

ILNAS

Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

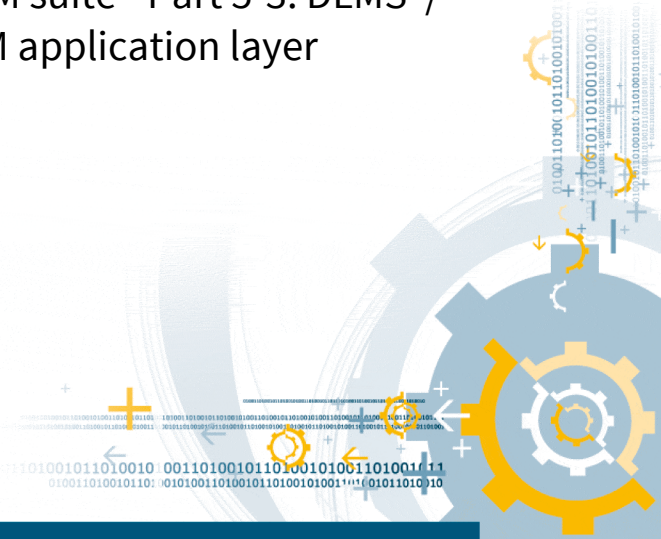
ILNAS-EN IEC 62056-5-3:2023

Échange des données de comptage de l'électricité - La suite DLMS[®]/COSEM - Partie 5-3: Couche application DLMS[®]/ COSEM

Datenkommunikation der elektrischen
Energiamessung - DLMS[®]/COSEM - Teil
5-3: DLMS/COSEM-Anwendungsschicht

Electricity metering data exchange - The
DLMS[®]/COSEM suite - Part 5-3: DLMS[®]/
COSEM application layer

11/2023



Avant-propos national

Cette Norme Européenne EN IEC 62056-5-3:2023 a été adoptée comme Norme Luxembourgeoise ILNAS-EN IEC 62056-5-3:2023.

Toute personne intéressée, membre d'une organisation basée au Luxembourg, peut participer gratuitement à l'élaboration de normes luxembourgeoises (ILNAS), européennes (CEN, CENELEC) et internationales (ISO, IEC) :

- Influencer et participer à la conception de normes
- Anticiper les développements futurs
- Participer aux réunions des comités techniques

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

CETTE PUBLICATION EST PROTÉGÉE PAR LE DROIT D'AUTEUR

Aucun contenu de la présente publication ne peut être reproduit ou utilisé sous quelque forme ou par quelque procédé que ce soit - électronique, mécanique, photocopie ou par d'autres moyens sans autorisation préalable !

ILNAS-EN IEC 62056-5-3:2023

NORME EUROPÉENNE **EN IEC 62056-5-3**
EUROPÄISCHE NORM
EUROPEAN STANDARD

Novembre 2023

ICS 17.220; 35.110; 91.140.50

Remplace l'EN 62056-5-3:2017

Version française

**Échange des données de comptage de l'électricité - La suite
DLMS®/COSEM - Partie 5-3: Couche application
DLMS®/COSEM
(IEC 62056-5-3:2023)**

Datenkommunikation der elektrischen Energiemessung -
DLMS®/COSEM - Teil 5-3: DLMS®/COSEM-
Anwendungsschicht
(IEC 62056-5-3:2023)

Electricity metering data exchange - The DLMS®/COSEM
suite - Part 5-3: DLMS®/COSEM application layer
(IEC 62056-5-3:2023)

La présente Norme Européenne a été adoptée par le CENELEC le 2023-11-02. Les membres du CENELEC sont tenus de se soumettre au Règlement Intérieur du CEN/CENELEC, qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à cette Norme Européenne.

Les listes mises à jour et les références bibliographiques relatives à ces normes nationales peuvent être obtenues auprès du CEN-CENELEC Management Centre ou auprès des membres du CENELEC.

La présente Norme Européenne existe en trois versions officielles (allemand, anglais, français). Une version dans une autre langue faite par traduction sous la responsabilité d'un membre du CENELEC dans sa langue nationale, et notifiée au CEN-CENELEC Management Centre, a le même statut que les versions officielles.

Les membres du CENELEC sont les comités électrotechniques nationaux des pays suivants: Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République de Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovaquie, Suède, Suisse et Turquie.



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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Bruxelles

Avant-propos européen

Le texte du document 13/1890/FDIS, future édition 4 de IEC 62056-5-3, préparé par le CE 13 de l'IEC, "Comptage et pilotage de l'énergie électrique", a été soumis au vote parallèle IEC-CENELEC et approuvé par le CENELEC en tant que EN IEC 62056-5-3:2023.

