



Bundesamt
für Sicherheit in der
Informationstechnik



Technische Richtlinie BSI TR-03144 Anhang

eHealth –

**Sicherungsmechanismen im Umfeld der TR-Zertifizierung
von G2-Karten-Produkten**

Version 1.1 – 22.05.2015

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E-Mail: bsi@bsi.bund.de

Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2015

Inhaltsverzeichnis

1	Einleitung.....	4
1.1	Gegenstand, Zielsetzung und Übersicht des Dokuments.....	4
1.2	Einordnung des Dokuments.....	4
1.3	Terminologie.....	5
1.4	Abkürzungen.....	5
1.5	Änderungshistorie.....	6
2	Rollenkonzept.....	8
3	Artefakte und ihre Sicherung.....	10
4	Übersicht über die Signaturschlüsselpaare.....	21
5	Kryptographische Vorgaben.....	23
6	Schlüsselverwaltung.....	24
	Literaturverzeichnis.....	26

Tabellenverzeichnis

Tabelle 1: Änderungshistorie.....	7
Tabelle 2: Aufgaben und Aufgabenbeschreibung.....	8
Tabelle 3: Zuordnung von Rollen und ihren Aufgaben.....	9
Tabelle 4: Artefakte und ihre Sicherheitsziele.....	11
Tabelle 5: Artefakte und ihre Sicherungsmechanismen.....	19
Tabelle 6: Übersicht der Signaturschlüsselpaare.....	22

1 Einleitung

1.1 Gegenstand, Zielsetzung und Übersicht des Dokuments

Im Rahmen der TR-Konformitätsprüfung von eHealth Karten-Produkten der Kartengeneration G2 nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) unter Verwendung des Konsistenz-Prüftools gemäß der Technischen Richtlinie BSI TR-03143 ([TR-03143]) werden aus Sicherheitsgründen heraus an verschiedenen Stellen Sicherungsmechanismen wie z.B. Signaturen verwendet. Das vorliegende Dokument betrachtet die hierzu erforderlichen Details, insbesondere hinsichtlich des Key Managements sowie hinsichtlich technischer und/oder organisatorischer Verfahren und Maßnahmen.

Berücksichtigt werden in den nachfolgenden Ausführungen nur die für die TR-Konformitätsprüfung eines Karten-Produktes nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) auf Seiten des Herstellers des Karten-Produktes, der TR-Prüfstelle für das betreffende Karten-Produkt, der CC-Prüfstelle für die dem Karten-Produkt unterliegende Karten-Plattform, der TR-Zertifizierungsstelle des BSI und der gematik für die Nutzung des Konsistenz-Prüftools der gematik grundsätzlich benötigten Artefakte. Nicht betrachtet werden die vom Hersteller des Karten-Produktes und der dem Karten-Produkt unterliegenden Karten-Plattform für die TR-Konformitätsprüfung des betreffenden Karten-Produktes beizusteuernenden Hersteller-abhängigen Artefakte (wie z.B. das Karten-Produkt selbst, zugehörige Benutzerdokumentation zur Karten-Plattform und zum Karten-Produkt usw.) mit Ausnahme des Challenge/Fingerprint-Referenzwert-Paars der Karten-Plattform. Für diese Beistellungen des Herstellers des Karten-Produktes und der dem Karten-Produkt unterliegenden Karten-Plattform kommen in der Regel Hersteller-spezifische Sicherungsmechanismen, insbesondere für den Auslieferungsweg zum tragen, die außerhalb des Scopes des vorliegenden Dokuments liegen.

Der vorliegende Anhang zur Technischen Richtlinie BSI TR-03144 ([TR-03144]) richtet sich an TR-Prüfstellen, die die TR-Konformitätsprüfung von Karten-Produkten der Kartengeneration G2 im Rahmen des G2-Zertifizierungskonzepts wie in der Technischen Richtlinie BSI TR-03106 ([TR-03106]) dargestellt auf Basis der Technischen Richtlinie BSI TR-03144 ([TR-03144]) durchführen. Weiterhin richtet sich der vorliegende Anhang zur Technischen Richtlinie BSI TR-03144 ([TR-03144]) an Hersteller von Karten-Produkten der Generation G2, die ihre Karten-Produkte einer TR-Zertifizierung nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) im Rahmen des G2-Zertifizierungskonzepts mit dem Ziel einer Zulassung ihrer Karten-Produkte durch die gematik für einen Einsatz in der Telematikinfrastruktur im deutschen Gesundheitswesen unterziehen.

Das vorliegende Dokument beschreibt in Kap. 2 das für die Ausgestaltung der oben genannten Sicherungsmechanismen vorgesehene Rollenkonzept. In Kap. 3 werden die Artefakte und ihre Sicherung genauer beleuchtet. Kap. 4 gibt eine Übersicht über die erforderlichen Signaturschlüsselpaare. In Kap. 5 werden kryptographische Vorgaben zusammengestellt und in Kap. 6 schließlich Informationen zur Schlüsselverwaltung bereitgestellt.

1.2 Einordnung des Dokuments

Das vorliegende Dokument bildet einen Anhang zur Technischen Richtlinie BSI TR-03144 ([TR-03144]), die die TR-Konformitätsprüfung und -Zertifizierung von eHealth Karten-Produkten der Kartengeneration G2 im Fokus hat.

