-NL davon überzeugen kann, dass die Chipkarte alle gesetzlich notwendigen Merkmale hat, um für sie unter Verwendung des Sicherheitsankers ein qualifiziertes Zertifikat erstellen zu dürfen. Der Sicherheitsanker wird in der Verantwortung eines ZDA-VP auf die Chipkarte aufgebracht.
Transportzustand	Der Zustand der Chipkarte, in dem sie vom ZDA-VP (ggf. über weitere Bearbeitungsschritte) zum Karteninhaber kommt und von diesem zur Beantragung eines qualifizierten Zertifikats dem ZDA-NL vorgelegt wird.
Vorpersonalisierung	Vorgang bei der Kartenproduktion, bei dem wesentliche Merkmale wie z.B. Sicherheitsanker oder kryptografische Schlüssel auf eine Chipkarte aufgebracht werden, auf deren Grundlage dann die eigent-

	liche „Personalisierung“ möglich wird
X.509-Gütesiegel	Siehe GS
ZDA	Zertifizierungsdiensteanbieter
ZDA-VP	ZDA, der im Rahmen dieser Spezifikation die Rolle eines ZDA bei der Vorpersonalisierung ausfüllt.
ZDA-NL	ZDA, der im Rahmen dieser Spezifikation die Rolle eines ZDA beim Nachladevorgang ausfüllt.
Zertifikatsprofil	Auf einem Basisstandard (hier [x.509V3]) basierende Festlegung von Zertifikatseigenschaften, die i.d.R.eine Auswahl aus den Optionen des Basisstandards darstellt.

10.4 Literaturverzeichnis

[Algorithmenkatalog]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) Veröffentlicht von der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (www.bundesnetzagentur.de), in der jeweils aktuellen Fassung
[EAC]	Advanced Security Mechanisms für Machine Readable Travel Documents, V. 0.92, Bundesamt für Sicherheit in der Informationstechnik (ohne Datum, unveröffentlicht)
[eGK-Spezifikation Teil 1]	Die Spezifikation der elektronischen Gesundheitskarte Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform Version 1.0.1 Standardentwurf 05.12. 2005
[eGK-Spezifikation Teil 2]	Die Spezifikation der elektronischen Gesundheitskarte Teil 2: Anwendungen und anwendungsspezifische Strukturen Version 1.0 .0 Standardentwurf 12.12.2005
[ISO HF2]	ISO 10118 - 2, Information technology - Security techniques - Hash functions, Part 2: Hash functions using an n-bit block cipher algorithm, 1994
[QES eGK]	Spezifikation Kartenmanagement – Nachladen qualifizierter Zertifikate, Anhang 1: Elektronische Gesundhkeitskarte, Version 0.99 vom 23. März
[X.509V3]	ITU-T X.509: Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, 1997