

DIN EN 62056-5-3

ICS 33.200; 35.100.70; 35.240.99; 91.140.50

Einsprüche bis 2018-12-05
Vorgesehen als Ersatz für
DIN EN 62056-5-3:2017-07**Entwurf**

**Datenkommunikation der elektrischen Energiemessung –
DLMS/COSEM –
Teil 5-3: DLMS/COSEM-Anwendungsschicht
(IEC 62056-5-3:2017);
Englische Fassung EN 62056-5-3:2017**

Electricity metering data exchange –
The DLMS/COSEM suite –
Part 5-3: DLMS/COSEM application layer
(IEC 62056-5-3:2017);
English version EN 62056-5-3:2017

Échange des données de comptage de l'électricité –
La suite DLMS/COSEM –
Partie 5-3: Couche application DLMS/COSEM
(IEC 62056-5-3:2017);
Version anglaise EN 62056-5-3:2017

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-10-05 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 380 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Für dieses Dokument ist das nationale Arbeitsgremium K 461 „Messeinrichtungen und -systeme für Elektrizität“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom TC 13 „Electrical energy measurement and control“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (maintenance result date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für die vorliegende Norm erfüllt.

Da sich die Benutzer des vorliegenden Normentwurfs der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN 62605 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe, Symbole und Abkürzungen festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA des vorliegenden Normentwurfs hinzugefügt. Für die meisten der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Dieser Normentwurf steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Änderungen

Gegenüber DIN EN 62056-5-3:2017-07 wurden folgende Änderungen vorgenommen:

- a) Die wesentlichen Änderungen sind im Anhang K (informativ) beschrieben.

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung^{N1}

1 Anwendungsbereich

Dieser Teil von IEC 62056 legt die DLMS/COSEM-Anwendungsschicht in Bezug auf die Struktur, die Dienste und die Protokolle für DLMS/COSEM-Clients und -Server fest und definiert Regeln zur Spezifikation der DLMS/COSEM-Kommunikationsprofile.

Es werden Dienste für die Einrichtung und Freigabe von Anwendungsassoziationen festgelegt und Datenkommunikationsdienste für den Zugriff auf die Methoden und Attribute von in IEC 62056-6-2 definierten COSEM-Schnittstellenobjekten entweder unter Anwendung des logischen Namens (LN) oder des Kurznamens (SN).

Anhang A (normativ) legt fest, wie die COSEM-Anwendungsschicht in verschiedenen Kommunikationsprofilen anzuwenden ist. Es wird angegeben, wie verschiedene Kommunikationsprofile aufgebaut werden können, um Daten mit Zählern nach dem COSEM-Schnittstellenmodell auszutauschen, und welche notwendigen Elemente im jeweiligen Kommunikationsprofil festzulegen sind. Die tatsächlichen medienspezifischen Kommunikationsprofile werden in den einzelnen Teilen der Normenreihe IEC 62056 festgelegt.

Anhang B (normativ) beschreibt den SMS-Short-Wrapper.

Anhang C (normativ) legt das Gateway-Protokoll fest.

Anhang D, Annex E und Annex F (informativ) enthalten Codierungsbeispiele für APDUs.

Anhang G (normativ) stellt elliptische Kurven und Domain-Parameter der NSA Suite B bereit.

Anhang H (informativ) stellt ein Beispiel für ein Anwender-Signaturzertifikat unter Verwendung von P-256, signiert mit P-256 bereit.

Anhang I (normativ) legt die Anwendung von Schlüssel-Vereinbarungsplänen in DLMS/COSEM fest.

Anhang J (informativ) legt Beispiele für den Austausch von geschützten xDLMS APDUs zwischen einem Dritten und einem Server fest.

Anhang K (informativ) führt die wichtigsten technischen Änderungen in dieser Ausgabe der Norm auf.

3 Begriffe, Abkürzungen und Symbole

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC TR 62051:1999, IEC TR 62051-1, RFC 4106 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: unter <http://www.iso.org/obp>

3.1 Allgemeine Begriffe zu DLMS/COSEM

3.1.1

ACSE APDU

APDU, das vom Dienstelement der Assoziationssteuerung (en: Association Control Service Element, ACSE) verwendet wird

^{N1} Nationale Fußnote: Die Nummerierung der IEC 62065-5-3:2017-08 wurde beibehalten.

3.1.2

Anwendungsassoziation

kooperative Beziehung zwischen zwei Anwendungsinstanzen, die durch ihren Austausch der Protokollsteuerinformation der Anwendungsschicht durch ihre Nutzung von Darstellungsdiensten entsteht

3.1.3

Anwendungskontext

Menge von Anwendungs-Dienstelementen, bezogenen Angaben und jeden sonstigen notwendigen Informationen für das Zusammenwirken von Anwendungsinstanzen bei einer Anwendungsassoziation

3.1.4

Anwendungsinstanz

systemunabhängige Anwendungsvorgänge, die dem Anwendungsagenten in Form von Anwendungsdiensten zur Verfügung gestellt werden, z. B. ein Satz von Anwendungsdienstelementen, die zusammen alle oder einen Teil der Kommunikationsaspekte eines Anwendungsprozesses ausführen

3.1.5

Anwendungsprozess

Element in einem realen offenen System, das die Informationsverarbeitung für eine bestimmte Anwendung ausführt

[QUELLE: ISO/IEC 7498-1:1994, 4.1.4]

3.1.6

Authentifizierungsmechanismus

Spezifikation einer bestimmten Menge von Authentifizierungs-Funktionsregeln zur Festlegung, Verarbeitung und Übertragung von Authentifizierungswerten

[QUELLE: ISO/IEC 15953:1999, 3.5.11]

3.1.7

Client

Anwendungsprozess, der im Datenerfassungssystem läuft

3.1.8

Client/Server

Beziehung zwischen zwei Computerprogrammen, bei der ein Programm, der Client, eine Dienstanforderung an ein anderes Programm, den Server, stellt, der diese Anforderung erfüllt

3.1.9

COSEM

Begleitspezifikation für die Energiemessung (en: Companion Specification for Energy Metering); bezieht sich auf das COSEM-Objektmodell

3.1.10

COSEM APDU

umfasst ACSE APDUs und xDLMS APDUs

3.1.11

COSEM-Daten

COSEM-Objekt-Attributwerte, Methodenaufwurf und Rückgabeparameter

3.1.12

COSEM-Schnittstellenklasse

Instanz mit einer speziellen Menge von Attributen und Methoden, die eine bestimmte Funktion allein oder in Bezug zu anderen COSEM-Schnittstellenklassen modelliert

3.1.13

COSEM-Objekt

Instanz einer COSEM-Schnittstellenklasse

3.1.14

DLMS/COSEM

bezieht sich auf die Anwendungsschicht, die xDLMS-Dienste für den Zugriff auf Schnittstellenobjekt-Attribute bereitstellt. Bezieht sich außerdem auch gemeinsam auf die DLMS/COSEM-Anwendungsschicht und das COSEM-Datenmodell

3.1.15

DLMS-Kontext

Spezifikation der Dienstelemente der DLMS und der Semantik der Kommunikation, die während der Lebensdauer einer Anwendungsassoziation anzuwenden ist

[QUELLE: IEC 61334-4-41:1996, 3.3.5]

3.1.16

Authentifizierung einer Instanz

Bestätigung, dass eine Instanz die ist, die sie behauptet zu sein

[QUELLE: ISO/IEC 9798-1:2010, 3.14]

3.1.17

logisches Gerät

abstrakte Instanz innerhalb eines physikalischen Gerätes, die eine Untermenge der Funktionalität darstellt, die mit COSEM-Objekten modelliert wird

3.1.18

Master

zentrale Station – Station, die die Initiative ergreift und den Datenfluss steuert

3.1.19

gegenseitige Authentifizierung

Authentifizierung von Instanzen, die für beide Instanzen die Zusicherung der Identität der jeweils anderen bietet

Anmerkung 1 zum Begriff: Der DLMS/COSEM HLS-Authentifizierungsmechanismus stellt gegenseitige Authentifizierung bereit.

[QUELLE: ISO/IEC 9798-1:2010, 3.18, geändert durch Hinzufügen der Anmerkung 1]

3.1.20

physikalisches Gerät

physikalische Messeinrichtung, die das Element der höchsten Ebene, die im COSEM-Schnittstellenmodell für Messeinrichtungen angewendet wird, ist

3.1.21

Pull-Operation

Kommunikationsart, bei der die Anforderung einer bestimmten Transaktion vom Client initiiert wird

3.1.22

Push-Operation

Kommunikationsart, bei der die Anforderung einer bestimmten Transaktion vom Server initiiert wird

3.1.23

Systemtitel

eindeutiger Systembezeichner

3.1.24

Server

Anwendungsprozess, der in einer Messeinrichtung abläuft

3.1.25

Slave

Station, die auf Anfragen einer Masterstation antwortet

Anmerkung 1 zum Begriff: Ein Zähler ist üblicherweise eine Slave-Station.

3.1.26

einseitige Authentifizierung

Authentifizierung von Instanzen, die für eine Instanz die Zusicherung der Identität der anderen bietet, nicht jedoch umgekehrt

Anmerkung 1 zum Begriff: Der DLMS/COSEM LLS-Authentifizierungsmechanismus stellt einseitige Authentifizierung bereit.

[QUELLE: ISO/IEC 9798-1:2010, 3.39]

3.1.27

xDLMS

erweiterte DLMS; bezieht sich auf das DLMS-Protokoll mit den in diesem Dokument festgelegten Erweiterungen

3.1.28

xDLMS APDU

APDU, das vom xDLMS-Anwendungsdienstelement (xDLMS ASE) verwendet wird

3.1.29

xDLMS-Nachricht

xDLMS APDU, das zwischen einem Client und einem Server oder zwischen einem Dritten und einem Server ausgetauscht wird

3.2 Begriffe, die sich auf die kryptografische Sicherheit beziehen

3.2.1

Zugriffssteuerung

beschränkt den Zugriff auf Ressourcen ausschließlich auf privilegierte Instanzen

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.2

asymmetrischer Schlüsselalgorithmus

siehe Verschlüsselungsalgorithmus des öffentlichen Schlüssels

3.2.3

Authentifizierung

Prozess, der die Informationsquelle feststellt, die Zusicherung der Identität einer Instanz bietet oder die Sicherstellung der Integrität von Kommunikationssitzungen, Nachrichten, Dokumenten oder gespeicherten Daten bietet

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.4

Authentifizierungscode

kryptografische Prüfsumme, die auf einer anerkannten Sicherheitsfunktion beruht (auch bekannt als Nachrichtenauthentifizierungscode)

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.5

Zertifikat

siehe Zertifikat des öffentlichen Schlüssels

3.2.6

Zertifizierungsstelle CA

(en: Certification Authority)

Instanz der Infrastruktur des öffentlichen Schlüssels (PKI, en: Public Key Infrastructure), die für die Ausstellung von Zertifikaten des öffentlichen Schlüssels und die Forderung nach Übereinstimmung mit einer PKI-Richtlinie verantwortlich ist

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.7

Zertifikatsrichtlinie CP

(en: Certificate Policy)

spezialisierte Form einer Verwaltungsrichtlinie, die auf elektronische Transaktionen abgestimmt ist, die während des Zertifikatsmanagements durchgeführt werden. Eine Zertifikatsrichtlinie behandelt alle Gesichtspunkte, die mit der Erzeugung, Herstellung, Verteilung, Abrechnung, Wiederherstellung und Verwaltung von digitalen Zertifikaten zusammenhängen. Indirekt kann eine Zertifikatsrichtlinie auch die Transaktionen steuern, die unter Anwendung eines Kommunikationssystems durchgeführt werden, das von einem zertifikatsbasierten Sicherheitssystem geschützt ist. Durch Steuerung kritischer Zertifikaterweiterungen können derartige Richtlinien und die damit verbundene Technologie zur Durchsetzung die Bereitstellung der Sicherheitsdienste unterstützen, die von bestimmten Anwendungen gefordert werden.

