ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

ILNAS

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

ILNAS-EN 62056-5-3:2017

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

Datenkommunikation der elektrischen Energiemessung - DLMS/COSEM - Teil 5-3: DLMS/COSEM-Anwendungsschicht

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

11/2017

Avant-propos national

Cette Norme Européenne EN 62056-5-3:2017 a été adoptée comme Norme Luxembourgeoise ILNAS-EN 62056-5-3:2017.

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

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

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 62056-5-3:2017

NORME EUROPÉENNE
EUROPÄISCHE NORM
EUROPEAN STANDARD

EN 62056-5-3

Novembre 2017

ICS 17.220; 35.110; 91.140.50

Remplace EN 62056-5-3:2016

Version française

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

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

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

La présente Norme Européenne a été adoptée par le CENELEC le 2017-09-14. 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, Ancienne République yougoslave de Macédoine, 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 Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

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

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

© 2017 CENELEC Tous droits d'exploitation sous quelque forme et de quelque manière que ce soit réservés dans le monde entier aux membres du CENELEC.

Avant-propos européen

Le texte du document 13/1744/FDIS, future édition 3 de l'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 62056-5-3:2017.

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) 2018-06-14
- date limite à laquelle les normes nationales conflictuelles doivent être annulées (dow) 2020-09-14

Ce document remplace l' EN 62056-5-3:2016.

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.

Notice d'entérinement

Le texte de la Norme internationale IEC 62056-5-3:2017 a été approuvé par le CENELEC comme Norme Européenne sans aucune modification.

Dans la version officielle, ajouter dans la Bibliographie les notes suivantes pour les normes indiquées:

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

1) A publier. Au stade de projet.

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

Annexe ZA
(normative)
Références normatives aux 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 Des informations actualisées sur les versions les plus récentes des Normes européennes répertoriées dans la présente annexe sont disponibles sur: www.cenelec.eu.

Publication	Année	Titre	EN/HD	Année
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 62056-6-2	2017	Échange des données de comptage de l'électricité - La suite DLMS/COSEM - Partie 6-2: Classes d'interfaces COSEM	FprEN 62056-6-2	2017
IEC 62056-8-3	2013	Échange des 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/TR 62051	1999	Lecture des compteurs électriques - Glossaire de termes	-	-
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	-	-
ISO/IEC 8824-1	-	Technologies de l'information - Notation de syntaxe abstraite numéro un (ASN.1): Spécification de la notation de base	-	-
ISO/IEC 8825-1	2015	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	Information technology - Open Systems Interconnection - Service definition for the application service object association control service element	-	-
ISO/IEC 15954	1999	Information technology - Open Systems Interconnection - Connection-mode protocol for the application service object association control service element	-	-
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)	-	-
ITU-T V.44	2000	Series V: Data Communication over the telephone network - Error control - Data compression procedure	-	-

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

ITU-T X.509	2008	Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks	-	-
ITU-T X.693	-	Information technology - ASN.1 encoding rules: XML Encoding rules (XER)	-	-
ITU-T X.693 Corrigendum 1	-	Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) Technical Corrigendum 1	-	-
ITU-T X.694	-	Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1	-	-
ITU-T X.694 Corrigendum	-	Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 Technical corrigendum 1	-	-
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	-	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC	-	-
NIST SP 800-56A rev2	-	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	-	-
NIST SP 800-57	-	Recommendation for Key Management, Part 1: General (Revision 3)	-	-
NSA1	-	Suite B Implementer's Guide to FIPS 186-3- (ECDSA)		-
NSA2	-	Suite B Implementer's guide to NIST SP800-56A	-	-
NSA3	-	NSA Suite B Base Certificate and CRL Profile	-	-
RFC 3394	-	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 5280	-	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	-	-

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

IEC 62056-5-3

Edition 3.0 2017-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

IEC 62056-5-3:2017-08(en-fr)

