Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie TR-03116-3

Kryptographische Vorgaben für Projekte der Bundesregierung

Teil 3 - Intelligente Messsysteme

Stand 2014 - Draft

Datum: 17.03.2014

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

Inhaltsverzeichnis

1 Einleitung....5
1.1 Smart Meter Gateways....5
2 Kryptographische Algorithmen....7
2.1 Kryptographische Basisverfahren....7
2.2 Domainparameter für Elliptische Kurven....7
2.3 Zufallszahlengeneratoren....8
3 Public Key Infrastruktur....9
4 TLS-Kommunikation im WAN....10
4.1 Cipher Suites und Kurvenparameter....10
4.2 Authentifizierung und TLS-Zertifikate....11
5 TLS-Kommunikation im HAN....12
5.1 Migration kryptographischer Verfahren und Schlüssel....12
6 TLS-Kommunikation im LMN....13
6.1 ECC-basierte Kommunikation....13
6.2 Migration kryptographischer Verfahren und Schlüssel....14
7 Kommunikation im LMN auf Basis symmetrischer Kryptographie....15
7.1 Voraussetzungen....15
7.2 Schlüsselableitung....16
7.3 Übertragung von Zählerdaten....16
8 Inhaltsdatenverschlüsselung und -signatur....18
8.1 Authenticated-Enveloped-data Content Type....18
8.2 Signed-Data Content Type....19
9 PACE und Secure Messaging....20
10 Zertifizierung....21
10.1 Smart Meter Gateway....21
10.2 Sicherheitsmodul....21

Tabellenverzeichnis

Tabelle 1: Verfahren zur Absicherung der Infrastruktur von Messsytemen....6
Tabelle 2: Kryptographische Primitive....7
Tabelle 3: Vom Sicherheitsmodul zu unterstützende Domain-Parameter....7
Tabelle 4: Signatur der Zertifikate....9
Tabelle 5: Mindestens zu unterstützende Verfahren....10
Tabelle 6: Optional unterstützbare Verfahren....11
Tabelle 7: Authentifizierung....11
Tabelle 8: Laufzeiten der HAN-Zertifikate....12
Tabelle 9: Laufzeiten der LMN-Zertifikate....13
Tabelle 10: Berechnung der abgeleiteten Schlüssel....16
Tabelle 11: Symmetrische Absicherung der Datenübertragung....17
Tabelle 12: Inhaltsdatenverschlüsselung....18
Tabelle 13: Schlüsseltransport für die Inhaltsdatenverschlüsselung....19

Tabelle 14: Algorithmen für die CMS Key Encryption.....19
Tabelle 15: Signatur der verschlüsselten Inhaltsdaten.....19
Tabelle 16: PACE und Secure Messaging.....20

1 Einleitung

Die Technische Richtlinie BSI TR-03116 stellt eine Vorgabe für Projekte des Bundes dar. Die Technische Richtlinie ist in vier 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 und den elektronischen Aufenthaltstitel.
- Im vorliegenden Teil 3 werden die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in die Infrastruktur intelligenter Messsysteme im Energiesektor beschrieben.
- Teil 4 der Technischen Richtline beschreibt die Sicherheitsanforderungen für die Verwendung von SSL/TLS, S/MIME und OpenPGP in eGovernment-Anwendungen.

Die Vorgaben des vorliegenden Teil 3 der Technischen Richtlinie basieren auf Prognosen über die Sicherheit der verwendeten kryptographischen Verfahren und Schlüssellängen über einen Zeitraum von 6 Jahren, zur Zeit bis zum Jahr 2020. Eine weitere Verwendung des Verfahrens über diesen Zeitraum hinaus ist nicht ausgeschlossen und wird mit 2020+ gekennzeichnet.

1.1 Smart Meter Gateways

Die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit der Komponenten von Smart-Metering-Systemen werden in der Technischen Richtlinie TR-03109 [6] spezifiziert.

Basierend auf den Technischen Richtlinien TR-02102-1 [4], TR-02102-2 [5] und TR-03111 [12] werden in diesem Dokument verbindlich die einzusetzenden kryptographischen Verfahren und Primitive sowie zu verwendenden Schlüssellängen für die Absicherung der Infrastruktur von Messsystemen vorgegeben.

Tabelle 1 gibt einen Überblick über die verwendeten Verfahren und ihren Einsatzzweck.