[QUELLE: NIST SP 800-32:2001]

3.2.8

Challenge

zeitvarianter Parameter, der von einem Prüfer erzeugt wird

[QUELLE: ITU-T X.811:1995, 3.8]

3.2.9

Chiffrierung

Authentifizierung und/oder Verschlüsselung mittels symmetrischer Schlüsselalgorithmen

3.2.10

Chiffretext

Daten in ihrer verschlüsselten Form

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.11

Cofaktor

Ordnung der Gruppe elliptischer Kurven, dividiert durch die (erste) Ordnung des Generatorpunkts (d. h. des Basispunkts, festgelegt in den Domain-Parametern)

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.12

Vertraulichkeit

Eigenschaft, dass sensible Informationen nicht gegenüber unberechtigten Instanzen enthüllt werden

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.13

kryptografischer Algorithmus

eindeutiges Berechnungsverfahren, das variable Eingaben einschließlich eines kryptografischen Schlüssels nimmt und eine Ausgabe erzeugt

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.14

kryptografischer Schlüssel Schlüssel

Parameter, der in Verbindung mit einem kryptografischen Algorithmus verwendet wird und der dessen Handhabung derart bestimmt, dass eine Instanz, der der Schlüssel bekannt ist, die Operation wiedergeben oder umkehren kann, während eine Instanz ohne Kenntnis des Schlüssels dies nicht kann

Anmerkung 1 zum Begriff: Beispiele schließen Folgendes ein:

1. die Umwandlung von Klartext-Daten in Chiffretext-Daten;
2. die Umwandlung von Chiffretext-Daten in Klartext-Daten;
3. die Berechnung einer digitalen Signatur anhand von Daten;
4. die Verifizierung einer digitalen Signatur;
5. die Berechnung eines Authentifizierungscodes anhand von Daten;
6. die Verifizierung eines Authentifizierungscodes anhand von Daten und eines empfangenen Authentifizierungscodes;
7. die Berechnung eines gemeinsamen Geheimnisses, das zur Ableitung von Schlüsselmaterial verwendet wird.

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.15

Kryptoperiode

Zeitspanne, für die die Anwendung eines spezifischen Schlüssels zugelassen ist oder in der die Schlüssel für ein gegebenes System oder eine gegebene Anwendung wirksam bleiben

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.16

zugehöriger Schlüssel

bezüglich DLMS/COSEM ein symmetrischer Schlüssel, der innerhalb einer einzigen Instanz einer Anwendungsassoziation angewendet wird. Siehe auch Einmalschlüssel

3.2.17

überholt

nicht empfohlen für neue Implementierungen

3.2.18

digitale Signatur

Ergebnis einer kryptografischen Umwandlung von Daten, das bei ordnungsgemäßer Implementierung mit unterstützender Infrastruktur und nach einer Richtlinie folgende Dienste bereitstellt:

- 1) Authentifizierung des Ursprungs;
- 2) Datenintegrität; und
- 3) Nichtabstreitbarkeit des Unterzeichners

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.19

direkt vertrauenswürdige Zertifizierungsstelle

Zertifizierungsstelle, deren öffentlicher Schlüssel von einer Endinstanz eingeholt und auf sichere, vertrauenswürdige Weise gespeichert wurde, und deren öffentlicher Schlüssel von dieser Endinstanz im Zusammenhang mit einer oder mehreren Anwendungen anerkannt wird

[QUELLE: ISO/IEC 15945:2002, 3.4]

3.2.20

Schlüssel einer direkt vertrauenswürdigen Zertifizierungsstelle

öffentlicher Schlüssel einer direkt vertrauenswürdigen Zertifizierungsstelle. Er wurde von einer Endinstanz eingeholt und auf sichere, vertrauenswürdige Weise gespeichert. Er dient der Verifizierung von Zertifikaten, ohne selbst mittels eines von einer anderen Zertifizierungsstelle erzeugten Zertifikats verifiziert zu werden.

Anmerkung 1 zum Begriff: Direkt vertrauenswürdige Zertifizierungsstellen und Schlüssel von direkt vertrauenswürdigen Zertifizierungsstellen können sich von Instanz zu Instanz unterscheiden. Eine Instanz kann mehrere Zertifizierungsstellen als direkt vertrauenswürdige Zertifizierungsstellen betrachten.

[QUELLE: ISO/IEC 15945:2002, 3.5]

3.2.21

Verteilung

siehe Schlüsselverteilung

3.2.22

Domain-Parameter

Parameter, die mit einem kryptografischen Algorithmus angewendet werden, und einer Nutzer-Domain gemein sind

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.23

Verschlüsselung

Prozess der Umwandlung von Klartext in Chiffretext unter Anwendung eines kryptografischen Algorithmus und eines Schlüssels

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.24

flüchtiger Schlüssel

kryptografischer Schlüssel, der für jede Ausführung eines Schlüsseleinführungsprozesses erzeugt wird und der andere Anforderungen des Schlüsseltyps erfüllt (z. B. für jeden Nachrichtenaustausch oder jede Sitzung eindeutig zu sein). In bestimmten Fällen werden flüchtige Schlüssel innerhalb einer einzigen Sitzung mehr als einmal benutzt (z. B. bei Sammelaufrufen), wobei der Absender nur ein flüchtiges Schlüsselpaar je Nachricht erzeugt und der private Schlüssel mit dem öffentlichen Schlüssel jedes Empfängers gesondert kombiniert wird.

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.25

allgemeiner Schlüssel

Schlüssel, der zur Anwendung über einen relativ langen Zeitraum üblicherweise in vielen Instanzen einer DLMS/COSEM-Anwendungsassoziation vorgesehen ist, siehe auch statischer symmetrischer Schlüssel

3.2.26

Hash-Funktion

Funktion, die eine Bitfolge beliebiger Länge auf einer Bitfolge fester Länge abbildet. Anerkannte Hash-Funktionen erfüllen die folgenden Eigenschaften:

- 1) einseitige Ausrichtung: Für einen vorher spezifizierten Ausgabewert ist es mathematisch unmöglich, auf dessen Eingabewert zurückzuschließen; und
- 2) Kollisionsbeständigkeit: Es ist mathematisch unmöglich, einen zweiten Eingabewert zu finden, der denselben Ausgabewert ergibt.

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.27

Hash-Wert

Ergebnis der Anwendung einer Hash-Funktion auf eine Information

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.28

Initialisierungsvektor

IV

(en: initialization vector)

Vektor, der bei der Festlegung des Ausgangspunkts eines kryptografischen Prozesses angewendet wird

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.29

Identifizierung

Prozess der Verifizierung der Identität eines Nutzers, Prozesses oder Geräts, üblicherweise als Vorbedingung für die Gewährung des Zugriffs auf Ressourcen in einem IT-System

[QUELLE: NIST SP 800-47:2002]

3.2.30

Schlüssel

siehe kryptografischer Schlüssel

3.2.31

Schlüsselvereinbarung

Verfahren der Einführung eines (paarweisen) Schlüssels, bei dem das resultierende geheime Schlüsselmaterial von den Informationen abhängt, die von beiden Teilnehmern beigesteuert werden, so dass keine Partei den Wert des geheimen Schlüsselmaterials unabhängig von den Beiträgen der anderen Partei vorher bestimmen kann. Im Unterschied zu Schlüsselweitergabe

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.32

Schlüsselbestätigung

Verfahren der Bereitstellung einer Zusicherung für eine Partei (den Empfänger der Schlüsselbestätigung), dass eine andere Partei (der Anbieter der Schlüsselbestätigung) tatsächlich im Besitz des richtigen geheimen Schlüsselmaterials und/oder des gemeinsamen Geheimnisses ist

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.33

Schlüssel-Ableitungsfunktion

Funktion, mit der Schlüsselmaterial aus einem gemeinsamen Geheimnis (oder einem Schlüssel) und weiteren Informationen abgeleitet wird

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.34

Schlüsselverteilung

Weitergabe eines Schlüssels und von anderem Schlüsselmaterial von einer Instanz, der der Schlüssel entweder gehört oder die den Schlüssel erzeugt, zu einer anderen Instanz, die den Schlüssel benutzen soll

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.35

Schlüssel-Verschlüsselungsschlüssel

kryptografischer Schlüssel, der zur Verschlüsselung oder Entschlüsselung anderer Schlüssel verwendet wird

Anmerkung 1 zum Begriff: In DLMS/COSEM ist das der Masterschlüssel.

[QUELLE: NIST SP 800-57:2012, Teil 1, modifiziert durch Hinzufügen der Anmerkung]

3.2.36

Schlüsseleinführung

Verfahren, das zu Schlüsselmaterial führt, das von verschiedenen Parteien geteilt wird

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.37

Schlüsselpaar

öffentlicher Schlüssel und sein zugehöriger privater Schlüssel; ein Schlüsselpaar wird mit einem öffentlichen Schlüsselalgorithmus angewendet

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.38

Schlüsselaufhebung

Funktion im Lebenszyklus von Schlüsselmaterial; Vorgang, mit dem betroffenen Instanzen vor dem Ende der festgelegten Kryptoperiode des Schlüsselmaterials mitgeteilt wird, dass dieses Schlüsselmaterial operativ nicht mehr genutzt werden sollte

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.39

Schlüsselweitergabe

Verfahren der Einführung eines (paarweisen) Schlüssels, bei dem eine Partei (der Sender) einen Wert für das geheime Schlüsselmaterial auswählt und diesen Wert dann sicher an eine andere Partei (den Empfänger) verteilt. Im Unterschied zu Schlüsselvereinbarung

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.40

Schlüsselverpackung

Verfahren zur Verschlüsselung von Schlüsselmaterial (zusammen mit der zugehörigen Integritätsinformation), das sowohl Vertrauenswürdigkeit als auch den Schutz der Integrität unter Anwendung eines symmetrischen Schlüssels bietet

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.41

Nachrichtenauthentifizierungscode

MAC

(en: message authentication code)

mit einem symmetrischen Schlüssel erzeugte kryptografische Prüfsumme bei Daten, die sowohl versehentliche als auch beabsichtigte Änderungen von Daten erkennt

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.42

Message Digest

Ergebnis der Anwendung einer Hash-Funktion auf eine Nachricht. Auch als „Hash-Wert“ bekannt

[QUELLE: FIPS PUB 186-4:2013]

3.2.43

Standardkurve

(en: named curve)

eine Menge von ECDH-Domain-Parametern ist auch als „Kurve“ bekannt. Eine Kurve ist eine „Standardkurve“, wenn die Domain-Parameter gut bekannt und festgelegt sind und mit einem Objektbezeichner identifiziert werden können; anderenfalls wird sie als „Spezialkurve“ (en: custom curve) bezeichnet.

