Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung

Teil 5: Anwendungen der Secure Element API

Stand 2023

Datum: 24. April 2023

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

E-Mail: registrierkassen@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

Die Technische Richtlinie BSI TR-03116 stellt eine Vorgabe für Projekte des Bundes dar. Die Technische Richtlinie ist in sechs Teile gegliedert:

- Teil 1 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren im Gesundheitswesen für die elektronische Gesundheitskarte (eGK), den Heilberufeausweis (HBA) und der technischen Komponenten der Telematikinfrastruktur.
- Teil 2 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in hoheitlichen Dokumenten und eID-Dokumenten basierend auf Extended Access Control, zurzeit für den elektronischen Reisepass, den elektronischen Personalausweis, den elektronischen Aufenthaltstitel, die eID-Karte für Unionsbürger, die Smart-eID, Änderungsaufkleber hoheitlicher Dokumente, VISA-Aufkleber und den Ankunftsnachweis.
- Teil 3 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in der Infrastruktur intelligenter Messsysteme im Energiesektor.
- Teil 4 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz der Kommunikationsverfahren SSL/TLS, S/MIME, SAML/XML-Security und OpenPGP in Anwendungen des Bundes.
- Der vorliegende Teil 5 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in Anwendungen der Secure Element API (wie Technischen Sicherheitseinrichtungen elektronischer Aufzeichnungssysteme).
- Teil 6 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in der Infrastruktur kooperativer intelligenter Verkehrssysteme (Cooperative Intelligent Transport Systems / C-ITS).

1.1 Geltungsbereich

Die Anforderungen an die Funktionalität und Interoperabilität der Secure Element API werden in der Technischen Richtlinie BSI TR-03151-1 [1] spezifiziert.

In diesem Dokument werden die in Anwendungen der Secure Element API einzusetzenden kryptographischen Verfahren und zu verwendenden Schlüssellängen verbindlich vorgegeben. Die Vorgaben basieren auf der Technischen Richtlinie BSI TR-03111 [2] sowie auf den Empfehlungen in der Technischen Richtlinie BSI TR-02102-1 [3] und in SOG-IS Agreed Cryptographic Mechanisms [4].

Tabelle 1 gibt eine Übersicht über die kryptographischen Primitive, die in diesem Dokument verwendet werden.

Verfahren	*Algorithmus*
Digitale Signatur	ECDSA [2] ECSDSA [2]
Hashfunktion	SHA-2 oder SHA-3 [5]
Elliptische Kurven	NIST-Domain-Parameter über Primkörpern [6] Brainpool-Domain-Parameter [7]

Tabelle 1: Kryptographische Primitive

1.1.1 Elektronische Aufzeichnungssysteme

Eine Anwendung der Secure Element API sind Technische Sicherheitseinrichtungen elektronischer Aufzeichnungssysteme gemäß Abgabenordnung [8] und Kassensicherungsverordnung [9]. Die Anforderungen an die Funktionalität und Interoperabilität der Technischen Sicherheitseinrichtungen werden in der Technischen Richtlinie BSI TR-03153-1 [10] festgelegt.

Tabelle 2 gibt einen Überblick über die verwendeten Verfahren und ihren Einsatzzweck.

Einsatzzweck	*Verfahren*
Absicherung elektronischer Aufzeichnungen	Digitale Signatur
Seriennummer einer Technischen Sicherheitseinrichtung	Hashfunktion

Tabelle 2: Kryptographische Verfahren und ihr Einsatzzweck

1.2 Begrifflichkeiten

1.2.1 Verwendungszeiträume

Die Vorgaben des vorliegenden Teils 5 der Technischen Richtlinie basieren auf Prognosen über die Sicherheit der verwendeten kryptographischen Verfahren über einen Zeitraum von 4 Jahren, zurzeit bis einschließlich 2026. Ist eine weitere Verwendung über diesen Zeitraum hinaus nicht ausgeschlossen, so wird dies mit 2026+ gekennzeichnet.

1.2.2 Schlüsselworte

Anforderungen als Ausdruck normativer Festlegungen werden durch die in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS/MÜSSEN, DARF NICHT/DÜRFEN NICHT, VERPFLICHTEND, SOLLTE/SOLLTEN, EMPFOHLEN, SOLLTE NICHT/SOLLTEN NICHT, KANN/KÖNNEN/DARF/DÜRFEN, und OPTIONAL gekennzeichnet.