Einsatzzweck	***Verfahren***
Sicherstellung der Authentizität von öffentlichen Schlüsseln (vgl. [9])	Public Key Infrastruktur (vgl. Abschnitt 3)
Absicherung der Kommunikation zwischen Smart Meter Gateway und externen Marktteilnehmern im WAN(vgl. [6])	TLS (vgl. Abschnitt 4)
Absicherung der Kommunikation zwischen Smart Meter Gateway und Teilnehmern im HAN(vgl. [6])	TLS (vgl. Abschnitt 5)
Absicherung der Kommunikation von Zählern mit dem Smart Meter Gateway im LMN (vgl. [6])	TLS (vgl. Abschnitt 6)

Einsatzzweck	***Verfahren***
Absicherung der Kommunikation von Zählern mit dem Smart Meter Gateway im LMN für Daten mit niedrigem Schutzbedarf (vgl. [6])	Symmetrische Kryptographie (vgl Abschnitt 7)
Vertrauliche, authentische Ende-zu-Ende-Übertragung von Daten über das WAN an den Endempfänger (vgl. auch [6])	Inhaltsdatenverschlüsselung und MAC-Sicherung (vgl. Abschnitt 8)
Gegenseitige Authentisierung zwischen Smart-Meter Gateway und Sicherheitsmodul sowie Aufbau eines sicheren Kanals	PACE (vgl. Abschnitt 9)
Vertrauliche, authentische Kommunikation zwischen Smart-Meter Gateway und Sicherheitsmodul	Secure Messaging (vgl. Abschnitt 9)

Tabelle 1: Verfahren zur Absicherung der Infrastruktur von Messsytemen

2 Kryptographische Algorithmen

2.1 Kryptographische Basisverfahren

Tabelle 2 gibt eine Übersicht über die kryptographischen Primitive, die in diesem Dokument verwendet werden.

Digitale Signatur	ECDSA [12]
Schlüsseleinigung	ECKA-DH [12]
Schlüsseltransport	ECKA-EG [12]
Blockchiffre	AES [25] • CBC-Mode [23] • CMAC-Mode [14] • GCM-Mode [26]
Hashfunktionen	SHA-2 Familie [24]

Tabelle 2: Kryptographische Primitive

2.2 Domainparameter für Elliptische Kurven

Für kryptographische Algorithmen und Protokolle basierend auf Elliptischen Kurven (d.h. TLS, ECDSA und ECKA) werden NIST-Domain-Parameter über Primkörpern [18] bzw. Brainpool-Domain-Parameter [21] in den entsprechenden Bitlängen verwendet.

Um eine einfache Migration auf andere Verfahren zu ermöglichen, muss das Sicherheitsmodul eines Smart-Meter-Gateways

- die Schlüsselerzeugung
- PACE, ECKA-DH, ECKA-EG, ECDSA Signaturerzeugung und -verifikation

gemäß den Vorgaben in [12] für alle Domain-Parameter aus Tabelle 3 unterstützen.

EC-Domain-Parameter	*Verwendung von*	*Verwendung bis*
BrainpoolP256r1 [21]	2013	2020+
BrainpoolP384r1 [21]	2013	2020+
BrainpoolP512r1 [21]	2013	2020+
NIST P-256 [18]	2013	2020+
NIST P-384 [18]	2013	2020+

Tabelle 3: Vom Sicherheitsmodul zu unterstützende Domain-Parameter

Als Encoding für die Punkte der elliptischen Kurven soll das Uncompressed Encoding gemäß [12] verwendet werden.

2.3 Zufallszahlengeneratoren

Für die Erzeugung von Zufallszahlen und kryptographischen Schlüsseln (inkl. Ephemeralschlüsseln) sind in allen verwendeten kryptographischen Protokollen Zufallszahlengeneratoren aus einer der folgenden Klassen (siehe [1]) zu verwenden:

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

3 Public Key Infrastruktur

Die Authentizität der öffentlichen Schlüssel von Smart-Meter-Gateways und externen Marktteilnehmern, welche auf der WAN-Seite zur gegenseitigen Authentisierung und zum Aufbau eines verschlüsselten, integritätsgesicherten TLS-Kanals bzw. zur Verschlüsselung oder Signatur von Daten auf Inhaltsebene eingesetzt werden, wird durch die Smart Metering Public Key Infrastruktur (SM-PKI) sichergestellt. Die SM-PKI wird in [9] spezifiziert.

Die SM-PKI besteht aus einer *Root-CA* als nationale Wurzelinstanz, *Sub-CAs* für die Ausstellung der Endnutzerzertifikate sowie den *Zertifikaten der Endnutzer* und wird in [9] spezifiziert. Zu den Endnutzern gehören die Marktteilnehmer und die Smart Meter Gateways.

Als Signaturverfahren, mit dem die X.509-Zertifikate und -Sperrlisten signiert werden, muss das Verfahren ECDSA gemäß [12], 5.2.2 verwendet werden.

Tabelle 4 legt die zu verwendenden Hashfunktionen und Kurvenparameter verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Erstellung der Zertifikate.

Verfahren/Parameter	*Vorgaben*	*Verwendung von*	*Verwendung bis*
Root-CA			
Signaturalgorithmus	`ECDSA-With-SHA384` [12]	2013	2020+
EC-Domain-Parameter	NIST P-384 [18] BrainpoolP384r1 [21]	2013 2014	2014 2020+
Sub-CAs			
Signaturalgorithmus	`ECDSA-With-SHA256` [12]	2013	2020+
EC-Domain-Parameter	NIST P-256 [18] BrainpoolP256r1 [21]	2013 2014	2014 2020+

Tabelle 4: Signatur der Zertifikate

Die Laufzeiten der Zertifikate werden in [9] verbindlich vorgegeben.

