Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

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

Teil 6: Kooperative intelligente Verkehrssysteme (C-ITS)

Stand 2023

Datum: 24. April 2023

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

E-Mail: cits@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.
- Teil 5 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in Anwendungen der Secure Element API (wie Technischen Sicherheitseinrichtungen elektronischer Aufzeichnungssysteme).
- Der vorliegende Teil 6 beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in der Infrastruktur kooperativer intelligenter Verkehrssysteme (Cooperative Intelligent Transport Systems / C-ITS).

1.1 Geltungsbereich

Im vorliegenden Teil 6 der Technischen Richtlinie werden die einzusetzenden kryptographischen Verfahren und Schlüssellängen für Teilnehmer an der Infrastruktur kooperativer intelligenter Verkehrssysteme nach BSI TR-03164 [1] vorgegeben. Die Vorgaben basieren auf den Technischen Richtlinien BSI TR-02102-1 [2] und BSI TR-03111 [3].

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

Verfahren	*Algorithmus*
Digitale Signatur	ECDSA gemäß BSI TR-03111 [3]
Schlüsseleinigung	ECIES gemäß IEEE 1609 [4]
Elliptische Kurven	Brainpool-Domain-Parameter gemäß RFC 5639 [5]
Blockchiffre (Mode)	AES (CCM-Mode)

Tabelle 1: Kryptographische Algorithmen

1.2 Begrifflichkeiten

1.2.1 Verwendungszeiträume

Die Vorgaben des vorliegenden Teils 6 der Technischen Richtlinie basieren auf Prognosen über die Sicherheit der verwendeten kryptographischen Verfahren und Schlüssellängen über einen Zeitraum von 7 Jahren, zur Zeit bis einschließlich 2029. Ist eine weitere Verwendung über diesen Zeitraum hinaus nicht ausgeschlossen, so wird dies mit 2029+ gekennzeichnet.

Diese Technische Richtlinie führt auch Vorgaben mit abgelaufenem Verwendungszeitraum auf, sofern entsprechende Anwendungen möglicherweise weiterhin im Feld bzw. in Nutzung sind.

Wird ein Verwendungsende ohne „+“ angegeben, so sollte ein Migrationsplan für die Ausphasung in der entsprechenden Anwendung erstellt werden.

Liegt ein Verwendungsanfang in der Zukunft, so sollten rechtzeitig angemessene Tests konzipiert und durchgeführt werden, durch die überprüft werden kann, ob alle notwendigen Voraussetzungen für die Einführung erfüllt sind. Der Testzeitpunkt sollte so gewählt sein, dass mögliche aufgedeckte Mängel noch vor dem Verwendungsanfang behoben werden können.

1.2.2 Schlüsselworte

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

Die verwendeten Schlüsselworte sind auf Basis der folgenden Übersetzungstabelle gemäß RFC 2119 [6] zu interpretieren:

Deutsch	*Englisch*
MUSS / MÜSSEN	MUST / SHALL
DARF NICHT / DÜRFEN NICHT	MUST NOT
VERPFLICHTEND	REQUIRED
SOLLTE / SOLLTEN	SHOULD
SOLLTE NICHT / SOLLTEN NICHT	SHOULD NOT
EMPFOHLEN	RECOMMENDED

Deutsch	*Englisch*
KANN / KÖNNEN / DARF / DÜRFEN	MAY
OPTIONAL	OPTIONAL

Tabelle 2: Schlüsselworte

1.2.3 Definitionen und Abkürzungen

In diesem Dokument werden folgende Abkürzungen verwendet:

Abkürzung	**Erklärung**
AA	Authorization Authority
AT	Authorization Ticket
CA	Certificate Authority
C-ITS	Cooperative Intelligent Transport System
CP	Certificate Policy
CRL	Certificate Revocation List
CTL	Certificate Trust List
EA	Enrolment Authority
EC	Enrolment Credential
ECC	Elliptic Curve Cryptography
ECTL	European Certificate Trust List
PKI	Public Key Infrastruktur
RCA / Root CA	Root Certificate Authority
Sub-CA	EA and AA
TLM	Trust List Manager

Tabelle 3: Verwendete Abkürzungen

2 Kryptographische Vorgaben

Teilnehmer an der Infrastruktur kooperativer intelligenter Verkehrssysteme MÜSSEN die allgemeinen Anforderungen für die Unterstützung und Verwendung kryptographischer Verfahren gemäß Annex 3 zu 2010/40/EU [7] einhalten. Im Folgenden werden die Vorgaben für die Verwendung kryptographischer Verfahren für nationale Anwendungen präzisiert.