Les dates suivantes sont fixées:

- date limite à laquelle ce document doit être mis en application au niveau national par publication d'une norme nationale identique ou par entérinement (dop) 2024-08-02
- date limite à laquelle les normes nationales conflictuelles doivent être annulées (dow) 2026-11-02

Ce document remplace l'EN 62056-5-3:2017 ainsi que l'ensemble de ses amendements et corrigenda (le cas échéant).

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. Le CENELEC ne saurait être tenu pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

Le présent document a été élaboré en réponse à une demande de normalisation adressée au CENELEC par la Commission européenne.

Il convient que l'utilisateur adresse tout retour d'information et toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve sur le site web du CENELEC.

Notice d'entérinement

Le texte de la Norme internationale IEC 62056-5-3:2023 a été approuvé par le CENELEC comme Norme Européenne sans aucune modification.

Dans la version officielle, ajouter dans la Bibliographie la note suivante pour la norme indiquée:

ISO 3166 (série) NOTE Approuvée comme EN ISO 3166 (série)

Annexe ZA (normative)

Références normatives à d'autres publications internationales avec les publications européennes correspondantes

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

NOTE 1 Dans le cas où une publication internationale est modifiée par des modifications communes, indiqué par (mod), l'EN/le HD correspondant(e) s'applique.

NOTE 2 Les informations les plus récentes concernant les dernières versions des Normes Européennes listées dans la présente annexe sont disponibles à l'adresse suivante: www.cenelec.eu.

<u>Publication</u>	<u>Année</u>	<u>Titre</u>	<u>EN/HD</u>	<u>Année</u>
IEC 61334-4-41	1996	Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs - Partie 4: Protocoles de communication de données - Section 41: Protocoles d'application - Spécification des messages de ligne de distribution	EN 61334-4-41	1996
IEC 61334-6	2000	Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs - Partie 6: Règles d'encodage A-XDR	EN 61334-6	2000
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	2023	Échange des données de comptage de l'électricité - La suite DLMS®/COSEM - Partie 6-2: Classes d'interfaces COSEM	EN IEC 62056-6-2	2023
IEC 62056-7-3	2017	Electricity metering data exchange - The DLMS®/COSEM suite - Part 7-3: Wired and wireless M-Bus communication profiles for local and neighbourhood networks	EN 62056-7-3	2017
IEC 62056-7-6	2013	Echange des données de comptage de l'électricité - La suite DLMS®/COSEM - Partie 7-6: Profil de communication à 3 couches, orienté connexion et basé sur HDLC	EN 62056-7-6	2013
IEC 62056-8-3	2013	Echange de données de comptage de l'électricité - La suite DLMS®/COSEM - Partie 8-3: Profil de communication pour réseaux de voisinage CPL S-FSK	EN 62056-8-3	2013

IEC 62056-8-11	— ¹	Electricity metering data exchange - The DLMS®/COSEM suite - Part 8-11: Communication profile for Wi-SUN field area mesh networks	EN IEC 62056-8-11	— ²
IEC 62056-8-12	2023	Échange des données de comptage de l'électricité - La suite DLMS®/COSEM - Partie 8-12: Profil de communication pour réseaux étendus à basse consommation (LPWAN)	EN IEC 62056-8-12	2023
IEC 62056-9-7	2013	Echange de données de comptage de l'électricité - La suite DLMS®/COSEM - Partie 9-7: Profil de communication pour réseaux TCP-UDP/IP	EN 62056-9-7	2013
ISO/IEC 8824-1	2008	Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation	-	-
ISO/IEC 8825-1	2008	Technologies de l'information - Règles de codage ASN.1: Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER)	-	-
ISO/IEC 15953	1999	Technologies de l'information - Interconnexion des systèmes ouverts - Définition du service pour l'élément de service de contrôle d'association des objets de service d'application	-	-
ISO/IEC 15954	1999	Technologies de l'information - Interconnexion des systèmes ouverts - Protocole en mode connexion pour l'élément de service de contrôle d'association des objets de service d'application	-	-
ISO/IEC 7498-1	1994	Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Modèle de référence de base: Le modèle de base	-	-
ITU-T X.509	2008	Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks	-	-
ITU-T X.693	2008	Information technology - ASN.1 encoding rules: XML Encoding rules (XER)	-	-
ITU-T X.693 Corrigendum 1	2011	Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) Technical Corrigendum 1	-	-
ITU-T X.694	2008	Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1	-	-

¹ En cours d'élaboration. Stade au moment de la publication: IEC CDV.

² En cours d'élaboration. Stade au moment de la publication: prEN IEC 62056-8-11 :2023.