4 TLS-Kommunikation im WAN

Das TLS-Protokoll dient im WAN zum Aufbau eines verschlüsselten/integritätsgesicherten und gegenseitig authentisierten Kanals zwischen Smart-Meter-Gateway und autorisierten Marktteilnehmern.

Das TLS-Protokoll muss mindestens nach Version 1.2 [19] implementiert werden. Ein Fallback auf eine ältere TLS-Version darf nicht möglich sein. Eine TLS-Session darf (inklusive eventueller Session Resumptions) maximal 48 Stunden aktiv sein. Innerhalb der erlaubten Session-Lebensdauer ist Session-Resumption erlaubt. Im Falle einer Stateless Resumption sind dabei die Anforderungen aus [15], insbesondere Kap. 5, zu beachten. Es darf kein Session Renegotiation möglich sein.

4.1 Cipher Suites und Kurvenparameter

Die Implementierung muss gemäß [20] mit ephemeralem ECDH erfolgen. Dabei stehen grundsätzlich folgende Cipher Suites zur Verfügung:

- `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384`
- `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`

Die Wahl der Cipher Suite legt folgende Bereiche des TLS-Protokolls fest:

- Schlüsselaustausch
- Authentifizierung
- Hashfunktion
- Verschlüsselung und Message Authentication Code (MAC)

Tabelle 5 legt die Cipher Suites und elliptischen Kurven, die für die TLS-Kommunikation im WAN von Marktteilnehmern, Gateway-Admistratoren und Smart Meter Gateways mindestens unterstützt werden müssen, verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Herstellung des Gateways.

Vorgaben		***Verwendung von***	***Verwendung bis***
Cipher Suite	`TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256`	2013	2020+
EC-Parameter	NIST P-256 [18] BrainpoolP256r1 [21]	2013 2015	2020+ 2020+

Tabelle 5: Mindestens zu unterstützende Verfahren

Um eine langfristige Nutzung zu ermöglichen, sollten für TLS zusätzlich auch die in Tabelle 6 genannten Cipher Suites und Elliptische Kurven unterstützt werden.

Vorgaben	*Verwendung von*	*Verwendung bis*
Cipher Suites		
`TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384`	2013	2020+
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`	2013	2020+
`TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`	2013	2020+
Elliptische Kurven		
BrainpoolP256r1[1] [21]	2013	2014
BrainpoolP384r1 [21]	2013	2020+
BrainpoolP512r1 [21]	2013	2020+
NIST P-384 [18]	2013	2020+

Tabelle 6: Optional unterstützbare Verfahren

Andere Cipher Suites oder Elliptische Kurven als die aus Tabelle 5 oder Tabelle 6 dürfen für die Kommunikation im WAN nicht unterstützt werden.

4.2 Authentifizierung und TLS-Zertifikate

Zur gegenseitigen Authentifizierung, benötigt jede Partei ein TLS-Zertifikat aus der SM-PKI für ein Schlüsselpaar, das zur Erzeugung von Signaturen mit ECDSA (gemäß [12]) geeignet ist.

Tabelle 7 legt die zu verwendenden Hashfunktionen und Kurvenparameter verbindlich fest. Der Verwendungszeitraum bezieht sich auf die Erstellung der Zertifikate.

Verfahren	*Vorgaben*	*Verwendung von*	*Verwendung bis*
Hash	SHA-256	2013	2020+
EC-Domain-Parameter	NIST P-256 [18] BrainpoolP256r1 [21]	2013 2015	2014 2020+

Tabelle 7: Authentifizierung

1 Mit Ablauf des Jahres 2014 wird gemäß Tabelle 7 die Unterstützung dieser Kurve für TLS im WAN verpflichtend.

5 TLS-Kommunikation im HAN

Das TLS-Protokoll dient im HAN zum Aufbau eines authentisierten sicheren Kanals zwischen Smart Meter Gateway und Komponenten im HAN (wie etwa die Anzeigeeinheit oder CLS-Systeme) (vgl. [7]).

Für die Verwendung von TLS im HAN gelten grundsätzlich die gleichen Vorgaben für die Kryptographie wie im WAN (vgl. Kapitel 4). Für die Zertifikate im HAN sind ebenso die Vorgaben aus Tabelle 7 verbindlich. Tabelle 8 gibt die maximalen Laufzeiten der Zertifikate für die Teilnehmer im HAN verbindlich vor.

Zertifikat	*Gültigkeitszeit*	*Private Key Usage*
Zählerzertifikat	Maximal 5 Jahre	Maximal 5 Jahre
SM-GW-Zertifikat	Maximal 5 Jahre	Maximal 5 Jahre

Tabelle 8: Laufzeiten der HAN-Zertifikate

5.1 Migration kryptographischer Verfahren und Schlüssel

Es wird empfohlen, Komponenten im HAN mit der Möglichkeit auszustatten, neue Schlüssel einzuspielen/zu erzeugen und ggf. per Firmware-Update neue kryptographische Verfahren einzuspielen, um so eine weitere Verwendbarkeit der Komponenten auch nach einer erforderlichen Migration kryptographischer Verfahren zu ermöglichen.