Die Technische Richtlinie BSI TR-03144 ([TR-03144]) gliedert sich in das Zertifizierungskonzept für die eHealth-Karten der Kartengeneration G2 ein und ist als nachgelagerte Dokumentation zur

Technischen Richtlinie BSI TR-03106 „eHealth – Zertifizierungskonzept für Karten der Generation G2“ ([TR-03106]), die eine detaillierte Beschreibung dieses Zertifizierungskonzepts für die G2-Karten beinhaltet, zu betrachten.

Die Technische Richtlinie BSI TR-03144 ([TR-03144]) referenziert weiterhin auf die Technische Richtlinie BSI TR-03143 „eHealth G2-COS Konsistenz-Prüftool“ ([TR-03143]), die das für das G2-Zertifizierungskonzept bzw. für die TR-Konformitätsprüfung von Karten-Produkten nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) erforderliche Konsistenz-Prüftool der gematik spezifiziert sowie die TR-Zertifizierung dieses Konsistenz-Prüftools selbst regelt. Die TR-Zertifizierung eines Karten-Produktes, die Gegenstand der Technischen Richtlinie BSI TR-03144 ([TR-03144]) ist, macht von dem nach der Technischen Richtlinie BSI TR-03143 ([TR-03143]) zertifizierten Konsistenz-Prüftool der gematik wesentlich Gebrauch.

1.3 Terminologie

Dieser Anhang zur Technischen Richtlinie BSI TR-03144 ([TR-03144]) ist grundsätzlich als normativ anzusehen. Informative Teile werden explizit als solche gekennzeichnet (mit dem Vermerk „informativ“ oder „Hinweis“).

Ferner orientiert sich dieser Anhang zur Technischen Richtlinie BSI TR-03144 ([TR-03144]) an den dort vereinbarten Begrifflichkeiten und deren Beschreibungen.

1.4 Abkürzungen

In diesem Anhang zur Technischen Richtlinie BSI TR-03144 ([TR-03144]) sowie in den Dokumenten [TR-03106] und [TR-03143] werden folgende Abkürzungen verwendet:

A	Application
ADF	Application Dedicated File
ATR	Answer To Reset
BMG	Bundesministerium für Gesundheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CMS	Card Management System
COS	Card Operating System
DF	Dedicated File
EF	Elementary File
eGK	elektronische Gesundheitskarte
FW	Firmware
G1	eHealth Kartengeneration G1
G2	eHealth Kartengeneration G2
G2-COS	G2 Card Operating System
gSMC-K	gerätespezifische Security Module Card Typ K

gSMC-KT	gerätespezifische Security Module Card Typ KT
HBA	Heilberufsausweis
IC	Integrated Circuit
PDF	Portable Document Format
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile (Common Criteria)
PT	Prüftool
PUK	Personal Unblocking Key
QES	Qualified Electronic Signature
RSA	Rivest, Shamir, Adleman
SAK	Signaturanwendungskomponente
SFR	Security Functional Requirement (Common Criteria)
SGB	Sozialgesetzbuch
SHA	Secure Hash Algorithm
SigG	Signaturgesetz
SigV	Signaturverordnung
SMC-B	Security Module Card Typ B
SSCD	Secure Signature Creation Device
SSEE	Sichere Signaturerstellungseinheit
TI	Telematikinfrastruktur
TOE	Target Of Evaluation (Common Criteria)
TR	Technische Richtlinie
VSDD	Versichertenstammdatendienst
XML	Extensible Markup Language
ZDA	Zertifizierungsdiensteanbieter

1.5 Änderungshistorie

Version	Datum	Änderung
v0.1	05.06.2014	Erstausgabe
v1.0	29.07.2014	Veröffentlichung
v1.1	22.05.2015	Einzelne inhaltliche Ergänzungen und Klarstellungen in verschiedenen Kapiteln

Version	Datum	Änderung

Tabelle 1: Änderungshistorie

2 Rollenkonzept

Im Rahmen der TR-Konformitätsprüfung eines Karten-Produktes nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) unter Nutzung des Konsistenz-Prüftools werden grundsätzlich einige Artefakte benötigt, die aus Sicherheitsgründen heraus abzusichern sind. Siehe hierzu die genaueren Ausführungen in Kap. 3.

In der nachfolgenden Tabelle 2 werden die für diese Absicherung der Artefakte anfallenden Aufgaben zusammengestellt und genauer beschrieben.

Notation: Der konkrete Inhalt der Beschreibung „Sicherung der ...“ in der nachstehenden Tabelle 2 wird in den folgenden Kapiteln genauer bestimmt und ausgeführt.

Aufgabe	Aufgabenbeschreibung
R_Prüftool-Code	Sicherung der Implementierung des Konsistenz-Prüftools.
R_Prüftool-Schemata	Sicherung der zum Konsistenz-Prüftool zugehörigen XML-Schemata der G2-COS-Spezifikation, der Challenge/Fingerprint-Referenzwert-Paare und der Testberichte.
R_Prüftool-Dokumentation	Sicherung der zum Konsistenz-Prüftool zugehörigen Dokumentation (Benutzerdokumentation usw.).
R_Prüftool-Konf-Dateien	Sicherung der vom Konsistenz-Prüftool im Rahmen der Überprüfung eines Karten-Produktes benötigten Konfigurationsdateien. Hinweis: Diese gemäß den Vorgaben der Benutzerdokumentation zum Konsistenz-Prüftool codierten Dateien enthalten jeweils eine Signatur bzw. einen Signaturprüf Schlüssel (siehe untenstehende Ausführungen in Kap. 3).
R_Objektsys-Spezifikation	Sicherung der XML-Dateien der Objektsystem-Spezifikationen (XML-Master / XML-Derivat).
R_Plattform-Fingerprint	Sicherung der Challenge/Fingerprint-Referenzwert-Paare einer Karten-Plattform.
R_Testbericht	Sicherung des vom Konsistenz-Prüftool ausgegebenen Testberichts.
R_Schlüsseltabelle	Verwaltung und Sicherung der Schlüsseltabelle mit den Signaturprüf-schlüsseln (siehe Kap. 6).

