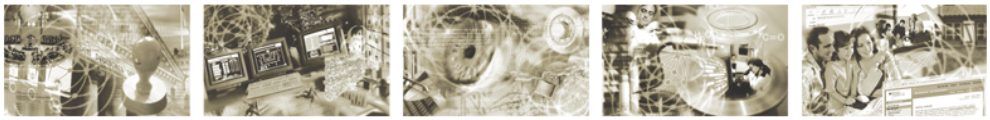
Bundesamt
für Sicherheit in der
Informationstechnik



Technische Richtlinie BSI TR-03144 Anhang

eHealth –

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

Version 1.2 – 27.07.2017

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Tabellenverzeichnis

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 beizusteuernden *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]) implementierten und 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
APDU	Application Protocol Data Unit
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
eIDAS	Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste
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
PTV	Produkttypversion
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
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
v1.2	27.07.2017	Anpassung an das Update der BSI TR-03143 (Version 1.1, 2017), Bugfixing, Einfügung von Klarstellungen, Aktualisierung von Referenzen und bzgl. eIDAS

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 für Objektsystem-Spezifikationen, Fingerprint-Sollwerte, Übersetzungstabellen und 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 Konfigurationsdateien enthalten jeweils eine Signatur bzw. einen Signaturprüfschlüssel (siehe untenstehende Ausführungen in Kap. 3).
R_Objektsys-Spezifikation	Sicherung der XML-Datei der Objektsystem-Spezifikation (XML-Master / XML-Derivat).
R_Plattform-Fingerprint	Sicherung des Challenge/Fingerprint-Referenzwert-Paars einer Karten-Plattform.
R_Übersetzungstabelle	Sicherung der XML-Datei mit der Übersetzungstabelle zu einer Karten-Plattform.
R_Testbericht	Sicherung des vom Konsistenz-Prüftool für ein Karten-Produkt ausgegebenen Testberichts.
R_Schlüsseltabelle	Verwaltung und Sicherung der Schlüsseltabelle mit den Signaturprüfschlüsseln (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 falls eine Übersetzungstabelle von der TR-Prüfstelle generiert und signiert wird: R_Prüftool-Konf-Dateien R_Übersetzungstabelle
CC-Prüfstelle für Karten-Plattform	R_Plattform-Fingerprint falls eine Übersetzungstabelle von der CC-Prüfstelle generiert und signiert wird: R_Prüftool-Konf-Dateien R_Übersetzungstabelle
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-Prüftools 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 Signaturprüfschlüsseln an das Konsistenz-Prüftool benutzt werden. Formatierungsvorgaben für solche Konfigurationsdateien sind Gegenstand der zum Konsistenz-Prüftool zugehörigen Benutzerdokumentation.

Artefakt	**Sicherheitsziel(e)**	**Kryptographische Sicherung**	**Art der Signatur**
Konsistenz-Prüftool			
Code / Dateien mit den Java-Bibliotheken des Konsistenz-Prüftools (inklusive Java-Laufzeitumgebung)	Integrität, Authentizität	Signatur	äußere technische Signatur
XML-Schema für Objektsystem-Spezifikationen (zugehörig zum Konsistenz-Prüftool)	Integrität, Authentizität	Signatur	äußere technische Signatur
XML-Schema für Fingerprint-Sollwerte (zugehörig zum Konsistenz-Prüftool)	Integrität, Authentizität	Signatur	äußere technische Signatur
XML-Schema für Übersetzungstabellen (zugehörig zum Konsistenz-Prüftool)	Integrität, Authentizität	Signatur	äußere technische Signatur
XML-Schema für Testberichte (zugehörig zum Konsistenz-Prüftool)	Integrität, Authentizität	Signatur	äußere technische Signatur
Benutzerdokumentation zum Konsistenz-Prüftool	Integrität, Authentizität	Signatur (bei elektronischer Auslieferung)	äußere technische Signatur
TR-Zertifikat und -Konformitätsreport zum Konsistenz-Prüftool	Integrität, Authentizität	---	---
Inputquellen für das Konsistenz-Prüftool			
Konfigurationsdatei mit der Signatur über das Konsistenz-Prüftool (Code / Dateien mit den Java-Bibliotheken inklusive Java-Laufzeitumgebung)	Integrität, Authentizität	---	---
Konfigurationsdatei mit der Signatur über das XML-Schema für Objektsystem-Spezifikationen	Integrität, Authentizität	---	---