6 TLS-Kommunikation im LMN

Zähler müssen für die Kommunikation mit dem zugehörigen Smart Meter Gateway im Allgemeinen ebenfalls TLS verwenden. Insbesondere muss für die bidirektionale Kommunikation zwischen Smart Meter Gateway und Zähler mindestens in folgenden Einsatzszenarien TLS unterstützt werden:

- Wechsel des gemeinsamen, zählerindividuellen Schlüssels gemäß 7.1.1,
- Auslesen von Zählerdaten,
- Auswahl der auszulesenden Daten.

Das TLS-Protokoll muss mindestens nach Version 1.2 [19] implementiert werden. Ein Fallback auf eine ältere TLS-Version darf nicht möglich sein. Eine TLS-Session darf (inklusive eventueller Session Resumptions) maximal 1 Monat laufen. Dabei dürfen maximal 5 MB an Daten innerhalb einer Session ausgetauscht werden. Innerhalb der erlaubten Session-Lebensdauer ist Session-Resumption erlaubt. Im Falle einer Stateless Resumption sind dabei die Anforderungen aus [15], insbesondere Kap. 5, zu beachten. Es darf kein Session Renegotiation möglich sein.

Die Implementierung von TLS auf einem TLS-fähigen Zähler muss ECC-basiert (unter Verwendung der Cipher Suites aus Kapitel 4) erfolgen.

Von einem Smart-Meter Gateway bzw. TLS-Zähler dürfen keine weiteren TLS-Cipher-Suites als die in Kapitel 4.1 genannten für die Kommunikation im LMN unterstützt werden.

6.1 ECC-basierte Kommunikation

Die Vorgaben aus Kapitel 4 sind auch für die ECC-basierte Kommunikation verbindlich.

Tabelle 9 gibt die maximalen Laufzeiten der Zählerzertifikate verbindlich vor. Die Zertifikate sind selbst-signiert, d.h. das Smart Meter Gateway besitzt für die TLS-Kommunikation im WAN und im LMN separate Zertifikate.

Zertifikat	*Gültigkeitszeit*	*Private Key Usage*
Zählerzertifikat	Maximal 7 Jahre	Maximal 7 Jahre
SM-GW-Zertifikat	Maximal 7 Jahre	Maximal 7 Jahre

Tabelle 9: Laufzeiten der LMN-Zertifikate

6.1.1 Initialer Austausch und Update der LMN-Zertifikate

Für Zähler, die TLS unterstützen, muss das initiale Schlüsselpaar im Allgemeinen vom Hersteller erstellt und authentisch in den Zähler eingebracht werden. Bei erstmaligem Anschluss an ein neues SM-GW muss ein authentischer Austausch der TLS-Zertifikate mit dem Smart Meter Gateway erfolgen.

Alternativ kann das initiale Schlüsselpaar des Zählers auch vom Smart Meter Gateway erzeugt und zusammen mit den Zertifikaten des Smart Meter Gateways an den Zähler verschlüsselt und authentisch an den Zähler übertragen werden.

Der initiale Übertragung der Zertifikate bzw. die Einbringung des initialen Schlüsselmaterials vom Smart Meter Gateway auf dem Zähler erfolgt mit dem in Kapitel 7 beschriebenen symmetrischen Verfahren.

Unmittelbar nach Austauch/Einbringung der TLS-Zertifikate muss ein TLS-Kanal aufgebaut und der zählerindividuelle Schlüssel für die Kommunikation auf Basis symmetrischer Kryptographie gemäß dem Vorgaben von Kap. 7.1.1 gewechselt werden.

Es ist geplant, den Austausch der Zertifikate auch durch Aufbau eines verschlüsselten Kanals via Passworteingabe und PACE (siehe auch [8], [10]) zu ermöglichen.

Für das Update eines Smart-Meter-Gateway-Zertifikats muss ein neues Schlüsselpaar erzeugt werden und anschließend muss das neue selbst-signierte Zertifikat über den aufgebauten TLS-Kanal an den Zähler gesendet werden.

Für das Update eines Zähler-Zertifikats muss das Smart-Meter-Gateway ein neues Schlüsselpaar erzeugen und anschließend muss das neue selbst-signierte Zertifikat mit dem zugehörigen privaten Schlüssel über den aufgebauten TLS-Kanal an den Zähler gesendet werden.

6.2 Migration kryptographischer Verfahren und Schlüssel

Die gewünschte Verwendungszeit von TLS-Zählern kann deutlich über den Prognose-Zeitraum hinausgehen. Daher wird empfohlen, Zähler mit der Möglichkeit auszustatten, neue Schlüssel einzuspielen/zu erzeugen und ggf. per Firmware-Update neue kryptographische Verfahren einzuspielen, um so eine weitere Verwendbarkeit des TLS-Zählers zu ermöglichen.