Tabelle 2: Aufgaben und Aufgabenbeschreibung

In der nachfolgenden Tabelle 3 erfolgt eine Zuordnung der in die TR-Konformitätsprüfung eines Karten-Produktes nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) involvierten Rollen und der in Tabelle 2 definierten Aufgaben.

Rolle	Aufgaben
TR-Prüfstelle für Karten-Produkt	R_Testbericht

Rolle	Aufgaben
CC-Prüfstelle für Karten-Plattform	R_Plattform-Fingerprint
gematik	R_Prüftool-Code R_Prüftool-Schemata R_Prüftool-Dokumentation R_Prüftool-Konf-Dateien R_Objektsys-Spezifikation
TR-Zertifizierungsstelle (BSI)	R_Schlüsseltabelle

Tabelle 3: Zuordnung von Rollen und ihren Aufgaben

3 Artefakte und ihre Sicherung

In der nachfolgenden Tabelle 4 werden die für die TR-Konformitätsprüfung eines Karten-Produktes nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) für die Nutzung des Konsistenz-Prüf-tools grundsätzlich benötigten Artefakte zusammengestellt. Für jedes Artefakt werden seine Sicherheitsziele definiert und Informationen zu seiner kryptographischen Sicherung angegeben.

In den nachfolgenden Ausführungen wird der Begriff „Konfigurationsdatei“ für Dateien verwendet, die zur Übergabe von Signaturen und Signaturprüfchlüsseln an das Konsistenz-Prüf-tool benutzt werden. Formatierungsvorgaben für solche Konfigurationsdateien sind Gegenstand der zum Konsistenz-Prüf-tool zugehörigen Benutzerdokumentation.

Artefakt	Sicherheitsziel(e)	Kryptographische Sicherung	Art der Signatur
Konsistenz-Prüf-tool			
Code / Dateien mit den Java-Bibliotheken des Konsistenz-Prüf-tools (inklusive Java-Laufzeitumgebung)	Integrität, Authentizität	Signatur	äußere technische Signatur
XML-Schema der G2-COS-Spezifikation (zugehörig zum Konsistenz-Prüf-tool)	Integrität, Authentizität	Signatur	äußere technische Signatur
XML-Schema der Challenge/Fingerprint-Referenzwert-Paare (zugehörig zum Konsistenz-Prüf-tool)	Integrität, Authentizität	Signatur	äußere technische Signatur
XML-Schema der Testberichte (zugehörig zum Konsistenz-Prüf-tool)	Integrität, Authentizität	Signatur	äußere technische Signatur
Benutzerdokumentation zum Konsistenz-Prüf-tool	Integrität, Authentizität	Signatur (bei elektronischer Auslieferung)	äußere technische Signatur
TR-Zertifikat und -Konformitätsreport zum Konsistenz-Prüf-tool	Integrität, Authentizität	---	---
Inputquellen für das Konsistenz-Prüf-tool			
Konfigurationsdatei mit der Signatur über das Konsistenz-Prüf-tool (Code / Dateien mit den Java-Bibliotheken inklusive Java-Laufzeitumgebung)	Integrität, Authentizität	---	---
Konfigurationsdatei mit der Signatur über das XML-Schema der G2-COS-Spezifikation	Integrität, Authentizität	---	---
Konfigurationsdatei mit der Signatur über das XML-Schema der Challenge/Fingerprint-Referenzwert-	Integrität, Authentizität	---	---

Artefakt	Sicherheitsziel(e)	Kryptographische Sicherung	Art der Signatur
Paare			
Konfigurationsdatei mit der Signatur über das XML-Schema der Testberichte	Integrität, Authentizität	---	---
Konfigurationsdatei mit der Signatur über die XML-Datei der Objektsystem-Spezifikation xy (XML-Master / XML-Derivat) (xy = eGK/HBA/SMC-B/gSMC-K/gSMC-KT/...)	Integrität, Authentizität	---	---
Konfigurationsdatei mit der Signatur über das Challenge/Fingerprint-Referenzwert-Paar der Karten-Plattform	Integrität, Authentizität	---	---
Konfigurationsdatei mit dem Signaturprüfchlüssel für die Prüfung der Signatur über die XML-Datei der Objektsystem-Spezifikation xy (XML-Master / XML-Derivat) (xy = eGK/HBA/SMC-B/gSMC-K/gSMC-KT/...)	Integrität, Authentizität	---	---
Konfigurationsdatei mit dem Signaturprüfchlüssel für die Prüfung der Signatur über das Challenge/Fingerprint-Referenzwert-Paar der Karten-Plattform	Integrität, Authentizität	---	---
XML-Datei der Objektsystem-Spezifikation xy (XML-Master / XML-Derivat) (xy = eGK/HBA/SMC-B/gSMC-K/gSMC-KT/...)	Integrität, Authentizität	Signatur	äußere technische Signatur
Challenge/Fingerprint-Referenzwert-Paar der Karten-Plattform	Integrität, Authentizität, Vertraulichkeit	Signatur, Verschlüsselung	äußere technische Signatur
Output des Konsistenz-Prüftools			
Testbericht	Integrität, Authentizität, ggf. Vertraulichkeit	---	---