[QUELLE: RFC 5349, 2008]

3.2.44

Nonce

zeitlich veränderlicher Wert, bei dem meist eine hinreichend geringe Aussicht auf Wiederholung besteht. Beispielsweise darf die Nonce ein zufälliger Wert sein, der für jede Anwendung erneut erzeugt wird, ein Zeitstempel, eine Sequenznummer oder eine Kombination davon

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.45

Nichtabstreitbarkeit

Dienstleistung, die der Zusicherung der Integrität und des Ursprungs von Daten in einer solchen Weise dient, dass die Integrität und der Ursprung von einem Dritten als von einer bestimmten Instanz stammend, die in Besitz des privaten Schlüssels der beanspruchten Signatur ist, verifiziert werden kann

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.46

Passwort

Zeichenfolge (Buchstaben, Zahlen und andere Symbole), die dazu verwendet wird, eine Identität zu authentifizieren oder eine Zugriffsberechtigung zu verifizieren oder kryptografische Schlüssel abzuleiten

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.47

Klartext

verständliche Daten, die eine Bedeutung haben und ohne Anwendung einer Entschlüsselung verstanden werden können

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.48

privater Schlüssel

kryptografischer Schlüssel, der mit einem kryptografischen Algorithmus mit einem öffentlichen Schlüssel verwendet wird, und der eindeutig mit einer Instanz verbunden ist und nicht öffentlich gemacht wird. In einem asymmetrischen (öffentlichen) Kryptosystem ist der private Schlüssel mit einem öffentlichen Schlüssel verbunden. Abhängig vom Algorithmus darf der private Schlüssel beispielsweise verwendet werden, um:

- 1) den entsprechenden öffentlichen Schlüssel zu berechnen;
- 2) eine digitale Signatur zu berechnen, die von dem entsprechenden öffentlichen Schlüssel verifiziert werden darf;
- 3) Schlüssel zu dechiffrieren, die mit dem entsprechenden öffentlichen Schlüssel verschlüsselt waren; oder
- 4) ein gemeinsames Geheimnis während einer Schlüsselvereinbarungs-Transaktion zu berechnen.

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.49

geschützt

chiffriert und/oder digital signiert. Schutz darf bei xDLMS APDUs und/oder COSEM-Daten angewendet werden.

3.2.50

öffentlicher Schlüssel

kryptografischer Schlüssel, der mit einem kryptografischen Algorithmus mit einem öffentlichen Schlüssel verwendet wird, und der eindeutig mit einer Instanz verbunden ist und öffentlich gemacht werden darf. In einem asymmetrischen (öffentlichen) Kryptosystem ist der öffentliche Schlüssel mit einem privaten Schlüssel verbunden. Der öffentliche Schlüssel darf jedermann bekannt sein, und darf abhängig vom Algorithmus beispielsweise verwendet werden, um:

- 1) eine digitale Signatur zu verifizieren, die von dem entsprechenden privaten Schlüssel signiert ist;
- 2) Schlüssel zu chiffrieren, die mittels des entsprechenden privaten Schlüssels entschlüsselt werden können; oder
- 3) ein gemeinsames Geheimnis während einer Schlüsselvereinbarungs-Transaktion zu berechnen.

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.51

Zertifikat des öffentlichen Schlüssels

Datenstruktur, welche den/die Bezeichner einer Instanz, den öffentlichen Schlüssel der Instanz (einschließlich einer Angabe der damit zusammenhängenden Menge von Domain-Parametern) und möglicherweise weitere Informationen enthält, zusammen mit einer Signatur zu dieser Datenmenge, die von einer vertrauenswürdigen Partei, d. h. von einer Zertifizierungsstelle, generiert wird, wodurch der öffentliche Schlüssel an den/die eingeschlossenen Bezeichner gebunden wird

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.52

(asymmetrischer) kryptografischer Algorithmus mit einem öffentlichen Schlüssel

kryptografischer Algorithmus, der zwei zueinander in Beziehung stehende Schlüssel nutzt, einen öffentlichen Schlüssel und einen privaten Schlüssel. Die beiden Schlüssel haben die Eigenschaft, dass die Ermittlung des privaten Schlüssels aus dem öffentlichen Schlüssel mathematisch nicht möglich ist.

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.53

Infrastruktur des öffentlichen Schlüssels PKI

(en: Public Key Infrastructure)

Rahmen, der eingerichtet wird, um Zertifikate des öffentlichen Schlüssels auszustellen, aufrechtzuerhalten und aufzuheben

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.54

Empfänger <Schlüsselweitergabe>

Partei, die über eine Schlüsselweitergabe-Transaktion geheimes Schlüsselmaterial empfängt Im Unterschied zu Sender.

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.55

ein Zertifikat aufheben

vorzeitiges Beenden der Laufzeit eines Zertifikats mit Wirkung zu einem bestimmten Datum zu einer bestimmten Zeit

[QUELLE: NIST SP 800-32:2001]

3.2.56

Stammzertifizierungsstelle

Zertifizierungsstelle in einer hierarchischen Infrastruktur des öffentlichen Schlüssels, deren öffentlicher Schlüssel als vertrauenswürdiger Bezug (d. h. der Beginn von vertrauenswürdigen Pfaden) für eine Sicherheits-Domain dient

[QUELLE: NIST SP 800-32:2001]

3.2.57

geheimer Schlüssel

kryptografischer Schlüssel, der mit einem (symmetrischen) kryptografischen Algorithmus mit einem geheimen Schlüssel verwendet wird, und der eindeutig mit einer oder mehreren Instanz(en) verbunden ist und nicht öffentlich gemacht wird. Die Verwendung des Begriffs „geheim“ in diesem Zusammenhang unterstellt keine Klassifizierungsebene, sondern bedeutet eher die Notwendigkeit, den Schlüssel vor Enthüllung zu schützen

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.58

Sicherheitsdienste

Mechanismen, mit denen Vertraulichkeit, Datenintegrität, Authentifizierung und Nichtabstreitbarkeit von Informationen bereitgestellt werden

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.59

Sicherheitsstufe

(auch „Bits of Security“)

Nummer in Verbindung mit dem Aufwand (d. h. die Anzahl von Operationen), der erforderlich ist, um einen kryptographischen Algorithmus oder ein System zu brechen

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.60

selbst signiertes Zertifikat

Zertifikat des öffentlichen Schlüssels, dessen digitale Signatur durch den in dem Zertifikat enthaltenen öffentlichen Schlüssel verifiziert werden darf. Die Signatur auf einem selbst signierten Zertifikat schützt die Integrität der Daten, garantiert jedoch allerdings nicht die Authentizität der Informationen. Das Vertrauen in selbst signierte Zertifikate beruht auf den sicheren Verfahren, die bei ihrer Verteilung angewendet werden

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.61

Sender <Schlüsselweitergabe>

Partei, die bei einer Schlüsselweitergabe-Transaktion geheimes Schlüsselmaterial an den Empfänger sendet. Im Unterschied zu Empfänger

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.62

Sitzungsschlüssel

kryptografischer Schlüssel, der für die Anwendung über einen relativ kurzen Zeitraum eingeführt wird

Anmerkung 1 zum Begriff: In DLMS/COSEM ist der zugehörige Schlüssel ein Sitzungsschlüssel.

3.2.63

gemeinsames Geheimnis

geheimer Wert, der unter Anwendung eines Schlüsselvereinbarungs-Plans berechnet wurde und als Eingabe für ein(e) Schlüsselableitungs-Funktion/-verfahren genutzt wird

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.64

Signaturerzeugung

Anwendung eines digitalen Signaturalgorithmus und eines privaten Schlüssels zur Erzeugung einer digitalen Signatur für Daten

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.65

Signaturprüfung

Anwendung eines digitalen Signaturalgorithmus und eines öffentlichen Schlüssels zur Überprüfung einer digitalen Signatur für Daten

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.66

signierte Daten

Daten, für die eine digitale Signatur berechnet wurde

3.2.67

statischer symmetrischer Schlüssel

Schlüssel, der zur Anwendung über einen relativ langen Zeitraum üblicherweise in vielen Instanzen einer DLMS/COSEM-Anwendungsassoziation vorgesehen ist

Anmerkung 1 zum Begriff: In DLMS/COSEM ist er als allgemeiner Schlüssel bekannt.

3.2.68

statischer Schlüssel

Schlüssel, der zur Anwendung über einen relativ langen Zeitraum üblicherweise in vielen Instanzen eines kryptografischen Schlüsseleinführungs-Plans vorgesehen ist. Im Unterschied zu einem flüchtigen Schlüssel

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.69

nachgeordnete Zertifizierungsstelle

Zertifizierungsstelle (CA) in einer hierarchischen Infrastruktur des öffentlichen Schlüssels, deren Zertifikats-Signaturschlüssel von einer anderen CA zertifiziert wird, und deren Aktivitäten durch diese andere CA eingeschränkt werden

[QUELLE: NIST SP 800-32:2001]

3.2.70

symmetrischer Schlüssel

einzelner kryptografischer Schlüssel, der mit einem geheimen (symmetrischen) Schlüsselalgorithmus verwendet wird

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.71

symmetrischer Schlüsselalgorithmus

kryptografischer Algorithmus, der den gleichen geheimen Schlüssel für eine Operation und ihr Komplement verwendet (z. B. Verschlüsselung und Entschlüsselung)

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.72

Vertrauensanker

öffentlicher Schlüssel und Name einer Zertifizierungsstelle, die zur Validierung des ersten Zertifikats in einer Folge von Zertifikaten verwendet werden. Der öffentliche Schlüssel des Vertrauensankers wird zur Prüfung der Signatur auf einem Zertifikat verwendet, das von einer Vertrauensanker-Zertifizierungsstelle ausgestellt ist. Die Sicherheit des Validierungsprozesses hängt von der Authentizität und Integrität des Vertrauensankers ab. Vertrauensanker werden oft als selbst signierte Zertifikate verteilt

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.73

vertrauenswürdige Partei

Partei, die von einer Instanz mit der zuverlässigen Ausführung bestimmter Dienste für diese Instanz betraut wird. Eine Instanz könnte auch eine vertrauenswürdige Partei für sich selbst sein.

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.74

vertrauenswürdiger Dritter

Dritter, wie z. B. eine CA, dem von seinen Clients die Durchführung bestimmter Dienste anvertraut wird. (Im Unterschied dazu werden die Teilnehmer an einer Schlüsseleinführungs-Transaktion, die Partei U und die Partei V, als Erst- und Zweitpartei betrachtet).

[QUELLE: NIST SP 800-56A Rev. 2: 2013]

3.2.75

X.509-Zertifikat

das X.509-Zertifikat des öffentlichen Schlüssels oder das X.509-Attributzzertifikat, wie in der Norm ISO/ITU-T X.509 festgelegt. Am häufigsten (einschließlich in diesem Dokument) bezieht sich ein X.509-Zertifikat auf das X.509-Zertifikat des öffentlichen Schlüssels

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.2.76

X.509-Zertifikat des öffentlichen Schlüssels

digitales Zertifikat, das einen öffentlichen Schlüssel für eine Instanz und einen Namen für die Instanz zusammen mit einigen weiteren Informationen enthält, und das fälschungssicher ausgeführt ist durch die digitale Signatur der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, das in dem in der Norm ISO/ITU-T X.509 festgelegten Format codiert ist

[QUELLE: NIST SP 800-57:2012, Teil 1]

3.3 Begriffe und Abkürzungen, die sich auf den Galois-/Zählermodus beziehen

Die Quelle der Begriffe 3.3.1 bis 3.3.13 ist NIST SP 800-38D:2007.