7 Kommunikation im LMN auf Basis symmetrischer Kryptographie

Für Zähler, die nur unidirektional kommunizieren können, ist die Möglichkeit von TLS nicht gegeben. Da außerdem Bandbreite und Verfügbarkeit des Kommunikationskanals im LMN auch für bidirektional kommunizierende Zähler in der Regel starken Einschränkungen unterliegt, sind Zähler nicht immer imstande gemäß den zeitlichen Anforderungen einen TLS-Kanal mit einem Smart Meter Gateway aufzubauen.

Daher muss das Smart Meter Gateway diesen Zählern eine alternative Möglichkeit zum Senden von Mess- und Zähldaten bereitstellen. Diese Möglichkeit wird im Folgenden beschrieben. Es ist zu beachten, dass diese Art der Kommunikation nur für die Auswahl, den Abruf oder die Übertragung von Daten verwendet werden darf, wenn eine Verbindung per TLS nicht möglich ist.

7.1 Voraussetzungen

Zähler und Smart Meter Gateway verfügen über einen gemeinsamen geeigneten, symmetrischen, Schlüssel *MK*. Dieser Schlüssel *MK* muss eine Länge von 128 Bit besitzen und für jeden Zähler individuell zufällig (gemäß den Vorgaben von Kap. 2.3) erzeugt werden. Dieser Schlüssel wird im Folgenden meist kurz zählerindividueller Schlüssel *MK* genannt. Die Erzeugung von *MK* kann durch den Hersteller vorgenommen werden, der *MK* in den Zähler einbringt, oder durch den Zähler erfolgen, der *MK* an den Hersteller ausgibt.

Der Eigentümer des Zählers überträgt diesen Schlüssel *MK* vertraulich und authentisch an den Administrator des Gateways, der den Schlüssel, wie in [7] beschrieben, gesichert in das Gateway einbringt. Wird der Zähler an ein anderes Smart Meter Gateway angeschlossen, so hat der Administrator des neuen Gateways sicherzustellen, dass der symmetrische, zählerindividuelle Schlüssel *MK* erneut zufällig (nach den Vorgaben von 2.3) erzeugt und in den Zähler sowie das neue Smart Meter Gateway vertraulich und authentisch eingebracht wird. Bei Zählern, die nur unidirektional kommunizieren können, ist eine solche erneute Schlüsselerzeugung bei Wechsel des Gateways optional. Jeder Zähler verfügt über einen Transmission Counter *C* von 32 Bit. Der Transmission Counter darf nie überlaufen und darf nicht zurückgesetzt werden. Das Zurücksetzen des Transmission Counter *C* ist ausnahmsweise nur direkt nach der Erzeugung eines neuen zählerindiviuellen Schlüssels *MK* und vor dessen erster Verwendung erlaubt. Vor der Versendung einer Nachricht muss der Counterwert gegenüber dem Counterwert der zuletzt empfangenen bzw. gesendeten Nachricht erhöht werden (vgl. Kap. 7.2).

7.1.1 Wechsel des gemeinsamen, zählerindividuellen Schlüssels *MK* für bidirektionale Zähler

Alle Zähler, die bidirektional kommunizieren können, müssen mindestens einmal innerhalb von 2 Jahren erfolgreich einen TLS-Kanals aufbauen, um den gemeinsamen, für jeden Zähler individuell zufällig erzeugten Schlüssel *MK* für das symmetrische Verfahren zu wechseln.

Zur Berechnung des neuen zählerindividuellen Schlüssels *MK'* erzeugt das SM-GW eine Zufallszahl z_1 von 128 Bit und sendet diese innerhalb des TLS-Kanals an den Zähler. Der Schlüssel ist

dann $MK'=MAC(MK, z_1)$. Optional kann zusätzlich der Zähler eine Zufallszahl z_2 von 128 Bit erzeugen und diese an das Smart Meter Gateway übertragen. Der neue gemeinsame, zählerindividuelle Schlüssel wird dann als $MK'=MAC(MK, z_1||z_2)$ gesetzt. Der hierbei zu verwendende MAC-Algorithmus wird in Tabelle 10 verbindlich vorgegeben.

7.2 Schlüsselableitung

Vor jeder Übertragung eines neuen Datensatzes werden aus dem Schlüssel *MK* die Schlüssel K_{Enc} (für die Verschlüsselung) und K_{MAC} (für die MAC-Berechnung) abgeleitet.

Die Berechnung von K_{Enc} bzw. K_{MAC} geschieht jeweils durch MAC-Bildung des aktuellen Counterwertes mit dem im Folgenden beschriebenen Verfahren unter Verwendung der Primitive aus Tabelle 10. Hierbei muss stets sichergestellt werden, dass der in die Schlüsselableitung für einen zu sendenden Datensatz eingehende Counterwert größer ist als der zugehörige Counterstand der zuletzt empfangenen bzw. gesendeten Nachricht.

