Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie TR-03109

Anhang A: Kryptographische Vorgaben für die Infrastruktur von Messsystemen

Version: 0.20 - Stand 10.10.2011

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

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Im vorliegenden Anhang zur TR-03109 [3] werden die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren für die Infrastruktur von Messsystemen im Energiesektor beschrieben.

Die Vorgaben des vorliegenden Anhangs 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 2017. Eine weitere Verwendung des Verfahrens über diesen Zeitraum hinaus ist nicht ausgeschlossen und wird mit 2017+ gekennzeichnet.

1.1 Smart Meter Gateways

Die Anforderungen an die Sicherheit und Interoperabilität der Kommunikationseinheit von Messsystemen werden in der Technischen Richtlinie TR-03109 [3] spezifiziert.

Basierend auf den Technischen Richtlinien TR-02102 [4] und TR-03111 [6] 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. [7])	Public Key Infrastruktur (vgl. Abschnitt 3)
Absicherung der Kommunikation zwischen Smart Meter Gateway und externen Marktteilnehmern im WAN(vgl. [3])	TLS (vgl. Abschnitt 4)
Absicherung der Kommunikation von TLS-fähigen Zählern mit dem Smart Meter Gateway im LMN(vgl. [3])	TLS (vgl. Abschnitt 5)
Absicherung der Kommunikation von batteriebetriebenen (und nicht TLS-fähigen) Zählern mit dem Smart Meter Gateway (vgl. [3])	Symmetrische Verschlüsselung (vgl Abschnitt 6)
Vertrauliche, authentische Ende-zu-Ende-Übertragung von Daten über das WAN an den Endempfänger (vgl. auch [3])	Inhaltsdatenverschlüsselung (vgl. Abschnitt 7)

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 gegeben, die in diesem Dokument verwendet werden.

Digitale Signatur	ECDSA [1]
Schlüsseleinigung	ECKA-DH [6]
Schlüsseltransport	ECKA-EG [6]
Blockchiffre	AES [13] • CBC-Mode [9] • CMAC-Mode [10]
Hashfunktionen	SHA-2 Familie [14]

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-Kurven über Primkörpern [12] bzw. Brainpool-Kurven [11] in den entsprechenden Bitlängen verwendet.

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 [2]) 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 zur gegenseitigen Authentisierung und zum Aufbau eines verschlüsselten, integritätsgesicherten TLS-Kanals bzw. zur Verschlüsselung oder Signatur von Daten auf Inhaltsebene einge-

setzt werden, wird durch die Smart Meter Public Key Infrastruktur (SM-PKI) sichergestellt. Die SM-PKI wird in [7] 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 [7] spezifiziert. Zu den Endnutzern gehören die Marktteilnehmer und die Smart Meter Gateways.

Als Signaturverfahren, mit dem die X.509 Zertifikate signiert werden, muss das Verfahren ECDSA gemäß [6], 5.2.2 verwendet werden.

Tabelle 3 legt die zu verwendenden Hashfunktionen und Schlüssellängen verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Erstellung der Zertifikate.

Verfahren/Parameter	*Vorgaben*	*Verwendung von*	*Verwendung bis*
Root-CA			
Signaturalgorithmus	`ECDSA-With-SHA384` [6]	2011	2017+
Elliptische Kurve	NIST P-384 [12]	2011	2017+
Sub-CAs			
Signaturalgorithmus	`ECDSA-With-SHA256` [6]	2011	2017+
Elliptische Kurve	NIST P-256 [12]	2011	2017+

Tabelle 3: Signatur der Zertifikate

Hinweis: Die Verwendung der NIST-Kurven erfolgt übergangsweise. Es ist eine Umstellung auf Brainpool-Kurven gemäß [11] bis Ende 2015 vorgesehen.

In Tabelle 4 werden in Übereinstimmung mit [7] die Laufzeiten der Zertifikate angegeben.