ITU-T X.694 Corrigendum	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)	-	-
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 800-56A rev2	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)	-	-
NSA2	-	Suite B Implementer's guide to NIST SP800-56A	-	-
NSA3	-	NSA Suite B Base Certificate and CRL Profile	-	-
SEC1	2009	Standards for Efficient Cryptography: Elliptic Curve Cryptography. SECG. Version 2.0	-	-
RFC 3394	2002	Internet Engineering Task Force (IETF). Advanced Encryption Standard (AES) Key Wrap Algorithm. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories)	-	-
RFC 4106	-	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	-	-
RFC 4108	2005	Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages	-	-
RFC 5280	2008	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	-	-



INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Electricity metering data exchange – The DLMS®/COSEM suite –
Part 5-3: DLMS®/COSEM application layer**

**Échange des données de comptage de l'électricité – La suite DLMS®/COSEM –
Partie 5-3: Couche application DLMS®/COSEM**



SOMMAIRE

AVANT-PROPOS	386
INTRODUCTION	388
1 Domaine d'application	389
2 Références normatives	390
3 Termes, définitions, abréviations et symboles	392
3.1 Définitions générales concernant DLMS®/COSEM	392
3.2 Définitions liées à la sécurité cryptée	396
3.3 Définitions et abréviations liées au mode Galois/Counter	407
3.4 Abréviations générales	409
3.5 Symboles liés au mode Galois/Counter	413
3.6 Symboles liés à l'algorithme ECDSA	413
3.7 Symboles liés aux algorithmes à agrément de clé	414
4 Vue d'ensemble de DLMS®/COSEM	414
4.1 Échange d'informations dans DLMS®/COSEM	414
4.1.1 Généralités	414
4.1.2 Modèle de communication	415
4.1.3 Nommage et adressage	416
4.1.4 Opération orientée connexion	419
4.1.5 Associations d'applications	420
4.1.6 Type de messagerie	422
4.1.7 Échange de données entre des tierces parties et des serveurs DLMS®/COSEM	423
4.1.8 Profils de communication	423
4.1.9 Modèle de système de comptage DLMS®/COSEM	424
4.1.10 Modèle de serveurs DLMS®/COSEM	425
4.1.11 Modèle d'un client DLMS®/COSEM	427
4.1.12 Interopérabilité et interconnectivité dans DLMS®/COSEM	428
4.1.13 Assurance d'interconnectivité: service d'identification de protocole	428
4.1.14 Intégration de système et installation de comptage	428
4.2 Principales caractéristiques de la couche application DLMS®/COSEM	429
4.2.1 Généralités	429
4.2.2 Structure de la couche application DLMS®/COSEM	429
4.2.3 Élément de service de contrôle d'association (ACSE)	431
4.2.4 Élément de service d'application xDLMS	432
4.2.5 Services de gestion de couche	440
4.2.6 Récapitulatif des services de la couche application DLMS®/COSEM	440
4.2.7 Protocoles de la couche application DLMS®/COSEM	441
5 Sécurité des informations dans DLMS®/COSEM	442
5.1 Vue d'ensemble	442
5.2 Concept de sécurité DLMS®/COSEM	442
5.2.1 Vue d'ensemble	442
5.2.2 Identification et authentification	442
5.2.3 Contexte de sécurité	446
5.2.4 Droits d'accès	446
5.2.5 Sécurité des messages de la couche application	447
5.2.6 Sécurité des données COSEM	449
5.3 Algorithmes cryptographiques	449

5.3.1	Vue d'ensemble	449
5.3.2	Fonction de hachage	450
5.3.3	Algorithmes à clé symétrique	451
5.3.4	Algorithmes à clé publique	458
5.3.5	Génération de nombres aléatoires	470
5.3.6	Compression	470
5.3.7	Suite de sécurité	470
5.4	Clés cryptographiques — Vue d'ensemble	471
5.5	Clés utilisées avec des algorithmes à clé symétrique	471
5.5.1	Types de clés symétriques	471
5.5.2	Informations relatives aux clés avec APDU general-ciphering et protection des données	474
5.5.3	Identification de clé	475
5.5.4	Enveloppement de clé	475
5.5.5	Agrément de clé	475
5.5.6	Périodes cryptographiques à clé symétrique	476
5.6	Clés utilisées avec des algorithmes à clé publique	476
5.6.1	Vue d'ensemble	476
5.6.2	Génération de paires de clés	477
5.6.3	Certificats de clé publique et infrastructure à clé publique	477
5.6.4	Certificat et profil d'extension de certificat	480
5.6.5	Types de certificats d'entités finales de la Suite B à prendre en charge par les serveurs DLMS®/COSEM	488
5.6.6	Gestion des certificats	489
5.7	Application de la protection cryptographique	494
5.7.1	Vue d'ensemble	494
5.7.2	Protection des APDU xDLMS	494
5.7.3	Protection multicouche par plusieurs parties	507
5.7.4	Mécanismes d'authentification HLS	508
5.7.5	Protection des données COSEM	511
6	Spécification de service de la couche application DLMS®/COSEM	512
6.1	Primitives de service et paramètres	512
6.2	Service COSEM-OPEN	514
6.3	Service COSEM-RELEASE	519
6.4	Service COSEM-ABORT	522
6.5	Paramètres de protection et de transfert de bloc général	523
6.6	Service GET	529
6.7	Service SET	532
6.8	Service ACTION	537
6.9	Service ACCESS	541
6.9.1	Vue d'ensemble — Principales fonctionnalités	541
6.9.2	Spécification de service	543
6.10	Service DataNotification	548
6.11	Service EventNotification	549
6.12	Service TriggerEventNotificationSending	551
6.13	Spécification d'accès variable	551
6.14	Service Read	552
6.15	Service Write	556
6.16	Service UnconfirmedWrite	560

