eHealth – Zertifizierungskonzept für die Kartengeneration G2

Susanne Pingel

Bundesamt für Sicherheit in der Informationstechnik (BSI)
susanne.pingel@bsi.bund.de

Zusammenfassung

Zielsetzung ist es, ein flexibles, effizientes und transparentes Zertifizierungskonzept für die eHealth-Karten der Generation G2 aufzusetzen und auszugestalten. Dieses Zertifizierungskonzept ist Gegenstand der Technischen Richtlinie BSI TR-03106 „eHealth – Zertifizierungskonzept für Karten der Generation G2“. Hinsichtlich seines Stellenwertes und seiner Vorteile zeichnet sich das neue Zertifizierungskonzept für die eHealth-Karten der Generation G2 dadurch aus, dass es im Vergleich zum bisher gelebten Zertifizierungskonzept für die Karten der Generation G1 insgesamt gesehen mehr Effizienz, Flexibilität und Transparenz bietet. So können insbesondere an vielen Stellen Prozess- und Prüfaufwände reduziert oder vereinfacht sowie auch erlangte Prozess- und Prüfergebnisse für weitere (nachfolgende) Zulassungsverfahren und -prozesse seitens der gematik wiederverwendet werden. Das G2-Zertifizierungskonzept befindet sich in der Anwendung.

1 Hintergrund und Zielsetzung

Die verschiedenen Karten-Produkte der Kartengeneration G2 bauen auf einer gemeinsamen Kartenbetriebssystem-Plattform auf, die als relativ stabil anzusehen ist und die relativ selten (größeren) Änderungen unterliegt, während die darauf aufsetzenden eHealth-Applikationen, die die verschiedenen Kartentypen ausmachen, häufiger Anpassungen und Änderungen erfahren (z.B. durch Hinzufügen, Wegfallen, Größenänderungen von Datenfeldern usw.). Entsprechende Erfahrungen liegen aus der Kartengeneration G1 vor.

Das bislang für die eHealth-Karten der Generation G1 bestehende und praktizierte Zertifizierungskonzept erfordert für die Karten-Produkte eine CC-Zertifizierung, die das komplette Karten-Produkt, also Halbleiter-, Betriebssystem- und Applikationsebene, umfasst. Bei den eHealth-Karten der Generation G1 gibt es dabei für jeden Kartentyp ein spezifisches Protection Profile (PP), auf dessen Grundlage die eHealth-Karten zertifiziert werden. Für jede Änderung an der Spezifikation der eHealth-Applikationen durchlaufen die Karten-Produkte zumindest eine Re-Zertifizierung oder ein Maintenance-Verfahren. Auch ist bei Änderungen an der Spezifikation der eHealth-Applikationen das betreffende Kartentyp-spezifische PP auf Änderungsbedarf hin zu überprüfen und ggf. zu überarbeiten, womit in letzterem Fall eine anschließende (Re-)Zertifizierung bzw. ein Maintenance-Verfahren für das PP erforderlich wird.

Vor diesem Hintergrund entstand auf Seiten der gematik, der Karten-Hersteller und des BSI der Wunsch nach einem flexibleren, transparenten Zertifizierungskonzept für die G2-Karten-Produkte verbunden mit dem Wunsch nach einer Reduzierung der Kosten- und Zeitaufwände.

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 177-188.

Bei der Gestaltung eines neuen Zertifizierungskonzepts für die eHealth-Karten der Generation G2 ist wie bisher als Gesetzesgrundlage folgender Auszug aus SGB V, § 291b heranzuziehen:

„(1a) [...] Die Gesellschaft für Telematik prüft die Funktionsfähigkeit und Interoperabilität auf der Grundlage der von ihr veröffentlichten Prüfkriterien. Der Nachweis der Sicherheit erfolgt nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik durch eine Sicherheitszertifizierung. Hierzu entwickelt das Bundesamt für Sicherheit in der Informationstechnik geeignete Prüfvorschriften und veröffentlicht diese im Bundesanzeiger. Das Nähere zum Zulassungsverfahren und zu den Prüfkriterien wird von der Gesellschaft für Telematik in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik beschlossen. [...]“

Für das neue Zertifizierungskonzept für die eHealth-Karten der Generation G2 ist zu berücksichtigen, dass die vorstehend genannten dem BSI zugewiesenen gesetzlichen Aufgaben weiterhin erfüllt bleiben und bei den Prüfungen der Karten-Produkte bzgl. ihrer Sicherheit keine Lücken im Prüfprozess bzw. in den Prüfaussagen entstehen. Das Zertifizierungskonzept nutzt beim BSI bereits seit Jahren etablierte Prozesse der Zertifizierung nach Common Criteria (CC) und Technischer Richtlinie (TR) und sieht die folgenden Kernpunkte vor:

- CC-Zertifizierung der Karten-Plattform (siehe Abschnitt 2.1).
- TR-Zertifizierung von Karten-Produkten (siehe Abschnitt 2.5).
- Spezielle Prüfmechanismen und -werkzeuge, insbesondere für einen Konsistenzabgleich von Karten-Produkten gegen die Kartentyp-spezifischen Objektsystem-Spezifikationen mittels TR-zertifiziertem Konsistenz-Prüftool (siehe Abschnitt 2.3 und 2.4).

Das G2-Zertifizierungskonzept ersetzt hierdurch die bisher im Bereich von Karten-Produkten der Generation G1 durchgeführte CC-Zertifizierung der Karten-Produkte. Ziel ist es dabei, für ein G2-Karten-Produkt eine Aussage zu seiner sicherheitstechnischen Eignung für seinen Einsatz in der Telematikinfrastruktur im deutschen Gesundheitswesen zu erlangen.