Artefakt	Sicherheitsziel(e)	Kryptographische Sicherung	Art der Signatur
Konfigurationsdatei mit der Signatur über das XML-Schema für Fingerprint-Sollwerte	Integrität, Authentizität	---	---
Konfigurationsdatei mit der Signatur über das XML-Schema für Übersetzungstabellen	Integrität, Authentizität	---	---
Konfigurationsdatei mit der Signatur über das XML-Schema für 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 der Signatur über die Übersetzungstabelle (XML-Datei) zur Karten-Plattform	Integrität, Authentizität	---	---
Konfigurationsdatei mit dem Signaturprüfschlüssel 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 Signaturprüfschlüssel für die Prüfung der Signatur über das Challenge/Fingerprint-Referenzwert-Paar der Karten-Plattform	Integrität, Authentizität	---	---
Konfigurationsdatei mit dem Signaturprüfschlüssel für die Prüfung der Signatur über die Übersetzungstabelle (XML-Datei) zur 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-	Integrität,	Signatur,	äußere technische

Artefakt	Sicherheitsziel(e)	Kryptographische Sicherung	Art der Signatur
Paar der Karten-Plattform	Authentizität, Vertraulichkeit	Verschlüsselung	Signatur
Übersetzungstabelle (XML-Datei) zur Karten-Plattform	Integrität, Authentizität	Signatur	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-Prüftools 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 Signaturprüfschlüsseln siehe (Übersichts-) Tabelle 6 in Kap. 4.

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels (abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)
Konsistenz-Prüftool			
Code / Dateien mit den Java-Bibliotheken des Konsistenz-Prüftools (inklusive Java-Laufzeitumgebung)	Äußere technische Signatur über den Code des Konsistenz-Prüftools. Automatische Signaturprüfung im Konsistenz-Prüftool selbst im Rahmen seines Selbsttests. Für die automatische Signaturprüfung ist ein vorhergehender Import der zugehörigen Konfigurationsdatei mit der zu prüfenden Signatur über das Konsistenz-Prüftool in das Konsistenz-Prüftool erforderlich. Zusätzlich kann eine externe Signaturprüfung (ohne Nutzung des Konsistenz-Prüftools) durchgeführt werden.	S_Prüftool-Code	P_Prüftool-Code ist im Konsistenz-Prüftool selbst hinterlegt

Artefakt	**Technische / Organisatorische Lösung**	**Typ des Signaturschlüssels**	**Speicherort des Signaturprüfschlüssels** (abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)
XML-Schema für Objektsystem-Spezifikationen (zugehörig zum Konsistenz-Prüftool)	Äußere technische Signatur über das XML-Schema. Automatische Signaturprüfung im Konsistenz-Prüftool selbst. 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. Zusätzlich kann eine externe Signaturprüfung (ohne Nutzung des Konsistenz-Prüftools) durchgeführt werden.	S_Prüftool-Schema	P_Prüftool-Schema ist im Konsistenz-Prüftool selbst hinterlegt
XML-Schema für Fingerprint-Sollwerte (zugehörig zum Konsistenz-Prüftool)	Äußere technische Signatur über das XML-Schema. Automatische Signaturprüfung im Konsistenz-Prüftool selbst. 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. Zusätzlich kann eine externe Signaturprüfung (ohne Nutzung des Konsistenz-Prüftools) durchgeführt werden.	S_Prüftool-Schema	P_Prüftool-Schema ist im Konsistenz-Prüftool selbst hinterlegt
XML-Schema für Übersetzungstabellen (zugehörig zum Konsistenz-Prüftool)	Äußere technische Signatur über das XML-Schema. Automatische Signaturprüfung im Konsistenz-Prüftool selbst. 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.	S_Prüftool-Schema	P_Prüftool-Schema ist im Konsistenz-Prüftool selbst hinterlegt