6.17	Service InformationReport	561
6.18	Services de gestion de couches côté client: Service SetMapperTable.request.....	562
6.19	Récapitulatif des services et de la mise en correspondance de services de transfert de données LN/SN	562
7	Spécification du protocole de couche application DLMS@/COSEM	564
7.1	Fonction de commande	564
7.1.1	Définitions des états de la fonction de commande côté client.....	564
7.1.2	Définitions des états de la fonction de commande côté serveur	565
7.2	Services ACSE et APDU	567
7.2.1	Unités fonctionnelles ACSE, services et paramètres de service	567
7.2.2	Noms COSEM enregistrés	570
7.2.3	Règles de codage d'APDU.....	573
7.2.4	Protocole d'établissement d'association d'applications	573
7.2.5	Protocole de libération d'association d'applications	579
7.3	Protocole des services de transfert de données	582
7.3.1	Négociation de services et d'options — Bloc de conformité	582
7.3.2	Appels de service confirmés et non confirmés	583
7.3.3	Protocole du service GET	585
7.3.4	Protocole du service SET	588
7.3.5	Protocole du service ACTION	591
7.3.6	Protocole du service ACCESS	593
7.3.7	Protocole du service DataNotification	595
7.3.8	Protocole du service EventNotification.....	598
7.3.9	Protocole du service Read.....	599
7.3.10	Protocole du service Write.....	603
7.3.11	Protocole du service UnconfirmedWrite	607
7.3.12	Protocole du service InformationReport	608
7.3.13	Protocole du mécanisme de transfert de bloc général.....	609
7.3.14	Protocole de mécanisme d'exception.....	632
8	Syntaxe abstraite des APDU ACSE et COSEM	633
9	Schéma XML des APDU COSEM.....	652
9.1	Généralités	652
9.2	Schéma XML	652
Annexe A (normative) Utilisation de la couche application DLMS@/COSEM dans différents profils de communication		
A.1	Généralités	674
A.2	Environnements de communication ciblés.....	674
A.3	Structure du profil	674
A.4	Schémas d'identification et d'adressage	674
A.5	Services de couche de support et mise en correspondance de services.....	675
A.6	Paramètres spécifiques au profil de communication des services d'AL COSEM.....	675
A.7	Considérations / contraintes spécifiques à l'utilisation de certains services dans un profil donné	675
A.8	Profil de communication à 3 couches, orienté connexion et basé sur HDLC	675
A.9	Profils de communication basés sur TCP-UDP/IP (COSEM_on_IP).....	675
A.10	Profils de communication M-Bus filaire et sans fil.....	675
A.11	Profil PLC S-FSK	675

Annexe B (normative) Couche d'adaptation réduite pour SMS	676
Annexe C (normative) Protocole de passerelle.....	677
C.1 Généralités	677
C.2 Protocole de passerelle	678
C.3 HES dans le WAN/NN agissant comme initiateur (opération Pull).....	679
C.4 Dispositifs finaux dans le LAN agissant comme initiateurs (opération Push)	680
C.4.1 Généralités	680
C.4.2 Dispositif final ayant des connaissances sur le WAN/NN	680
C.4.3 Dispositifs finaux sans connaissances sur le WAN/NN.....	681
C.5 Sécurité	681
Annexe D (informative) Exemples de codages AARQ et AARE	682
D.1 Généralités	682
D.2 Codage des APDU xDLMS InitiateRequest/InitiateResponse	682
D.3 Spécification des APDU AARQ et AARE	685
D.4 Données pour les exemples	686
D.5 Codage de l'APDU AARQ	687
D.6 Codage de l'APDU AARE.....	690
Annexe E (informative) Exemples de codage: APDU AARQ et AARE utilisant un contexte chiffré d'application.....	696
E.1 Codage A-XDR de l'APDU xDLMS InitiateRequest contenant une clé dédiée	696
E.2 Cryptage authentifié de l'APDU xDLMS InitiateRequest	697
E.3 APDU AARQ	698
E.4 Codage A-XDR de l'APDU xDLMS InitiateResponse	700
E.5 Cryptage authentifié de l'APDU xDLMS InitiateResponse.....	701
E.6 APDU AARE	702
E.7 APDU RLRQ (contenant une APDU xDLMS InitiateRequest chiffrée)	704
E.8 APDU RLRE (contenant une APDU xDLMS InitiateResponse chiffrée).....	705
Annexe F (informative) Exemples de services de transfert de données	706
F.1 Exemples GET / Read, SET / Write.....	706
F.2 Exemple de service ACCESS.....	723
F.3 Exemple de codage compact-array	724
F.3.1 Généralités	724
F.3.2 Spécification de compact-array.....	725
F.3.3 Exemple 1: codage compact-array d'un array de cinq valeurs long- unsigned.....	726
F.3.4 Exemple 2: codage compact-array de cinq valeurs octet-string	727
F.3.5 Exemple 3: codage du tampon d'un objet générique Profile	728
F.4 Exemples de codage de l'attribut buffer de l'IC "Profile generic"	729
F.4.1 Généralités	729
F.4.2 Exemple de codage normal pour Get-response avec Profile generic.....	730
F.4.3 Exemple de codage null-data compressées pour Get-response avec Profile generic	732
F.4.4 Exemple de codage compact-array pour Get-response avec Profile generic	735
F.4.5 Exemple de codage null-data et delta-value pour Get-response avec Profile generic	737
F.4.6 Comparaison de différentes méthodes de codage pour l'APDU get- response	740
F.4.7 Combinaison des différentes méthodes de codage et compression V.44.....	740