Auf den ersten Blick betrachtet kann eine CC-Zertifizierung einer Karten-Plattform für die Karten-Hersteller – je nachdem wie diese in der Vergangenheit insbesondere für die Kartengeneration G1 ihre Karten-Produkte und zugehörigen CC-Evaluierungsverfahren und Herstellerdokumente aufgesetzt haben – einen gewissen Mehraufwand im Vergleich zu einer CC-Zertifizierung eines Karten-Produktes in der Ausprägung HBA, eGK, SMC-B usw. bedeuten. Gleichermaßen kann in Nachfolge dessen auch mit einem Mehraufwand auf Seiten der CC-Prüfstellen und auch auf Seiten der Zertifizierungsstelle zu rechnen sein. Dieser Mehraufwand relativiert sich jedoch erheblich im Hinblick auf die zu erwartende Vielzahl von verschiedenen Kartentypen und Karten-Produkten, da für eine Aussage zur sicherheitstechnischen Eignung solcher Karten-Produkte nun auf die CC-Zertifizierung der jeweils unterliegenden Karten-Plattform zurückgegriffen werden kann und dort nur ein einmaliger Aufwand entsteht (sofern von einer stabilen Betriebssystem-Spezifikation ausgegangen wird). Für die eHealth-Applikationen in den Karten-Produkten kann sich darauf aufbauend ein schlanker, effizienter und flexibler Prüfprozess anschließen.

Das G2-Zertifizierungskonzept verlangt nur nach der Erstellung und Pflege eines einzigen PPs - desjenigen für die Karten-Plattform - anstelle der Erfordernis, wie bei den G1-Karten PPs für jeden einzelnen Kartentyp aufsetzen und beständig aktualisieren und re-zertifizieren bzw. einem Maintenance-Verfahren unterziehen zu müssen. Auch hier können zum einen beträchtliche Aufwände reduziert werden. Zum anderen kann mit dem nun schlankeren Prüfprozess für die eHealth-Applikationen der Karten-Produkte flexibler und zeitnäher auf Änderungen in den Objektsystem-Spezifikationen für die Karten-Produkte reagiert werden.

Das G2-Zertifizierungskonzept mit der neu gestalteten Sicherheitszertifizierung der eHealth-Karten der Generation G2 ist Teil des sog. „Kooperationskonzepts für die Kartengeneration G2“ zwischen gematik und BSI. Unter dem Kooperationskonzept ist dabei die Vorgehens- und Verfahrensweise für die Zulassung von Karten-Plattformen und Karten-Produkten der Kartengeneration G2 für deren Einsatz in der Telematikinfrastruktur im deutschen Gesundheitswesen durch die gematik zu verstehen. Das neue Zertifizierungskonzept, das in erster Linie Sicherheitsaspekte von Karten-Plattformen und Karten-Produkten der Generation G2 im Fokus hat und sich mit Sicherheitsprüfungen und dem Erlangen von diesbzgl. Sicherheitsnachweisen und -aussagen für diese Karten beschäftigt, wird auch Zulassungsprozesse für Karten-Produkte auf Seiten der gematik im Bereich ihrer funktionalen Tests, Anwendungstests und sonstigen Zulassungstests vereinfachen, beschleunigen und solider gestalten. So können einzelne Komponenten und Prüfmechanismen des G2-Zertifizierungskonzepts auch für die Tests der gematik im Rahmen von Zulassungsprozessen für die G2-Karten wiederverwendet werden.

Das neue Zertifizierungskonzept für die eHealth-Karten der Generation G2 ist Gegenstand der Technischen Richtlinie *BSI TR-03106 „eHealth – Zertifizierungskonzept für Karten der Generation G2“* [TR-03106]. Diese TR trägt den Charakter eines Konzeptpapiers und legt die grundsätzlichen Eckpfeiler, Vorgehensweisen und Randbedingungen der neu gestalteten Sicherheitszertifizierung der G2-Karten fest. Ergebnisse weitergehender Detailarbeiten sind Gegenstand weiterer nachgelagerter Dokumentation zur TR-03106. Hierzu gehören:

- Common Criteria Protection Profile „Card Operating System Generation 2 (PP COS G2)“ [PP-0082] für die G2-Karten-Plattform,
- Wrapper-Spezifikation [WRAP],
- Technische Richtlinie *BSI TR-03143 „eHealth G2-COS Konsistenz-Prüftool“* [TR-03143] für das im Rahmen der TR-Konformitätsprüfung bzw. des Konsistenzabgleichs von Karten-Produkten eingesetzte Konsistenz-Prüftool,
- Technische Richtlinie *BSI TR-03144 „eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2“* [TR-03144] mit ihrem Anhang „eHealth – Sicherungsmechanismen im Umfeld der TR-Zertifizierung von G2-Karten-Produkten“ [TR-03144A] für die TR-Konformitätsprüfung von Karten-Produkten.

2 G2-Zertifizierungskonzept

Die verschiedenen Kartentypen der Kartengeneration G2 – (derzeit) in der Ausprägung eGK (elektronische Gesundheitskarte), HBA (Heilberufsausweis), SMC-B (Security Module Card Typ B / Institutskarte), gSMC-KT (gerätespezifische Security Module Card Typ Kartenterminal) und gSMC-K (gerätespezifische Security Module Card Typ Konnektor) – bauen auf einer gemeinsamen G2-Kartenbetriebssystem-Plattform gemäß der G2-COS-Spezifikation ([G2-COS]) der gematik auf. Neben verpflichtenden Anteilen beinhaltet die G2-COS-Spezifikation optionale Funktionspakete, die nur für bestimmte Kartentypen erforderlich sind.

Je Kartentyp gibt es jeweils eine eigene gematik-Spezifikation der Kartenkonfiguration, die sog. Objektsystem-Spezifikation. Diese beschreibt insbesondere das Objektsystem des jeweiligen Kartentyps mit den zugehörigen dedizierten Zugriffsregeln und legt die erforderlichen Funktionspakete der G2-COS-Spezifikation fest.

Unterschieden wird zwischen den Begriffen „Karten-Plattform“ und „Karten-Produkt“:

- *Karten-Plattform*: Kombination aus Halbleiter und implementiertem G2-COS.

- *Karten-Produkt*: Karten-Plattform mit eHealth-Applikation(en). Zu unterscheiden sind hierbei *initialisierte Karten-Produkte* und *personalisierte Karten-Produkte*.