Tabelle 4: Artefakte und ihre Sicherheitsziele

In der nachfolgenden Tabelle 5 werden die für die TR-Konformitätsprüfung eines Karten-Produktes nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) für die Nutzung des Konsistenz-Prüf-

tools grundsätzlich benötigten Artefakte aus Tabelle 4 genauer betrachtet und für jedes Artefakt geeignete Sicherungsmechanismen technischer und/oder organisatorischer Art angegeben.

Notation: Für die Bezeichnung von Typen von Signaturschlüsseln und Signaturprüfchlüsseln siehe (Übersichts-) Tabelle 6 in Kap. 4.

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels (abgesehen von der Schlüsselstabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)
Konsistenz-Prüftool			
Code / Dateien mit den Java-Bibliotheken des Konsistenz-Prüftools (inklusive Java-Laufzeitumgebung)	<p>Äußere technische Signatur über den Code des Konsistenz-Prüftools.</p> <p>Automatische Signaturprüfung im Konsistenz-Prüftool selbst im Rahmen seines Selbsttests.</p> <p>Für die automatische Signaturprüfung ist ein vorhergehender Import der zugehörigen Konfigurationsdatei mit der zu prüfenden Signatur über das Konsistenz-Prüftool erforderlich.</p> <p>Zusätzlich kann eine externe Signaturprüfung (ohne Nutzung des Konsistenz-Prüftools) durchgeführt werden.</p>	S_Prüftool-Code	P_Prüftool-Code ist im Konsistenz-Prüftool selbst hinterlegt
XML-Schema der G2-COS-Spezifikation (zugehörig zum Konsistenz-Prüftool)	<p>Äußere technische Signatur über das XML-Schema.</p> <p>Automatische Signaturprüfung im Konsistenz-Prüftool selbst.</p> <p>Für die automatische Signaturprüfung ist ein vorhergehender Import des XML-Schemas und der zugehörigen Konfigurationsdatei mit der zu prüfenden Signatur über das XML-Schema in das Konsistenz-Prüftool erforderlich.</p> <p>Zusätzlich kann eine externe Signaturprüfung (ohne Nutzung des Konsistenz-Prüftools) durchgeführt werden.</p>	S_Prüftool-Schema	P_Prüftool-Schema ist im Konsistenz-Prüftool selbst hinterlegt
XML-Schema der Challenge/Fingerprint-Referenzwert-Paare (zugehörig zum Konsistenz-Prüftool)	<p>Äußere technische Signatur über das XML-Schema.</p> <p>Automatische Signaturprüfung im Konsistenz-Prüftool selbst.</p> <p>Für die automatische Signaturprüfung ist ein vorhergehender Import des XML-Schemas und der zugehörigen Konfigurationsdatei mit der zu prüfenden Signatur über das XML-</p>	S_Prüftool-Schema	P_Prüftool-Schema ist im Konsistenz-Prüftool selbst hinterlegt

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels <small>(abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)</small>
	<p>Schema in das Konsistenz-Prüftool erforderlich.</p> <p>Zusätzlich kann eine externe Signaturprüfung (ohne Nutzung des Konsistenz-Prüftools) durchgeführt werden.</p>		
<p>XML-Schema der Testberichte (zugehörig zum Konsistenz-Prüftool)</p>	<p>Äußere technische Signatur über das XML-Schema.</p> <p>Automatische Signaturprüfung im Konsistenz-Prüftool selbst.</p> <p>Für die automatische Signaturprüfung ist ein vorhergehender Import des XML-Schemas und der zugehörigen Konfigurationsdatei mit der zu prüfenden Signatur über das XML-Schema in das Konsistenz-Prüftool erforderlich.</p> <p>Zusätzlich kann eine externe Signaturprüfung (ohne Nutzung des Konsistenz-Prüftools) durchgeführt werden.</p>	S_Prüftool-Schema	P_Prüftool-Schema ist im Konsistenz-Prüftool selbst hinterlegt
<p>Benutzerdokumentation zum Konsistenz-Prüftool</p>	<p>Integre/authentische Auslieferung der Dokumentation durch die gematik in Papierform oder in elektronischer Form.</p> <p>Äußere Signatur über die Dokumentation im Falle einer elektronischen Auslieferung.</p>	(S_Prüftool-Dok)	---
<p>TR-Zertifikat und -Konformitätsreport zum Konsistenz-Prüftool</p>	<p>Bezug von den Webseiten des BSI oder sonstige integre/authentische Auslieferung einer Kopie des Originals.</p>	---	---
Inputquellen für das Konsistenz-Prüftool			
<p>Konfigurationsdatei mit der Signatur über das Konsistenz-Prüftool (Code / Dateien mit den Java-Bibliotheken inklusive Java-Laufzeitumge-</p>	<p>Im Konsistenz-Prüftool erfolgt unter Verwendung des im Konsistenz-Prüftool hinterlegten Signaturprüfschlüssels P_Prüftool-Code eine Prüfung der in der Konfigurationsdatei enthaltenen Signatur über das</p>	---	---