Annexe G (normative) Courbes elliptiques et paramètres de domaine de la Suite B NSA.....	742
Annexe H (informative) Exemple de certificat de signature d'entité finale utilisant P-256 signé avec P-256.....	744
H.1 Champs des certificats de clé publique	744
H.2 Exemple de certificat Root-CA utilisant P-256 signé avec P-256	745
H.3 Exemple de certificat de signature numérique d'entité finale utilisant P-256 signé avec P-256	746
Annexe I (normative) Utilisation des mécanismes d'agrément de clé dans DLMS®/COSEM.....	747
I.1 Schéma Ephemeral Unified Model C(2e, 0s, ECC CDH).....	747
I.2 Schéma One-pass Diffie-Hellman C(1e, 1s, ECC CDH).....	750
I.3 Schéma de modèle unifié statique C(0e, 2s, ECC CDH).....	753
Annexe J (informative) Échange d'APDU xDLMS protégées entre TP et serveur.....	757
J.1 Généralités	757
J.2 Exemple 1: protection similaire dans les deux sens.....	757
J.3 Exemple 2: protection différente dans les deux sens.....	758
Annexe K (informative) Modifications techniques majeures par rapport à l'IEC 62056-5-3:2017	760
Bibliographie.....	763
Figure 1 – Modèle client/serveur et protocoles de communication.....	416
Figure 2 – Nommage et adressage dans DLMS®/COSEM	417
Figure 3 – Session complète de communication dans l'environnement CO.....	420
Figure 4 – Types de messagerie DLMS®/COSEM.....	422
Figure 5 – Profil générique de communication DLMS®/COSEM	424
Figure 6 – Modèle de système de comptage DLMS®/COSEM.....	425
Figure 7 – Modèle de serveur DLMS®/COSEM	426
Figure 8 – Modèle de client DLMS®/COSEM utilisant plusieurs piles de protocoles	427
Figure 9 – Structure des couches d'application DLMS®/COSEM.....	430
Figure 10 – Concept de messages xDLMS composables	438
Figure 11 – Récapitulatif des services de l'AL DLMS®/COSEM	441
Figure 12 – Mécanismes d'authentification.....	444
Figure 13 – Conception de sécurité des messages client-serveur	447
Figure 14 – Concept de sécurité de bout en bout sur les messages	448
Figure 15 – Fonction de hachage.....	450
Figure 16 – Cryptage et décryptage	451
Figure 17 – Codes d'authentification de message (MAC)	453
Figure 18 – Fonctions du GCM	454
Figure 19 – Signatures numériques.....	461
Figure 20 – Schéma C(2e, 0s): chaque partie apporte uniquement une paire de clés éphémères.....	463
Figure 21 – Schémas C(1e, 1s): la partie U apporte une paire de clés éphémères, et la partie V apporte une paire de clés statiques	465
Figure 22 – Schéma C(0e, 2s): chaque partie apporte uniquement une paire de clés statiques	467
Figure 23 – Architecture d'une infrastructure à clé publique (exemple).....	479

