DIN EN 62056-5-3

ICS 33.200; 35.100.70; 35.240.99; 91.140.50

Ersatz für
DIN EN 62056-5-3:2017-07
Siehe Anwendungsbeginn

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

Gesamtumfang 366 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2017-09-14 angenommene Europäische Norm als DIN-Norm ist 2020-06-01.

Für DIN EN 62056-5-3:2017-07 besteht eine Übergangsfrist bis 2020-09-14.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 62056-5-3:2018-11.

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 dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „http://webstore.iec.ch“ zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument
– 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 der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN 62056-5-3:2017 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe, Abkürzungen und Symbole festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA der vorliegenden Norm 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. Diese Norm steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. Weder das Deutsche Komitee, noch IEC, noch CENELEC sind dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Das Deutsche Komitee weist daraufhin, dass die Seitenangaben im Index nicht übereinstimmen und sich auf das IEC-Ausgangsdokument (IEC 62056-5-3:2017) beziehen.

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.

Frühere Ausgaben

DIN EN 62056-53: 2003-01, 2007-08
DIN EN 62056-53 Berichtigung 1: 2003-04
DIN EN 62056-5-3: 2014-09, 2017-07

Nationaler Anhang NA
(informativ)

Auszugsweise Übersetzung

Reihenfolge und Inhalt der folgenden Abschnitte sind identisch mit denen in den jeweiligen Abschnitten der Englischen Fassung.

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, Anhang E und Anhang 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: verfügbar unter http://www.electropedia.org/
– ISO Online Browsing Platform: verfügbar unter http://www.iso.org/obp

3.1 Allgemeine Begriffe zu DLMS/COSEM

3.1.1
ACSE APDU
APDU, die vom Dienstelement der Assoziationssteuerung (ACSE) verwendet wird

3.1.2
Anwendungsassoziation
kooperative Beziehung zwischen zwei Anwendungsinstanzen, entstanden durch ihren Austausch von Information zur Anwendungsprotokollsteuerung durch ihre Nutzung von Darstellungsdiensten

3.1.3
Anwendungskontext
Menge von Anwendungsdienstelementen, zugehörigen Optionen und jeglichen sonstigen notwendigen Informationen, die für das Zusammenwirken von Anwendungsinstanzen bei einer Anwendungsassoziation erforderlich sind

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; verweist auf das COSEM-Objektmodell

3.1.10
COSEM APDU
umfasst ACSE APDUs und xDLMS APDUs

3.1.11
COSEM-Daten
COSEM-Objekt-Attributwerte, Methodenaufruf 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
verweist auf die Anwendungsschicht, die xDLMS-Dienste für den Zugriff auf Schnittstellenobjekt-Attribute bereitstellt. Verweist außerdem auch auf die DLMS/COSEM-Anwendungsschicht und das COSEM-Datenmodell zusammen.

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 ist, die im COSEM-Schnittstellenmodell für Messeinrichtungen angewendet wird

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; verweist auf das DLMS-Protokoll mit den in diesem Dokument festgelegten Erweiterungen

3.1.28
xDLMS APDU
APDU, die vom xDLMS-Anwendungsdienstelement (xDLMS ASE) verwendet wird

3.1.29
xDLMS-Nachricht
xDLMS APDU, die 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 kryptografischer Algorithmus mit einem öffentlichen Schlüssel

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
Instanz in einer Infrastruktur für öffentliche Schlüssel (PKI), 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[N1]
(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 Zertifikatserweiterungen 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]

[N1] Nationale Fußnote: In IEC 62056-5-3:2017 fehlt in 3.4 (Allgemeine Abkürzungen) die Erläuterung der Abkürzung.

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 Sitzungsschlüssel.

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 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;
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
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 (paarweisen) Schlüsseleinführung, 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 Gegensatz 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]