Als *Initialisierung einer Karten-Plattform* wird das Laden der zur Karten-Plattform ggf. vorhandenen Patches zur Komplettierung der Implementierung des G2-COS bezeichnet. Unter der *Initialisierung eines Karten-Produktes* wird das Laden der zugehörigen Kartentyp-spezifischen personenunabhängigen Daten der jeweiligen eHealth-Applikationen auf die Karten-Plattform verstanden. Insbesondere werden bei der Initialisierung des Karten-Produktes die wesentlichen Sicherheitsstrukturen der jeweiligen Applikationen aufgebracht. Relevant ist hierbei die betreffende Kartentyp-spezifische Objektsystem-Spezifikation, die genaue Informationen darüber beinhaltet, welche Objekte, Sicherheitsattribute und öffentlichen Schlüsseldaten für den betreffenden Kartentyp zu installieren und initialisieren sind. Von der Initialisierung zu unterscheiden ist die *Personalisierung eines Karten-Produktes*, bei der zur Individualisierung eines initialisierten Karten-Produktes die personenbezogenen Daten in die jeweiligen Applikationen des Karten-Produktes geladen werden.

Das Zertifizierungskonzept für die eHealth-Karten der Generation G2 sieht die in den folgenden Kapiteln beschriebenen Eckpunkte und Vorgehensweisen vor.

2.1 CC-Zertifizierung der Karten-Plattform

Nach Common Criteria (CC) zertifiziert wird zukünftig die Karten-Plattform, d.h. die Kombination aus der Implementierung des G2-COS (inkl. ggf. vorhandener Patches) zusammen mit dem darunter liegenden Halbleiter (in der Regel als Composite-Verfahren ausgeführt).

Für die CC-Zertifizierung der Karten-Plattform wird ein Protection Profile (PP) für die Karten-Plattform erstellt, das die eHealth-spezifischen (Sicherheits-) Aspekte und Anforderungen sowie die dem G2-COS hinterliegenden generellen Strukturen, Funktionalitäten und (Sicherheits-) Mechanismen adäquat und ausreichend adressiert (PP-0082, G2-COS-PP). Das G2-COS-PP selbst wird CC-zertifiziert (Zertifizierungs-ID: BSI-CC-PP-0082 bzw. Folge-IDs für nachfolgende Re-Zertifizierungen des PPs). Als Evaluierungslevel ist EAL 4+ mit den Augmentierungen ALC_DVS.2, ATE_DPT.2 und AVA_VAN.5 vorgesehen. Gründe für die Augmentierungen ALC_DVS.2 und ATE_DPT.2 sind, dass mit dem Zertifizierungskonzept der Gedanke der Zertifizierung einer offenen Plattform verfolgt wird und daher die Evaluierungstiefe, insbesondere bzgl. der Aspekte Test und Lebenszyklus (inklusive Sicherheit der Entwicklungsumgebung und -prozesse, Auslieferung), ausreichend tief zu gestalten ist. Die Augmentierung AVA_VAN.5 resultiert aus der Forderung im eHealth-Bereich nach einem Schutz gegen hohes Angriffspotential.

Die Karten-Plattform bietet mindestens Sicherheitsmechanismen für die Separierung von Applikationen sowie einen ausreichend abgesicherten Zugriffsregel-Mechanismus für die Prüfung und Aus-/Verwertung von Zugriffsregeln, die dem für den eHealth-Bereich angenommenen Angriffspotential angemessen sind. Dies ist entsprechend im G2-COS-PP modelliert und damit Gegenstand der CC-Zertifizierung der Karten-Plattform.

Die Modularisierung des G2-COS – die in der G2-COS-Spezifikation als verpflichtend vorgeschriebene Basisfunktionalität und die als optional ausgewiesenen Funktionspakete – wird im G2-COS-PP mittels des sog. Package-Konzepts abgebildet. Die vom Hersteller für seine Karten-Plattform konkret getroffene Auswahl an Funktionspaketen der G2-COS-Spezifikation spiegelt sich in den Sicherheitsvorgaben zur Karten-Plattform in der entsprechenden konkreten Auswahl an Packages aus dem G2-COS-PP wider.

Bedingt durch das Zertifizierungskonzept für die Karten der Generation G2 werden für die CC-Zertifizierung der Karten-Plattform weitere spezielle Aspekte für den Evaluierungsgegenstand relevant, die im G2-COS-PP entsprechend verankert werden. So hat die Karten-Plattform insbesondere eine Auslese-Schnittstelle zum Auslesen von Sicherheitsattributen und öffentlichen Schlüsseldaten der vom G2-COS verwalteten Objektsysteme und Objekte eines auf der Karten-Plattform aufbauenden Karten-Produktes sowie ggf. zum Auslesen sonstiger Hersteller-spezifischer sicherheitsrelevanter Attribute bereitzustellen. Ferner wird die Karten-Plattform um einen sog. Wrapper ergänzt, der eine Aufbereitung der über die Auslese-Schnittstelle der Karten-Plattform ausgelesenen Daten in ein speziell vorgegebenes Format zu ihrer weiteren Verwendung und Auswertung vornimmt. Die Auslese-Schnittstelle wie auch der Wrapper der Karten-Plattform sind Gegenstand der CC-Zertifizierung der Karten-Plattform und werden im G2-COS-PP geeignet modelliert.

Bei der Evaluierung der Karten-Plattform im Rahmen ihrer CC-Zertifizierung werden insbesondere Prüfungen dahingehend vorgenommen, inwieweit in der Karten-Plattform Hersteller-spezifisch zusätzliche, über die G2-COS-Spezifikation und ihre (innerhalb des Funktionspakets mit der Basisfunktionalität und der optionalen Funktionspakete) verpflichtenden Anteile hinausgehende Funktionalitäten und Strukturen (wie z.B. weitere Kommandos oder Kommando-Varianten, weitere Sicherheitsattribute des Objektsystems, weitere Sicherheitsattribute der in der G2-COS-Spezifikation spezifizierten Objekttypen, weitere Objekttypen, sonstige weitere sicherheitsrelevante Attribute der Karten-Plattform usw.) durch den Hersteller der Karten-Plattform implementiert wurden. Informationen über zusätzliche Funktionalitäten und Strukturen der Karten-Plattform, die Einfluss auf die auf der Karten-Plattform aufbauenden Karten-Produkte und ihre Sicherheit nehmen (können), sind zu ihrer weiteren Verwendung, insbesondere für die TR-Konformitätsprüfung initialisierter Karten-Produkte, in geeigneter Form weiterzugeben (z.B. über die Benutzerdokumentation oder den CC-Zertifizierungsreport zur Karten-Plattform).