Die verwendeten Schlüsselworte sind auf Basis der folgenden Übersetzungstabelle gemäß RFC 2119 [11] zu interpretieren:

Deutsch	*Englisch*
MUSS / MÜSSEN	MUST, SHALL
DARF NICHT / DÜRFEN NICHT	MUST NOT, SHALL NOT
VERPFLICHTEND	REQUIRED
SOLLTE / SOLLTEN	SHOULD
SOLLTE NICHT / SOLLTEN NICHT	SHOULD NOT
EMPFOHLEN	RECOMMENDED
KANN / KÖNNEN / DARF / DÜRFEN	MAY
OPTIONAL	OPTIONAL

Tabelle 3: Schlüsselworte

2 Kryptographische Algorithmen

2.1 Zufallszahlengeneratoren

Für die Erzeugung von Zufallszahlen und kryptographischen Schlüsseln MÜSSEN in allen verwendeten kryptographischen Verfahren Zufallszahlengeneratoren aus einer der folgenden Klassen (siehe BSI AIS 20/31 [12]) verwendet werden:

- DRG.3 oder höher;
- PTG.2 oder höher.

Es wird EMPFOHLEN, die Zufallszahlengeneratorklasse PTG.3 zu verwenden.

Bei der Verwendung von PTG.2 ist ggf. eine geeignete kryptographische Nachbearbeitung der Zufallszahlen erforderlich, um eine mögliche Schiefe der Zufallszahlen zu verhindern (beispielsweise durch DRG.3).

Für die Konvertierung von Zufallsbits in Zufallszahlen (ECC-Nonces) MÜSSEN die Empfehlungen von Anhang B der Technischen Richtlinie BSI TR-02102-1 [3] eingehalten werden.

2.2 Absicherung elektronischer Aufzeichnungen

Eine Anwendung der Secure Element API MUSS für die Erzeugung von Signaturen ein Verfahren aus Tabelle 4 verwenden. Die Verwendungszeiträume beziehen sich auf die Herstellung des Sicherheitsmoduls.

Signaturverfahren	*Signaturformat*	*Verwendung von*	*Verwendung bis*
ECDSA [2]	Plain-Format	2018	2026+
ECSDSA [2]	Plain-Format	2018	2026+

Tabelle 4: Zulässige Verfahren für die Signaturberechnung

Als Hashfunktion innerhalb des Signaturverfahrens MUSS eine Hashfunktion aus Tabelle 5 verwendet werden.

Hashfunktion	*Minimale Outputlänge der Hashfunktion*	*Verwendung von*	*Verwendung bis*
ECDSA oder ECSDSA			
SHA-2	256 Bit	2018	2026+
SHA-3	256 Bit	2018	2026+

Tabelle 5: Zulässige Hashfunktionen für die Signaturberechnung

Als ECC-Domain-Parameter für die Berechnung einer Signatur MUSS eine elliptische Kurve aus Tabelle 6 verwendet werden. Die Verwendungszeiträume beziehen sich auf die Herstellung des Sicherheitsmoduls.

EC-Domain-Parameter	*Verwendung von*	*Verwendung bis*
brainpoolP256r1 [7]	2018	2026+
brainpoolP384r1 [7]	2018	2026+
brainpoolP512r1 [7]	2018	2026+
NIST P-256 (secp256r1) [6]	2018	2026+
NIST P-384 (secp384r1) [6]	2018	2026+
NIST P-521 (secp521r1) [6]	2018	2026+

Tabelle 6: Zulässige Domain-Parameter für die Signaturerzeugung

Die ECC-Domain-Parameter MÜSSEN im Zertifikat als Named Curve angegeben werden. Als Encoding für die Punkte der elliptischen Kurven MUSS das Uncompressed Encoding gemäß BSI TR-03111 [2] verwendet werden.

Verifizierende Stellen MÜSSEN alle Verfahren und Parameter der Tabellen 4-6 unterstützen, um eine reibungslose Verifikation der Signatur sicherstellen zu können. Andere Verfahren und Parameter, als die in den Tabellen 4-6 angegebenen, DÜRFEN für die Verifikation von Signaturen NICHT akzeptiert werden.

2.3 Zertifikate und Public-Key-Infrastrukturen

Die Authentizität des Schlüssels von Anwendungen der Secure Element API wird über ein Zertifikat sichergestellt. Die Prüfung der Authentizität des Zertifikats und die Zuordnung zum Zertifikatsinhaber erfolgt hierbei i.d.R. über eine Public-Key-Infrastruktur[1].

Für die Erzeugung der Signatur von Zertifikaten MUSS ein Verfahren aus Tabelle 7 verwendet werden. Die Verwendungszeiträume beziehen sich auf die Erstellung der Zertifikate.

Signaturverfahren	*Verwendung von*	*Verwendung bis*
ECDSA [2]	2018	2026+
ECSDSA [2]	2018	2026+

Tabelle 7: Zulässige Verfahren für die Signatur von Zertifikaten

Als Hashfunktion für die Signatur von Zertifikaten MUSS eine Hashfunktion aus Tabelle 8 verwendet werden.