Zertifikat	*Gültigkeitszeit*	*Private Key Usage*
Root-Zertifikat	10 Jahre	5 Jahre
Sub-CA-Zertifikat	9 Jahre	3 Jahre
Endnutzerzertifikate (TLS, Verschlüsselung, Signatur)	2 Jahre	2 Jahre

Tabelle 4: Laufzeiten der Zertifikate (Informativ)

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 1.1 [15] implementiert werden. Eine TLS-Session darf maximal 2 Tage laufen. Es darf keine Wiederaufnahme von Sessions (Session Resuming) möglich sein.

4.1 Cipher Suites und Kurvenparameter

Die Implemetierung muss gemäß [8] 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`

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 von Marktteilnehmern 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`	2011	2017+
Kurve	NIST P-256 [12]	2011	2017+

Tabelle 5: Mindestens zu unterstützende Verfahren

Hinweis: Die Verwendung der NIST-Kurven erfolgt übergangsweise. Es ist eine Umstellung auf Brainpool-Kurven gemäß [11] bis Ende 2015 vorgesehen.

Um eine langfristige Nutzung zu ermöglichen, sollten für TLS 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`	2011	2017+
Elliptische Kurven		
BrainpoolP256r1 [11]	2011	2017+
BrainpoolP384r1 [11]	2011	2017+
BrainpoolP512r1 [11]	2011	2017+
NIST P-384 [12]	2011	2017+
NIST P-521 [12]	2011	2017+

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.

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

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

gemäß den Vorgaben in [6] für alle elliptischen Kurven aus Tabelle 5 und Tabelle 6 unterstützen.

4.2 Authentifizierung und TLS-Zertifikate

Zur gegenseitigen Authentifizierung, benötigt jede Partei ein TLS-Zertifikat für ein Schlüsselpaar, das zur Erzeugung von Signaturen mit ECDSA gemäß [1] geeignet ist.

Tabelle 7 legt die zu verwendenden Hashfunktionen und Kurvenparameter verbindlich fest.

Verfahren	*Vorgaben*	*Verwendung von*	*Verwendung bis*
Hash	SHA-256	2011	2017+
Elliptische Kurve	NIST P-256 [12]	2011	2017+

Tabelle 7: Authentifizierung

Hinweis: Die Verwendung der NIST-Kurven erfolgt übergangsweise. Es ist eine Umstellung auf Brainpool-Kurven gemäß [11] bis Ende 2015 vorgesehen.

5 TLS-Kommunikation im LMN

Im Allgemeinen verwenden Zähler für die Kommunikation mit dem zugehörigen Smart-Meter-Gateway ebenfalls TLS. Das TLS-Protokoll muss mindestens nach Version 1.1 [15] implementiert werden. Eine TLS-Session darf maximal 2 Tage laufen. Es darf keine Wiederaufnahme von Sessions (Session Resuming) möglich sein.

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

Von einem Smart-Meter Gateway bzw. TLS-Zähler dürfen keine weiteren TLS-Cipher-Suites als die in Kapitel 5.1 genannten für die Kommunikation im LMN unterstützt werden.

5.1 ECC-basierte Kommunikation

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

Tabelle 8 gibt die maximalen Laufzeiten der Zählerzertifikate verbindlich vor. Die Zertifikate sind selbst-signiert, d.h. insbesondere besitzt das Smart Meter Gateway für die TLS-Kommunikation im WAN und im LMN separate Zertifikate.

Zertifikat	*Gültigkeitszeit*	*Private Key Usage*
Zählerzertifikat	Maximal 10 Jahre	Maximal 10 Jahre
SM-GW-Zertifikat	Maximal 10 Jahre	Maximal 10 Jahre

Tabelle 8: Laufzeiten der Zählerzertifikate

5.1.1 Initialer Austausch und Update der Zertifikate

Für Zähler, die TLS unterstützen, muss bei erstmaligem Anschluss an ein neues SM-GW ein authentischer Austausch der TLS-Zertifikate mit dem Smart Meter Gateway erfolgen. Dieser Austausch der Zertifikate erfolgt mit dem in Kapitel 6 beschriebenen symmetrischen Verfahren.

Es ist geplant, den Austausch der Zertifikate auch durch Aufbau eines verschlüsselten Kanals via Passworteingabe und PACE (siehe auch [5]) zu ermöglichen.