Weiterhin werden bei der Evaluierung der Karten-Plattform im Rahmen ihrer CC-Zertifizierung insbesondere Prüfungen dahingehend vorgenommen, inwieweit die Karten-Plattform die Änderung von im Rahmen der Initialisierung eines auf dieser Karten-Plattform aufbauenden Karten-Produktes initialisierten Sicherheitsattributen und öffentlichen Schlüsseldaten des Objektsystems und seiner Objekte zulässt.

Für die CC-Zertifizierung der Karten-Plattform werden für den Test der Karten-Plattform (CC-Aspekte ATE/AVA) zum einen generische Testfälle (d.h. unabhängig von konkreten eHealth-Applikationen) wie zum anderen auch spezifische Testfälle im Hinblick auf die derzeit bekannten eHealth-Applikationen vorspezifiziert und für die CC-Zertifizierung der Karten-Plattform verpflichtend als Mindestmenge an durchzuführenden Tests vorgeschrieben (Verankerung im G2-COS-PP). Hierzu gehören auch mindestens zu betrachtende Use Cases, die für den eHealth-Bereich relevant und auf die derzeit bekannten eHealth-Applikationen abgestimmt sind. Die für den Test einer Karten-Plattform zu betrachtenden Use Cases berücksichtigen das Paket-Konzept der G2-COS-Spezifikation. Zielsetzung für das Heranziehen von generischen Testfällen, eHealth-spezifischen Testfällen und Use Cases ist, die Tests der Karten-Plattform gezielt, strukturiert, ausreichend, effizient und vergleichbar zu gestalten.

2.2 Prüfung der eHealth-Spezifikationen

Auf Seiten des BSI erfolgt aufgrund der Anforderungen im SGB V, §291b auf Anfrage des BMG eine generelle Prüfung der G2-COS-Spezifikation sowie der Objektsystem-Spezifikationen der gematik unter Sicherheitsaspekten. Die Prüfung der G2-COS-Spezifikation hat insbesondere die für das G2-COS definierten generellen Strukturen, Funktionalitäten und (Sicherheits-) Mechanismen des G2-COS im Fokus; die Prüfung der Objektsystem-Spezifikationen erfolgt unter Berücksichtigung der Spezifika des G2-COS und hat insbesondere die für die einzelnen Kartentypen definierten spezifischen Objektsysteme mit ihren Objekten und deren Sicherheitsattributen (insbesondere Zugriffsregeln) im Blick.

Diese Prüfung der G2-COS-Spezifikation und der Objektsystem-Spezifikationen für die einzelnen Kartentypen unter Sicherheitsaspekten durch das BSI erfolgt im Vorfeld und unabhängig von Zulassungsverfahren konkreter Karten-Plattformen und Karten-Produkte. Diese Prüfung kann als eine Art „einmalige Offline-Prüfung“ betrachtet werden und entspricht den derzeitigen vom BSI bereits im Umfeld der Kartengeneration G1 wahrgenommenen Aufgaben. Im Rahmen dieser Prüfung vom BSI erzielte Prüfergebnisse werden vom BSI an das BMG zur weiteren Verwendung zurückgemeldet. Mit Freigabe der Objektsystem-Spezifikationen durch die Gesellschafter werden insbesondere die Kartentyp-spezifischen Objektsysteme mit ihren Strukturen und Objekten sowie deren sicherheitstechnische Eigenschaften festgelegt.

2.3 Konsistenzabgleich von Karten-Produkten

Das G2-COS verwaltet verschiedene Typen von Objekten, wie Folder (Ordner in der Ausprägung Dedicated File, Application, Application Dedicated File), Files (Elementary Files), Key-Objekte (versch. Ausprägung für symmetrische und asymmetrische Kryptographie) und PIN-Objekte (versch. Ausprägung, z.B. reguläre PIN, Multireferenz-PIN, PUK).

Neben den eigentlichen Nutzdaten (wie z.B. Schlüsseldaten bei Key-Objekten) werden für die Objekte dieser Objekttypen jeweils zusätzlich Objekttyp-spezifische Sicherheitsattribute abgelegt, vom G2-COS verwaltet und im laufenden Betrieb bei der Ausführung von Karten-Kommandos ausgewertet und ggf. bearbeitet. Über diese Sicherheitsattribute werden die Sicherheitsstrukturen des jeweiligen Kartentyps bestimmt, womit diesen Sicherheitsattributen eine besondere Rolle zukommt. Zu den Sicherheitsattributen zählen insbesondere Zugriffsregeln, Life Cycle-Informationen sowie Key- und PIN-Zusatzattribute wie Objekt- und Algorithmen-Identifier, Fehlbedienungszähler usw. In vergleichbarer Weise ist auch das Objektsystem eines Karten-Produktes selbst mit Sicherheitsattributen versehen und erfolgt eine Nutzung und Verarbeitung des Objektsystems durch das G2-COS unter Auswertung seiner Sicherheitsattribute. Auch hier tragen die Sicherheitsattribute des Objektsystems zur Sicherheitsstruktur des jeweiligen Kartentyps bei, ebenso wie die von Seiten der betreffenden Objektsystem-Spezifikation intendierte hierarchische Struktur des Objektsystems.

Bestimmte Sicherheitsattribute dieser Objekte bzw. Objekttypen werden zum Zeitpunkt der Produktion (z.B. Initialisierung) oder Personalisierung eines Karten-Produktes aufgebracht oder nachfolgend im Rahmen des Managements eines personalisierten Karten-Produktes gesetzt. Genauere Informationen zu den generell vom G2-COS verwalteten Sicherheitsattributen finden sich in der G2-COS-Spezifikation; genauere Informationen zur konkreten Belegung der Sicherheitsattribute des für den jeweiligen Kartentyp relevanten Objektsystems und seine Objekte sind den Objektsystem-Spezifikationen für die einzelnen Kartentypen zu entnehmen.

