

SOMMAIRE

AVANT-PROPOS	87
INTRODUCTION	89
1 Domaine d'application	90
2 Références normatives	90
3 Termes, définitions, termes abrégés et notation	91
3.1 Termes et définitions	91
3.2 Termes abrégés	92
3.3 Notation	93
4 Conventions de numérotation utilisées dans le présent document	93
5 Modèle de référence d'un compteur intelligent	93
5.1 Diagramme fonctionnel générique de référence	93
5.2 Modèle de référence de protocole de transfert de jetons	95
5.3 Flux de données du POSApplicationProcess vers le TokenCarrier	96
5.4 Flux de données du TokenCarrier vers le MeterApplicationProcess	96
5.5 MeterFunctionObjects / spécifications d'accompagnement	97
6 Protocole de couche application POSToTokenCarrierInterface	97
6.1 APDU: ApplicationProtocolDataUnit	97
6.1.1 Eléments de données dans l'APDU	97
6.1.2 SupplierID	100
6.1.3 MeterID	100
6.1.4 TokenOriginationID	100
6.1.5 MessageIdentifier	100
6.1.6 SequentialTokenNumber (STN)	101
6.1.7 TruncatedSequentialTokenNumber (TSTN)	102
6.1.8 Déduction de la partie MS du STN et validation du TSTN	102
6.1.9 FunctionIndex	105
6.1.10 Lien entre le FunctionIndex et le STN	106
6.1.11 SingleTokenPayload	108
6.1.12 SuperTokenPayload	108
6.1.13 MessageAuthenticationCode (MAC) et TruncatedMAC (TMAC)	109
6.1.14 AdditionalAuthenticationData (AAD)	111
6.1.15 Préparation de l'AAD de la SingleTokenPayload, dérivation du TMAC et préparation de l'APDU	111
6.1.16 Préparation de l'AAD de la SuperTokenPayload, dérivation du TMAC et préparation de l'APDU	112
6.1.17 Décalage	115
6.2 Jetons	115
6.2.1 Définition et format des jetons	115
6.2.2 Class 4: RESERVEE POUR UNE FUTURE AFFECTATION	116
6.2.3 Jetons de Class 5	116
6.2.4 Classe 5: jetons non chiffrés	120
6.2.5 Classe 5: jetons chiffrés	122
6.3 Eléments de données des jetons	128
6.4 Fonctions de génération de la TCDU	129
6.5 Fonctions de sécurité	131
6.5.1 Exigences générales	131
6.5.2 Gestion des clés	131

6.5.3	Dérivation de clé.....	132
6.5.4	Processus de chiffrement	132
7	Protocole de couche application TokenCarriertoMeterInterface	132
7.1	APDU: ApplicationProtocolDataUnit	132
7.1.1	Eléments de données dans l'APDU.....	132
7.1.2	TokenData.....	132
7.1.3	AuthenticationResult.....	132
7.1.4	ValidationResult	133
7.1.5	TokenResult	133
7.2	Processus d'extraction de l'APDU	134
7.2.1	Processus d'extraction de l'APDU pour les jetons de Class 5	134
7.2.2	Processus d'extraction de l'APDU pour les jetons non chiffrés de SubClass 0	135
7.2.3	Processus d'extraction de l'APDU pour les jetons chiffrés de SubClass 8	135
7.3	Fonctions de sécurité.....	136
7.3.1	Attributs de clé et changements de clé	136
7.3.2	Algorithme de déchiffrement	137
7.3.3	TokenAuthentication	137
7.3.4	TokenValidation.....	137
7.3.5	TokenResult	138
8	Exigences du MeterApplicationProcess	138
8.1	Exigences générales.....	138
8.2	Acceptation/rejet des jetons	138
8.3	Indicateurs d'affichage et marquages.....	139
8.4	Jetons TransferCredit	139
8.5	Jetons Engineering/SpecialFunction	140
9	KMS: exigences génériques relatives au KeyManagementSystem	140
10	Maintenance des entités non affectées	140
Annexe A (informative)	Exemple de mise en œuvre du code de Verhoeff.....	141
A.1	Echantillon de code	141
Annexe B (informative)	Exemple de jeton ExtendedTransferCredit.....	143
B.1	Classe 5: SubClass 10: TransferCredit + Tariff	143
B.1.1	Généralités	143
B.1.2	Séquence de blocs/SuperTokenBlockToFollow	143
B.1.3	Plein tarif.....	144
B.1.4	Sous-informations tarifaires	144
B.1.5	Mois d'activation du tarif.....	144
B.1.6	Données tarifaires	145
B.1.7	Type de tarif	145
B.1.8	Sous-informations tarifaires	145
B.2	Class 5, SubClass 10, type de tarif 0: TransferCredit + tarif par tranche ou basé sur la période d'utilisation.....	146
B.2.1	Class 5, SubClass 10, type de tarif 0, sous-type 0: TransferCredit + tarif par tranche	146
B.2.2	Nombre de limites de tranche	147
B.2.3	Conversion des tranches	147
B.2.4	Taille des champs des tranches.....	148
B.2.5	Valeur de la tranche	148