Hashfunktion	*Minimale Outputlänge der Hashfunktion*	*Verwendung von*	*Verwendung bis*
ECDSA oder ECSDSA			
SHA-2	384 Bit	2018	2026+
SHA-3	384 Bit	2018	2026+

Tabelle 8: Zulässige Hashfunktionen für die Signatur von Zertifikaten

Als ECC-Domain-Parameter für die Signatur von Zertifikaten MUSS eine elliptische Kurve aus Tabelle 9 verwendet werden. Die Verwendungszeiträume beziehen sich auf die Erstellung der Zertifikate.

1 Die Vorgaben für die Public-Key-Infrastruktur sind in der Technischen Richtline BSI TR-03153-1 [10] festgelegt.

EC-Domain-Parameter	*Verwendung von*	*Verwendung bis*
brainpoolP384r1 [7]	2018	2026+
brainpoolP512r1 [7]	2018	2026+
NIST P-384 (secp384r1) [6]	2018	2026+
NIST P-521 (secp521r1) [6]	2018	2026+

Tabelle 9: Zulässige Domain-Parameter für die Signatur von Zertifikaten

Die ECC-Domain-Parameter MÜSSEN als Named Curve angegeben werden. Als Encoding für die Punkte der elliptischen Kurven MUSS das Uncompressed Encoding gemäß BSI TR-03111 [2] verwendet werden.

Verifizierende Stellen MÜSSEN alle Verfahren und Parameter der Tabellen 7-9 unterstützen, um eine reibungslose Verifikation eines Zertifikats sicherstellen zu können. Andere Verfahren und Parameter, als die in den Tabellen 7-9 angegebenen, DÜRFEN für die Verifikation von Zertifikaten NICHT akzeptiert werden.

3 Anwendungsspezifische Vorgaben

3.1 Technische Sicherheitseinrichtungen elektronischer Aufzeichnungssysteme

Dieses Kapitel enthält weitergehende Vorgaben für Technische Sicherheitseinrichtungen elektronischer Aufzeichnungssysteme gemäß BSI TR-03153-1 [10].

3.1.1 Seriennummer einer Technischen Sicherheitseinrichtung

Als Seriennummer der Technischen Sicherheitseinrichtung eines elektronischen Aufzeichnungssystems dient der Hashwert des öffentlichen Schlüssels der Technischen Sicherheitseinrichtung.

Die hierbei zu verwendende Hashfunktion wird von Tabelle 10 vorgegeben. Der Verwendungszeitraum bezieht sich auf die Herstellung der Technischen Sicherheitseinrichtung.

Hashfunktion	*Outputlänge der Hashfunktion*	*Verwendung von*	*Verwendung bis*
SHA-2	256 Bit	2018	2026+

Tabelle 10: Hashfunktion zur Erzeugung der Seriennummer einer TSE

3.1.2 Update von Transaktionen

Im Rahmen der Aufzeichnung von Vorgängen sind Transaktionen im Falle der Aktualisierung von Vorgangsdaten nach dem Start und vor Beendigung regelmäßig zu aktualisieren (UpdateTransaction gemäß BSI TR-03153-1 [10]).

Tabelle 11 gibt das Zeitintervall MAX_UPDATE_DELAY an, innerhalb dessen die Transaktionen nach einer Änderung von Anwendungsdaten durch das elektronische Aufzeichnungssystem durch Aufruf der Funktion UpdateTransaction in der Technischen Sicherheitseinrichtung zu aktualisieren sind. Der Verwendungszeitraum bezieht sich auf den Einsatzzeitpunkt des elektronischen Aufzeichnungssystems.

Maximales Zeitintervall in Sekunden	*Verwendung von*	*Verwendung bis*
45	2018	2026+

Tabelle 11: Zeitintervall für die Aktualisierung einer Transaktion

Für den Wert „MAX_PROTECTION_DELAY“ wird aktuell kein Wert definiert.

Literaturverzeichnis

[1] BSI TR-03151-1, Technical Guideline Secure Element API (SE API), Part 1: Interface Definition, 2023

[2] BSI TR-03111, Elliptic Curve Cryptography (ECC), Version 2.10, 2018

[3] BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2023

[4] SOG-IS , Agreed Cryptographic Mechanisms, Version 1.2, 2020

[6] NIST FIPS PUB 180-4, Secure Hash Standard (SHS), 2015

[7] IETF RFC 5114, M. Lepinski, S. Kent, Additional Diffie-Hellman Groups for Use with IETF Standards, 2008

[8] IETF RFC 5639, M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010

[1] Abgabenordnung

[9] Kassensicherungsverordnung

[10] BSI TR-03153-1, Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Teil 1: Anforderungen an die Technische Sicherheitseinrichtung, 2023

[11] IETF RFC 2119, S. Bradner, Key words for use in RFCs to indicate requirement levels, 1997

[12] BSI AIS 20/31, A proposal for: Functionality classes for random number generators, Version 2.0, 2011