Aus Sicherheitssicht ist es erforderlich, alle Objekte des Kartentyp-spezifischen Objektsystems, wie sie nach Abschluss der Personalisierung und damit für den Beginn des Wirkbetriebs beim Endnutzer des jeweiligen Karten-Produktes in der betreffenden Objektsystem-Spezifikation vorgesehen sind, bereits im Rahmen der Initialisierung des Karten-Produktes gemäß der für den Kartentyp vorgesehenen hierarchischen Struktur des Objektsystems zu installieren. Die Installation von Objekten bedeutet dabei zunächst die grundsätzliche Anlage dieser Objekte im seitens der Objektsystem-Spezifikation vorgesehenen Objektsystem mit der für sie seitens der G2-COS-Spezifikation vorgesehenen Objektstruktur.

Aus Sicherheitssicht ist es darüber hinaus erforderlich, auch einige der Sicherheitsattribute des Kartentyp-spezifischen Objektsystems und der Objekte dieses Objektsystems bereits im Rahmen der Initialisierung des Karten-Produktes zu setzen. Hierzu gehören diejenigen Sicherheitsattribute des Objektsystems und der Objekte, die die Sicherheitsstruktur des Kartentyp-spezifischen Objektsystems bestimmen, also mindestens die Zugriffsregeln sowie weitere Sicherheitsattribute der Key- und PIN-Objekte wie Identifier dieser Objekte und Identifier für Krypto-Algorithmen. Weiterhin bestimmen auch für Authentisierungszwecke vorgesehene Public Key-Objekte die Sicherheitsstruktur der verschiedenen Kartentypen. So wird es aus Sicherheitssicht auch erforderlich, gewisse öffentliche Schlüssel(daten) bereits zu initialisieren.

Vorgaben (Sollwerte) und Informationen zu dem für ein Karten-Produkt (mindestens) zu installierenden und initialisierenden Objektsystem mit seiner hierarchischen Struktur und seinen Objekten sowie zu den (mindestens) zu initialisierenden Sicherheitsattributen und öffentlichen Schlüsseldaten sind in den Objektsystem-Spezifikationen der Kartentypen enthalten.

Im Rahmen der Initialisierung eines Karten-Produktes aufgebrachte Sicherheitsattribute – wie insbesondere Zugriffsregeln – sind nachfolgend nicht mehr veränderbar, insbesondere auch nicht durch zusätzliche, über die G2-COS-Spezifikation hinausgehende Hersteller-spezifische Kommandos. Ausnahme hiervon bilden lediglich diejenigen Sicherheitsattribute, die im laufenden Betrieb eines Karten-Produktes über die regulären Betriebssystem-Kommandos der G2-COS-Spezifikation verändert oder neu angelegt werden (können), z.B. über ein Card Management System. Die Änderung oder Neuanlage solcher Sicherheitsattribute erfolgt dann wie von der G2-COS-Spezifikation und den jeweiligen Objektsystem-Spezifikationen vorgesehen.

Hintergrund für diese Anforderungen bzgl. der Installation und Initialisierung des Objektsystems, seiner Objekte und der zugehörigen Sicherheitsattribute und öffentlichen Schlüsseldaten ist, dass wie bisher bei den Karten der Generation G1, wo initialisierte Karten Gegenstand der CC-Zertifizierung sind und dort insbesondere die wesentlichen Sicherheitsstrukturen der eHealth-Applikationen (wie z.B. das Kartentyp-spezifische Objektsystem mit seiner hierarchischen Struktur, seinen Objekten und Zugriffsregeln) und ihre Implementierung im Rahmen der CC-Evaluierung geprüft werden, für die G2-Karten-Produkte eine vergleichbare Sicherheitsaussage erzielt werden soll. Vom Setzen gewisser Sicherheitsattribute (wie z.B. Zugriffsregeln) im Rahmen der Personalisierung von Karten-Produkten ist daher abzusehen. Wie schon bei den Karten der Generation G1 erfolgt diese Abwägung unter dem Aspekt, dass anderenfalls der Personalisierungsstelle zu viel Freiheiten – auch im Hinblick auf eine möglicherweise unbeabsichtigte oder beabsichtigte fehlerhafte, nicht-spezifikationskonforme Personalisierung von Objektsystemen, Objekten oder Sicherheitsattributen – zugebilligt werden.

Zwecks Feststellung, ob die Implementierung des Objektsystems eines Karten-Produktes den Vorgaben der relevanten Objektsystem-Spezifikation entspricht, wird ein Konsistenzabgleich des betreffenden Karten-Produktes gegen die Objektsystem-Spezifikation durchgeführt.

Durch den Konsistenzabgleich eines Karten-Produktes ist zunächst sicherzustellen, dass für das Karten-Produkt das in der entsprechenden Objektsystem-Spezifikation vordefinierte Objektsystem vollständig und gemäß der dort vorgesehenen hierarchischen Struktur im Karten-Produkt implementiert ist, d.h. alle für das jeweilige Objektsystem in der Objektsystem-Spezifikation als verpflichtend ausgewiesenen Objekte im Karten-Produkt vorhanden und in der hierarchischen Struktur des implementierten Objektsystems korrekt angesiedelt sind.

Die den einzelnen Kartentypen und ihren spezifischen eHealth-Applikationen hinterliegenden Zugriffsregeln bilden die zentralen Sicherheitsstrukturen des jeweiligen Kartentyps. Die in den Objektsystem-Spezifikationen definierten Zugriffsregeln sind mithin als sicherheitskritische Werte einzustufen, und es ist über einen Konsistenzabgleich sicherzustellen, dass die konkrete Implementierung der Zugriffsregeln im Karten-Produkt konform zur Objektsystem-Spezifikation des relevanten Kartentyps erfolgt. Entsprechende Aussagen gelten für die übrigen Sicherheitsattribute der für die einzelnen Kartentypen relevanten Objektsysteme und ihre Objekte. Ferner ist die spezifikations-konforme Implementierung öffentlicher Schlüsseldaten im Karten-Produkt zu überprüfen.