3.3.1

zusätzliche authentifizierte Daten

AAD

(en: Additional Authenticated Data)

Eingabedaten für die authentifizierte Verschlüsselungsfunktion, die authentifiziert, aber nicht verschlüsselt sind

3.3.2

authentifizierte Entschlüsselung

Funktion des Galois-/Zählermodus (GCM, en: Galois/Counter Mode), bei der der Chiffretext in den Klartext entschlüsselt wird, und die Authentizität des Chiffretexts und die AAD verifiziert werden

3.3.3

authentifizierte Verschlüsselung

Funktion des Galois-/Zählermodus (GCM, en: Galois/Counter Mode), bei der der Klartext in den Chiffretext verschlüsselt wird, und ein Authentifizierungs-Tag für die AAD und den Chiffretext erzeugt wird

3.3.4

Authentifizierungs-Tag

Tag, T

kryptografische Prüfsumme bei Daten, die so ausgelegt ist, dass sowohl versehentliche Fehler als auch die absichtliche Änderung der Daten enthüllt werden

3.3.5

Blockverschlüsselung

parametrierte Familie von Permutationen von Bitfolgen einer festen Länge; der Parameter, der die Permutation bestimmt, ist eine Bitfolge, die als der Schlüssel bezeichnet wird

3.3.6

Chiffretext

verschlüsselte Form des Klartexts

3.3.7

festes Feld

bei der deterministischen Konstruktion von Initialisierungsvektoren (IV) das Feld, welches das Gerät oder den Kontext für die Instanz der authentifizierten Verschlüsselungsfunktion identifiziert

3.3.8

neu

Eigenschaft eines neu erzeugten Schlüssels, verschieden von jedem zuvor benutzten Schlüssel zu sein

3.3.9

GCM

Galois-/Zählermodus (en: Galois/Counter Mode)

3.3.10

Initialisierungsvektor

IV

(en: initialization vector)

Nonce, die mit einem Aufruf einer authentifizierten Verschlüsselung bei einem bestimmten Klartext und AAD verbunden ist

Anmerkung 1 zum Begriff: Für die Anwendung dieses Dokuments ist das Aufruffeld der Aufrufzähler.

3.3.11

Aufruffeld

bei der deterministischen Konstruktion von Initialisierungsvektoren (IV) das Feld, welches die Eingabesätze für die authentifizierte Verschlüsselungsfunktion bei einem bestimmten Gerät oder in einem bestimmten Kontext identifiziert

3.3.12

Schlüssel

Parameter der Blockverschlüsselung, welcher die Auswahl der vorwärts gerichteten Verschlüsselungsfunktion (en: forward cipher function) aus der Familie von Permutationen bestimmt

3.3.13

Klartext

P

Eingabedaten für die authentifizierte Verschlüsselungsfunktion, die sowohl authentifiziert als auch verschlüsselt sind

3.3.14

Security Control Byte

SC

Byte, das Informationen über die angewendete Chiffrierung bereitstellt

3.3.15

Security Header

SH

Verknüpfung des Security Control Bytes *SC* mit dem Aufrufzähler: $SH = SC \parallel IC$

3.4 Allgemeine Abkürzungen

Abkürzung	Bedeutung
.cnf	Dienstelement Bestätigung (en: confirm service primitive)
.ind	Dienstelement Meldung (en: indication service primitive)
.req	Dienstelement Anforderung (en: request service primitive)
.res	Dienstelement Antwort (en: response service primitive)
AA	Anwendungsassoziation (en: Application Association)
AARE	A-Associate-Antwort – eine APDU des ACSE (en: A-Associate Response)
AARQ	A-Associate-Anforderung – eine APDU des ACSE (en: A-Associate Request)
ACPM	Protokollmaschine der Assoziationssteuerung (en: Association Control Protocol Machine)
ACSE	Dienstelement der Assoziationssteuerung (en: Association Control Service Element)
AE	Anwendungsinstanz (en: Application Entity)
AES	erweiterter Verschlüsselungsstandard (en: Advanced Encryption Standard)
AL	Anwendungsschicht (en: Application Layer)
AP	Anwendungsprozess (en: Application Process)
APDU	Protokolldateneinheit der Anwendungsschicht (en: Application Layer Protocol Data Unit)
API	Anwendungsprogrammierschnittstelle (en: Application Programming Interface)
ASE	Anwendungsdienstelement (en: Application Service Element)
ASO	Anwendungsdienstobjekt (en: Application Service Object)
ATM	asynchroner Transfermodus (en: Asynchronous Transfer Mode)
A-XDR	angepasste erweiterte Datendarstellung (en: Adapted Extended Data Representation)
base_name	Kurzname (short_name), der dem ersten Attribut (logical_name) eines COSEM-Objekts entspricht

Abkürzung	Bedeutung
BER	grundlegende Codierungsregeln (en: Basic Encoding Rules)
BD	Blockdaten (en: Block Data)
BN	Blocknummer (en: Block Number)
BNA	Blocknummer quittiert (en: Block Number Acknowledged)
BS	Bitfolge (en: Bit string)
BTS	Blocktransfer-Streaming (en: Block Transfer Streaming)
BTW	Blocktransfer-Fenster (en: Block Transfer Window)
CA	Zertifizierungsstelle (en: Certification Authority)
CF	Steuerfunktion (en: Control Function)
CL	verbindungsfrei (en: Connectionless)
class_id	Klassenbezeichner für die COSEM-Schnittstelle (en: COSEM interface class identification code)
CMP	Zertifikat-Verwaltungsprotokoll (en: Certificate Management Protocol). Siehe RFC 4210.
CO	verbindungsorientiert (en: Connection-oriented)
COSEM	Firmenspezifikation für die Gebührenerfassung des Energieverbrauchs (en: Companion Specification for Energy Metering)
COSEM_on_IP	das TCP-UDP/IP-basierte COSEM-Kommunikationsprofil
CRC	zyklische Redundanzprüfung (en: Cyclic Redundancy Check)
CRL	Zertifikatsperrliste (en: Certificate revocation list). Siehe RFC 5280.
CSR	Zertifikatsignierungsanforderung (en: Certificate Signing Request)
DCE	Datenkommunikationsausrüstung (Kommunikationsschnittstelle oder Modem) (en: Data Communication Equipment (communications interface or modem))
DCS	Datenerfassungssystem (en: Data Collection System)
DISC	Abbruch (ein HDLC-Rahmentyp) (en: Disconnect (a HDLC frame type))
DLMS	standardisierte Sprache für die Zählerkommunikation (en: Device Language Message Specification)
DM	Modus Abgebrochen (ein HDLC-Rahmentyp) (en: Disconnected Mode (a HDLC frame type))
DSA	digitaler Signaturalgorithmus, festgelegt in FIPS PUB 186-4:2013 (en: Digital Signature Algorithm)
DSAP	Dienstzugangspunkt der Datenverbindung (en: Data Link Service Access Point)

Abkürzung	Bedeutung
DSO	Energieverteilnetzbetreiber (en: Energy Distribution System Operator)
DTE	Datenstationseinrichtung (Rechner, Endgeräte oder Drucker) (en: Data Terminal Equipment (computers, terminals or printers))
ECC	Elliptische-Kurven-Kryptografie (en: Elliptic Curve Cryptography)
ECDH	Elliptische-Kurven-Diffie-Hellman-Schlüsselvereinbarungsprotokoll (en: Elliptic Curve Diffie-Hellman key agreement protocol)
ECDSA	digitaler Elliptische-Kurven-Signaturalgorithmus, festgelegt in ANSI X9.62 und FIPS PUB 186-4:2013 (en: Elliptic Curve Digital Signature Algorithm)
ECP	elliptischer Kurvenpunkt (en: Elliptic Curve Point)
EUI-64	erweiterter eindeutiger 64-Bit-Bezeichner (en: 64-bit Extended Unique Identifier)
FCS	Blockprüfzeichenfolge (en: Frame Check Sequence)
FDDI	Datenschnittstelle für Glasfasernetzwerke (en: Fibre Distributed Data Interface)
FE	Feldelement (bezogen auf öffentliche Schlüsselalgorithmen)
FIPS	Federal Information Processing Standard (Bundesstandard für Informationsverarbeitung)
FRMR	Blockrückweisung (ein HDLC-Rahmentyp) (en: Frame Reject (a HDLC frame type))
FTP	Dateiübertragungsprotokoll File Transfer Protocol
GAK	allgemeiner Authentifizierungsschlüssel (en: Global Authentication Key)
GBEK	globaler Broadcast-Verschlüsselungsschlüssel (en: Global Broadcast Encryption Key)
GBT	allgemeine Blockübertragung (en: General Block Transfer)
GCM	Galois-/Zähler-Modus, ein Algorithmus für eine authentifizierte Verschlüsselung mit zugehörigen Daten (en: Galois/Counter Mode)
GMAC	eine Spezialisierung des GCM für die Erzeugung eines nicht verschlüsselten Nachrichtenauthentifizierungscodes (MAC) von Daten
GMT	westeuropäische Zeit (en: Greenwich Mean Time)
GSM	globales System für mobile Kommunikation (en: Global System for Mobile communications)
GUEK	globaler Unicast-Verschlüsselungsschlüssel (en: Global Unicast Encryption Key)
GW	Gateway
HCS	Header-Prüfzeichenfolge (en: Header Check Sequence)
HDLC	Datenverknüpfungssteuerung der höchsten Ebene (en: High-level Data Link Control)
HES	Head-End-System, auch bekannt als Datenerfassungssystem ANMERKUNG Eigentümer des HES kann der Energiedienstleister oder der Netzbetreiber sein.
HHU	Handgerät (en: Hand Held Unit)

Abkürzung	Bedeutung
HLS	höchste Sicherheit (COSEM) (en: High Level Security (COSEM))
HMAC	verschlüsselter Hash-Nachrichtenauthentifizierungscode, der in FIPS 198-1 festgelegt ist (en: Keyed-Hash Message Authentication Code)
HSM	Hardware-Sicherheitsmodul (en: Hardware Security Module)
HTTP	Hypertext-Übertragungsprotokoll (en: Hypertext Transfer Protocol)
I	Information (ein HDLC-Rahmentyp) (en: Information (a HDLC frame type))
IANA	Internet Assigned Numbers Authority
IC	Schnittstellenklasse (en: Interface Class)
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internetprotokoll (en: Internet Protocol)
ISO	Internationale Organisation für Normung (en: International Organization for Standardization)
IV	Initialisierungsvektor (en: Initialization Vector)
KEK	Schlüssel-Verschlüsselungsschlüssel (en: Key Encrypting Key)
LAN	lokales Netzwerk (en: Local Area Network)
LB	letzter Block (en: Last Block)
LDN	Name des logischen Geräts (en: Logical Device Name)
LLC	logische Verknüpfungssteuerung (Teilschicht) (en: Logical Link Control)
LLS	niedrigste Sicherheitsstufe (en: Low Level Security)
LNAP	Zugangspunkt eines lokalen Netzwerks (en: Local Network Access Point)
LPDU	LLC-Protokolldateneinheit (en: LLC Protocol Data Unit)
L-SAP	Dienstzugangspunkt der LLC-Teilschicht (en: LLC sublayer Service Access Point)
LSB	niedrigstwertiges Bit (en: Least Significant Bit)
LSDU	LLC-Dienst-Dateneinheit (en: LLC Service Data Unit)
m	vorgeschrieben, verwendet in Verbindung mit Attribut- und Verfahrensdefinitionen
MAC	Medienzugriffssteuerung (Teilschicht) (en: Medium Access Control)
MAC	Nachrichtenauthentifizierungscode (Kryptography) (en: Message Authentication Code)
MIB	Verwaltungsinformationsbasis (en: Management Information Base)