SOMMAIRE

AVANT-PROPOS 358
INTRODUCTION 360
1 Domaine d'application 361
2 Références normatives 361
3 Termes, définitions, abréviations et symboles 363
3.1 Définitions générales concernant DLMS/COSEM 363
3.2 Définitions liées à la sécurité chiffrée 366
3.3 Définitions et abréviations liées au mode Galois/Counter 377
3.4 Abréviations générales 378
3.5 Symboles liés au mode Galois/Counter 382
3.6 Symboles liés à l'algorithme ECDSA 383
3.7 Symboles liés aux algorithmes à agrément de clé 383
4 Aperçu de DLMS/COSEM 384
4.1 Échange d'informations dans DLMS/COSEM 384
4.1.1 Généralités 384
4.1.2 Modèle de communication 384
4.1.3 Dénomination et adressage 386
4.1.4 Opération orientée connexion 389
4.1.5 Associations d'applications 390
4.1.6 Types de messageries 392
4.1.7 Échange de données entre des tierces parties et des serveurs DLMS/COSEM 393
4.1.8 Profils de communication 393
4.1.9 Modèle de système de comptage DLMS/COSEM 396
4.1.10 Modèle de serveurs DLMS/COSEM 396
4.1.11 Modèle d'un client DLMS/COSEM 399
4.1.12 Interopérabilité et interconnectivité dans DLMS/COSEM 401
4.1.13 Garantie de l'interconnectivité: service d'identification de protocole 402
4.1.14 Intégration de système et installation de comptage 402
4.2 Caractéristiques principales de la couche application DLMS/COSEM 403
4.2.1 Généralités 403
4.2.2 Structure de la couche application DLMS/COSEM 403
4.2.3 L'élément de service de contrôle d'association, ACSE 406
4.2.4 Élément de service d'application xDLMS 407
4.2.5 Services de gestion de couche 414
4.2.6 Récapitulatif des services de la couche application DLMS/COSEM 414
4.2.7 Protocoles de la couche application DLMS/COSEM 415
5 Sécurité des informations dans DLMS/COSEM 416
5.1 Aperçu 416
5.2 Concept de sécurité DLMS/COSEM 416
5.2.1 Aperçu 416
5.2.2 Identification et authentification 416
5.2.3 Contexte de sécurité 421
5.2.4 Droits d'accès 421
5.2.5 Sécurité des messages de la couche application 421
5.2.6 Sécurité des données COSEM 424
5.3 Algorithmes cryptographiques 424

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

5.3.1 Aperçu 424
5.3.2 Fonction de hachage 425
5.3.3 Algorithmes à clé symétrique 426
5.3.4 Algorithmes à clé publique 433
5.3.5 Génération de nombres aléatoires 446
5.3.6 Compression 446
5.3.7 Suite de sécurité 446
5.4 Clés cryptographiques – aperçu 447
5.5 Clés utilisées avec des algorithmes à clé symétrique 447
5.5.1 Types de clés symétriques 447
5.5.2 Informations relatives aux clés avec APDU general-ciphering et protection des données 450
5.5.3 Identification de clé 451
5.5.4 Enveloppement de clé 451
5.5.5 Agrément de clé 451
5.5.6 Périodes cryptographiques à clé symétrique 452
5.6 Clés utilisées avec des algorithmes à clé publique 452
5.6.1 Aperçu 452
5.6.2 Génération de paires de clés 453
5.6.3 Certificats de clé publique et infrastructure à clé publique 453
5.6.4 Certificat et profil d'extension de certificat 456
5.6.5 Types de certificats d'entités finales de la Suite B à prendre en charge par les serveurs DLMS/COSEM 464
5.6.6 Gestion des certificats 465
5.7 Application de la protection cryptographique 470
5.7.1 Aperçu 470
5.7.2 Protection des APDU xDLMS 470
5.7.3 Protection multicouche par plusieurs parties 487
5.7.4 Mécanismes d'authentification HLS 487
5.7.5 Protection des données COSEM 490
6 Spécification de service de la couche application DLMS/COSEM 491
6.1 Primitives de service et paramètres 491
6.2 Service COSEM-OPEN 494
6.3 Service COSEM-RELEASE 499
6.4 Service COSEM-ABORT 502
6.5 Paramètres de protection et de transfert général de blocs 503
6.6 Service GET 509
6.7 Service SET 512
6.8 Service ACTION 516
6.9 Service ACCESS 519
6.9.1 Aperçu – Principales fonctionnalités 519
6.9.2 Spécification de service 521
6.10 Service DataNotification 526
6.11 Service EventNotification 527
6.12 Service TriggerEventNotificationSending 528
6.13 Spécification d'accès variable 529
6.14 Service Read 530
6.15 Service Write 534
6.16 Service UnconfirmedWrite 537