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

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels (abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)
	tionsdatei in das Konsistenz-Prüftool erforderlich. Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.		
Konfigurationsdatei mit der Signatur über das XML-Schema für Objektsystem-Spezifikationen	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. Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüftool erforderlich. Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.	---	---
Konfigurationsdatei mit der Signatur über das XML-Schema für Fingerprint-Sollwerte	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. Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüftool erforderlich. Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.	---	---
Konfigurationsdatei mit der Signatur über das XML-Schema für Übersetzungstabellen	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. Für die Signaturprüfung ist ein vorhergehender Import der Konfigura-	---	---

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels (abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)
	tionsdatei in das Konsistenz-Prüftool erforderlich. Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.		
Konfigurationsdatei mit der Signatur über das XML-Schema für Testberichte	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. Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüftool erforderlich. Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.	---	---
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/...)	Im Konsistenz-Prüftool erfolgt unter Verwendung des in das Konsistenz-Prüftool importierten Signaturprüfschlüssels 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. Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüftool erforderlich. Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.	---	---
Konfigurationsdatei mit der Signatur über das Challenge/Fingerprint-Referenzwert-Paar der Karten-Plattform	Im Konsistenz-Prüftool erfolgt unter Verwendung des in das Konsistenz-Prüftool importierten Signaturprüfschlüssels P_Plattform-FP (Import mittels seiner zugehörigen Konfigurationsdatei, siehe unten) eine Prü-	---	---

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels (abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)
	fung der in der Konfigurationsdatei enthaltenen Signatur über das Challenge/Fingerprint-Referenzwert-Paar. Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüftool erforderlich. Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.		
Konfigurationsdatei mit der Signatur über die Übersetzungstabelle (XML-Datei) zur Karten-Plattform	Im Konsistenz-Prüftool erfolgt unter Verwendung des in das Konsistenz-Prüftool importierten Signaturprüfschlüssels P_Übersetzung (Import mittels seiner zugehörigen Konfigurationsdatei, siehe unten) eine Prüfung der in der Konfigurationsdatei enthaltenen Signatur über die XML-Datei mit der Übersetzungstabelle. Für die Signaturprüfung ist ein vorhergehender Import der Konfigurationsdatei in das Konsistenz-Prüftool erforderlich. Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden.	---	---
Konfigurationsdatei mit dem Signaturprüfschlüssel 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/...)	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). Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden. Es erfolgt ein Import der Konfigurationsdatei in das Konsistenz-Prüftool, damit der enthaltene Signaturprüfschlüssel P_Objektsys-Spez im	---	---