Abkürzung	Bedeutung
MSAP	Dienstzugangspunkt der MAC-Teilschicht (im HDLC-basierten Profil entspricht dieser der HDLC-Adresse) (en: MAC sublayer Service Access Point)
MSB	höchstwertiges Bit (en: Most Significant Bit)
MSC	Nachrichtenfolgediagramm (en: Message Sequence Chart)
MSDU	MAC-Dienst-Dateneinheit (en: MAC Service Data Unit)
N(R)	Empfangssequenz-Nummer (en: Receive sequence Number)
N(S)	Sendesequenz-Nummer (en: Send sequence Number)
NDM	abhängiger Wartebetrieb (en: Normal Disconnected Mode)
NIST	National Institute of Standards and Technology
NNAP	Zugangspunkt eines Neighbourhood Networks (en: Neighbourhood Network Access Point)
NRM	Aufforderungsbetrieb (en: Normal Response Mode)
o	freigestellt, verwendet in Verbindung mit Attribut- und Verfahrensdefinitionen
OBIS	Objektidentifikationssystem (en: Object Identification System)
OCSP	Online-Zertifikat-Statusprotokoll (en: Online Certificate Status Protocol)
OID	Objektbezeichner (en: Object Identifier)
OOB	außerhalb des Bandes (en: Out of Band)
OS	Oktett-Folge (en: Octet string)
OSI	Kommunikation offener Systeme (en: Open System Interconnection)
OTA	über die Luft (en: Over The Air)
P/F	Poll-Bit/Final-Bit (en: Poll/Final)
PAR	positive Bestätigung mit erneuter Übertragung (en: Positive Acknowledgement with Retransmission)
PDU	Protokolldateneinheit (en: Protocol Data Unit)
PhL	Bitübertragungsschicht (en: Physical Layer)
PHSDU	PH-SDU
PKCS	Standard für asymmetrische Kryptografie, festgelegt von RSA Laboratories
PKI	Infrastruktur des öffentlichen Schlüssels (en: Public Key Infrastructure)
PLC	Trägerfrequenzübertragung auf Hochspannungsleitungen (TFH) (en: Power line carrier)

Abkürzung	Bedeutung
PPP	Punkt-zu-Punkt-Protokoll (en: Point-to-Point Protocol)
PSDU	Dienst-Dateneinheit der Bitübertragungsschicht (en: Physical layer Service Data Unit)
PSTN	öffentliches Telefonnetz (en: Public Switched Telephone Network)
RA	Registrierungsstelle (en: Registration Authority)
RLRE	A-Release-Antwort – eine APDU des ACSE (en: A-Release Response)
RLRQ	A-Release-Anforderung – eine APDU des ACSE (en: A-Release Request)
RNG	Zufallszahlengenerator (en: Random Number Generator)
RNR	nicht empfangsbereit (ein HDLC-Rahmentyp) (en: Receive Not Ready (a HDLC frame type))
RR	empfangsbereit (ein HDLC-Rahmentyp) (en: Receive Ready (a HDLC frame type))
RSA	Algorithmus, der von Rivest, Shamir und Adelman entwickelt wurde; festgelegt in ANS X9.31 und PKCS #1.
SAP	Dienstzugangspunkt (en: Service Access Point)
SDU	Dienst-Dateneinheit (en: Service Data Unit)
SHA	sicherer Hash-Algorithmus; festgelegt in FIPS PUB 180-4:2012 (en: Secure Hash Algorithm)
SNMP	einfaches Netzwerkverwaltungsprotokoll (en: Simple Network Management Protocol)
SNRM	Aufforderungsbetrieb einstellen (ein HDLC-Rahmentyp) (en: Set Normal Response Mode (a HDLC frame type))
STR	Streaming
tbsCertificate	zu signierendes Zertifikat (en: To be signed certificate)
TCP	Übertragungssteuerungsprotokoll (en: Transmission Control Protocol)
TDEA	Triple-Datenverschlüsselungsalgorithmus (en: Triple Data Encryption Algorithm)
TL	Transportschicht (en: Transport Layer)
TPDU	Protokolldateneinheit der Transportschicht (en: Transport Layer Protocol Data Unit)
TWA	wechselseitige Datenübermittlung (en: Two Way Alternate)
UA	Bestätigung ohne Folgenummer (ein HDLC-Rahmentyp) (en: Unnumbered Acknowledge (a HDLC frame type))
UDP	Benutzer-Datagramm-Protokoll (en: User Datagram Protocol)
UI	nicht nummerierte Information (ein HDLC-Rahmentyp) (en: Unnumbered Information (a HDLC frame type))

Abkürzung	Bedeutung
UNC	Klasse unsymmetrischer Konfigurationen im Aufforderungsbetrieb (en: Unbalanced operation Normal response mode Class)
USS	nicht nummerierter Sendestatus (en: Unnumbered Send Status)
V(R)	Variable des Empfangszustands (en: Receive state Variable)
V(S)	Variable des Sendezustands (en: Send state Variable)
VAA	virtuelle Anwendungsassoziation (en: Virtual Application Association)
WPDU	Wrapper-Protokolldateneinheit (en: Wrapper Protocol Data Unit)
xDLMS ASE	erweitertes DLMS-Anwendungsdienstelement (en: Extended DLMS Application Service Element)
Siehe auch die Auflistung der Abkürzungen, die sich speziell auf einen kryptografischen Algorithmus beziehen, in den entsprechenden Abschnitten.	

3.5 Symbole, die sich auf den Galois-/Zählermodus beziehen

Symbol	Bedeutung
A	zusätzliche authentifizierte Daten, AAD
AK	Authentifizierungsschlüssel, ein Parameter, der Teil der AAD ist
C	Chiffretext
EK	Verschlüsselungs-Schlüssel, d. h. der Blockverschlüsselungs-Schlüssel
IC	Aufrufzähler, Teil des Initialisierungsvektors. Siehe auch Aufruffeld.
IV	Initialisierungsvektor
$\text{len}(X)$	Die Bit-Länge der Bitfolge X .
$\text{LEN}(X)$	Die Oktett-Länge der Oktettfolge X .
P	Klartext
SC	Security Control Byte
SH	Security Header
$_{\text{Sys-}T}$	Systemtitel
T	Authentifizierungs-Tag
t	Die Bit-Länge des Authentifizierungs-Tags. ANMERKUNG Dies entspricht $\text{len}(T)$.
$X \parallel Y$	Verknüpfung der beiden Folgen X und Y .

3.6 Symbole, die sich auf den ECDSA-Algorithmus beziehen

Symbol	Bedeutung
d	Der private Schlüssel der ECDSA, bei dem es sich um eine Ganzzahl im Bereich $[1, n - 1]$ handelt.
$Q = (x_Q, y_Q)$	Ein öffentlicher Schlüssel der ECDSA. Die Koordinaten x_Q und y_Q sind Ganzzahlen im Bereich $[0, q - 1]$, und $Q = dG$.
k	Die Geheimnummer je Nachricht der ECDSA, bei der es sich um eine Ganzzahl im Bereich $[1, n - 1]$ handelt.
r	Eine Komponente einer digitalen Signatur der ECDSA. Es ist eine Ganzzahl im Bereich $[1, n - 1]$. Siehe die Definition von (r, s) .
s	Eine Komponente einer digitalen Signatur der ECDSA. Es ist eine Ganzzahl im Bereich $[1, n - 1]$. Siehe die Definition von (r, s) .
(r, s)	Eine digitale Signatur der ECDSA, wobei r und s die Komponenten der digitalen Signatur sind.
M	Die Nachricht, die unter Anwendung des digitalen Signaturalgorithmus signiert wird.
$\text{Hash}(M)$	Das Ergebnis einer Hash-Berechnung (Message Digest oder Hash-Wert) für Nachricht M unter Anwendung einer anerkannten Hash-Funktion.

3.7 Symbole, die sich auf die Schlüsselvereinbarungs-Algorithmen beziehen

Symbol	Bedeutung
$d_{e,U}, d_{e,V}$	Flüchtige private Schlüssel von Partei U und Partei V. Dabei handelt es sich um Ganzzahlen im Bereich $[1, n-1]$.
$d_{s,U}, d_{s,V}$	Statische private Schlüssel von Partei U und Partei V. Dabei handelt es sich um Ganzzahlen im Bereich $[1, n-1]$.
ID_U	Der Bezeichner der Partei U (der Initiator).
ID_V	Der Bezeichner der Partei V (der Responder).
$Q_{e,U}, Q_{e,V}$	Flüchtige öffentliche Schlüssel von Partei U und Partei V. Dabei handelt es sich um Punkte auf der elliptischen Kurve, die von den Domain-Parametern bestimmt werden.
$Q_{s,U}, Q_{s,V}$	Statische öffentliche Schlüssel von Partei U und Partei V. Dabei handelt es sich um Punkte auf der elliptischen Kurve, die von den Domain-Parametern bestimmt werden.
U, V	stellen die beiden Parteien in einem (paarweisen) Schlüsseleinrichtungsplan dar.
Z	Ein gemeinsames Geheimnis (dargestellt als Byte-Folge), das genutzt wird, um geheimes Schlüsselmaterial unter Anwendung eines Schlüsselableitungsverfahrens abzuleiten. [Quelle: NIST SP 800-56A Rev. 2:2013]

– Leerseite –

NORME EUROPÉENNE

EUROPÄISCHE NORM

November 2017

ICS 17.220; 35.110; 91.140.50

Supersedes EN 62056-5-3:2016

English Version

Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer (IEC 62056-5-3:2017)

Échange des données de comptage de l'électricité - La
suite DLMS/COSEM - Partie 5-3: Couche application
DLMS/COSEM
(IEC 62056-5-3:2017)

Datenkommunikation der elektrischen Energiemessung -
DLMS/COSEM - Teil 5-3: DLMS/COSEM-
Anwendungsschicht
(IEC 62056-5-3:2017)

This European Standard was approved by CENELEC on 2017-09-14. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2017 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

European foreword

The text of document 13/1744/FDIS, future edition 3 of IEC 62056-5-3, prepared by IEC/TC 13 "Electrical energy measurement and control" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62056-5-3:2017.

The following dates are fixed:

- latest date by which the document has to be (dop) 2018-06-14
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2020-09-14
standards conflicting with the
document have to be withdrawn

This document supersedes EN 62056-5-3:2016.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62056-5-3:2017 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61334-4-32:1996	NOTE	Harmonized as EN 61334-4-32:1996.
IEC 61334-4-511:2000	NOTE	Harmonized as EN 61334-4-511:2000.
IEC 61334-4-512:2000	NOTE	Harmonized as EN 61334-4-512:2001.
IEC 61334-5-1:2001	NOTE	Harmonized as EN 61334-5-1:2001.
IEC 62056-1-0	NOTE	Harmonized as EN 62056-1-0.
IEC 62056-6-1:2017 ¹⁾	NOTE	Harmonized as FprEN 62056-6-1:2017.
IEC 62056-7-3:2017	NOTE	Harmonized as EN 62056-7-3:2017.
IEC 62056-7-6:2013	NOTE	Harmonized as EN 62056-7-6:2013.
IEC 62056-9-7:2013	NOTE	Harmonized as EN 62056-9-7:2013.
IEC 62056-8-5	NOTE	Harmonized as EN 62056-8-5.
IEC 62056-8-5	NOTE	Harmonized as EN 62056-8-5.

1) To be published. At draft stage.