Für den Update eines Zertifikats muss das neue selbst-signierte Zertifikat über den aufgebauten TLS-Kanals gesendet werden.

5.2 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 Firmwareupdate neue kryptographische Verfahren einzuspielen, um so eine weitere Verwendbarkeit des TLS-Zählers zu ermöglichen.

6 Kommunikation batteriebetriebener Zähler im LMN

Batteriebetriebene Zähler können häufig keinen TLS-Kanal aufbauen. Daher muss das Smart Meter Gateway diesen Zählern im Folgenden beschriebene alternative Möglichkeit zum Senden von Verbrauchsdaten bereitstellen. Diese Art von Kommunikation ist nur für die Versendung von Daten mit niedrigem Schutzbedarf geeignet, da kein Schlüsselwechsel möglich ist und die Zähler länger als 10 Jahre im Feld sein können.

6.1 Voraussetzungen

Der batteriebetriebene Zähler und das SM-GW verfügen über einen gemeinsamen geeigneten, symmetrischen, zählerinidividuellen Schlüssel *M*. Dieser Schlüssel wird vom Zählerhersteller zufällig (nach den Vorgaben von 2.3) erzeugt und vertraulich und authentisch an den Administrator des Gateways übertragen, der die Schlüssel, wie in [3] beschrieben, gesichert in das Gateway einbringt.

Der batteriebetriebene Zähler verfügt über einen Counter *C* von 32 Bit. Der Counter darf keinen Überlauf besitzen und niemals zurückgesetzt werden (dies gilt auch für den Fall, dass der Zähler an ein anderes Gateway angeschlossen wird).

6.2 Schlüsselableitung

Vor jeder Übertragung von Zählerdaten werden aus dem Schlüssel *M* 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 in Tabelle 9 vorgegebenen Verfahren.

Verfahren	***Mode***	***Länge***	***Verwendung von***	***Verwendung bis***
Berechnung von K_{Enc} bzw. K_{MAC}				
AES	CMAC gemäß [10]	128	2011	2017+

Tabelle 9: Berechnung der abgeleiteten Schlüssel

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

- K_{enc}=*MAC(M,0||C||Zähler-ID)* bzw.
- K_{MAC}= *MAC(M,1||C||Zähler-ID),*

wobei 0 bzw. 1 jeweils von der Länge 1 Byte sind. Nach der Berechnung von K_{Enc} und K_{MAC} wird der Counter inkrementiert.

6.3 Übertragung von Zählerdaten

Die Übertragung von Zählerdaten an das SM-GW muss verschlüsselt und MAC-gesichert erfolgen. Öffentliche Metadaten (Zähler-ID) können unverschlüsselt übertragen werden.

Tabelle 10 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})				
AES	CBC (IV=0) gemäß [13]	128	2011	2017+
Authentizität und Integritätssicherung (mit K_{MAC})				
AES	CMAC gemäß [10]	128	2011	2017+

Tabelle 10: Datenübertragung batteriebetriebener Zähler

Anmerkung:

1. Zur Detektion von Replay-Attacken sendet der Zähler den aktuellen Stand des Counters mit. Das Smart Meter Gateway muss bei jeder empfangenen Nachricht den Counter berechnen und prüfen, dass der Counter der empfangenen Nachricht größer als der der letzten Nachricht ist.

7 Inhaltsdatenverschlüsselung

In der Infrastruktur von Messsystemen kann Übermittlung von Daten zwischen SM-GW und einem autorisierten Marktteilnehmer auch über dritte Parteien (Messstellenbetreiber) erfolgen. Im Weitverkehrsnetz 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 [16].

Hierbei muss das im Folgenden vorgestellte Schema implementiert werden.

7.1 Enveloped-data Content Type

Die Inhaltsdaten werden symmetrisch verschlüsselt. Tabelle 11 legt die dafür zu verwendende Chiffre verbindlich fest.