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

6.17 Service InformationReport 539
6.18 Services de gestion de couches côté client: Demande SetMapperTable.request 540
6.19 Récapitulatif des services et de la mise en correspondance de services de transfert de données LN/SN 540
7 Spécification du protocole de couche application DLMS/COSEM 541
7.1 Fonction de commande 541
7.1.1 Définitions des états de la fonction de commande côté client 541
7.1.2 Définitions des états de la fonction de commande côté serveur 543
7.2 Services ACSE et APDU 544
7.2.1 Unités fonctionnelles ACSE, services et paramètres de service 544
7.2.2 Noms COSEM enregistrés 547
7.2.3 Règles de codage d'APDU 550
7.2.4 Protocole d'établissement d'association d'applications 550
7.2.5 Protocole de libération d'association d'applications 556
7.3 Protocole des services de transfert de données 562
7.3.1 Négociation de services et d'options – Bloc de conformité 562
7.3.2 Appels de service confirmés et non confirmés 563
7.3.3 Protocole du service GET 564
7.3.4 Protocole du service SET 569
7.3.5 Protocole du service ACTION 572
7.3.6 Protocole du service ACCESS 575
7.3.7 Protocole du service DataNotification 576
7.3.8 Protocole du service EventNotification 577
7.3.9 Protocole du service Read 577
7.3.10 Protocole du service Write 583
7.3.11 Protocole du service UnconfirmedWrite 588
7.3.12 Protocole du service InformationReport 589
7.3.13 Protocole du mécanisme de transfert général de blocs 590
8 Syntaxe abstraite des APDU ACSE et COSEM 605
9 Schéma XML des APDU COSEM 618
9.1 Généralités 618
9.2 Schéma XML 619
Annexe A (normative) Utilisation de la couche application DLMS/COSEM dans différents profils de communication 640
A.1 Généralités 640
A.2 Environnements de communication ciblés 640
A.3 Structure du profil 640
A.4 Schémas d'identification et d'adressage 640
A.5 Services de couche de support et mise en correspondance de services 641
A.6 Paramètres spécifiques au profil de communication des services d'AL COSEM 641
A.7 Considérations / contraintes spécifiques à l'utilisation de certains services dans un profil donné 641
A.8 Profil de communication à 3 couches, orienté connexion et basé sur HDLC 641
A.9 Profils de communication basés sur TCP-UDP/IP (COSEM_on_IP) 641
A.10 Profils de communication M-Bus câblés et sans fil 641
A.11 Profil CPL S-FSK 641