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels (abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)
	Konsistenz-Prüftool zur weiteren Verwendung zur Verfügung steht.		
Konfigurationsdatei mit dem Signaturprüfschlüssel für die Prüfung der Signatur über das Challenge/ Fingerprint-Referenzwert-Paar der Karten-Plattform	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). Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden. 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.	---	---
Konfigurationsdatei mit dem Signaturprüfschlüssel für die Prüfung der Signatur über die Übersetzungstabelle (XML-Datei) zur Karten-Plattform	Außerhalb des Konsistenz-Prüftools erfolgt eine Überprüfung der Integrität/Authentizität der Konfigurationsdatei bzw. des darin enthaltenen Signaturprüfschlüssels P_Übersetzung gegen die mit S_Schlüsseltabelle signierte Schlüsseltabelle von Signaturprüfschlüsseln (siehe Kap. 6). Auf eine kryptographische Sicherung der Konfigurationsdatei selbst kann verzichtet werden. Es erfolgt ein Import der Konfigurationsdatei in das Konsistenz-Prüftool, damit der enthaltene Signaturprüfschlüssel P_Übersetzung im Konsistenz-Prüftool zur weiteren Verwendung zur Verfügung steht.	---	---
XML-Datei der Objektsystem-Spezifikation xy (XML-Master / XML-Derivat) (xy = eGK/HBA/ SMC-B/gSMC-K/	Äußere Signatur der XML-Datei. Im Konsistenz-Prüftool erfolgt unter Verwendung des Signaturprüfschlüssels P_Objektsys-Spez eine Prüfung der Signatur über die XML-Datei der Objektsystem-Spezifikati-	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)
gSMC-KT/...)	on xy. Für die Signaturprüfung ist ein vorhergehender Import der zugehörigen Konfigurationsdatei mit dem Signaturprüfschlüssel P_Objektsys-Spez in das Konsistenz-Prüftool erforderlich.		
Challenge/Fingerprint-Referenzwert-Paar der Karten-Plattform	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. 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. Hinweis: Das Konsistenz-Prüftool benötigt für die Weiterverwendung des Challenge/Fingerprint-Referenzwert-Paars dieses im Klartext, da das Konsistenz-Prüftool selbst keine Entschlüsselungsfunktion bereitstellt. Äußere Signatur des Challenge/Fingerprint-Referenzwert-Paars. Im Konsistenz-Prüftool erfolgt unter Verwendung des Signaturprüfschlüssels P_Plattform-FP eine Prüfung der Signatur über das Challenge/Fingerprint-Referenzwert-Paar.	S_Plattform-FP	Konfigurationsdatei mit dem Signaturprüfschlüssel P_Plattform-FP

Artefakt	**Technische / Organisatorische Lösung**	**Typ des Signaturschlüssels**	**Speicherort des Signaturprüfschlüssels** (abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)
	Für die Signaturprüfung ist ein vorhergehender Import der zugehörigen Konfigurationsdatei mit dem Signaturprüfschlüssel P_Plattform-FP in das Konsistenz-Prüftool erforderlich.		
Übersetzungstabelle (XML-Datei) zur Karten-Plattform	Äußere Signatur der XML-Datei. Im Konsistenz-Prüftool erfolgt unter Verwendung des Signaturprüfschlüssels P_Übersetzung eine Prüfung der Signatur über die XML-Datei mit der Übersetzungstabelle. Für die Signaturprüfung ist ein vorhergehender Import der zugehörigen Konfigurationsdatei mit dem Signaturprüfschlüssel P_Übersetzung in das Konsistenz-Prüftool erforderlich.	S_Übersetzung	Konfigurationsdatei mit dem Signaturprüfschlüssel P_Übersetzung
Output des Konsistenz-Prüftools			
Testbericht	Es wird auf eine kryptographische Sicherung durch das Konsistenz-Prüftool selbst verzichtet. 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. Der vom Konsistenz-Prüftool ausgegebene Testbericht wird dem TR-Prüfbericht der TR-Prüfstelle für das betreffende Karten-Produkt beigefügt. Dieser TR-Prüfbericht wird insgesamt von der TR-Prüfstelle in Papierform unterschrieben und der TR-Zertifizierungsstelle des BSI	---	---

Artefakt	Technische / Organisatorische Lösung	Typ des Signaturschlüssels	Speicherort des Signaturprüfschlüssels (abgesehen von der Schlüsseltabelle der TR-Zertifizierungsstelle des BSI, siehe Kap. 6)
	übermittelt.		

Tabelle 5: Artefakte und ihre Sicherungsmechanismen

Hinweis:

Die Signaturen über die XML-Schemata für Objektsystem-Spezifikationen, Fingerprint-Sollwerte, Übersetzungstabellen und Testberichte sowie die Signaturen über die XML-Dateien der Objektsystem-Spezifikationen (XML-Master / XML-Derivat) und der Übersetzungstabellen 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-Prüftool 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 Signaturprüfschlüsseln), 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 Signaturprüfschlüssel (direkt oder indirekt, z.B. bei der Nutzung des Konsistenz-Prüftools) verwenden.