Für den Konsistenzabgleich eines Karten-Produktes gegen die relevante Objektsystem-Spezifikation kommen spezielle, aufeinander abgestimmte Werkzeuge mit spezifischen Funktionalitäten und Schnittstellen zum Einsatz. Genauer wird der Konsistenzabgleich über die Auslese-Schnittstelle und den Wrapper der Karten-Plattform unter Verwendung des Konsistenz-Prüftools „PT eHealth G2-COS“ realisiert.

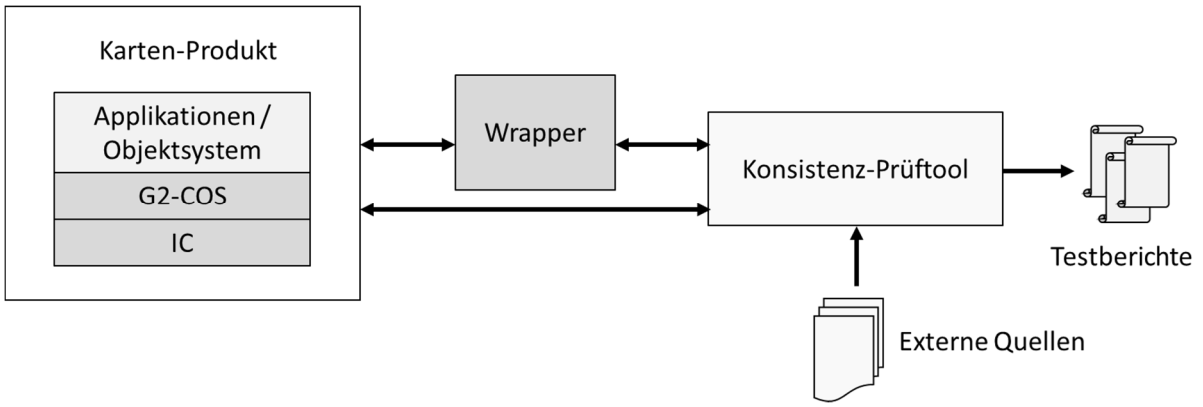

Abb. 1: Konsistenzabgleich eines Karten-Produktes

2.3.1 Auslese-Schnittstelle und Wrapper der Karten-Plattform

Die Karten-Plattform stellt Hersteller-spezifisch eine geeignete Auslese-Schnittstelle zum Auslesen der seitens der G2-COS-Spezifikation prinzipiell vorgesehenen und im Karten-Produkt für sein Objektsystem und seine Objekte konkret implementierten Sicherheitsattribute und öffentlichen Schlüsseldaten bereit. Je nach Erfordernis, z.B. im Hinblick auf spätere TR-Konformitätsprüfungen von auf der Karten-Plattform aufbauenden Karten-Produkten, ermöglicht die Auslese-Schnittstelle darüber hinaus ein Auslesen zusätzlicher, über die G2-COS-Spezifikation hinausgehender Hersteller-spezifisch implementierter sicherheitsrelevanter Attribute (wie z.B. zusätzlicher interner Sicherheitsattribute des Objektsystems oder von Objekten, Sicherheitsattribute neuer Objekttypen usw.), sofern diese für den für ein Karten-Produkt angestrebten Konsistenzabgleich bzw. für die sicherheitstechnische Bewertung der Implementierung des Objektsystems erforderlich sind. Zur Karten-Plattform wird ferner ein sog. Wrapper zur Aufbereitung der ausgelesenen Daten sowie zur Weitergabe der aufbereiteten Daten an das

Konsistenz-Prüftool „PT eHealth G2-COS“ zur dortigen weiteren Verarbeitung bzw. Auswertung bereitgestellt. Der Wrapper setzt insbesondere das Hersteller-spezifische Format der über die Auslese-Schnittstelle der Karten-Plattform ausgelesenen Daten in ein vom Konsistenz-Prüftool „PT eHealth G2-COS“ vorgegebenes Format um. Hierzu wird von der gematik in Zusammenarbeit mit dem BSI eine Spezifikation für den Wrapper erstellt, die von den Herstellern der Karten-Plattform für ihre Implementierung des Wrappers verpflichtend einzuhalten ist.

Über die Auslese-Schnittstelle und den Wrapper der Karten-Plattform wird ermöglicht, für ein auf dieser Karten-Plattform aufbauendes Karten-Produkt eine komplette Übersicht über das im Karten-Produkt implementierte Objektsystem inkl. seiner hierarchischen Struktur, seiner Objekte und deren Sicherheitsattribute bzw. öffentlichen Schlüsseldaten zu erhalten. Aus Effizienzgründen und zur Vermeidung von Fehlerquellen erfolgt stets eine vollständige Ausgabe der Sicherheitsattribute und öffentlichen Schlüsseldaten aus dem Karten-Produkt.

Die Auslese-Schnittstelle und der Wrapper der Karten-Plattform (inkl. zugehöriger Dokumentation) sind verpflichtend Gegenstand der CC-Zertifizierung der Karten-Plattform und werden im Rahmen der Evaluierung auf ihre funktionale Korrektheit und Vollständigkeit hin geprüft.

2.3.2 Konsistenz-Prüftool „PT eHealth G2-COS“

Das Konsistenz-Prüftool führt für Karten-Produkte einen Konsistenzabgleich des im Karten-Produkt implementierten Objektsystems mit seinen Sicherheitsattributen, seiner hierarchischen Struktur, seinen Objekten und deren Sicherheitsattributen sowie den öffentlichen Schlüsseldaten gegen die entsprechende Objektsystem-Spezifikation durch. Hierzu bedient sich das Konsistenz-Prüftool des Wrappers der unterliegenden Karten-Plattform.

Der vom Konsistenz-Prüftool durchgeführte Konsistenzabgleich prüft die Vollständigkeit und Korrektheit der hierarchischen Struktur des implementierten Objektsystems und seiner Objekte sowie die Vollständigkeit und Korrektheit der implementierten Sicherheitsattribute und öffentlichen Schlüsseldaten gegen die Vorgaben der entsprechenden Objektsystem-Spezifikation. Das Konsistenz-Prüftool erkennt im implementierten Objektsystem des Karten-Produktes das Vorhandensein zusätzlicher Objekte, Objekttypen, Sicherheitsattribute, öffentlicher Schlüsseldaten und sonstiger zusätzlicher Hersteller-spezifisch implementierter sicherheitsrelevanter Attribute, die über die G2-COS-Spezifikation und die relevante Objektsystem-Spezifikation hinausgehen, soweit dies von der Auslese-Schnittstelle und vom Wrapper der dem Karten-Produkt unterliegenden Karten-Plattform unterstützt wird.