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

Annexe B (normative) Couche d'adaptation réduite pour SMS 642
Annexe C (normative) Protocole passerelle 643
C.1 Généralités 643
C.2 Protocole passerelle 644
C.3 HES dans le WAN/NN agissant comme Initiator (initiateur; Opération Pull) 645
C.4 Dispositifs finaux dans le LAN agissant comme Initiators (initiateurs, opération Push) 646
C.4.1 Généralités 646
C.4.2 Dispositif final ayant des connaissances sur le WAN/NN 647
C.4.3 Dispositifs finaux sans connaissances sur le WAN/NN 648
C.5 Sécurité 648
Annexe D (informative) Exemples de codages AARQ et AARE 649
D.1 Généralités 649
D.2 Codage des APDU xDLMS InitiateRequest/InitiateResponse 649
D.3 Spécification des APDU AARQ et AARE 652
D.4 Données pour les exemples 653
D.5 Codage de l'APDU AARQ 654
D.6 Codage de l'APDU AARE 657
Annexe E (informative) Exemples de codages: APDU AARQ et AARE utilisant un contexte d'application crypté 663
E.1 Codage A-XDR de l'APDU xDLMS InitiateRequest contenant une clé dédiée 663
E.2 Chiffrement authentifié de l'APDU xDLMS InitiateRequest 664
E.3 APDU AARQ 665
E.4 Codage A-XDR de l'APDU xDLMS InitiateResponse 667
E.5 Chiffrement authentifié de l'APDU xDLMS InitiateResponse 668
E.6 APDU AARE 669
E.7 APDU RLRQ (contenant une APDU xDLMS InitiateRequest chiffrée) 671
E.8 APDU RLRE (contenant une APDU xDLMS InitiateResponse chiffrée) 671
Annexe F (informative) Exemples de services de transfert de données 673
F.1 Exemples GET / Read, SET / Write 673
F.2 Exemple de service ACCESS 690
F.3 Exemple de codage compact-array 691
F.3.1 Généralités 691
F.3.2 Spécification de compact-array 691
F.3.3 Exemple 1: Codage compact-array d'un array de cinq valeurs long-unsigned 693
F.3.4 Exemple 2: Codage compact-array de cinq valeurs octet-string 694
F.3.5 Exemple 3: Codage du tampon d'un objet générique Profile (profil) 695
Annexe G (normative) Courbes elliptiques et paramètres de domaine de la Suite B NSA 698
Annexe H (informative) Exemple de certificat de signature d'entité finale utilisant P-256 signé avec P-256 700
Annexe I (normative) Utilisation des mécanismes d'agrément de clé dans DLMS/COSEM 702
I.1 Schéma Ephemeral Unified Model C(2e, 0s, ECC CDH) 702
I.2 Schéma Diffie-Hellman en une passe C(1e, 1s, ECC CDH) 705
I.3 Schéma de modèle unifié statique C(0e, 2s, ECC CDH) 710

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

Annexe J (informative) Échange d'APDU xDLMS protégées entre TP et serveur 715
J.1 Généralités 715
J.2 Exemple 1: Protection similaire dans les deux sens 715
J.3 Exemple 2: Protection différente dans les deux sens 717
Annexe K (informative) Modifications techniques majeures par rapport à l'IEC 62056-5-3:2016 720
Bibliographie 723
Index 727

Figure 1 – Modèle client–serveur et protocoles de communication 386
Figure 2 – Dénomination et adressage dans DLMS/COSEM 387
Figure 3 – Session complète de communication dans l'environnement CO 390
Figure 4 – Types de messageries DLMS/COSEM 393
Figure 5 – Profil générique de communication DLMS/COSEM 395
Figure 6 – Modèle de système de comptage DLMS/COSEM 396
Figure 7 – Modèle de serveur DLMS/COSEM 399
Figure 8 – Modèle de client DLMS/COSEM utilisant plusieurs piles de protocoles 401
Figure 9 – Structure des couches d'application DLMS/COSEM 405
Figure 10 – Concept de messages xDLMS composables 412
Figure 11 – Récapitulatif des services de l'AL DLMS/COSEM 415
Figure 12 – Mécanismes d'authentification 419
Figure 13 – Conception de sécurité des messages client-serveur 422
Figure 14 – Concept de sécurité de bout en bout de messages 424
Figure 15 – Fonction de hachage 426
Figure 16 – Chiffrement et déchiffrement 427
Figure 17 – Codes d'authentification de message (MAC) 428
Figure 18 – Fonctions du GCM 430
Figure 19 – Signatures numériques 437
Figure 20 – Schéma C(2e, 0s): chaque partie apporte uniquement une paire de clés éphémères 439
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 441
Figure 22 – Schéma C(0e, 2s): chaque partie apporte uniquement une paire de clés statiques 443
Figure 23 – Architecture d'une infrastructure à clé publique (exemple) 456
Figure 24 – MSC pour l'approvisionnement du serveur en certificats de la CA 466
Figure 25 – MSC pour la personnalisation de sécurité du serveur 467
Figure 26 – Approvisionnement du serveur en certificat du client 468
Figure 27 – Approvisionnement du client/de la tierce partie en certificat du serveur 469
Figure 28 – Suppression de certificat du serveur 470
Figure 29 – Protection cryptographique des informations utilisant AES-GCM 475
Figure 30 – Structure des APDU xDLMS de chiffrement global spécifique au service / de chiffrement dédié spécifique au service 477
Figure 31 – Structure des APDU xDLMS general-glo-ciphering et general-ded-ciphering 479