Verfahren	*Mode*	*Länge*	*Verwendung von*	*Verwendung bis*
Verschlüsselung				
AES	CBC (IV=0) gemäß [13] mit Padding gemäß [16], Abschnitt 6.3	128	2011	2017+
Authentizität und Integritätssicherung				
AES	CMAC gemäß [10]	128	2011	2017+

Tabelle 11: Inhaltsdatenverschlüsselung

Bemerkung: Die Wahl von IV=0 in der obigen Tabelle ist möglich, da bei jeder erneuten Inhaltsdatenverschlüsselung die symmetrischen Schlüssel neu generiert werden. Siehe Abschnitt 7.1.1 für Details zur Schlüsselableitung.

7.1.1 Ableitung des symmetrischen Schlüssels

Der Schlüssel für die symmetrische Verschlüsselung der Inhaltsdaten muss per ECKA-EG [6] berechnet werden. Das Verfahren ist gemäß [6], Kapitel 5.3.1.1 zu implementieren. Für die Ableitung der Schlüssel K_{Enc} und K_{MAC} ist dabei die X9.63 Key Derivation Function aus [6], Kapitel 4.3.3, zu verwenden.

Tabelle 12 legt die 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	2011	2017+
Elliptische Kurve	NIST P-256 [12]	2011	2017+

Tabelle 12: Schlüsseltransport für die Inhaltsdatenverschlüsselung

7.2 Signed-Data Content Type

Die verschlüsselten Inhaltsdaten (s. Enveloped-data Content Type, siehe 7.1) müssen anschließend signiert werden. Hierzu ist ECDSA, implementiert nach [1], zu verwenden.

Tabelle 13 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	2011	2017+
Elliptische Kurve	NIST P-256 [12]	2011	2017+

Tabelle 13: Signatur der verschlüsselten Inhaltsdaten

Hinweis: Die Verwendung der NIST-Kurven erfolgt übergangsweise. Es ist eine Umstellung auf Brainpool-Kurven gemäß [11] bis Ende 2015 vorgesehen.

8 Zertifizierung

Die Smart Meter Gateways und Sicherheitsmodule müssen nach den Common Criteria zertifiziert sein. Der Inhaber des Common Criteria Zertifikates muss die Widerstandsfähigkeit des jeweiligen zertifizierten Smart Meter Gateways gegen neue Angriffsmethoden alle 12 Monate vom BSI neu bewerten lassen. Das Common Criteria Zertifikat muss einen Hinweis enthalten, dass bei der Evaluierung des Smart Meter Gateways/Sicherheitsmoduls die Anforderungen dieser Technischen Richtlinie berücksichtigt wurden.

8.1 Smart Meter Gateway

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

8.2 Sicherheitsmodul

Im Rahmen der erforderlichen Zertifizierung muss die Konformität des Sicherheitsmoduls zum Schutzprofil BSI-CC-PP-xxxx nachgewiesen werden.

Literaturverzeichnis

[1] ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm, 2005

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

[3] BSI BSI TR-03109, Anforderungen an die Interoperabilität der Kommunikationseinheit eines Messsystems, 2011

[4] BSI TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen Version 1.0, 2008

[5] BSI TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents, 2010

[6] BSI TR-03111, Elliptic Curve Cryptography (ECC) Version 1.11, 2009

[7] BSI TR-031xx, Die Public Key Infrastruktur für Smart Meter, 2011

[8] E. Rescorla , TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), RFC 5289, 2008

[9] ISO/IEC 10116:2006, Information technology -- Security techniques -- Modes of operation for an n-bit block cipher, 2006

[10] J. H. Song, J. Lee, T. Iwata , RFC 4493, The AES-CMAC Algorithm, 2006

[11] Lochter, Manfred; Merkle, Johannes RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010

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

[13] NIST , FIPS 197, Advances Encryption Standard (AES), 2001

[14] NIST , FIPS 180-3: Secure Hash Standard, 2008

[15] P. Eronen, H. Tschofenig , RFC 4279: Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), 2005

[16] T. Dierks, E. Rescorla , RFC 4346: Transport Layer Security (TLS) Version 1.1, 2006

[17] , RFC 3852 Cryptographic Message Syntax,