Da die Spezifikation des G2-COS als grundsätzliches Regelwerk für den Konsistenzabgleich eines Karten-Produktes zu betrachten ist, auf dem die Istwert-Sollwert-Vergleiche des Karten-Produktes gegen die relevante Objektsystem-Spezifikation im Konsistenz-Prüftool durchgeführt werden, bildet die G2-COS-Spezifikation einen wesentlichen Bestandteil des Konsistenz-Prüftools. Für den Konsistenzabgleich prüft das Konsistenz-Prüftool das jeweilige Karten-Produkt gegen Sollwert-Vorgaben, die das Konsistenz-Prüftool aus der für das Karten-Produkt relevanten Objektsystem-Spezifikation bezieht.

Das Konsistenz-Prüftool generiert detaillierte Testberichte zu dem für ein Karten-Produkt durchgeführten Konsistenzabgleich. Der Testbericht weist insbesondere Abweichungen von der relevanten Objektsystem-Spezifikation aus, sowie auch vom Konsistenz-Prüftool im implementierten Objektsystem des Karten-Produktes erkannte zusätzliche Objekte, Objekttypen, Sicherheitsattribute, öffentliche Schlüsseldaten und sonstige zusätzliche Hersteller-spezifisch im-

plementierte sicherheitsrelevante Attribute, die über die G2-COS-Spezifikation und die relevante Objektsystem-Spezifikation hinausgehen (soweit von Auslese-Schnittstelle und Wrapper der unterliegenden Karten-Plattform unterstützt). Die weitere Aus- und Bewertung der Testberichte zu einem Karten-Produkt liegt außerhalb der Funktionalität des Prüftools.

Das Konsistenz-Prüftool, dessen Implementierung auf Basis der in der Technischen Richtlinie BSI TR-03143 „eHealth G2-COS Konsistenz-Prüftool“ enthaltenen Spezifikation erfolgt, unterliegt selbst einer TR-Zertifizierung.

2.4 Fingerprint-Abgleich der Implementierung des G2-COS

Im Rahmen der Konformitätsprüfung und Zulassung von Karten-Produkten wird es erforderlich, die Integrität und Authentizität der unterliegenden Karten-Plattform zu überprüfen. Insbesondere wird es erforderlich zu überprüfen, ob ggf. vorhandene Patches des implementierten G2-COS im Rahmen der Initialisierung der Karten-Plattform korrekt eingebracht wurden, mit den im Rahmen der CC-Zertifizierung der Karten-Plattform geprüften Patches übereinstimmen und sich dieses im Karten-Produkt unverändert wiederfindet.

Die Karten-Plattform stellt hierzu einen geeigneten, nicht-manipulierbaren technischen Mechanismus bereit, der die Integritäts- und Authentizitätsprüfung der (einem Karten-Produkt unterliegenden) Karten-Plattform inkl. der im Rahmen der Produktion bzw. Initialisierung eingebrachten Patches ermöglicht. Dieser Mechanismus umfasst die Berechnung eines sog. Fingerprints über die gesamte Implementierung des G2-COS (ausführbarer Code) und wird im Karten-Kommando FINGERPRINT der G2-COS-Spezifikation als Challenge-Response-Verfahren implementiert. Der von der Karten-Plattform bereitgestellte Fingerprint-Mechanismus ist über das G2-COS-PP Gegenstand der CC-Zertifizierung der Karten-Plattform und wird dort insbesondere auf seine Wirksamkeit geprüft.

Das Konsistenz-Prüftool „PT eHealth G2-COS“ wird um eine Funktionalität zur Integritäts- und Authentizitätsprüfung der (einem Karten-Produkt unterliegenden) Karten-Plattform erweitert. Insbesondere ermöglicht die Schnittstelle zum Import von Input aus externen Quellen zusätzlich den Import eines (signierten) Challenge/Fingerprint-Referenzwert-Paars, das als Sollwert in einem Fingerprint-Abgleich herangezogen wird. Das Konsistenz-Prüftool führt einen Abgleich des zur Challenge neu berechneten Fingerprints gegen den zur Challenge gehörigen Fingerprint-Referenzwert durch und teilt das Vergleichsergebnis im Testbericht mit.

2.5 TR-Zertifizierung von Karten-Produkten

G2-Karten-Produkte werden in *initialisiertem* Zustand einer Prüfung und Zertifizierung nach der Technischen Richtlinie BSI TR-03144 „eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2“ unterzogen. Die TR-Zertifizierung eines Karten-Produktes nach der TR-03144 erfolgt dabei grundsätzlich nach den in [VB-TR] dargestellten Regularien. Der Hersteller des Karten-Produktes stellt einen Zertifizierungsantrag beim BSI und beauftragt für die TR-Konformitätsprüfung des Karten-Produktes eine der im deutschen Zertifizierungsschema für Common Criteria anerkannten Prüfstellen, die in den Bereichen Smartcards & Similar Devices sowie eHealth (G2-Karten) entsprechendes Know How besitzen und dort aktiv tätig sind, als TR-Prüfstelle. Idealerweise ist die für die TR-Konformitätsprüfung des betreffenden Karten-Produktes vorgesehene TR-Prüfstelle diejenige Prüfstelle, die die CC-Evaluierung der unterliegenden Karten-Plattform durchgeführt hat.