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

Figure 32 – Structure des APDU xDLMS general-ciphering 480
Figure 33 – Structure des APDU general-signing 486
Figure 34 – Primitives de service 491
Figure 35 – Diagrammes de séquences temporelles 492
Figure 36 – Paramètres supplémentaires de service pour contrôler la protection cryptographique et le GBT 505
Figure 37 – Diagramme d'états partiel pour la fonction de commande côté client 542
Figure 38 – Diagramme d'états partiel pour la fonction de commande côté serveur 543
Figure 39 – MSC pour l'établissement réussi d'une AA précédé de l'établissement réussi d'une connexion de couche inférieure de support 553
Figure 40 – Libération d'AA sans perte de données à l'aide du service A-RELEASE 558
Figure 41 – Libération d'AA sans perte de données par déconnexion de la couche de support 560
Figure 42 – Abandon d'une AA après la primitive PH-ABORT.indication 562
Figure 43 – MSC du service GET 565
Figure 44 – MSC du service GET avec transfert de blocs 566
Figure 45 – MSC du service GET avec transfert de blocs, GET long abandonné 568
Figure 46 – MSC du service SET 570
Figure 47 – MSC du service SET avec transfert de blocs 570
Figure 48 – MSC du service ACTION 573
Figure 49 – MSC du service ACTION avec transfert de bloc 574
Figure 50 – Service ACCESS avec réponse longue 575
Figure 51 – Service ACCESS avec demande et réponse longues 576
Figure 52 – MSC du service Read utilisé pour lire un attribut 580
Figure 53 – MSC du service Read utilisé pour appeler une méthode 581
Figure 54 – MSC du service Read utilisé pour lire un attribut, avec transfert de blocs 582
Figure 55 – MSC du service Write utilisé pour écrire un attribut 586
Figure 56 – MSC du service Write utilisé pour appeler une méthode 586
Figure 57– MSC du service Write utilisé pour écrire un attribut, avec transfert de blocs 587
Figure 58 – MSC du service UnconfirmedWrite utilisé pour écrire un attribut 589
Figure 59 – Appels de service partiels et APDU GBT 592
Figure 60 – Service GET avec GBT, passage à la diffusion en flux 594
Figure 61 – Service GET avec appels partiels, GBT et diffusion en flux, récupération du 4e bloc envoyé dans le deuxième flux 596
Figure 62 – Service GET avec appels partiels, GBT et diffusion en flux, récupération des 4e et 5e blocs 597
Figure 63 – Service GET avec appels partiels, GBT et diffusion en flux, récupération du dernier bloc 599
Figure 64 – Service SET avec GBT, avec serveur ne prenant pas en charge la diffusion en flux, récupération du 3e bloc 600
Figure 65 – Service ACTION-WITH-LIST avec GBT bidirectionnel et récupération de blocs 602
Figure 66 – Service DataNotification avec GBT, avec appel partiel 604
Figure B.1 – Couche d'adaptation réduite 642
Figure C.1 – Architecture générale avec passerelle 644
Figure C.2 – Champs utilisés pour le préfixage des APDU COSEM 644