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels <small>(abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)</small>
bung)	<p>Konsistenz-Prüftool.</p> <p>Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüftool erforderlich.</p> <p>Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.</p>		
Konfigurationsdatei mit der Signatur über das XML-Schema der G2-COS-Spezifikation	<p>Im Konsistenz-Prüftool erfolgt unter Verwendung des im Konsistenz-Prüftool hinterlegten Signaturprüfschlüssels P_Prüftool-Schema eine Prüfung der in der Konfigurationsdatei enthaltenen Signatur über das XML-Schema.</p> <p>Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüftool erforderlich.</p> <p>Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.</p>	---	---
Konfigurationsdatei mit der Signatur über das XML-Schema der Challenge/Fingerprint-Referenzwert-Paare	<p>Im Konsistenz-Prüftool erfolgt unter Verwendung des im Konsistenz-Prüftool hinterlegten Signaturprüfschlüssels P_Prüftool-Schema eine Prüfung der in der Konfigurationsdatei enthaltenen Signatur über das XML-Schema.</p> <p>Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüftool erforderlich.</p> <p>Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.</p>	---	---
Konfigurationsdatei mit der Signatur über das XML-Schema der Testberichte	<p>Im Konsistenz-Prüftool erfolgt unter Verwendung des im Konsistenz-Prüftool hinterlegten Signaturprüfschlüssels P_Prüftool-Schema eine Prüfung der in der Konfigurations-</p>	---	---

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfchlüssels <small>(abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)</small>
	<p>datei enthaltenen Signatur über das XML-Schema.</p> <p>Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüf tool erforderlich.</p> <p>Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.</p>		
<p>Konfigurationsdatei mit der Signatur über die XML-Datei der Objektsystem-Spezifikation xy (XML-Master / XML-Derivat) (xy = eGK/HBA/SMC-B/gSMC-K/gSMC-KT/...)</p>	<p>Im Konsistenz-Prüf tool erfolgt unter Verwendung des in das Konsistenz-Prüf tool importierten Signaturprüfchlüssels P_Objektsys-Spez (Import mittels seiner zugehörigen Konfigurationsdatei, siehe unten) eine Prüfung der in der Konfigurationsdatei enthaltenen Signatur über die XML-Datei der Objektsystem-Spezifikation xy.</p> <p>Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüf tool erforderlich.</p> <p>Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.</p>	---	---
<p>Konfigurationsdatei mit der Signatur über das Challenge/Fingerprint-Referenzwert-Paar der Karten-Plattform</p>	<p>Im Konsistenz-Prüf tool erfolgt unter Verwendung des in das Konsistenz-Prüf tool importierten Signaturprüfchlüssels P_Plattform-FP (Import mittels seiner zugehörigen Konfigurationsdatei, siehe unten) eine Prüfung der in der Konfigurationsdatei enthaltenen Signatur über das Challenge/Fingerprint-Referenzwert-Paar.</p> <p>Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüf tool erforderlich.</p> <p>Auf eine kryptographische Sicherung der Konfigurationsdatei selbst</p>	---	---

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels <small>(abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)</small>
	kann verzichtet werden.		
<p>Konfigurationsdatei mit dem Signaturprüfschlüssel für die Prüfung der Signatur über die XML-Datei der Objektsystem-Spezifikation xy (XML-Master / XML-Derivat)</p> <p>(xy = eGK/HBA/SMC-B/gSMC-K/gSMC-KT/...)</p>	<p>Außerhalb des Konsistenz-Prüftools erfolgt eine Überprüfung der Integrität/Authentizität der Konfigurationsdatei bzw. des darin enthaltenen Signaturprüfschlüssels P_Objektsys-Spez gegen die mit S_Schlüsseltabelle signierte Schlüsseltabelle von Signaturprüfschlüsseln (siehe Kap. 6).</p> <p>Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.</p> <p>Es erfolgt ein Import der Konfigurationsdatei in das Konsistenz-Prüftool, damit der enthaltene Signaturprüfschlüssel P_Objektsys-Spez im Konsistenz-Prüftool zur weiteren Verwendung zur Verfügung steht.</p>	---	---
<p>Konfigurationsdatei mit dem Signaturprüfschlüssel für die Prüfung der Signatur über das Challenge/Fingerprint-Referenzwert-Paar der Karten-Plattform</p>	<p>Außerhalb des Konsistenz-Prüftools erfolgt eine Überprüfung der Integrität/Authentizität der Konfigurationsdatei bzw. des darin enthaltenen Signaturprüfschlüssels P_Plattform-FP gegen die mit S_Schlüsseltabelle signierte Schlüsseltabelle von Signaturprüfschlüsseln (siehe Kap. 6).</p> <p>Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.</p> <p>Es erfolgt ein Import der Konfigurationsdatei in das Konsistenz-Prüftool, damit der enthaltene Signaturprüfschlüssel P_Plattform-FP im Konsistenz-Prüftool zur weiteren Verwendung zur Verfügung steht.</p>	---	---
<p>XML-Datei der Objektsystem-Spezifikation xy (XML-Master / XML-Derivat)</p>	<p>Äußere Signatur der XML-Datei.</p> <p>Im Konsistenz-Prüftool erfolgt unter Verwendung des Signaturprüf-</p>	S_Objektsys-Spez	Konfigurationsdatei mit dem Signaturprüfschlüssel P_Objektsys-Spez