Signaturschlüsselpaar **(Signaturschlüssel / Signaturprüfschlüssel)**	**Verwendungszweck des Signaturschlüssels**	**Generierende Stelle / Inhaber des Signaturschlüsselpaars**	**Verwendende Stelle des Signaturprüfschlüssels**
S_Prüftool-Code / P_Prüftool-Code	Signatur über die Implementierung des Konsistenz-Prüftools	gematik	• TR-Zertifizierungsstelle (BSI) • TR-Prüfstellen für Karten-Produkte Hinweis: Der Signaturprüfschlüssel P_Prüftool-Code ist im Konsistenz-Prüftool enthalten.
S_Prüftool-Schema / P_Prüftool-Schema	Signatur über die zum Konsistenz-Prüftool zugehörigen XML-Schemata für Objektsystem-Spezifikationen, Fingerprint-Sollwerte, Übersetzungstabellen und Testberichte	gematik	• TR-Zertifizierungsstelle (BSI) • TR-Prüfstellen für Karten-Produkte Hinweis: Der Signaturprüfschlüssel P_Prüftool-Schema ist im Konsistenz-Prüftool enthalten.
S_Prüftool-Dok / P_Prüftool-Dok	Signatur der Benutzerdokumentation zum Konsistenz-Prüftool (sofern elektronische Auslieferung vorgesehen)	gematik	• TR-Zertifizierungsstelle (BSI) • TR-Prüfstellen für Karten-Produkte
S_Objektsys-Spez / P_Objektsys-Spez	Signatur über die XML-Datei der Objektsystem-Spezifikation (XML-Master / XML-Derivat)	gematik	• TR-Zertifizierungsstelle (BSI) • TR-Prüfstellen für Karten-Produkte Hinweis: Der Signaturprüfschlüssel P_Objektsys-Spez ist in der zur Objektsystem-Spezifikation zugehörigen Konfigurationsdatei für das Konsistenz-Prüftool enthalten.

Signaturschlüsselpaar **(Signaturschlüssel / Signaturprüfschlüssel)**	**Verwendungszweck des Signaturschlüssels**	**Generierende Stelle / Inhaber des Signaturschlüsselpaars**	**Verwendende Stelle des Signaturprüfschlüssels**
S_Plattform-FP / P_Plattform-FP	Signatur über das Challenge/Fingerprint-Referenzwert-Paar einer Karten-Plattform	CC-Prüfstelle der betreffenden Karten-Plattform	• TR-Zertifizierungsstelle (BSI) • TR-Prüfstellen für Karten-Produkte, die auf der betreffenden Karten-Plattform aufsetzen Hinweis: Der Signaturprüfschlüssel P_Plattform-FP ist in der zum Challenge/Fingerprint-Referenzwert-Paar zugehörigen Konfigurationsdatei für das Konsistenz-Prüftool enthalten.
S_Übersetzung / P_Übersetzung	Signatur über die Übersetzungstabelle (XML-Datei) zu einer Karten-Plattform	CC-Prüfstelle der (dem betreffenden Karten-Produkt unterliegenden) Karten-Plattform oder TR-Prüfstelle des betreffenden Karten-Produktes	• TR-Zertifizierungsstelle (BSI) • TR-Prüfstelle des betreffenden Karten-Produktes Hinweis: Der Signaturprüfschlüssel P_Übersetzung ist in der zur Übersetzungstabelle zugehörigen Konfigurationsdatei für das Konsistenz-Prüftool enthalten.
S_Schlüsseltabelle / P_Schlüsseltabelle	Signatur über die Schlüsseltabelle mit den Signaturprüfschlüsseln	TR-Zertifizierungsstelle (BSI)	• gematik • TR-Prüfstellen für Karten-Produkte

Tabelle 6: Übersicht der Signaturschlüsselpaare

Es besteht die Möglichkeit, die Signaturschlüsselpaare

- (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 Schlüsselpaar zu repräsentieren.