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

Figure C.3 – Tableau de séquences de messages Pull 646
Figure C.4 – Tableau de séquences de messages Push 647
Figure I.1 – MSC pour agrément de clé utilisant le schéma Ephemeral Unified Model C(2e, 0s, ECC CDH) 703
Figure I.2 – APDU xDLMS chiffrée protégée par une clé éphémère établie à l'aide d'un schéma Diffie-Hellman en une passe (1e, 1s, ECC CDH) 706
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) 712
Figure J.1 – Échange d'APDU xDLMS protégées entre TP et serveur: exemple 1 717
Figure J.2 – Échange d'APDU xDLMS protégées entre TP et serveur: exemple 2 719

Tableau 1 – SAP client et serveur 388
Tableau 2 – Explication de la signification des paramètres PDU Size pour DLMS/COSEM 414
Tableau 3 – Courbes elliptiques dans les suites de sécurité DLMS/COSEM 435
Tableau 4 – Récapitulatif de mécanisme d'agrément de clé Ephemeral Unified Model 440
Tableau 5 – Récapitulatif de mécanisme d'agrément de clé Diffie-Hellman en une passe 442
Tableau 6 – Récapitulatif du mécanisme d'agrément de clé du modèle unifié statique 444
Tableau 7 – Sous-champs et sous-chaînes *OtherInfo* 445
Tableau 8 – ID d'algorithmes cryptographiques 446
Tableau 9 – Suites de sécurité DLMS/COSEM 447
Tableau 10 – Types de clés symétriques 449
Tableau 11 – Informations relatives aux clés avec APDU general-ciphering et protection des données 450
Tableau 12 – Types de clés asymétriques et leur utilisation 452
Tableau 13 – Structure de certificat X.509 v3 457
Tableau 14 – Champs du tbsCertificate X.509 v3 458
Tableau 15 – Schéma de dénomination pour l'instance de la Root-CA (informatif) 459
Tableau 16 – Schéma de dénomination pour l'instance de la Sub-CA (informatif) 459
Tableau 17 – Schéma de dénomination pour l'instance de l'entité finale 459
Tableau 18 – Extensions de certificat X.509 v3 461
Tableau 19 – Extensions Key Usage 462
Tableau 20 – Valeurs Subject Alternative Name (nom alternatif d'objet) 463
Tableau 21 – Valeurs Issuer Alternative Name (nom alternatif de l'émetteur) 463
Tableau 22 – Valeurs de l'extension Basic constraints 464
Tableau 23 – Certificats traités par des entités finales DLMS/COSEM 465
Tableau 24 – Valeurs de la politique de sécurité («Security setup» version 1) 471
Tableau 25 – Valeurs des droits d'accès («Association LN» ver 3 «Association SN» ver 4) 472
Tableau 26 – APDU xDLMS chiffrées 473
Tableau 27 – Octet de contrôle de sécurité 475
Tableau 28 – Texte brut et données supplémentaires authentifiées 476
Tableau 29 – Utilisation des champs des APDU xDLMS de chiffrement 481
Tableau 30 – Exemple: APDU xDLMS glo-get-request 482