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels (abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)
(xy = eGK/HBA/SMC-B/gSMC-K/gSMC-KT/...)	<p>schlüssels P_Objektsys-Spez eine Prüfung der Signatur über die XML-Datei der Objektsystem-Spezifikation xy.</p> <p>Für die Signaturprüfung ist ein vorhergehender Import der zugehörigen Konfigurationsdatei mit dem Signaturprüfschlüssel P_Objektsys-Spez in das Konsistenz-Prüftool erforderlich.</p>		
Challenge/Fingerprint-Referenzwert-Paar der Karten-Plattform	<p>Die vertrauliche Übermittlung des signierten Challenge/Fingerprint-Referenzwert-Paars vom Hersteller der dem Karten-Produkt unterliegenden Karten-Plattform an die TR-Prüfstelle für das betreffende Karten-Produkt erfolgt verschlüsselt. Das erforderliche Schlüsselmaterial zur Verschlüsselung des Datenaustausches ist vorab gesichert zwischen dem Hersteller der Karten-Plattform und der TR-Prüfstelle für das Karten-Produkt auszutauschen.</p> <p>Für den Hersteller der Karten-Plattform und die TR-Prüfstelle für das Karten-Produkt wird von einer ausreichend gesicherten Umgebung ausgegangen, so dass ein dort im Klartext vorliegendes Challenge/Fingerprint-Referenzwert-Paar ausreichend gesichert behandelt wird.</p> <p>Hinweis: Das Konsistenz-Prüftool benötigt für die Weiterverwendung des Challenge/Fingerprint-Referenzwert-Paars dieses im Klartext, da das Konsistenz-Prüftool selbst keine Entschlüsselungsfunktion bereitstellt.</p> <p>Äußere Signatur des Challenge/Fingerprint-Referenzwert-Paars.</p> <p>Im Konsistenz-Prüftool erfolgt unter Verwendung des Signaturprüfschlüssels P_Plattform-FP eine Prü-</p>	S_Plattform-FP	Konfigurationsdatei mit dem Signaturprüfschlüssel P_Plattform-FP

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels <small>(abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)</small>
	<p>fung der Signatur über das Challenge/Fingerprint-Referenzwert-Paar.</p> <p>Für die Signaturprüfung ist ein vorhergehender Import der zugehörigen Konfigurationsdatei mit dem Signaturprüfschlüssel P_Plattform-FP in das Konsistenz-Prüftool erforderlich.</p>		
Output des Konsistenz-Prüftools			
Testbericht	<p>Es wird auf eine kryptographische Sicherung durch das Konsistenz-Prüftool selbst verzichtet.</p> <p>Es steht der TR-Prüfstelle für das betreffende Karten-Produkt aber frei, zusätzlich selbst eine kryptographische Sicherung an den Testbericht (z.B. in Form einer Signatur und/oder Verschlüsselung) anzubringen. In diesem Fall obliegt es der TR-Prüfstelle, zugehöriges Schlüsselmaterial (z.B. für die Prüfung der Signatur und/oder die Entschlüsselung) gesichert mit der den Testbericht nutzenden Stelle auszutauschen.</p> <p>Der vom Konsistenz-Prüftool ausgegebene Testbericht wird dem TR-Prüfbericht der TR-Prüfstelle für das betreffende Karten-Produkt beigelegt. Dieser TR-Prüfbericht wird insgesamt von der TR-Prüfstelle in Papierform unterschrieben und der TR-Zertifizierungsstelle des BSI übermittelt.</p>	---	---

Tabelle 5: Artefakte und ihre Sicherungsmechanismen

Hinweis:

Die Signaturen über die XML-Schemata für die G2-COS-Spezifikation, Challenge/Fingerprint-Referenzwert-Paare und Testberichte sowie die Signaturen über die XML-Dateien der Objektsystem-Spezifikationen (XML-Master / XML-Derivat) sind *nicht* Bestandteil der zuvor genannten XML-Strukturen. Diese Signaturen werden jeweils als äußere Signaturen an die XML-Schemata bzw. XML-Dateien angebracht. Hintergrund hierfür ist, dass XML-Signaturen für XML-Schemata nach dem standardisierten XML-Signatur-Verfahren nicht möglich sind. Um eine einheitliche Implementierung der Signaturprüfung im Konsistenz-Prüfwerkzeug zu erreichen, wird auch für XML-Dateien entsprechend mit einer äußeren Signatur gearbeitet. Weiterer Vorteil äußerer Signaturen im vorliegenden Fall ist die größere Flexibilität bzgl. der Auswahl kryptographischer Verfahren.

4 Übersicht über die Signaturschlüsselpaare

In der nachfolgenden Tabelle 6 wird eine Übersicht über die benötigten Typen von Signaturschlüsselpaaren (bzw. Signaturschlüsseln und zugehörigen Signaturprüfchlüsseln), deren Verwendungszweck und deren Inhaber bzw. Nutzer gegeben. Siehe hierzu auch Kap. 3.

Notation: In der letzten Tabellenspalte werden nur diejenigen Stellen benannt, die mindestens den betreffenden Signaturprüfchlüssel (direkt oder indirekt, z.B. bei Nutzung des Konsistenz-Prüftools) verwenden.