Für die sichere (d.h. integre und authentische) Auslieferung der Signaturprüfschlüssel an die TR-Zertifizierungsstelle für die Schlüsseltabelle (siehe Kap. 6) ist der jeweilige Inhaber des zugehörigen Signaturschlüsselpaars bzw. dessen zugeordnete Stelle 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 eingesetzte PGP-Implementierung soll weiterhin für den Signaturprüfschlüssel die Erstellung und Ausgabe eines PGP-Fingerprints ermöglichen, der dann in der Schlüsseltabelle mit den Signaturprüfschlüsseln (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 Signaturprüfschlüsseln (siehe auch Kap. 4) aufgesetzt und gepflegt.

Die Schlüsseltabelle liefert eine Übersicht über die verwendeten Signaturprüfschlüssel und stellt für jeden eingetragenen Signaturprüfschlüssel 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-Prüfstelle für Karten-Produkt, TR-Zertifizierungsstelle (BSI).
- Name des Inhabers des zugehörigen Signaturschlüsselpaars.
- Schlüssel-ID des Signaturprüfschlüssels.
- Typ des Signaturprüfschlüssels.

  Als Typ des Signaturprüfschlüssels kommt zur Auswahl:

  P_Prüftool-Code, P_Prüftool-Schema, P_Prüftool-Dok, P_Objektsys-Spez, P_Plattform-FP, P_Übersetzung, P_Schlüsseltabelle.
- Laufzeit (insbesondere Ablaufdatum) des zugehörigen Signaturschlüsselpaars.
- PGP-Fingerprint des Signaturprüfschlüssels.

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

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

Die Ausgestaltung und Verwaltung der Schlüsseltabelle erfolgt durch die TR-Zertifizierungsstelle des BSI. Die Schlüsselinhaber bzw. deren zugeordnete Stelle haben der TR-Zertifizierungsstelle des BSI für die Schlüsseltabelle ihre Signaturprüfschlüssel sowie die benötigten weiteren Informationen zu ihren Schlüsseln in integrer und authentischer Weise bereitzustellen. Die Vergabe der Schlüssel-ID für einen Signaturprüfschlüssel erfolgt durch die TR-Zertifizierungsstelle des BSI. Die Schlüsseltabelle unterliegt einer Versionierung und wird mit Versionsnummer und Datum versehen.

Die Schlüsseltabelle kann für Zwecke der TR-Konformitätsprüfung von Karten-Produkten nach der Technischen Richtlinie BSI TR-03144 ([TR-03144]) von der TR-Zertifizierungsstelle des BSI von den in eine solche Prüfung involvierten Stellen bezogen werden. Gleiches gilt für Zwecke weitergehender Prüf- oder Zulassungs-Prozesse/Verfahren von Karten-Plattformen und Karten-Produkten auf Seiten der gematik, die außerhalb der vorgenannten TR-Konformitätsprüfung von Karten-Produkten liegen.

Hinweis: Je nach Erfordernis kann die Schlüsseltabelle auch an CC-Prüfstellen weitergegeben werden, die im Rahmen der CC-Zertifizierung von Karten-Produkten als Sichere Signaturerstellungseinheit (SSEE) nach eIDAS vom Konsistenz-Prüftool Gebrauch machen wollen.

Für eine integre 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 Signaturprüfschlüssel vom Typ P_Schlüsseltabelle wird mit seiner Schlüssel-ID in der Schlüsseltabelle ausgewiesen. (Hinweis: Auf eine Signatur eines jeden einzelnen in der Schlüsseltabelle eingetragenen Signaturprüfschlüssels durch die TR-Zertifizierungsstelle des BSI kann (und soll aus Effizienzgründen) verzichtet werden, da eine Signatur über die Schlüsseltabelle, die insbesondere für jeden eingetragenen Signaturprüfschlüssel 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. Donnerhacke, H. Finney, D. Shaw, R. Thayer, OpenPGP Message Format, 2007, IETF