CONTENTS

European Foreword	2
INTRODUCTION	12
1 Scope	13
2 Normative references	13
3 Terms, definitions, abbreviated terms and symbols	15
3.1 General DLMS/COSEM definitions	15
3.2 Definitions related to cryptographic security	18
3.3 Definitions and abbreviated terms related to the Galois/Counter Mode	28
3.4 General abbreviated terms	30
3.5 Symbols related to the Galois/Counter Mode	34
3.6 Symbols related the ECDSA algorithm	34
3.7 Symbols related to the key agreement algorithms	34
4 Overview of DLMS/COSEM	35
4.1 Information exchange in DLMS/COSEM	35
4.1.1 General	35
4.1.2 Communication model	35
4.1.3 Naming and addressing	37
4.1.4 Connection oriented operation	39
4.1.5 Application associations	40
4.1.6 Messaging patterns	42
4.1.7 Data exchange between third parties and DLMS/COSEM servers	42
4.1.8 Communication profiles	43
4.1.9 Model of a DLMS/COSEM metering system	44
4.1.10 Model of DLMS/COSEM servers	45
4.1.11 Model of a DLMS/COSEM client	46
4.1.12 Interoperability and interconnectivity in DLMS/COSEM	48
4.1.13 Ensuring interconnectivity: the protocol identification service	48
4.1.14 System integration and meter installation	48
4.2 DLMS/COSEM application layer main features	49
4.2.1 General	49
4.2.2 DLMS/COSEM application layer structure	49
4.2.3 The Association Control Service Element, ACSE	50
4.2.4 The xDLMS application service element	51
4.2.5 Layer management services	58
4.2.6 Summary of DLMS/COSEM application layer services	58
4.2.7 DLMS/COSEM application layer protocols	59
5 Information security in DLMS/COSEM	59
5.1 Overview	59
5.2 The DLMS/COSEM security concept	60
5.2.1 Overview	60
5.2.2 Identification and authentication	60
5.2.3 Security context	63
5.2.4 Access rights	63
5.2.5 Application layer message security	63
5.2.6 COSEM data security	65

5.3	Cryptographic algorithms.....	66
5.3.1	Overview	66
5.3.2	Hash function.....	66
5.3.3	Symmetric key algorithms.....	67
5.3.4	Public key algorithms	73
5.3.5	Random number generation.....	84
5.3.6	Compression.....	85
5.3.7	Security suite	85
5.4	Cryptographic keys – overview	86
5.5	Key used with symmetric key algorithms	86
5.5.1	Symmetric keys types.....	86
5.5.2	Key information with general-ciphering APDU and data protection	88
5.5.3	Key identification.....	89
5.5.4	Key wrapping	89
5.5.5	Key agreement	89
5.5.6	Symmetric key cryptoperiods.....	90
5.6	Keys used with public key algorithms	90
5.6.1	Overview	90
5.6.2	Key pair generation.....	91
5.6.3	Public key certificates and infrastructure	91
5.6.4	Certificate and certificate extension profile	94
5.6.5	Suite B end entity certificate types to be supported by DLMS/COSEM servers	102
5.6.6	Management of certificates	103
5.7	Applying cryptographic protection.....	108
5.7.1	Overview	108
5.7.2	Protecting xDLMS APDUs	108
5.7.3	Multi-layer protection by multiple parties	121
5.7.4	HLS authentication mechanisms	122
5.7.5	Protecting COSEM data.....	125
6	DLMS/COSEM application layer service specification	126
6.1	Service primitives and parameters	126
6.2	The COSEM-OPEN service.....	128
6.3	The COSEM-RELEASE service.....	133
6.4	COSEM-ABORT service.....	136
6.5	Protection and general block transfer parameters	136
6.6	The GET service	141
6.7	The SET service	144
6.8	The ACTION service	148
6.9	The ACCESS service	151
6.9.1	Overview – Main features	151
6.9.2	Service specification	153
6.10	The DataNotification service	158
6.11	The EventNotification service	159
6.12	The TriggerEventNotificationSending service	160
6.13	Variable access specification	161
6.14	The Read service	161
6.15	The Write service	165

6.16	The UnconfirmedWrite service.....	168
6.17	The InformationReport service	170
6.18	Client side layer management services: the SetMapperTable.request	171
6.19	Summary of services and LN/SN data transfer service mapping.....	171
7	DLMS/COSEM application layer protocol specification.....	173
7.1	The control function.....	173
7.1.1	State definitions of the client side control function	173
7.1.2	State definitions of the server side control function.....	174
7.2	The ACSE services and APDUs.....	176
7.2.1	ACSE functional units, services and service parameters	176
7.2.2	Registered COSEM names.....	179
7.2.3	APDU encoding rules.....	182
7.2.4	Protocol for application association establishment.....	182
7.2.5	Protocol for application association release	187
7.3	Protocol for the data transfer services	191
7.3.1	Negotiation of services and options – the conformance block.....	191
7.3.2	Confirmed and unconfirmed service invocations	192
7.3.3	Protocol for the GET service.....	193
7.3.4	Protocol for the SET service	197
7.3.5	Protocol for the ACTION service	200
7.3.6	Protocol for the ACCESS service	202
7.3.7	Protocol of the DataNotification service	204
7.3.8	Protocol for the EventNotification service.....	204
7.3.9	Protocol for the Read service.....	204
7.3.10	Protocol for the Write service	208
7.3.11	Protocol for the UnconfirmedWrite service.....	213
7.3.12	Protocol for the InformationReport service.....	214
7.3.13	Protocol of general block transfer mechanism	215
8	Abstract syntax of ACSE and COSEM APDUs	226
9	COSEM APDU XML schema	240
9.1	General	240
9.2	XML Schema	240
Annex A (normative)	Using the DLMS/COSEM application layer in various communications profiles	262
A.1	General	262
A.2	Targeted communication environments.....	262
A.3	The structure of the profile	262
A.4	Identification and addressing schemes	262
A.5	Supporting layer services and service mapping	263
A.6	Communication profile specific parameters of the COSEM AL services	263
A.7	Specific considerations / constraints using certain services within a given profile.....	263
A.8	The 3-layer, connection-oriented, HDLC based communication profile	263
A.9	The TCP-UDP/IP based communication profiles (COSEM_on_IP).....	263
A.10	The wired and wireless M-Bus communication profiles	263
A.11	The S-FSK PLC profile.....	263
Annex B (normative)	SMS short wrapper.....	264
Annex C (normative)	Gateway protocol.....	265

C.1	General.....	265
C.2	The gateway protocol	266
C.3	HES in the WAN/NN acting as Initiator (Pull operation).....	266
C.4	End devices in the LAN acting as Initiators (Push operation).....	268
C.4.1	General.....	268
C.4.2	End device with WAN/NN knowledge.....	268
C.4.3	End devices without WAN/NN knowledge	269
C.5	Security	269
Annex D (informative)	AARQ and AARE encoding examples	270
D.1	General.....	270
D.2	Encoding of the xDLMS InitiateRequest / InitiateResponse APDU	270
D.3	Specification of the AARQ and AARE APDUs	273
D.4	Data for the examples	274
D.5	Encoding of the AARQ APDU	275
D.6	Encoding of the AARE APDU	278
Annex E (informative)	Encoding examples: AARQ and AARE APDUs using a ciphered application context.....	284
E.1	A-XDR encoding of the xDLMS InitiateRequest APDU, carrying a dedicated key	284
E.2	Authenticated encryption of the xDLMS InitiateRequest APDU	285
E.3	The AARQ APDU	286
E.4	A-XDR encoding of the xDLMS InitiateResponse APDU	288
E.5	Authenticated encryption of the xDLMS InitiateResponse APDU	289
E.6	The AARE APDU.....	290
E.7	The RLRQ APDU (carrying a ciphered xDLMS InitiateRequest APDU).....	292
E.8	The RLRE APDU (carrying a ciphered xDLMS InitiateResponse APDU)	293
Annex F (informative)	Data transfer service examples.....	294
F.1	GET / Read, SET / Write examples	294
F.2	ACCESS service example	311
F.3	Compact array encoding example.....	312
F.3.1	General.....	312
F.3.2	The specification of compact-array	313
F.3.3	Example 1: Compact array encoding an array of five long-unsigned values.	314
F.3.4	Example 2: Compact-array encoding of five octet-string values.....	315
F.3.5	Example 3: Encoding of the buffer of a Profile generic object	316
Annex G (normative)	NSA Suite B elliptic curves and domain parameters	319
Annex H (informative)	Example of an End entity signature certificate using P-256 signed with P-256	321
Annex I (normative)	Use of key agreement schemes in DLMS/COSEM.....	323
I.1	Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme	323
I.2	One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme.....	327
I.3	Static Unified Model C(0e, 2s, ECC CDH) scheme.....	331
Annex J (informative)	Exchanging protected xDLMS APDUs between TP and server	335
J.1	General.....	335
J.2	Example 1: Protection is the same in the two directions	335
J.3	Example 2: Protection is different in the two directions	336
Annex K (informative)	Significant technical changes with respect to IEC 62056-5-3:2016.	339
Bibliography		342

Index.....	347
Annex ZA (normative) Normative references to international publications with their corresponding European publications.....	364
Figure 1 – Client–server model and communication protocols	36
Figure 2 – Naming and addressing in DLMS/COSEM	37
Figure 3 – A complete communication session in the CO environment.....	40
Figure 4 – DLMS/COSEM messaging patterns.....	42
Figure 5 – DLMS/COSEM generic communication profile	44
Figure 6 – Model of a DLMS/COSEM metering system	45
Figure 7 – DLMS/COSEM server model	46
Figure 8 – Model of a DLMS/COSEM client using multiple protocol stacks.....	47
Figure 9 – The structure of the DLMS/COSEM application layers	49
Figure 10 – The concept of composable xDLMS messages.....	56
Figure 11 – Summary of DLMS/COSEM AL services	59
Figure 12 – Authentication mechanisms.....	61
Figure 13 – Client – server message security concept.....	64
Figure 14 – End-to-end message security concept.....	65
Figure 15 – Hash function	67
Figure 16 – Encryption and decryption.....	68
Figure 17 – Message Authentication Codes (MACs).....	69
Figure 18 – GCM functions.....	70
Figure 19 – Digital signatures.....	77
Figure 20 – C(2e, 0s) scheme: each party contributes only an ephemeral key pair.....	79
Figure 21 – C(1e, 1s) schemes: party U contributes an ephemeral key pair, and party V contributes a static key pair.....	80
Figure 22 – C(0e, 2s) scheme: each party contributes only a static key pair.....	82
Figure 23 – Architecture of a Public Key Infrastructure (example).....	93
Figure 24 – MSC for provisioning the server with CA certificates.....	104
Figure 25 – MSC for security personalisation of the server	105
Figure 26 – Provisioning the server with the certificate of the client	106
Figure 27 – Provisioning the client / third party with a certificate of the server	107
Figure 28 – Remove certificate from the server.....	107
Figure 29 – Cryptographic protection of information using AES-GCM	111
Figure 30 – Structure of service-specific global / dedicated ciphering xDLMS APDUs.....	113
Figure 31 – Structure of general-glo-ciphering and general-ded-ciphering xDLMS APDUs	114
Figure 32 – Structure of general-ciphering xDLMS APDUs	115
Figure 33 – Structure of general-signing APDUs	121
Figure 34 – Service primitives	126
Figure 35 – Time sequence diagrams.....	127
Figure 36 – Additional service parameters to control cryptographic protection and GBT	137