Figure 24 – MSC pour l’approvisionnement du serveur en certificats de la CA	490
Figure 25 – MSC pour la personnalisation de sécurité du serveur	491
Figure 26 – Approvisionnement du serveur en certificat du client	492
Figure 27 – Approvisionnement du client/de la tierce partie en certificat du serveur	493
Figure 28 – Suppression de certificat du serveur	493
Figure 29 – Protection cryptographique des informations à l’aide d’AES-GCM	497
Figure 30 – Structure des APDU xDLMS de chiffrement global spécifique au service / de chiffrement dédié spécifique au service.....	499
Figure 31 – Structure des APDU xDLMS general-glo-ciphering et general-ded- ciphering.....	500
Figure 32 – Structure des APDU xDLMS general-ciphering.....	501
Figure 33 – Structure des APDU general-signing	507
Figure 34 – Primitives de service	512
Figure 35 – Diagrammes de séquences temporelles	513
Figure 36 – Paramètres de service supplémentaires pour contrôler la protection cryptographique et le GBT	524
Figure 37 – Diagramme d’états partiel pour la fonction de commande côté client.....	564
Figure 38 – Diagramme d’états partiel pour la fonction de commande côté serveur.....	566
Figure 39 – MSC pour l’établissement réussi d’une AA précédé de l’établissement réussi d’une connexion de couches inférieures	575
Figure 40 – Libération d’AA sans perte de données à l’aide du service A-RELEASE	580
Figure 41 – Libération d’AA sans perte de données par déconnexion de la couche de support	581
Figure 42 – Abandon d’une AA après la primitive PH-ABORT.indication	582
Figure 43 – MSC du service GET	586
Figure 44 – MSC du service GET avec transfert de blocs.....	586
Figure 45 – MSC du service GET avec transfert de blocs, transfert long abandonné.....	588
Figure 46 – MSC du service SET	589
Figure 47 – MSC du service SET avec transfert de blocs	590
Figure 48 – MSC du service ACTION.....	592
Figure 49 – MSC du service ACTION avec transfert de bloc	593
Figure 50 – Service ACCESS avec réponse longue	594
Figure 51 – Service ACCESS avec demande et réponse longues	595
Figure 52 – MSC pour le service DataNotification, situation 1)	596
Figure 53 – MSC pour le service DataNotification, situation 2)	597
Figure 54 – MSC pour le service DataNotification, situation 3)	598
Figure 55 – MSC du service Read utilisé pour lire un attribut	601
Figure 56 – MSC du service Read utilisé pour appeler une méthode.....	601
Figure 57 – MSC du service Read utilisé pour lire un attribut, avec transfert de blocs.....	602
Figure 58 – MSC du service Write utilisé pour écrire un attribut	606
Figure 59 – MSC du service Write utilisé pour appeler une méthode.....	606
Figure 60 – MSC du service Write utilisé pour écrire un attribut, avec transfert de blocs.....	607
Figure 61 – MSC du service UnconfirmedWrite utilisé pour écrire un attribut	608
Figure 62 – Appels de service partiels et APDU GBT	611
Figure 63 – Procédure de GBT	614

Figure 64 – Sous-procédure Envoyer le flux d'APDU GBT	618
Figure 65 – Sous-procédure Traiter l'APDU GBT	620
Figure 66 – Sous-procédure Vérifier la RQ et combler les trous	622
Figure 67 – Service GET avec GBT, passage à la diffusion en flux	623
Figure 68 – Service GET avec appels partiels, GBT et en flux, récupération du 4 ^e bloc envoyé dans le 2 ^e flux	625
Figure 69 – Service GET avec appels partiels, GBT et en flux, récupération des 4 ^e et 5 ^e blocs	626
Figure 70 – Service GET avec appels partiels, GBT et en flux, récupération du dernier bloc.....	627
Figure 71 – Service SET avec GBT, avec serveur ne prenant pas en charge du flux, récupération du 3 ^e bloc	628
Figure 72 – Service ACTION-WITH-LIST avec GBT bidirectionnel et récupération de blocs.....	629
Figure 73 – Service DataNotification avec GBT, avec appel partiel	631
Figure B.1 – Couche d'adaptation réduite	676
Figure C.1 – Architecture générale avec passerelle	677
Figure C.2 – Champs utilisés pour le préfixage des APDU COSEM.....	678
Figure C.3 – Tableau de séquence de messages Pull	679
Figure C.4 – Tableau de séquence de messages Push	680
Figure I.1 – MSC pour agrément de clé utilisant le schéma Ephemeral Unified Model C(2e, 0s, ECC CDH)	747
Figure I.2 – APDU xDLMS chiffrée protégée par une clé éphémère établie à l'aide d'un schéma One-pass Diffie-Hellman (1e, 1s, ECC CDH)	750
Figure I.3 – APDU xDLMS chiffrée protégée par une clé éphémère établie à l'aide du schéma de modèle unifié statique C(0e, 2s, ECC CDH)	754
Figure J.1 – Échange d'APDU xDLMS protégées entre TP et serveur: exemple 1	758
Figure J.2 – Échange d'APDU xDLMS protégées entre TP et serveur: exemple 2	759
Tableau 1 – SAP client et serveur	418
Tableau 2 —Explication de la signification des paramètres PDU Size pour DLMS®/COSEM.....	440
Tableau 3 – Courbes elliptiques dans les suites de sécurité DLMS®/COSEM	459
Tableau 4 – Récapitulatif de mécanisme d'agrément de clé Ephemeral Unified Model	464
Tableau 5 – Récapitulatif de mécanisme d'agrément de clé One-pass Diffie-Hellman	466
Tableau 6 – Récapitulatif du mécanisme d'agrément de clé du modèle unifié statique	468
Tableau 7 – Sous-champs et sous-chaînes <i>OtherInfo</i>	469
Tableau 8 – ID d'algorithmes de sécurité	470
Tableau 9 – Suites de sécurité DLMS®/COSEM	471
Tableau 10 – Types de clés symétriques	473
Tableau 11 – Informations relatives aux clés avec APDU general-ciphering et protection des données	474
Tableau 12 – Types de clés asymétriques et leur utilisation	476
Tableau 13 – Structure de certificat X.509 v3.....	481
Tableau 14 – Champs du tbsCertificate X.509 v3	482