Signaturschlüsselpaar (Signaturschlüssel / Signaturprüfchlüssel)	Verwendungszweck des Signaturschlüssels	Generierende Stelle / Inhaber des Signa- turschlüssel- paars	Verwendende Stelle des Si- gnaturprüfchlüssels
S_Prüftool-Code / P_Prüftool-Code	Signatur über die Imple- mentierung des Konsistenz- Prüftools	gematik	<ul style="list-style-type: none"> TR-Zertifizierungsstelle (BSI) TR-Prüfstellen für Karten-Produkte Hinweis: Der Signaturprüfchlüssel P_Prüftool-Code ist im Konsistenz-Prüftool enthalten.
S_Prüftool-Schema / P_Prüftool-Schema	Signatur über die zum Kon- sistenz-Prüftool zu- gehörigen XML-Schemata der G2-COS-Spezifikation, der Challenge/Fingerprint- Referenzwert-Paare und der Testberichte	gematik	<ul style="list-style-type: none"> TR-Zertifizierungsstelle (BSI) TR-Prüfstellen für Karten-Produkte Hinweis: Der Signaturprüfchlüssel P_Prüftool-Schema ist im Konsistenz-Prüftool enthalten.
S_Prüftool-Dok /P_Prüftool-Dok	Signatur der Benutzerdoku- mentation zum Konsistenz- Prüftool (sofern elektro- nisch Auslieferung vorgese- hen)	gematik	<ul style="list-style-type: none"> TR-Zertifizierungsstelle (BSI) TR-Prüfstellen für Karten-Produkte
S_Objektsys-Spez / P_Objektsys-Spez	Signatur über die XML- Dateien der Objektsystem- Spezifikationen (XML- Master / XML-Derivat)	gematik	<ul style="list-style-type: none"> TR-Zertifizierungsstelle (BSI) TR-Prüfstellen für Karten-Produkte Hinweis: Der Signaturprüfchlüssel P_Objektsys-Spez ist in der zur Objektsystem-Spezifikation zugehörigen Konfigurationsdatei für das

Signatursschlüsselpaar (Signatursschlüssel / Signaturprüfsschlüssel)	Verwendungszweck des Signatursschlüssels	Generierende Stelle / Inhaber des Signa- turschlüssel- paars	Verwendende Stelle des Si- gnaturprüfsschlüssels
			Konsistenz-Prüftool enthal- ten.
S_Plattform-FP / P_Plattform-FP	Signatur über das Challenge/Fingerprint-Referenzwert-Paar einer Karten-Plattform	CC-Prüfstelle der (dem betreffenden Karten-Produkt unterliegenden) Karten-Plattform	<ul style="list-style-type: none"> • TR-Zertifizierungsstelle (BSI) • TR-Prüfstellen für Karten-Produkte, die auf der betreffenden Karten-Plattform aufsetzen • gematik (zur Verwendung im Rahmen von weiteren Prüf- oder Zulassungsprozessen/-verfahren für Karten-Plattformen und Karten-Produkte, die außerhalb der TR-Konformitätsprüfung von Karten-Produkten nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) liegen) <p>Hinweis: Der Signaturprüfsschlüssel P_Plattform-FP ist in der zum Challenge/Fingerprint-Referenzwert-Paar zugehörigen Konfigurationsdatei für das Konsistenz-Prüftool enthalten.</p>
S_Schlüsseltabelle / P_Schlüsseltabelle	Signatur über die Schlüssel-tabelle mit den Signatur- prüfsschlüsseln	TR-Zertifizierungs- stelle (BSI)	<ul style="list-style-type: none"> • gematik • TR-Prüfstellen für Karten-Produkte

Tabelle 6: Übersicht der Signatursschlüsselpaare

Es besteht die Möglichkeit, die Signatursschlüsselpaare

- (S_Prüftool-Code, P_Prüftool-Code),
- (S_Prüftool-Schema, P_Prüftool-Schema),
- (S_Prüftool-Dok, P_Prüftool-Dok) und
- (S_Objektsys-Spez, P_Objektsys-Spez)

zusammenzufassen, also durch ein einziges Schlüssel-paar zu repräsentieren.

Für die sichere (d.h. integre und authentische) Auslieferung der Signaturprüfsschlüssel ist der jeweilige Inhaber des zugehörigen Signatursschlüsselpaars verantwortlich.

5 Kryptographische Vorgaben

Für die in Kap. 3 genannten Signaturen soll RSA mit einer Schlüssellänge von mindestens 2048 Bit mit SHA-256 (mit einem ausreichend sicheren Signatur-/Paddingverfahren) verwendet werden.

Für die Erzeugung von Signaturen (siehe Kap. 3) soll (zunächst) eine PGP-Implementierung, die konform zur standardisierten Version OpenPGP gemäß [RFC 4880] ist, eingesetzt werden.

Die Generierung der Signaturschlüsselpaare soll ebenfalls durch eine solche PGP-Implementierung erfolgen. Die PGP-Signaturschlüsselpaare werden dabei in einem zu [RFC 4880] konformen PGP-Format angelegt; das Feld userID ist dabei mit dem Namen der Organisation, der der Inhaber des Signaturschlüsselpaars angehört, zu füllen. Für weitere Details hierzu sei auf die Benutzerdokumentation zum Konsistenz-Prüftool verwiesen.

Die für die Generierung eines Signaturschlüsselpaars (und für die Erzeugung von Signaturen) eingesetzte PGP-Implementierung soll weiterhin für den Signaturprüfchlüssel die Erstellung und Ausgabe eines PGP-Fingerprints ermöglichen, der in der Schlüsseltabelle mit den Signaturprüfchlüsseln (siehe Kap. 6) hinterlegt wird.