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

Tableau 31 – Service ACCESS avec le mécanisme d'agrément de clé Diffie-Hellman en une passe C(1e, 1s, ECC CDH) et general-ciphering 484
Tableau 32 – Mécanismes d'authentification HLS DLMS/COSEM 488
Tableau 33 – Exemple de HLS utilisant le mécanisme d'authentification 5 avec GMAC 489
Tableau 34 – Exemple de HLS utilisant le mécanisme d'authentification 7 avec ECDSA 490
Tableau 35 – Codes des paramètres de service de l'AL 493
Tableau 36 – Paramètres de service des primitives de service COSEM-OPEN 495
Tableau 37 – Paramètres de service des primitives de service COSEM-RELEASE 500
Tableau 38 – Paramètres de service des primitives de service COSEM-ABORT 503
Tableau 39 – Paramètres supplémentaires de service 505
Tableau 40 – Paramètres de sécurité 506
Tableau 41 – APDU utilisées avec les types de protections de sécurité (Security_Protection_Type) 508
Tableau 42 – Paramètres de service du service GET 510
Tableau 43 – Types de demandes et de réponses du service GET 511
Tableau 44 – Paramètres de service du service SET 513
Tableau 45 – Types de demandes et de réponses du service SET 514
Tableau 46 – Paramètres de service du service ACTION 516
Tableau 47 – Types de demandes et de réponses du service ACTION 517
Tableau 48 – Paramètres de service du service ACCESS 523
Tableau 49 – Paramètres de service des primitives de service DataNotification 526
Tableau 50 – Paramètres de service des primitives de service EventNotification 527
Tableau 51– Paramètres de service de la primitive de service TriggerEventNotificationSending.request 528
Tableau 52 – Spécification d'accès variable 529
Tableau 53 – Paramètres de service du service Read 531
Tableau 54 – Utilisation des variantes du paramètre Variable_Access_Specification et des choix de Read.response 532
Tableau 55 – Paramètres de service du service Write 535
Tableau 56 – Utilisation des variantes de Variable_Access_Specification et des choix de Write.response 536
Tableau 57 – Paramètres de service du service UnconfirmedWrite 538
Tableau 58 – Utilisation des variantes de Variable_Access_Specification 538
Tableau 59 – Paramètres de service du service InformationReport 539
Tableau 60 – Paramètres de service des primitives de service SetMapperTable.request 540
Tableau 61 – Récapitulatif des services ACSE 540
Tableau 62 – Récapitulatif des services xDLMS 541
Tableau 63 – APDU d'unité fonctionnelle et leurs champs 545
Tableau 64 – Noms de contexte d'application COSEM 549
Tableau 65 – Noms de mécanismes d'authentification COSEM 549
Tableau 66 – ID d'algorithmes cryptographiques 550
Tableau 67 – Bloc de conformité xDLMS 563
Tableau 68 – Types et APDU de service GET 565
Tableau 69 – Types et APDU de service SET 569
Tableau 70 – Types et APDU de service ACTION 572

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

Tableau 71 – Mise en correspondance du service GET et du service Read 578
Tableau 72 – Mise en correspondance du service ACTION et du service Read 579
Tableau 73 – Mise en correspondance du service SET et du service Write *(1 sur 2)* 583
Tableau 74 – Mise en correspondance du service ACTION et du service Write 584
Tableau 75 – Mise en correspondance du service SET et du service UnconfirmedWrite 588
Tableau 76 – Mise en correspondance du service ACTION et du service UnconfirmedWrite 588
Tableau 77 – Mise en correspondance des services EventNotification et InformationReport 590
Tableau B.1 – Processus d'application réservés 642
Tableau D.1 – Bloc de conformité 650
Tableau D.2 – Codage A-XDR de l'APDU xDLMS InitiateRequest 651
Tableau D.3 – Codage A-XDR de l'APDU xDLMS InitiateResponse 652
Tableau D.4 – Codage BER de l'APDU AARQ 655
Tableau D.5 – APDU AARQ complète 657
Tableau D.6 – Codage BER de l'APDU AARE 658
Tableau D.7 – APDU AARE complète 662
Tableau E.1 – Codage A-XDR de l'APDU xDLMS InitiateRequest 664
Tableau E.2 – Chiffrement authentifié de l'APDU xDLMS InitiateRequest 665
Tableau E.3 – Codage BER de l'APDU AARQ 666
Tableau E.4– Codage A-XDR de l'APDU xDLMS InitiateResponse 668
Tableau E.5 – Chiffrement authentifié de l'APDU xDLMS InitiateResponse 669
Tableau E.6 – Codage BER de l'APDU AARE 670
Tableau E.7 – Codage BER de l'APDU RLRQ 671
Tableau E.8 – Codage BER de l'APDU RLRE 672
Tableau F.1 – Objets utilisés dans les exemples 673
Tableau F.2 – Exemple: Lecture de la valeur d'un attribut unique sans transfert de blocs 674
Tableau F.3 – Exemple: Lecture de la valeur d'une liste d'attributs sans transfert de blocs 675
Tableau F.4 – Exemple: Lecture de la valeur d'un attribut unique avec transfert de blocs 677
Tableau F.5 – Exemple: Lecture de la valeur d'une liste d'attributs avec transfert de blocs 679
Tableau F.6 – Exemple: Écriture de la valeur d'un attribut unique sans transfert de blocs 682
Tableau F.7 – Exemple: Écriture de la valeur d'une liste d'attributs sans transfert de blocs 683
Tableau F.8 – Exemple: Écriture de la valeur d'un attribut unique avec transfert de blocs 685
Tableau F.9 – Exemple: Écriture de la valeur d'une liste d'attributs avec transfert de blocs 687
Tableau F.10 – Exemple: Service ACCESS sans transfert général de blocs 690
Tableau G.1 – ECC_P256_Domain_Parameters 698
Tableau G.2 – ECC_P384_Domain_Parameters 699

