Bundesamt
für Sicherheit in der
Informationstechnik

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

Teil 5: Anwendungen der Secure Element API

Stand 2018

Datum: 6. Juni 2018

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

E-Mail: registrierkassen@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2018

Inhaltsverzeichnis

1 Einleitung ... 5
1.1 Anwendungen der Secure Element API ... 5
1.1.1 Elektronische Aufzeichnungssysteme ... 6
1.2 Schlüsselworte ... 6
2 Kryptographische Algorithmen ... 8
2.1 Zufallszahlengeneratoren ... 8
2.2 Absicherung elektronischer Aufzeichnungen ... 8
2.3 Zertifikate und Public Key Infrastrukturen ... 9
3 Anwendungsspezifische Vorgaben ... 11
3.1 Technische Sicherheitseinrichtungen elektronischer Aufzeichnungssysteme ... 11
3.1.1 Seriennummer einer Technischen Sicherheitseinrichtung ... 11
3.1.2 Update von Transaktionen ... 11
Literaturverzeichnis ... 12

Tabellenverzeichnis

Tabelle 1: Kryptographische Algorithmen ... 6
Tabelle 2: Kryptographische Verfahren und ihr Einsatzzweck ... 6
Tabelle 3: Zulässige Verfahren für die Signaturberechnung ... 8
Tabelle 4: Zulässige Hashfunktionen für die Signaturberechnung ... 8
Tabelle 5: Zulässige Domain-Parameter für die Signaturerzeugung ... 9
Tabelle 6: Zulässige Verfahren für die Signatur von Zertifikaten ... 9
Tabelle 7: Zulässige Hashfunktionen für die Signatur von Zertifikaten ... 9
Tabelle 8: Zulässige Domain-Parameter für die Signatur von Zertifikaten ... 10
Tabelle 9: Hashfunktion zur Erzeugung der Seriennummer einer TSE ... 11
Tabelle 10: Zeitintervall für die Aktualisierung einer Transaktion ... 11

1 Einleitung

Die Technische Richtlinie BSI TR-03116 stellt eine Vorgabe für Projekte des Bundes dar. Die Technische Richtlinie ist in fünf 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 Ausweisdokumenten, zur Zeit für den elektronischen Reisepass, den elektronischen Personalausweis, den elektronischen Aufenthaltstitel 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, XML-Security und OpenPGP in Anwendungen des Bundes.
- Der vorliegende Teil 5 der Technischen Richtlinie beschreibt Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in Anwendungen der Secure Element API (wie Technischen Sicherheitseinrichtungen elektronischer Aufzeichnungssysteme nach [1]).

Die Vorgaben der Technischen Richtlinie basieren auf Prognosen über die Sicherheit der verwendeten kryptographischen Verfahren,über einen Zeitraum von 4 Jahren, zur Zeit bis einschließlich 2021. Eine weitere Verwendung des Verfahrens über diesen Zeitraum hinaus ist nicht ausgeschlossen und wird mit 2021+ gekennzeichnet.

1.1 Anwendungen der Secure Element API

Die Anforderungen an die Funktionalität und Interoperabilität der Secure Element API wird in der Technischen Richtlinie TR-03151 [2] 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 den Technischen Richtlinien TR-02102 [3] und TR-03111 [4].

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

Verfahren	*Algorithmus*
Digitale Signatur	ECDSA [4] ECSDSA [4]
Hashfunktion	SHA-2 oder SHA-3 [5]
Elliptische Kurven	NIST-Domain-Parameter über Primkörpern [6] Brainpool-Domain-Parameter [7]

Tabelle 1: Kryptographische Algorithmen

1.1.1 Elektronische Aufzeichnungssysteme

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

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

Deutsch	***Englisch***
OPTIONAL	OPTIONAL

Tabelle 1: 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 [11]) verwendet werden:

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

Bei der Verwendung von PTG.2 wird empfohlen eine kryptographische Nachbearbeitung zu verwenden. Für die Konvertierung von Zufallsbits in Zufallszahlen (ECC-Nonces) sind die Empfehlungen von Anhang B der [3] einzuhalten.

2.2 Absicherung elektronischer Aufzeichnungen

Eine Anwendungen der Secure Element API MUSS für die Erzeugung von Signaturen ein Verfahren aus Tabelle 3 verwenden. Die Verwendungszeiträume bezieht sich auf die Herstellung des Sicherheitsmoduls.

Signaturverfahren	*Signaturformat*	*Verwendung von*	*Verwendung bis*
ECDSA [4]	Plain-Format	2018	2021+
ECSDSA [4]	Plain-Format	2018	2021+

Tabelle 3: Zulässige Verfahren für die Signaturberechnung

Als Hashfunktion innerhalb des Signaturverfahrens MUSS eine Hashfunktion der Tabelle 4 verwendet werden.

Hashfunktion	*Minimale Outputlänge der Hashfunktion*	*Verwendung von*	*Verwendung bis*
ECDSA oder ECSDSA			
SHA-2	256 Bit	2018	2021+
SHA-3	256 Bit	2018	2021+

Tabelle 4: Zulässige Hashfunktionen für die Signaturberechnung

Als ECC-Domain-Parameter für die Berechnung eine Signatur MUSS eine elliptische Kurve aus Tabelle 5 verwendet werden. Die Verwendungszeiträume beziehen sich auf die Herstellung des Sicherheitsmoduls.