Hinweis:

Zukünftig ist vorgesehen, die PGP-Lösung durch eine andere, PKI-basierte Lösung, die sich an den Vorgaben der Technischen Richtlinie BSI TR-03116-1 ([TR-03116-1]) orientiert, zu ersetzen.

6 Schlüsselverwaltung

Zwecks Schlüsselverwaltung wird eine Schlüsseltabelle mit den im Rahmen von TR-Konformitätsprüfungen von Karten-Produkten nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) verwendeten Signaturprüfchlüsseln (siehe auch Kap. 4) aufgesetzt und verwaltet.

Die Schlüsseltabelle liefert eine Übersicht über die verwendeten Signaturprüfchlüssel und stellt für jeden eingetragenen Signaturprüfchlüssel folgende Informationen bereit:

- Name und Anschrift der Stelle, der der Inhaber des zugehörigen Signaturschlüsselpaars angehört.

Als Stelle kommt zur Auswahl:

CC-Prüfstelle für Karten-Plattform, gematik, TR-Zertifizierungsstelle (BSI).

- Name des Inhabers des zugehörigen Signaturschlüsselpaars.
- Schlüssel-ID des Signaturprüfchlüssels.
- Typ des Signaturprüfchlüssels.

Als Typ des Signaturprüfchlüssels kommt zur Auswahl:

P_Prüftool-Code, P_Prüftool-Schema, P_Prüftool-Dok, P_Objektsys-Spez, P_Plattform-FP, P_Schlüsseltabelle.

- Laufzeit (insbesondere Ablaufdatum) des zugehörigen Signaturschlüsselpaars.
- PGP-Fingerprint des Signaturprüfchlüssels.

Es empfiehlt sich, für einen Signaturprüfchlüssel bzw. ein Signaturschlüsselpaar eine geeignete Vertreterregelung einzurichten bzw. pro Stelle mehrere Signaturschlüsselpaare bzw. Signaturprüfchlüssel vorzusehen.

Die Schlüsseltabelle enthält insbesondere den (bzw. die) Signaturprüfchlüssel der TR-Zertifizierungsstelle des BSI vom Typ P_Schlüsseltabelle.

Die Ausgestaltung und Verwaltung der Schlüsseltabelle erfolgt durch die TR-Zertifizierungsstelle des BSI. Die betreffenden Stellen haben hierzu der TR-Zertifizierungsstelle des BSI ihre Signaturprüfchlüssel sowie die benötigten weiteren Informationen zu ihren Schlüsseln in integrierter und authentischer Weise bereitzustellen. Die Vergabe der Schlüssel-ID für einen Signaturprüfchlüssel erfolgt durch die TR-Zertifizierungsstelle des BSI. Die Schlüsseltabelle unterliegt einer Versionierung und wird mit Versionsnummer und Datum versehen.

Die Schlüsseltabelle kann von den betreffenden Stellen für Zwecke der TR-Konformitätsprüfung von Karten-Produkten nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) (und für Zwecke weitergehender Prüf- und Zulassungsprozesse und -verfahren von Karten-Plattformen und Karten-Produkten auf Seiten der gematik, die außerhalb der vorgenannten TR-Konformitätsprüfung von Karten-Produkten liegen) von der TR-Zertifizierungsstelle des BSI bezogen werden.

Hinweis: Je nach Erfordernis kann die Schlüsseltabelle auch an CC-Prüfstellen weitergegeben werden, die für die Bestätigung eines Karten-Produktes nach SigG/SigV vom Konsistenz-Prüftool Gebrauch machen wollen.

Für eine integrierte und authentische Auslieferung der Schlüsseltabelle wird diese von der TR-Zertifizierungsstelle des BSI unter Verwendung eines Signaturschlüssels vom Typ S_Schlüsseltabelle signiert und zusammen mit ihrer Signatur ausgeliefert. Der für die Prüfung der Signatur über die

Schlüsseltabelle relevante Signaturprüfchlüssel wird mit seiner Schlüssel-ID in der Schlüsseltabelle ausgewiesen. (Hinweis: Auf eine Signatur eines jeden einzelnen in der Schlüsseltabelle eingetragenen Signaturprüfchlüssels durch die TR-Zertifizierungsstelle des BSI kann (und soll aus Effizienzgründen) verzichtet werden, da eine Signatur über die Schlüsseltabelle, die insbesondere für jeden eingetragenen Signaturprüfchlüssel seinen PGP-Fingerprint beinhaltet, als ausreichend zu erachten ist.)

Literaturverzeichnis

- [TR-03106] BSI TR-03106 eHealth - Zertifizierungskonzept für Karten der Generation G2, aktuelle Fassung, BSI
- [TR-03143] BSI TR-03143 eHealth G2-COS Konsistenz-Prüftool, aktuelle Fassung, BSI
- [TR-03144] BSI TR-03144 eHealth - Konformitätsnachweis für Karten-Produkte der Kartengeneration G2, aktuelle Fassung, BSI
- [TR-03116-1] BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, aktuelle Fassung, BSI
- [RFC 4880] RFC 4880, J. Callas, L. Donnerhacker, H. Finney, D. Shaw, R. Thayer, OpenPGP Message Format, 2007, IETF