Verfahren	***Mode***	***Länge***	***Verwendung von***	***Verwendung bis***
Berechnung von MK' bzw. K_{Enc} bzw. K_{MAC}				
AES	CMAC gemäß [14]	128	2013	2020+

Tabelle 10: Berechnung der abgeleiteten Schlüssel

Die Berechnung von K_{Enc} bzw. K_{MAC} für einen Datensatz erfolgt durch

- $K_{Enc}=MAC(MK,0x00||C||Zähler\text{-}ID)$ bzw.
- $K_{MAC}= MAC(MK,0x01||C||Zähler\text{-}ID)$,

wobei *0x00* bzw. *0x01* jeweils von der Länge 1 Byte sind. Der Input des MAC muss dabei vor Eingang in den MAC stets mit $16\text{-}(l \bmod 16)$ Oktetts vom Wert $I2OS(16\text{-}(l \bmod 16))$ auf Blocklänge aufgefüllt werden, wobei *l* jeweils die Bytelänge des Inputs und *I2OS()* die Konvertierungsfunktion von Integers nach Oktetts gemäß [12], Kap. 3.1.2, bezeichnet.

Erfolgt die Kommunikation bidirektional, d.h. auf den Eingang eines Datensatzes erfolgt die Versendung einer Antwortnachricht, so werden hierfür neue Schlüssel L_{Enc} und L_{MAC} via

- $L_{Enc}=MAC(MK,0x10||C'||Zähler\text{-}ID)$ bzw.
- $L_{MAC}= MAC(MK,0x11||C'||Zähler\text{-}ID)$

und dem gleichen Padding abgeleitet, wobei der Stand des Transmission Counters C' größer sein muss als der Counterstand des zuletzt empfangenen bzw. gesendeten Datensatzes.

7.3 Übertragung von Zählerdaten

Die Übertragung der Daten muss stets verschlüsselt und MAC-gesichert erfolgen. Die übertragenen Daten werden hierbei zuerst (mit dem abgeleiteten Schlüssel K_{enc} bzw. L_{Enc}) verschlüsselt und danach werden die verschlüsselten Daten (mit K_{MAC} bzw. L_{MAC}) MAC-gesichert.

Tabelle 11 legt die für die Datenübertragung zu verwendenden Verfahren verbindlich fest. Der Verwendungszeitraum bezieht sich auf die Herstellung des Zählers.

Verfahren	*Mode*	*Länge*	*Verwendung von*	*Verwendung bis*
Verschlüsselung (mit K_{Enc} bzw. L_{Enc})				
AES	CBC gemäß [23] (IV=0)	128	2013	2020+
Authentizität und Integritätssicherung (mit K_{MAC} bzw. L_{MAC})				
AES	CMAC gemäß [14] Der MAC-Wert kann optional auf die ersten 64 Bit gekürzt werden.	64	2013	2020+

Tabelle 11: Symmetrische Absicherung der Datenübertragung

Anmerkung:

1. Der Transmission Counter C, der für die Ableitung der Schlüssel. K_{Enc} bzw. K_{MAC} benötigt wird, muss unverschlüsselt aber MAC-gesichertübertragen werden. Zudem muss ein Zähler die Zähler-ID unverschlüsselt an das Smart Meter Gateway übertragen.
2. Die Wahl von IV=0 in der obigen Tabelle 11 ist möglich, da bei jeder Datenübertragung aus dem Counter insbesondere ein neuer Schlüssel K_{Enc} bzw. L_{Enc} abgeleitet wird.
3. Die Verschlüsselung und MAC-Sicherung erfolgt stets über einen vollständigen Datensatz von zu schützenden Daten. Der Transport des Datensatzes kann in mehreren Paketen erfolgen.
4. Zur Detektion von Replay-Attacken muss das Smart Meter Gateway bei jedem empfangenen Datensatz prüfen, dass der Transmission Counter des empfangenen Datensatzes größer als der des letzten empfangenen Datensatzes ist.
5. Um Replay-Attacken auch im Falle eines Stromausfalls zu vermeiden, muss stets sichergestellt werden, dass der aktuelle Wert des Transmission Counters auch nach einem Stromausfall des Smart Meter Gateways vorliegt. Die Toleranz für die Aktualität des Transmission Counters beträgt maximal 12 Stunden.

8 Inhaltsdatenverschlüsselung und -signatur

In der Infrastruktur von Messsystemen kann die Übermittlung von Daten zwischen Smart Meter Gateway und einem autorisierten Marktteilnehmer auch über dritte Parteien (etwa den Gateway-Administrator) erfolgen. Im Weitverkehrsnetz (WAN) geschieht der Austausch von Daten innerhalb eines TLS-Kanals daher stets auf der Basis von für den Endempfänger verschlüsselten und signierten Nachrichten im Cryptographic Message Syntax-Format gemäß [22].

Hierbei muss das im Folgenden vorgestellte Schema implementiert werden.