2.1 Zufallszahlengeneratoren

Für die Erzeugung von Zufallszahlen und kryptographischen Schlüsseln MÜSSEN in allen verwendeten kryptographischen Verfahren Zufallszahlengeneratoren aus einer der folgenden Klassen (siehe AIS 20/31 [8]) verwendet werden:

- DRG.4
- PTG.3
- NTG.1

Bis Ende 2022 waren Zufallszahlengeneratoren der Klasse DRG.3 zulässig.

2.2 Public Key Infrastruktur

Das Vertrauensmodell der Infrastruktur kooperativer intelligenter Verkehrssysteme besteht aus mehreren Public Key Infrastrukturen, welche jeweils aus folgenden Instanzen bestehen:

- **Root-CA (RCA)**
- **Sub-CA**, bestehend aus:
  - **Enrolment Authority (EA)**
  - **Authorization Authority (AA)**
- **Endnutzer**:
  - Hoheitliche und nicht-hoheitliche **C-ITS-Stations**

Die vertrauenswürdigen Root-Zertifikate werden von der Europäischen Kommission auf einer signierten **European Certificate Trust List (ECTL)** veröffentlicht.

2.2.1 Root-CA

Die RCA erstellt Zertifikate für die Enrolment und Authorization Authorities.

Tabelle 4 enthält die elliptische Kurve, die von einer nationalen RCA verwendet werden MUSS. Der Verwendungszeitraum bezieht sich auf die Erstellung des selbst-signierten Root-Zertifikats.

ECC-Domain-Parameter	*Point-Encoding*	*Verwendung von*	*Verwendung bis*
brainpoolP384r1 [5]	Uncompressed	2020	2029+

Tabelle 4: Domain-Parameter der RCA

Für die Signatur von Sub-CA-Zertifikaten und Sperrlisten ist gemäß Annex 3 zu 2010/40/EU [7] das Verfahren ECDSA zu verwenden. Tabelle 5 enthält die Parameter, die von der nationalen RCA hierbei verwendet werden MÜSSEN. Der Verwendungszeitraum bezieht sich auf die Erstellung der jeweiligen Zertifikate und Sperrlisten.

Signaturverfahren	*Verwendung von*	*Verwendung bis*
ECDSA_brainpoolP384r1_with_SHA384	2020	2029+

Tabelle 5: Verfahren für die Signaturberechnung durch die RCA

2.2.2 Sub-CA

EAs erstellen Enrolment Credentials, und AAs erstellen Authorization Tickets für Endnutzer der C-ITS-PKI. Die Zertifikate der EAs und AAs enthalten jeweils einen öffentlichen Schlüssel für die Signaturprüfung von Zertifikaten sowie einen öffentlichen Schlüssel für die Schlüsseleinigung (Key Agreement) zur Verschlüsselung von Zertifikatsrequests, vgl. Abschnitt 2.2.4.

Tabelle 6 enthält die elliptischen Kurven, die von einer nationalen EA verwendet werden MÜSSEN. Die Verwendungszeiträume beziehen sich auf die Erstellung des EA-Zertifikats.

Algorithmus	*ECC-Domain-Parameter*	*Point-Encoding*	*Verwendung von*	*Verwendung bis*
Signatur	brainpoolP256r1 [5]	Uncompressed	2020	2029+
Key Agreement	brainpoolP256r1 [5]	Uncompressed	2020	2029+

Tabelle 6: Domain-Parameter der EA

Für die Signatur von Enrolment Credentials ist gemäß Annex 3 zu 2010/40/EU [7] das Verfahren ECDSA zu verwenden. Tabelle 7 enthält die Parameter, die von einer nationalen EA hierbei verwendet werden MÜSSEN. Der Verwendungszeitraum bezieht sich auf die Erstellung der Zertifikate.

Signaturverfahren	*Verwendung von*	*Verwendung bis*
ECDSA_brainpoolP256r1_with_SHA256	2020	2029+

Tabelle 7: Verfahren für die Signaturberechnung durch die EA

Tabelle 8 enthält die elliptischen Kurven, die von einer nationalen AA verwendet werden MÜSSEN. Die Verwendungszeiträume beziehen sich auf die Erstellung des AA-Zertifikats.

Algorithmus	*ECC-Domain-Parameter*	*Point-Encoding*	*Verwendung von*	*Verwendung bis*
Signatur	brainpoolP256r1 [5]	Uncompressed	2020	2029+
Key Agreement	brainpoolP256r1 [5]	Uncompressed	2020	2029+

Tabelle 8: Domain-Parameter der AA

Für die Signatur von Authorization Tickets ist gemäß Annex 3 zu 2010/40/EU [7] das Verfahren ECDSA zu verwenden. Tabelle 9 enthält die Parameter, die von einer nationalen AA hierbei verwendet werden MÜSSEN. Der Verwendungszeitraum bezieht sich auf die Erstellung der Zertifikate.