Tableau 15 – Schéma de nommage pour l'instance de la Root-CA (informatif).....	483
Tableau 16 – Schéma de nommage pour l'instance de la Sub-CA (informatif).....	483
Tableau 17 – Schéma de nommage pour l'instance de l'entité finale.....	483
Tableau 18 – Extensions de certificat X.509 v3.....	485
Tableau 19 – Extensions KeyUsage.....	486
Tableau 20 – Valeurs Subject Alternative Name (nom alternatif d'objet).....	487
Tableau 21 – Valeurs Issuer Alternative Name (nom alternatif de l'émetteur).....	487
Tableau 22 – Valeurs de l'extension Basic Constraints.....	488
Tableau 23 – Certificats traités par des entités finales DLMS®/COSEM.....	489
Tableau 24 – Valeurs de la politique de sécurité ("Security setup" version 1).....	494
Tableau 25 – Valeurs des droits d'accès ("Association LN" ver 3, "Association SN" ver 4).....	495
Tableau 26 – APDU xDLMS chiffrées.....	496
Tableau 27 – Octet de contrôle de sécurité.....	498
Tableau 28 – Texte brut et données supplémentaires authentifiées.....	498
Tableau 29 – Utilisation des champs des APDU xDLMS de chiffrement.....	502
Tableau 30 – Exemple: APDU xDLMS glo-get-request.....	503
Tableau 31 – Service ACCESS avec le mécanisme d'agrément de clé One-pass Diffie-Hellman C(1e, 1s, ECC CDH) et general-ciphering.....	505
Tableau 32 – Mécanismes d'authentification HLS DLMS®/COSEM.....	509
Tableau 33 – Exemple de HLS utilisant le mécanisme d'authentification 5 avec GMAC.....	510
Tableau 34 – Exemple de HLS utilisant le mécanisme d'authentification 7 avec ECDSA.....	511
Tableau 35 – Codes des paramètres de service de l'AL.....	514
Tableau 36 – Paramètres de service des primitives de service COSEM-OPEN.....	515
Tableau 37 – Paramètres de service des primitives de service COSEM-RELEASE.....	520
Tableau 38 – Paramètres de service des primitives de service COSEM-ABORT.....	523
Tableau 39 – Paramètres de service supplémentaires.....	525
Tableau 40 – Paramètres de sécurité.....	526
Tableau 41 – APDU utilisées avec les types de protections de sécurité (Security_Protection_Type).....	528
Tableau 42 – Paramètres de service du service GET.....	530
Tableau 43 – Types de demandes et de réponses du service GET.....	531
Tableau 44 – Paramètres de service du service SET.....	533
Tableau 45 – Types de demandes et de réponses du service SET.....	534
Tableau 46 – Paramètres de service du service ACTION.....	537
Tableau 47 – Types de demandes et de réponses du service ACTION.....	538
Tableau 48 – Paramètres de service du service ACCESS.....	545
Tableau 49 – Paramètres de service des primitives de service DataNotification.....	548
Tableau 50 – Paramètres de service des primitives de service EventNotification.....	550
Tableau 51 – Paramètres de service de la primitive de service TriggerEventNotificationSending.request.....	551
Tableau 52 – Spécification d'accès variable.....	551
Tableau 53 – Paramètres de service du service Read.....	552
Tableau 54 – Utilisation des variantes du paramètre Variable_Access_Specification et des choix pour Read.response.....	554