Figure 37 – Partial state machine for the client side control function.....	173
Figure 38 – Partial state machine for the server side control function	175
Figure 39 – MSC for successful AA establishment preceded by a successful lower layer connection establishment	184
Figure 40 – Graceful AA release using the A-RELEASE service	189
Figure 41 – Graceful AA release by disconnecting the supporting layer.....	190
Figure 42 – Aborting an AA following a PH-ABORT.indication.....	191
Figure 43 – MSC of the GET service	194
Figure 44 – MSC of the GET service with block transfer.....	195
Figure 45 – MSC of the GET service with block transfer, long GET aborted.....	197
Figure 46 – MSC of the SET service.....	198
Figure 47 – MSC of the SET service with block transfer	198
Figure 48 – MSC of the ACTION service	200
Figure 49 – MSC of the ACTION service with block transfer	202
Figure 50 – ACCESS Service with long response	203
Figure 51 – ACCESS Service with long request and response	203
Figure 52 – MSC of the Read service used for reading an attribute	207
Figure 53 – MSC of the Read service used for invoking a method.....	207
Figure 54 – MSC of the Read service used for reading an attribute, with block transfer	208
Figure 55 – MSC of the Write service used for writing an attribute	211
Figure 56 – MSC of the Write service used for invoking a method.....	212
Figure 57 – MSC of the Write service used for writing an attribute, with block transfer	213
Figure 58 – MSC of the UnconfirmedWrite service used for writing an attribute	214
Figure 59 – Partial service invocations and GBT APDUs	217
Figure 60 – GET service with GBT, switching to streaming.....	219
Figure 61 – GET service with partial invocations, GBT and streaming, recovery of 4 th block sent in the 2nd stream	220
Figure 62 – GET service with partial invocations, GBT and streaming, recovery of 4 th and 5 th block	221
Figure 63 – GET service with partial invocations, GBT and streaming, recovery of last block	222
Figure 64 – SET service with GBT, with server not supporting streaming, recovery of 3rd block	223
Figure 65 – ACTION-WITH-LIST service with bi-directional GBT and block recovery	224
Figure 66 – DataNotification service with GBT with partial invocation	225
Figure B.1 – Short wrapper	264
Figure C.1 – General architecture with gateway	265
Figure C.2 – The fields used for pre-fixing the COSEM APDUs	266
Figure C.3 – Pull message sequence chart	267
Figure C.4 – Push message sequence chart.....	268
Figure I.1 – MSC for key agreement using the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme.....	323
Figure I.2 – Ciphred xDLMS APDU protected by an ephemeral key established using the One-pass Diffie-Hellman (1e, 1s, ECC CDH) scheme	327

Figure I.3 – Ciphered xDLMS APDU protected by an ephemeral key established using the Static Unified Model C(0e, 2s, ECC CDH) scheme.....	332
Figure J.1 – Exchanging protected xDLMS APDUs between TP and server: example 1	336
Figure J.2 – Exchanging protected xDLMS APDUs between TP and server: example 2	338
Table 1 – Client and server SAPs	38
Table 2 – Clarification of the meaning of PDU size for DLMS/COSEM	57
Table 3 – Elliptic curves in DLMS/COSEM security suites	75
Table 4 – Ephemeral Unified Model key agreement scheme summary	79
Table 5 – One-pass Diffie-Hellman key agreement scheme summary	81
Table 6 – Static Unified Model key agreement scheme summary	83
Table 7 – <i>OtherInfo</i> subfields and substrings	84
Table 8 – Cryptographic algorithm ID-s	84
Table 9 – DLMS/COSEM security suites	85
Table 10 – Symmetric keys types	87
Table 11 – Key information with general-ciphering APDU and data protection	88
Table 12 – Asymmetric keys types and their use	90
Table 13 – X.509 v3 Certificate structure	95
Table 14 – X.509 v3 tbsCertificate fields	96
Table 15 – Naming scheme for the Root-CA instance (informative)	97
Table 16 – Naming scheme for the Sub-CA instance (informative)	97
Table 17 – Naming scheme for the end entity instance	97
Table 18 – X.509 v3 Certificate extensions	99
Table 19 – Key Usage extensions	100
Table 20 – Subject Alternative Name values	101
Table 21 – Issuer Alternative Name values	101
Table 22 – Basic constraints extension values	101
Table 23 – Certificates handled by DLMS/COSEM end entities	103
Table 24 – Security policy values (“Security setup” version 1)	108
Table 25 – Access rights values (“Association LN” ver 3 “Association SN” ver 4)	109
Table 26 – Ciphered xDLMS APDUs	110
Table 27 – Security control byte	112
Table 28 – Plaintext and Additional Authenticated Data	112
Table 29 – Use of the fields of the ciphering xDLMS APDUs	116
Table 30 – Example: glo-get-request xDLMS APDU	117
Table 31 – ACCESS service with general-ciphering, One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) key agreement scheme	119
Table 32 – DLMS/COSEM HLS authentication mechanisms	123
Table 33 – HLS example using authentication-mechanism 5 with GMAC	124
Table 34 – HLS example using authentication-mechanism 7 with ECDSA	125
Table 35 – Codes for AL service parameters	128
Table 36 – Service parameters of the COSEM-OPEN service primitives	129

Table 37 – Service parameters of the COSEM-RELEASE service primitives.....	133
Table 38 – Service parameters of the COSEM-ABORT service primitives	136
Table 39 – Additional service parameters	138
Table 40 – Security parameters.....	139
Table 41 – APDUs used with security protection types.....	140
Table 42 – Service parameters of the GET service.....	142
Table 43 – GET service request and response types	143
Table 44 – Service parameters of the SET service.....	145
Table 45 – SET service request and response types	146
Table 46 – Service parameters of the ACTION service.....	148
Table 47 – ACTION service request and response types	149
Table 48 – Service parameters of the ACCESS service.....	155
Table 49 – Service parameters of the DataNotification service primitives	158
Table 50 – Service parameters of the EventNotification service primitives.....	159
Table 51 – Service parameters of the TriggerEventNotificationSending.request service primitive	160
Table 52 – Variable Access Specification	161
Table 53 – Service parameters of the Read service.....	162
Table 54 – Use of the Variable_Access_Specification variants and the Read.response choices	163
Table 55 – Service parameters of the Write service.....	166
Table 56 – Use of the Variable_Access_Specification variants and the Write.response choices	167
Table 57 – Service parameters of the UnconfirmedWrite service	169
Table 58 – Use of the Variable_Access_Specification variants	169
Table 59 – Service parameters of the InformationReport service	170
Table 60 – Service parameters of the SetMapperTable.request service primitives	171
Table 61 – Summary of ACSE services	171
Table 62 – Summary of xDLMS services	172
Table 63 – Functional Unit APDUs and their fields	177
Table 64 – COSEM application context names.....	180
Table 65 – COSEM authentication mechanism names	181
Table 66 – Cryptographic algorithm ID-s.....	182
Table 67 – xDLMS Conformance block.....	192
Table 68 – GET service types and APDUs	194
Table 69 – SET service types and APDUs	197
Table 70 – ACTION service types and APDUs	200
Table 71 – Mapping between the GET and the Read services.....	205
Table 72 – Mapping between the ACTION and the Read services	206
Table 73 – Mapping between the SET and the Write services (1 of 2).....	209
Table 74 – Mapping between the ACTION and the Write service	210
Table 75 – Mapping between the SET and the UnconfirmedWrite services	214
Table 76 – Mapping between the ACTION and the UnconfirmedWrite services.....	214

Table 77 – Mapping between the EventNotification and InformationReport services	215
Table B.1 – Reserved Application Processes	264
Table D.1 – Conformance block	271
Table D.2 – A-XDR encoding of the xDLMS InitiateRequest APDU	272
Table D.3 – A-XDR encoding of the xDLMS InitiateResponse APDU	273
Table D.4 – BER encoding of the AARQ APDU	276
Table D.5 – Complete AARQ APDU	278
Table D.6 – BER encoding of the AARE APDU	279
Table D.7 – The complete AARE APDU	283
Table E.1 – A-XDR encoding of the xDLMS InitiateRequest APDU	285
Table E.2 – Authenticated encryption of the xDLMS InitiateRequest APDU	286
Table E.3 – BER encoding of the AARQ APDU	287
Table E.4 – A-XDR encoding of the xDLMS InitiateResponse APDU	289
Table E.5 – Authenticated encryption of the xDLMS InitiateResponse APDU	290
Table E.6 – BER encoding of the AARE APDU	291
Table E.7 – BER encoding of the RLRQ APDU	292
Table E.8 – BER encoding of the RLRE APDU	293
Table F.1 – The objects used in the examples	294
Table F.2 – Example: Reading the value of a single attribute without block transfer	295
Table F.3 – Example: Reading the value of a list of attributes without block transfer	296
Table F.4 – Example: Reading the value of a single attribute with block transfer	298
Table F.5 – Example: Reading the value of a list of attributes with block transfer	300
Table F.6 – Example: Writing the value of a single attribute without block transfer	303
Table F.7 – Example: Writing the value of a list of attributes without block transfer	304
Table F.8 – Example: Writing the value of a single attribute with block transfer	306
Table F.9 – Example: Writing the value of a list of attributes with block transfer	308
Table F.10 – Example: ACCESS service without block transfer	311
Table G.1 – ECC_P256_Domain_Parameters	319
Table G.2 – ECC_P384_Domain_Parameters	320
Table I.1 – Test vector for key agreement using the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme	325
Table I.2 – Test vector for key agreement using the One-pass Diffie-Hellman (1e, 1s, ECC CDH) scheme	329
Table I.3 – Test vector for key agreement using the Static-Unified Model (0e, 2s, ECC CDH) scheme	333

INTRODUCTION

This third edition of IEC 62056-5-3 has been prepared by IEC TC13 WG14 with a significant contribution of the DLMS User Association, its D-type liaison partner.

This edition is in line with DLMS UA 1000-2, the “Green Book” Ed. 8.2:2017. The main new features are the ACCESS service, the new security suites 1 and 2 supporting symmetric key and public key cryptography, the general protection mechanism and the XML schema for COSEM APDUs.

Clause 5 is based on parts of NIST documents. Reprinted courtesy of the National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce.

ELECTRICITY METERING DATA EXCHANGE – THE DLMS/COSEM SUITE –

Part 5-3: DLMS/COSEM application layer

1 Scope

This part of IEC 62056 specifies the DLMS/COSEM application layer in terms of structure, services and protocols for DLMS/COSEM clients and servers, and defines rules to specify the DLMS/COSEM communication profiles.

It defines services for establishing and releasing application associations, and data communication services for accessing the methods and attributes of COSEM interface objects, defined in IEC 62056-6-2 using either logical name (LN) or short name (SN) referencing.

Annex A (normative) defines how to use the COSEM application layer in various communication profiles. It specifies how various communication profiles can be constructed for exchanging data with metering equipment using the COSEM interface model, and what are the necessary elements to specify in each communication profile. The actual, media-specific communication profiles are specified in separate parts of the IEC 62056 series.

Annex B (normative) specifies the SMS short wrapper.

Annex C (normative) specifies the gateway protocol.

Annex D, Annex E and Annex F (informative) include encoding examples for APDUs.

Annex G (normative) provides NSA Suite B elliptic curves and domain parameters.

Annex H (informative) provides an example of an End entity signature certificate using P-256 signed with P-256.

Annex I (normative) specifies the use of key agreement schemes in DLMS/COSEM.

Annex J (informative) provides examples of exchanging protected xDLMS APDUs between a third party and a server.

Annex K (informative) lists the main technical changes in this edition of the standard.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61334-4-41:1996, *Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 41: Application protocol – Distribution line message specification*

IEC 61334-6:2000, *Distribution automation using distribution line carrier systems – Part 6: A-XDR encoding rule*

IEC TR 62051:1999, *Electricity metering – Glossary of terms*

IEC TR 62051-1:2004, *Electricity metering – Data exchange for meter reading, tariff and load control – Glossary of terms – Part 1: Terms related to data exchange with metering equipment using DLMS/COSEM*

IEC 62056-6-2:2017, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes*

IEC 62056-8-3:2013, *Electricity metering data exchange – The DLMS/COSEM suite – Part 8-3: Communication profile for PLC S-FSK neighbourhood networks*

ISO/IEC 8824-1, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8825-1:2015, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 15953:1999, *Information technology – Open Systems Interconnection – Service definition for the Application Service Object Association Control Service Element*

NOTE This standard cancels and replaces ISO/IEC 8649:1996 and its Amd. 1:1997 and Amd. 2:1998, of which it constitutes a technical revision.

ISO/IEC 15954:1999, *Information technology – Open Systems Interconnection – Connection-mode protocol for the Application Service Object Association Control Service Element*

NOTE This standard cancels and replaces ISO/IEC 8650-1:1999 and its Amd. 1:1997 and Amd. 2:1998, of which it constitutes a technical revision.