Signaturverfahren	*Verwendung von*	*Verwendung bis*
ECDSA_brainpoolP256r1_with_SHA256	2020	2029+

Tabelle 9: Verfahren für die Signaturberechnung durch die AA

2.2.3 Endnutzer

Endnutzer erhalten Enrolment Credentials (ECs) von der EA und Authorization Tickets (ATs) von der AA.

Tabelle 10 enthält die elliptische Kurve, die in den ECs und ATs der Endnutzer verwendet werden MUSS. Die Verwendungszeiträume beziehen sich auf die Erstellung der Endnutzer-Zertifikate.

Algorithmus	*ECC-Domain-Parameter*	*Point-Encoding*	*Verwendung von*	*Verwendung bis*
Signatur	brainpoolP256r1 [5]	Compressed	2020	2029+

Tabelle 10: Domain-Parameter in ECs und ATs

2.2.4 Verschlüsselung von Zertifikatsrequests und -responses

Zertifikatsrequests von Endnutzern an EAs und AAs sowie die zugehörigen Zertifikatsresponses von EAs und AAs an Endnutzer sind gemäß Annex 3 zu 2010/40/EU [7] verschlüsselt zu übermitteln. Im Falle der Beantragung von Authorization Tickets müssen Teile des Zertifikatsrequests von der AA zur Prüfung der Identität und der zugehörigen Berechtigungen zudem gemäß ETSI TS 102 941 [9] an die EA verschlüsselt übermittelt werden.

Für die Verschlüsselung wird ein hybrides Kryptoverfahren verwendet. Hierbei wird der öffentliche Schlüssel des jeweiligen Empfängers genutzt, um zufällig erzeugte symmetrische Session Keys zu verschlüsseln (Key Encryption). Die Key Encryption erfolgt per ECIES gemäß IEEE 1609 [4]. Die Kurvenparameter, die durch den Sender jeweils für die Erzeugung des ephemeren Schlüsselpaars verwendet werden MÜSSEN, ergeben sich aus Tabelle 6 (für Requests an die EA), Tabelle 8 (für Requests an die AA) und Tabelle 10 (für Zertifikatsresponses an die Endnutzer).

Die Verschlüsselung der eigentlichen Zertifikatsrequests und Zertifikatsresponse (Content Encryption) erfolgt via AES128-CCM.

2.2.5 Gültigkeitszeiten

Die Nutzungszeiten der privaten Schlüssel und Gültigkeitszeiten der Zertifikate der nationalen PKI-Instanzen MÜSSEN den Anforderungen der Tabelle 11 entsprechen.

PKI-Instanz	*Maximal Nutzungszeit des privaten Schlüssels*	*Gültigkeitszeit des Zertifikat*
RCA	bis zu 5 Jahre und gleich der Gültigkeitszeit des Zertifikats	Bis zu 5 Jahre und gleich der Nutzungszeit des privaten Schlüssels
EA	bis zu 2,5 Jahre	bis zu 5 Jahre
AA	Bis zu 2,5 Jahre und gleich der Gültigkeitszeit des Zertifikats	bis zu 2,5 Jahre und gleich der Nutzungszeit des privaten Schlüssels
C-ITS subscriber	Bis zu 2,5 Jahre und gleich der Gültigkeitszeit des Zertifikats	bis zu 2,5 Jahre und gleich der Nutzungszeit des privaten Schlüssels
EC	Bis zu 2,5 Jahre und gleich der Gültigkeitszeit des Zertifikats	bis zu 2,5 Jahre und gleich der Nutzungszeit des privaten Schlüssels
AT	1 Woche	1 Woche

Tabelle 11: Gültigkeitszeiten der Zertifikate nationaler PKI-Instanzen

Literaturverzeichnis

[1] BSI TR-03164, Part 1: Guidance for Operation of a Public-Key Infrastructure for Cooperative Intelligent Transport Systems (C-ITS),

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

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

[4] IEEE Std 1609.2a, Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages - Amendment, 2017

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

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

[7] EU KOM, Annex 3 of the DRAFT Commission Delegated Regulation of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems, 2019

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

[9] ETSI TS 102 941, Intelligent Transport Systems (ITS) - Security - Trust and Privacy Management, V1.2.1, 2018