Tableau 55 – Paramètres de service du service Write.....	557
Tableau 56 – Utilisation des variantes de Variable_Access_Specification et des choix pour Write.response.....	558
Tableau 57 – Paramètres de service du service UnconfirmedWrite	560
Tableau 58 – Utilisation des variantes de Variable_Access_Specification	560
Tableau 59 – Paramètres de service du service InformationReport	562
Tableau 60 – Paramètres de service des primitives de service SetMapperTable.request	562
Tableau 61 – Récapitulatif des services ACSE.....	563
Tableau 62 – Récapitulatif des services xDLMS.....	563
Tableau 63 – APDU d'unité fonctionnelle et leurs champs.....	568
Tableau 64 – Noms de contexte d'application COSEM.....	572
Tableau 65 – Noms de mécanismes d'authentification COSEM.....	572
Tableau 66 – ID d'algorithmes cryptographiques.....	573
Tableau 67 – Bloc de conformité xDLMS.....	583
Tableau 68 – Types de service GET et APDU	585
Tableau 69 – Types de service SET et APDU	589
Tableau 70 – Types de service ACTION et APDU	592
Tableau 71 – Mise en correspondance du service GET et du service Read.....	599
Tableau 72 – Mise en correspondance du service ACTION et du service Read.....	600
Tableau 73 – Mise en correspondance du service SET et du service Write	603
Tableau 74 – Mise en correspondance du service ACTION et du service Write.....	604
Tableau 75 – Mise en correspondance du service SET et du service UnconfirmedWrite.....	608
Tableau 76 – Mise en correspondance du service ACTION et du service UnconfirmedWrite	608
Tableau 77 – Mise en correspondance des services EventNotification et InformationReport	609
Tableau 78 – Variables d'états de la procédure de GBT.....	616
Tableau 79 – Mécanisme d'exception xDLMS	632
Tableau B.1 – Processus d'application réservés	676
Tableau D.1 – Bloc de conformité	683
Tableau D.2 – Codage A-XDR de l'APDU xDLMS InitiateRequest	684
Tableau D.3 – Codage A-XDR de l'APDU xDLMS InitiateResponse	685
Tableau D.4 – Codage BER de l'APDU AARQ	688
Tableau D.5 – APDU AARQ complète	690
Tableau D.6 – Codage BER de l'APDU AARE.....	691
Tableau D.7 – APDU AARE complète	695
Tableau E.1 – Codage A-XDR de l'APDU xDLMS InitiateRequest	697
Tableau E.2 – Cryptage authentifié de l'APDU xDLMS InitiateRequest	698
Tableau E.3 – Codage BER de l'APDU AARQ.....	699
Tableau E.4 – Codage A-XDR de l'APDU xDLMS InitiateResponse	701
Tableau E.5 – Cryptage authentifié de l'APDU xDLMS InitiateResponse.....	702
Tableau E.6 – Codage BER de l'APDU AARE	703
Tableau E.7 – Codage BER de l'APDU RLRQ.....	704
Tableau E.8 – Codage BER de l'APDU RLRE	705

Tableau F.1 – Objets utilisés dans les exemples	706
Tableau F.2 – Exemple: lecture de la valeur d'un attribut unique sans transfert de blocs	707
Tableau F.3 – Exemple: lecture de la valeur d'une liste d'attributs sans transfert de blocs	708
Tableau F.4 – Exemple: lecture de la valeur d'un attribut unique avec transfert de blocs	710
Tableau F.5 – Exemple: lecture de la valeur d'une liste d'attributs avec transfert de blocs	712
Tableau F.6 – Exemple: écriture de la valeur d'un attribut unique sans transfert de blocs	715
Tableau F.7 – Exemple: écriture de la valeur d'une liste d'attributs sans transfert de blocs	716
Tableau F.8 – Exemple: écriture de la valeur d'un attribut unique avec transfert de blocs	718
Tableau F.9 – Exemple: écriture de la valeur d'une liste d'attributs avec transfert de blocs	720
Tableau F.10 – Exemple: service ACCESS sans transfert de bloc général	723
Tableau F.11 – Tampon "Profile generic" – get-response avec codage normal	730
Tableau F.12 – Tampon "Profile generic" – get-response avec compression null-data	732
Tableau F.13 – Tampon "Profile generic" – get-response avec codage compact-array	735
Tableau F.14 – Tampon "Profile generic" – get-response avec codage null-data et delta-value	738
Tableau F.15 – Comparaison de différentes méthodes de codage pour l'APDU get-response	740
Tableau F.16 – Combinaison des différentes méthodes de codage et compression V.44 pour l'APDU get-response	741
Tableau G.1 – ECC_P256_Domain_Parameters	742
Tableau G.2 – ECC_P384_Domain_Parameters	743
Tableau H.1 – Champs des certificats de clé publique utilisant P-256 signé avec P-256	744
Tableau I.1 – Vecteur d'essai pour agrément de clé utilisant le schéma Ephemeral Unified Model C(2e, 0s, ECC CDH)	748
Tableau I.2 – Vecteur d'essai pour agrément de clé utilisant le schéma One-pass Diffie-Hellman (1e, 1s, ECC CDH)	751
Tableau I.3 – Vecteur d'essai pour agrément de clé utilisant le schéma de modèle unifié statique (0e, 2s, ECC CDH)	755