ITU-T V.44:2000, *Series v: data communication over the telephone network – Error control – V.44:2000, Data compression procedures*

ITU-T X.509:2008, *Series x: data networks, open system communications and security – Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

ITU-T X.693 (11/2008), *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*

ITU-T X.693 Corrigendum 1 (10/2011), *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER) Technical Corrigendum 1*

ITU-T X.694 (11/2008), *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*

ITU-T X.694 Corrigendum 1 (10/2011), *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 Technical Corrigendum 1*

FIPS PUB 180-4:2012, *Secure hash standard (SHS)*

FIPS PUB 186-4:2013, *Digital Signature Standard (DSS)*

FIPS PUB 197:2001, *Advanced Encryption Standard (AES)*

NIST SP 800-21:2005, *Guideline for Implementing Cryptography in the Federal Government*

NIST SP 800-32:2001, *Introduction to Public Key Technology and the Federal PKI Infrastructure*

NIST SP 800-38D:2007, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*

NIST SP 800-56A Rev. 2: 2013, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*

NIST SP 800-57:2012, *Recommendation for Key Management – Part 1: General (Revision 3)*

NSA1, *Suite B Implementer's Guide to FIPS 186-3 (ECDSA)*, Feb 3rd 2010

NSA2, *Suite B Implementer's Guide to NIST SP800-56A*, 28th July 2009

NSA3, *NSA Suite B Base Certificate and CRL Profile*, 27th May 2008

RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories) September 2002
<http://tools.ietf.org/html/rfc3394>

RFC 4108, *Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages*, 2005,
<http://www.ietf.org/rfc/rfc4108>

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, 2008, <http://www.ietf.org/rfc/rfc5280>

3 Terms, definitions, abbreviated terms and symbols

For the purposes of this document, the terms and definitions given in IEC TR 62051:1999, in IEC TR 62051-1, in RFC 4106, and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1 General DLMS/COSEM definitions

3.1.1

ACSE APDU

APDU used by the Association Control Service Element (ACSE)

3.1.2

application association

cooperative relationship between two application entities, formed by their exchange of application protocol control information through their use of presentation services

3.1.3

application context

set of application service elements, related options and any other information necessary for the interworking of application entities in an application association

3.1.4

application entity

system-independent application activities that are made available as application services to the application agent, e.g., a set of application service elements that together perform all or part of the communication aspects of an application process

3.1.5

application process

element within a real open system which performs the information processing for a particular application

[SOURCE: ISO/IEC 7498-1:1994, 4.1.4]

NOTE Harmonized as EN 62056-8-5.

3.1.6

authentication mechanism

specification of a specific set of authentication-function rules for defining, processing, and transferring authentication-values

[SOURCE: ISO/IEC 15953:1999, 3.5.11]

3.1.7

client

application process running in the data collection system

3.1.8

client/server

relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfils the request

3.1.9

COSEM

Companion Specification for Energy Metering; refers to the COSEM object model

3.1.10

COSEM APDU

comprises ACSE APDUs and xDLMS APDUs

3.1.11

COSEM data

COSEM object attribute values, method invocation and return parameters

3.1.12

COSEM interface class

entity with specific set of attributes and methods modelling a certain function on its own or in relation with other COSEM interface classes

3.1.13

COSEM object

instance of a COSEM interface class

3.1.14

DLMS/COSEM

refers to the application layer providing xDLMS services to access COSEM interface object attributes. Also refers to the DLMS/COSEM Application layer and the COSEM data model together.

3.1.15

DLMS context

specification of the service elements of DLMS and semantics of communication to be used during the lifetime of an application association

[SOURCE: IEC 61334-4-41:1996, 3.3.5]

3.1.16

entity authentication

corroboration that an entity is the one claimed

[SOURCE: ISO/IEC 9798-1:2010, 3.14]

3.1.17

logical device

abstract entity within a physical device, representing a subset of the functionality modelled with COSEM objects

3.1.18

master

central station – station which takes the initiative and controls the data flow

3.1.19

mutual authentication

entity authentication which provides both entities with assurance of each other's identity

Note 1 to entry: The DLMS/COSEM HLS authentication mechanism provides mutual authentication.

[SOURCE: ISO/IEC 9798-1:2010, 3.18, modified by adding Note 1]

3.1.20

physical device

physical metering equipment, the highest level element used in the COSEM interface model of metering equipment

3.1.21

pull operation

style of communication where the request for a given transaction is initiated by the client

3.1.22

push operation

style of communication where the request for a given transaction is initiated by the server

3.1.23

system title

unique identifier of the system

3.1.24

server

application process running in a metering equipment

3.1.25

slave

station responding to requests of a master station

Note 1 to entry: A meter is normally a slave station.

3.1.26

unilateral authentication

entity authentication which provides one entity with assurance of the other's identity but not vice versa

Note 1 to entry: The DLMS/COSEM LLS authentication mechanism provides unilateral authentication.

[SOURCE: ISO/IEC 9798-1:2010, 3.39]

3.1.27

xDLMS

extended DLMS; refers to the DLMS protocol with the extensions specified in this document

3.1.28

xDLMS APDU

APDU used by the xDLMS Application Service Element (xDLMS ASE)

3.1.29

xDLMS message

xDLMS APDU exchanged between a client and a server or between a third party and a server

3.2 Definitions related to cryptographic security

3.2.1

access control

restricts access to resources to only privileged entities

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.2

asymmetric key algorithm

see Public key cryptographic algorithm

3.2.3

authentication

process that establishes the source of information, provides assurance of an entity's identity or provides assurance of the integrity of communications sessions, messages, documents or stored data

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.4

authentication code

cryptographic checksum based on an approved security function (also known as a Message Authentication Code)

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.5

certificate

see public key certificate

3.2.6

Certification Authority

CA

entity in a Public Key Infrastructure (PKI) that is responsible for issuing public key certificates and exacting compliance to a PKI policy

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.7

Certificate Policy

CP

specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

[SOURCE: NIST SP 800-32:2001]

3.2.8

challenge

time variant parameter generated by a verifier

[SOURCE: ITU-T X.811:1995, 3.8]

3.2.9

ciphering

authentication and / or encryption using symmetric key algorithms

3.2.10

ciphertext

data in its encrypted form

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.11

cofactor

order of the elliptic curve group divided by the (prime) order of the generator point (i.e. the base point) specified in the domain parameters

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.12

confidentiality

property that sensitive information is not disclosed to unauthorized entities

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.13

cryptographic algorithm

well-defined computational procedure that takes variable inputs including a cryptographic key and produces an output

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.14

cryptographic key

parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot

Note 1 to entry:

Examples include:

1. The transformation of plaintext data into ciphertext data,
2. The transformation of ciphertext data into plaintext data,
3. The computation of a digital signature from data,
4. The verification of a digital signature,
5. The computation of an authentication code from data,
6. The verification of an authentication code from data and a received authentication code,
7. The computation of a shared secret that is used to derive keying material.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.15

cryptoperiod

time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.16

dedicated key

in DLMS/COSEM, a symmetric key used within a single instance of an Application Association. See also session key

3.2.17

deprecated

not recommended for new implementations

3.2.18

digital signature

result of a cryptographic transformation of data that, when properly implemented with supporting infrastructure and policy, provides the services of:

- 1) origin authentication
- 2) data integrity, and
- 3) signer non-repudiation

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.19

directly trusted CA

CA whose public key has been obtained and is being stored by an end entity in a secure, trusted manner, and whose public key is accepted by that end entity in the context of one or more applications

[SOURCE: ISO/IEC 15945:2002, 3.4]

3.2.20

directly trusted CA key

public key of a directly trusted CA. It has been obtained and is being stored by an end entity in a secure, trusted manner. It is used to verify certificates without being itself verified by means of a certificate created by another CA.

Note 1 to entry: Directly trusted CAs and directly trusted CA keys may vary from entity to entity. An entity may regard several CAs as directly trusted CAs.

[SOURCE: ISO/IEC 15945:2002, 3.5]

3.2.21

distribution

see key distribution

3.2.22

domain parameters

parameters used with a cryptographic algorithm that are common to a domain of users

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.23

encryption

process of changing plaintext into ciphertext using a cryptographic algorithm and key

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.24

ephemeral key

cryptographic key that is generated for each execution of a key establishment process and that meets other requirements of the key type (e.g., unique to each message or session). In some cases ephemeral keys are used more than once, within a single “session (e.g., broadcast applications) where the sender generates only one ephemeral key pair per message and the private key is combined separately with each recipient’s public key.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.25

global key

key that is intended for use for a relatively long period of time and is typically intended for use in many instances of a DLMS/COSEM Application Association, see also static symmetric key

3.2.26

hash function

function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties:

- 1) One-way: It is computationally infeasible to find any input that maps to any pre-specified output, and
- 2) Collision resistant: It is computationally infeasible to find any two distinct inputs that map to the same output.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.27

hash value

result of applying a hash function to information

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.28

initialization vector

IV

vector used in defining the starting point of a cryptographic process

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.29

identification

process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system

[SOURCE: NIST SP 800-47:2002]

3.2.30

key

see cryptographic key

3.2.31

key agreement

(pair-wise) key-establishment procedure in which the resultant secret keying material is a function of information contributed by both participants, so that neither party can predetermine the value of the secret keying material independently from the contributions of the other party. Contrast with key-transport.

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.32

key-confirmation

procedure to provide assurance to one party (the key-confirmation recipient) that another party (the key-confirmation provider) actually possesses the correct secret keying material and/or shared secret

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.33

key-derivation function

function by which keying material is derived from a shared secret (or a key) and other information

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.34

key distribution

transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.35

key-encrypting key

cryptographic key that is used for the encryption or decryption of other keys

Note 1 to entry: In DLMS/COSEM it is the master key.

[SOURCE: NIST SP 800-57:2012, Part 1, modified by adding the Note]

3.2.36

key establishment

procedure that results in keying material that is shared among different parties

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.37

key pair

public key and its corresponding private key; a key pair is used with a public key algorithm

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.38

key revocation

function in the lifecycle of keying material; a process whereby a notice is made available to affected entities that keying material should be removed from operational use prior to the end of the established cryptoperiod of that keying material

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.39

key-transport

(pair-wise) key-establishment procedure whereby one party (the sender) selects a value for the secret keying material and then securely distributes that value to another party (the receiver). Contrast with key agreement.

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.40

key wrapping

method of encrypting keying material (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.41

message authentication code

MAC

cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.42

message digest

result of applying a hash function to a message. Also known as “hash value”

[SOURCE: FIPS PUB 186-4:2013]

3.2.43

named curve

set of ECDH domain parameters is also known as a "curve". A curve is a "named curve" if the domain parameters are well known and defined and can be identified by an Object Identifier; otherwise, it is called a "custom curve".

[SOURCE: RFC 5349:2008]

3.2.44

nonce

time-varying value that has at most an acceptably small chance of repeating. For example, the nonce may be a random value that is generated anew for each use, a timestamp, a sequence number, or some combination of these.

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.45

non-repudiation

service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party as having originated from a specific entity in possession of the private key of the claimed signatory

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.46

password

string of characters (letters, numbers and other symbols) that are used to authenticate an identity or to verify access authorization or to derive cryptographic keys

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.47

plaintext

intelligible data that has meaning and can be understood without the application of decryption

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.48

private key

cryptographic key, used with a public key cryptographic algorithm, which is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used, for example, to:

- 1) Compute the corresponding public key,
- 2) Compute a digital signature that may be verified by the corresponding public key,
- 3) Decrypt keys that were encrypted by the corresponding public key, or
- 4) Compute a shared secret during a key-agreement transaction.

[SOURCE: NIST SP 800-57:2012, Part 1]