8.1 Authenticated-Enveloped-data Content Type

Für die Inhaltsdatenverschlüsselung ist der Authenticated-Enveloped-Data Content Type (vgl. [16]) unter Verwendung eines ephemeral-statischem Diffie-Hellman nach den Vorgaben von [7] zu verwenden.

8.1.1 Content-Authenticated-Encryption

Die Inhaltsdaten werden symmetrisch verschlüsselt und die verschlüsselten Daten werden MAC-gesichert (Content-Authenticated-Encryption). Die Verfahren, die bei der Verschlüsselung und MAC-Sicherung der Inhaltsdaten verwendet werden sollen, werden in Tabelle 12 verbindlich vorgegeben.

Verfahren	*Vorgaben*	*Länge*	*Verwendung von*	*Verwendung bis*
AES-GCM				
Verschlüsselung und Authentizität	AES-GCM gemäß [17]	128	2013	2020+
AES-CBC-CMAC				
Verschlüsselung	AES-CBC (IV=0) gemäß [23] mit Padding gemäß [22], Abschnitt 6.3	128	2013	2020+
Authentizität	AES-CMAC gemäß [14]	128	2013	2020+

Tabelle 12: Inhaltsdatenverschlüsselung

Die Schlüssel für die Verschlüsselung und MAC-Sicherung der Inhaltsdaten müssen (unmittelbar vor ihrer Verwendung) zufällig erzeugt werden und dürfen jeweils nur für die Versendung einer Nachricht verwendet werden.

Bemerkung: Die Wahl von IV=0 in der obigen Tabelle ist möglich, da bei jeder erneuten Inhaltsdatenverschlüsselung, d.h. jedes neue Authenticated-Enveloped-Data-Paket, die symmetrischen Schlüssel neu generiert werden.

8.1.2 Schlüsselableitung und Key Encryption

Die zufällig erzeugten Schlüssel für die Verschlüsselung und MAC-Sicherung der Inhaltsdaten sind verschlüsselt im CMS-Container enthalten (Key Encryption).

Der Schlüssel *K* für die Key Encryption muss per ECKA-EG [12] berechnet werden. Die Ableitung von *K* muss mittels der X9.63 Key Derivation Function erfolgen (vgl. [12], Kap. 4.3.3). ECKA-EG ist dazu gemäß [12], Kap. 4.3.2.2 bzw. 5.3.1 (OIDs mit X9.63-KDF) zu implementieren.

Tabelle 13 legt die für ECKA-EG zu verwendenden Hashfunktionen und Kurvenparameter verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Erstellung der zugrundeliegenden Zertifikate.

Verfahren	*Vorgaben*	*Verwendung von*	*Verwendung bis*
Hash	SHA-256	2013	2020+
EC-Domain-Parameter	NIST P-256 [18] BrainpoolP256r1	2013 2015	2014 2020+

Tabelle 13: Schlüsseltransport für die Inhaltsdatenverschlüsselung

Die Key Encryption erfolgt mit dem abgeleiteten Schlüssel *K* auf Basis symmetrischer Kryptographie.Tabelle 14 legt die hierbei zu verwendenden Verfahren verbindlich fest.

Verfahren	*Mode*	*Länge*	*Verwendung von*	*Verwendung bis*
Verschlüsselung				
AES	Key-Wrap gemäß [13]	128	2013	2020+

Tabelle 14: Algorithmen für die CMS Key Encryption

8.2 Signed-Data Content Type

Die verschlüsselten und MAC-gesicherten Inhaltsdaten (Authenticated-Enveloped-Data Content Type, siehe 8.1) müssen anschließend signiert werden. Hierzu ist ECDSA, implementiert nach [12], zu verwenden.

Tabelle 15 legt die zu verwendenden Hashfunktionen und Kurvenparameter verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Erstellung der Zertifikate.

Verfahren	*Vorgaben*	*Verwendung von*	*Verwendung bis*
Hash	SHA-256	2013	2020+
EC-Domain-Parameter	NIST P-256 [18] BrainpoolP256r1 [21]	2013 2015	2014 2020+

Tabelle 15: Signatur der verschlüsselten Inhaltsdaten

9 PACE und Secure Messaging

Für den Zugriff des Smart-Meter Gateways auf das Sicherheitsmodul erfolgt eine gegenseitige Authentisierung beider Komponenten gemäß [8] mittels des PACE-Protokolls. PACE (Password Authenticated Connection Establishment) (vgl. [8] bzw. [10], [11]) ist ein passwort-basiertes Authentisierungs- und Schlüsseleinigungsverfahren, bei dem aus einer gemeinsamen PIN Sitzungsschlüssel hoher Entropie für das anschließende Secure Messaging abgeleitet werden. Secure Messaging liefert einen verschlüsselten, authentisierten Kanal zwischen den Smart Meter Gateway und dem Sicherheitsmodul (vgl. [8]).

Tabelle 16 legt die aktuell zu verwendenden kryptographischen Verfahren sowie die Anzahl der dezimalen Zeichen der PACE-PIN verbindlich fest. Die angegebenen Verwendungszeiträume beziehen sich auf die Herstellung des Sicherheitsmoduls..