EC-Domain-Parameter	*Verwendung von*	*Verwendung bis*
BrainpoolP256r1 [7]	2018	2021+
BrainpoolP384r1 [7]	2018	2021+
BrainpoolP512r1 [7]	2018	2021+

NIST P-256 (secp256r1) [6]	2018	2021+
NIST P-384 (secp384r1) [6]	2018	2021+
NIST P-521 [6]	2018	2021+

Tabelle 5: Zulässige Domain-Parameter für die Signaturerzeugung

Die ECC-Domain-Parameter SOLLEN im Zertifikat als Named Curve angegeben werden. Als Encoding für die Punkte der elliptischen Kurven MUSS das Uncompressed Encoding gemäß [4] verwendet werden.

Verifizierende Stellen MÜSSEN alle Verfahren und Parameter der Tabellen 3-5 unterstützen, um eine reibungslose Verifikation der Signatur sicherstellen zu können.Andere Verfahren und Parameter, als die in den Tabellen 6-8 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 Tabelle 6 verwenden. Die Verwendungszeiträume beziehen sich auf die Erstellung der Zertifikate.

Signaturverfahren	***Verwendung von***	***Verwendung bis***
ECDSA [4]	2018	2021+
ECSDSA [4]	2018	2021+

Tabelle 6: Zulässige Verfahren für die Signatur von Zertifikaten

Als Hashfunktion für die Signatur von Zertifikaten MUSS eine Hashfunktion der Tabelle 7 verwendet werden.

Hashfunktion	***Minimale Outputlänge der Hashfunktion***	***Verwendung von***	***Verwendung bis***
ECDSA oder ECSDSA			
SHA-2	384 Bit	2018	2021+
SHA-3	384 Bit	2018	2021+

Tabelle 7: Zulässige Hashfunktionen für die Signatur von Zertifikaten

Als ECC-Domain-Parameter für die Signatur von Zertifikaten MUSS eine elliptische Kurve aus Tabelle 8 verwendet werden. Die Verwendungszeiträume beziehen sich auf die Erstellung der Zertifikate.

1 Der Hersteller hat die notwendigen Informationen für die korrekte Prüfung gemäß BSI TR-03153 in einem Konzept darzulegen. Die Prüfung des Konzepts ist Bestandteil der CC-Zertifizierung, vgl. [12], [13].

EC-Domain-Parameter	*Verwendung von*	*Verwendung bis*
BrainpoolP384r1 [7]	2018	2021+
BrainpoolP512r1 [7]	2018	2021+
NIST P-384 (secp384r1) [6]	2018	2021+
NIST P-521 [6]	2018	2021+

Tabelle 8: Zulässige Domain-Parameter für die Signatur von Zertifikaten

Die ECC-Domain-Parameter SOLLEN als Named Curve angegeben werden. Als Encoding für die Punkte der elliptischen Kurven SOLL das Uncompressed Encoding gemäß [4] verwendet werden.

Verfizierende Stellen MÜSSEN alle Verfahren und Parameter der Tabellen 6-8 unterstützen, um eine reibungslose Verifikation eines Zertifikats sicherstellen zu können. Andere Verfahren und Parameter, als die in den Tabellen 6-8 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 [9].

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 9 vorgegeben. Die Verwendungszeiträume bezieht sich auf die Herstellung der Technischen Sicherheitseinrichtung.

Hashfunktion	*Outpulänge der Hashfunktion*	*Verwendung von*	*Verwendung bis*
SHA-2	256 Bit	2018	2021+

Tabelle 9: 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 [9]).

Tabelle 10 gibt das Zeitintervall MAX_UPDATE_DELAY an, innerhalb dessen die Transaktion nach einer Änderung von Anwendungsdaten durch das elektronische Aufzeichnungssystem durch Aufruf der Funktion UpdateTransaction in der Technischen Sicherheitseinrichtung zu aktualisieren sind. Die Verwendungszeiträume beziehen sich auf den Einsatzzeitpunkt des elektronischen Aufzeichnungssystems.

Maximales Zeitintervall in Sekunden	*Verwendung von*	*Verwendung bis*
45	2018	2021+

Tabelle 10: Zeitintervall für die Aktualisierung einer Transaktion

Literaturverzeichnis

[1] Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), diezuletzt durch Artikel 6 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist

[2] BSI TR-03151, Technical Guideline Secure Element Integration API, 2018

[3] BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2018

[4] BSI TR-03111, Elliptic Curve Cryptography (ECC) Version 2.0, 2018

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

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

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

[8] Kassensicherungsverordnung vom 26. September 2017 (BGBl. I S. 3515)

[9] BSI TR-03153, Technische sicherheitseinrichtung für elektronische Aufzeichnungssysteme, 2018

[10] Bradner, S. , Key words for use in RFCs to indicate requirement levels, 1997

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

[12] BSI CC-PP, Common Criteria Protection Profile Security Module Application for Electronic Record-keeping Systems, 2018

[13] BSI CC-PP, Common Criteria Protection Profile Cryptographic Service Provider, 2018