Prüfgegenstand für die TR-Konformitätsprüfung eines Karten-Produktes nach TR-03144 ist das Karten-Produkt in *initialisiertem* Zustand. Für die TR-Konformitätsprüfung werden gemäß TR-03144 folgende Prüfaspekte, -aufgaben und -schritte relevant:

- Identifikation des zu prüfenden Karten-Produktes und seiner unterliegenden Karten-Plattform. Formale Prüfung der für die TR-Konformitätsprüfung des Karten-Produktes eingereichten Objekte und Dokumentation auf Vollständigkeit und Konsistenz.
- Prüfung, ob die in die CC-Zertifizierung der Karten-Plattform eingegangenen optionalen Funktionspakete der G2-COS-Spezifikation den Erfordernissen des Karten-Produktes bzw. seines Kartentyps entsprechen.
- Fingerprint-Abgleich der Karten-Plattform unter Verwendung des zertifizierten Konsistenz-Prüftools „PT eHealth G2-COS“ und des zur Karten-Plattform zugehörigen Wrappers. Der Fingerprint-Abgleich erfolgt mit dem Ziel eines Integritäts- und Authentizitätsnachweises der dem Karten-Produkt unterliegenden CC-zertifizierten Karten-Plattform und ihrer G2-COS-Implementierung.
- Verifizierung der Sicherheit der dem Karten-Produkt unterliegenden Karten-Plattform auf Basis des CC-Zertifikats der Karten-Plattform (unter Berücksichtigung von Nachweisen über ggf. nachfolgende Maintenance-Verfahren oder Re-Assessments).
- Konsistenzabgleich des Karten-Produktes gegen die Objektsystem-Spezifikation mit dem Ziel des Nachweises einer spezifikationskonformen Implementierung des Objektsystems im Karten-Produkt. Der Konsistenzabgleich erfolgt mittels des zertifizierten Konsistenz-Prüftools „PT eHealth G2-COS“ unter Nutzung des Wrappers der dem Karten-Produkt unterliegenden Karten-Plattform.
- Prüfung, ob im Karten-Produkt die Auflagen aus der Benutzerdokumentation und der CC-Zertifizierung der dem Karten-Produkt unterliegenden Karten-Plattform erfüllt sind.
- Betrachtung des Karten-Produktes auf mögliche Schwachstellen hin, z.B. hinsichtlich für die dem Karten-Produkt unterliegende Karten-Plattform bzw. für das darauf aufbauende Karten-Produkt relevanter, in der Zeit seit der Erteilung des CC-Zertifikats für die Karten-Plattform (ggf. nachfolgender Re-Assessments der Karten-Plattform) neu bekannt gewordener Angriffsszenarien.
- Prüfung der Benutzerdokumentation zum Karten-Produkt daraufhin, ob diese Dokumentation eine verständliche, konsistente und vollständige Beschreibung des Karten-Produktes beinhaltet sowie alle erforderlichen Benutzungshinweise und Auflagen für das Karten-Produkt (insbesondere für den Personalisierer) benennt.

Die TR-Konformitätsprüfung des initialisierten Karten-Produktes durch die TR-Prüfstelle wird mit einer Aus- und Bewertung der Prüfergebnisse der vorgenannten Teilprüfungen und einer Dokumentation in Form eines TR-Prüfberichtes der TR-Prüfstelle zum Karten-Produkt abgeschlossen. Dies umfasst insbesondere eine Aus- und Bewertung des vom Konsistenz-Prüftool zum geprüften Karten-Produkt ausgegebenen Testberichtes. Der TR-Prüfbericht zum geprüften Karten-Produkt geht im Rahmen der TR-Zertifizierung des Karten-Produktes dem BSI zur weiteren Prüfung und Bewertung zu.

Eine erfolgreiche Konformitätsprüfung des Karten-Produktes erwartet ein gültiges CC-Zertifikat, einen erfolgreichen Fingerprint-Abgleich sowie ein positives Prüfergebnis bzgl. der Erfüllung aller Auflagen aus der Benutzerdokumentation und aus der CC-Zertifizierung der dem Karten-Produkt unterliegenden Karten-Plattform. Im Prüfaspekt des Konsistenzabgleichs

des im Karten-Produkt implementierten Objektsystems gegen die relevante Objektsystem-Spezifikation weist der vom Konsistenz-Prüftool ausgegebene Testbericht idealerweise kein Delta gegenüber den Sollwerten für den Konsistenzabgleich aus. Gibt es hingegen ein Delta, so ist dieses durch die TR-Prüfstelle unter sicherheitstechnischen Aspekten zu bewerten.

Bei positiver Bewertung des TR-Prüfberichtes der TR-Prüfstelle zum Karten-Produkt durch das BSI auf Basis der TR-03144 wird für das Karten-Produkt ein TR-Zertifikat mit zugehörigem TR-Konformitätsreport ausgestellt und dieses auf den Webseiten des BSI veröffentlicht. Das TR-Zertifikat für das Karten-Produkt dient dem Konformitätsnachweis des Karten-Produktes gegenüber den für den betreffenden Kartentyp relevanten Spezifikationen der gematik und trägt zu einer Aussage zur sicherheitstechnischen Eignung dieses Karten-Produktes für seinen Einsatz in der Telematikinfrastruktur im deutschen Gesundheitswesen bei. Das TR-Zertifikat des Karten-Produktes mit zugehörigem TR-Konformitätsreport geht als Nachweis in die gematik-Zulassung dieses Karten-Produktes ein.

Literatur

[TR-03106] Technische Richtlinie BSI TR-03106 „eHealth – Zertifizierungskonzept für Karten der Generation G2“, Version 1.1, BSI (2015)

[TR-03143] Technische Richtlinie BSI TR-03143 „eHealth G2-COS Konsistenz-Prüftool“, Version 1.0, BSI (2015)

[TR-03144] Technische Richtlinie BSI TR-03144 „eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2“, Version 1.1, BSI (2015)

[TR-03144A] Technische Richtlinie BSI TR-03144 Anhang „eHealth – Sicherungsme-chanismen im Umfeld der TR-Zertifizierung von G2-Karten-Produkten“, Version 1.1, BSI (2015)

[PP-0082] Common Criteria Protection Profile „Card Operating System Generation 2 (PP COS G2)“, Version 1.9, registriert unter der Zertifizierungs-ID BSI-CC-PP-0082-V2, BSI

[WRAP] Einführung der Gesundheitskarte Spezifikation Wrapper, Version 1.6.0 vom 12.11.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[G2-COS] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.7.0 vom 26.08.2014 (einschließlich Errata), gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[VB-TR] Zertifizierung nach Technischen Richtlinien, Verfahrensbeschreibung / Zertifizierungsschema, BSI (2015)