Vorgaben		***Verwendung von***	***Verwendung bis***
Algorithmus	`id-PACE-ECDH-GM-AES-CBC-CMAC-128` vgl. [8] bzw. [10], [11]	2013	2020+
EC-Domain-Parameter	NIST-P256 BrainpoolP256r1	2013 2015	2014 2020+
PACE-PIN	10 Dezimalziffern	2013	2020+

Tabelle 16: PACE und Secure Messaging

Da die gewünschte Verwendungszeit der Komponenten eines Smart-Metering-Sytstems deutlich über den Verwendungszeitraum hinausgeht, wird (insbesondere für Komponenten ohne Update-Möglichkeit) empfohlen zusätzlich auch die folgenden weiteren PACE-Algorithmen mit den Elliptischen Kurven der entsprechenden Bitlängen zu unterstützen:

- `id-PACE-ECDH-GM-AES-CBC-CMAC-192` vgl. [8] bzw. [10], [11]
- `id-PACE-ECDH-GM-AES-CBC-CMAC-256` vgl. [8] bzw. [10], [11]

Die PIN, die bei PACE zur Authentisierung des Smart-Meter Gateways gegenüber dem Sicherheitsmodul verwendet wird, muss im Smart Meter Gateway geeignet geschützt werden, etwa durch Speicherung der PIN im sicheren Bereich des Prozessors.

Eine Secure Messaging Session darf maximal 48 Stunden laufen.

10 Zertifizierung

Die Smart Meter Gateways und Sicherheitsmodule müssen nach den Common Criteria zertifiziert sein.

10.1 Smart Meter Gateway

Im Rahmen der erforderlichen Zertifizierung muss die Konformität des Smart Meter Gateways zum Schutzprofil BSI-CC-PP-0073 [2] nachgewiesen werden.

Das Common Criteria Zertifikat muss einen Hinweis enthalten, dass die Anforderungen dieser Technischen Richtlinie an das Smart Meter Gateway (siehe auch die entsprechenden Application Notes des PPs [2]) berücksichtigt wurden.

10.2 Sicherheitsmodul

Im Rahmen der erforderlichen Zertifizierung muss die Konformität des Sicherheitsmoduls zum Schutzprofil BSI-CC-PP-0077 [3] nachgewiesen werden.

Das Common Criteria Zertifikat muss einen Hinweis enthalten, dass die Anforderungen dieser Technischen Richtlinie an das Sicherheitsmodul (siehe auch die entsprechenden Application Notes des PPs [3]) berücksichtigt wurden.

Literaturverzeichnis

[1] BSI AIS 20/31, A proposal for: Functionality classes for random number generators, Version 2.0, 2011
[2] BSI CC-PP-0073, Protection Profile for the Gateway of a Smart Metering System, 2013
[3] BSI CC-PP-0077, Protection Profile for the Security Module of a Smart Metering System, 2013
[4] BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2014.01, 2014
[5] BSI TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 - Verwendung von Transport Layer Security (TLS), 2014
[6] BSI TR-03109, Technische Richtlinie BSI-TR-03109, 2013
[7] BSI TR-03109-1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, 2013
[8] BSI TR-03109-2, Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, 2013
[9] BSI TR-03109-4, Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways, 2013
[10] BSI TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents - Part 2, Version 2.10, 2012
[11] BSI TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents - Part 3, Version 2.11, 2013
[12] BSI TR-03111, Elliptic Curve Cryptography (ECC), Version 2.0, 2012
[13] IETF RFC 3394, J. Schaad, R. Housley, Advanced Encryption Standard (AES) Key Wrap Algorithm, 2002
[14] IETF RFC 4493, J. H. Song, J. Lee, T. Iwata: The AES-CMAC Algorithm, 2006
[15] IETF RFC 5077, J. Salowey, H. Zhou, P. Eronen, H. Tschofenig: Transport Layer Security (TLS) Session Resumption without Server-Side State, 2008
[16] IETF RFC 5083, R. Housley, Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type, 2007
[17] IETF RFC 5084, R. Housley, Using AES-CCM amd AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS), 2007
[18] IETF RFC 5114, M. Lepinski, S. Kent: Additional Diffie-Hellman Groups for Use with IETF Standards, 2008
[19] IETF RFC 5246, T. Dierks, E. Rescorla: Transport Layer Security (TLS) Version 1.2, 2008
[20] IETF RFC 5289, E. Rescorla: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), RFC 5289, 2008
[21] IETF RFC 5639, M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010
[22] IETF RFC 5652, R. Housley: Cryptographic Message Syntax (CMS), 2009
[23] ISO/IEC 10116:2006, Information technology -- Security techniques -- Modes of operation for an n-bit block cipher, 2006
[24] NIST FIPS 180-4, Secure Hash Standard (SHS), 2012
[25] NIST FIPS 197, Advanced Encryption Standard (AES), 2001
[26] NIST SP800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007