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

Tableau I.1 – Vecteur d'essai pour agrément de clé utilisant le schéma Ephemeral Unified Model C(2e, 0s, ECC CDH)..... 704

Tableau I.2 – Vecteur d'essai pour agrément de clé utilisant le schéma Diffie-Hellman en une passe (1e, 1s, ECC CDH)..... 708

Tableau I.3 – Vecteur d'essai pour agrément de clé utilisant le schéma de modèle unifié statique (0e, 2s, ECC CDH)..... 713

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

ÉCHANGE DES DONNÉES DE COMPTAGE DE L'ÉLECTRICITÉ – LA SUITE DLMS/COSEM –

Partie 5-3: Couche application DLMS/COSEM

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Commission Électrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité aux dispositions de la présente Norme internationale peut impliquer l'utilisation d'un service de maintenance concernant la pile de protocoles sur laquelle est basée la présente norme IEC 62056-5-3.

L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ce service de maintenance.

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

Le fournisseur du service de maintenance a donné l'assurance à l'IEC qu'il consent à fournir des services avec des demandeurs du monde entier, à des termes et conditions raisonnables et non discriminatoires. À ce propos, la déclaration du fournisseur du service de maintenance est enregistrée à l'IEC. Des informations peuvent être demandées à:

DLMS[1] User Association
Zug/Switzerland
www.dlms.com

La Norme internationale IEC 62056-5-3 a été établie par le comité d'études 13 de l'IEC: Comptage et pilotage de l'énergie électrique.

Cette troisième édition annule et remplace la deuxième édition de l'IEC 62056-5-3 parue en 2016. Cette édition constitue une révision technique.

Les modifications techniques majeures par rapport à l'édition précédente sont énumérées à l'Annexe K (Informative).

La présente version bilingue (2018-04) correspond à la version anglaise monolingue publiée en 2017-08.

Le texte anglais de cette norme est issu des documents 13/1744/FDIS et 13/1747/RVD.

Le rapport de vote 13/1747/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62056, publiées sous le titre général *Échange des données de comptage de l'électricité – La suite DLMS/COSEM*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo «colour inside» qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

[1] Device Language Message Specification (Spécification de message de langage de dispositif).

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop

INTRODUCTION

Cette troisième édition de l'IEC 62056-5-3 a été établie par le groupe de travail 14 du comité d'études 13 de l'IEC avec la contribution significative de la DLMS User Association, son partenaire de liaison de type D.

Cette édition est conforme à DLMS UA 1000-2, le «Green Book» Éd. 8.2:2017. Les principales nouvelles fonctions sont le service ACCESS, les nouvelles suites de sécurité 1 et 2 prenant en charge la cryptographie à clé symétrique et à clé asymétrique, le mécanisme de protection générale et le schéma XML pour les APDU COSEM.

L'Article 5 est basé sur des parties de documents du NIST. Réimprimé avec l'aimable autorisation du NIST (National Institute of Standards and Technology), Technology Administration, U.S. Department of Commerce.

ILNAS-EN 62056-5-3:2017 - Preview only Copy via ILNAS e-Shop