B.2.6	Class 5, SubClass 10, type de tarif 0, sous-type 1: TransferCredit + tarif basé sur la période d'utilisation (TOU).....	148
B.2.7	Définition des jours de la semaine	149
B.2.8	Définition des périodes	149
B.2.9	Définition des registres	150
B.3	Class 5, SubClass 10, type de tarif 1: Format des jetons TransferCredit + prix par tarif ou prix des charges fixes	151
B.3.1	Class 5, SubClass 10, type de tarif 1: sous-information tarifaires	151
B.3.2	Class 5, SubClass 10, type de tarif 1, sous-type 0: TransferCredit + prix par tarif.....	151
B.3.3	Class 5, SubClass 10, type de tarif 1: sous-information tarifaires	152
B.3.4	Nombre de prix par tarif	152
B.3.5	Multiplicateur de prix par tarif	152
B.3.6	Taille du champ de prix par tarif.....	153
B.3.7	Valeur de prix par tarif	153
B.3.8	Class 5, SubClass 10, type de tarif 1, sous-type 1: TransferCredit + prix des charges fixes.....	154
B.3.9	Nombre de prix des charges fixes	154
B.3.10	Multiplicateur de prix des charges fixes	154
B.3.11	Taille du champ de prix des charges fixes	154
B.3.12	Application des charges fixes	155
B.3.13	Valeur de prix des charges fixes	155
B.4	Class 5, SubClass 10, type de tarif 2: Format du jeton TransferCredit + taxe sur l'électricité (ED)	155
B.4.1	Taxe sur l'électricité (ED)	155
B.4.2	Taxe sur l'électricité sur les charges d'énergie	156
B.4.3	Taxe sur l'électricité sur les charges fixes.....	156
B.4.4	Nombre de tranches de taxes sur l'électricité.....	156
B.4.5	Taux de taxe sur l'électricité	156
B.4.6	Taille de tranche de la taxe sur l'électricité	157
B.5	Processus détaillé de génération de la TCDU pour la SubClass 0	158
B.6	Processus détaillé de génération de la TCDU pour la SubClass 8	158
B.7	Processus détaillé de génération de la TCDU pour la SubClass 10	159
B.8	Processus détaillé d'extraction de l'APDU pour la SubClass 10	160
	Bibliographie.....	163
	Figure 1 – Organigramme fonctionnel d'un compteur à paiement générique.....	94
	Figure 2 – Modèle de référence sous forme de pile protocolaire OSI réduite à 2 couches	95
	Figure 3 – Modèle générique du POSApplicationProcess vers le TokenCarrier	96
	Figure 4 – Flux de données du TokenCarrier vers le MeterApplicationProcess.....	96
	Figure 5 – Eléments de données génériques pour la construction de la charge utile de l'AAD pour la SingleTokenPayload.....	109
	Figure 6 – Eléments de données génériques pour la construction de la charge utile de l'AAD pour la SuperTokenPayload	110
	Figure 7 – Construction du InitializationVector (IV)	110
	Figure 8 – Construction du GMAC.....	111
	Figure 9 – Exemple de dérivation du TMAC de la SubClass 8 de Class 5 et de préparation d'APDU complète	112

Figure 10 – Exemple de dérivation du TMAC de la SubClass 10 de Class 5 et de préparation d'APDU complète	114
Figure 11 – Génération de la TCDU pour les jetons non chiffrés de SubClass 0.....	130
Figure 12 – Génération de la TCDU pour les jetons chiffrés de SubClass 8	131
Figure 13 – Processus d'extraction de l'APDU pour les jetons de Class 0	135
Figure 14 – Processus d'extraction de l'APDU pour les jetons de Class 8	136
Figure B.1 – Processus de génération de la TCDU pour la SubClass 0	158
Figure B.2 – Processus de génération de la TCDU pour la SubClass 8	159
Figure B.3 – Processus de génération de la TCDU pour la SubClass 10	160
Figure B.4 – Processus d'extraction de l'APDU pour la SubClass 10	161
 Tableau 1 – Eléments Basic et Derived pour la construction de l'APDU	97
Tableau 2 – Détail du MessageIdentifier par sous-classe et classe fonctionnelle SubClass	100
Tableau 3 – Exemple de définition de L_N et U_N pour chaque SubClass	103
Tableau 4 – Processus de validation du STN et de déduction du MS(N)	104
Tableau 5 – Exemple (a) de dernier jeton accepté	104
Tableau 6 – Exemple (b) de dernier jeton accepté	104
Tableau 7 – Exemple (c) de dernier jeton accepté	105
Tableau 8 – Exemple (d) de dernier jeton accepté	105
Tableau 9 – Constantes numériques et leur finalité.....	115
Tableau 10 – Définition et format des jetons	116
Tableau 11 – Affectation des SubClass de la Class 5	117
Tableau 12 – Limites de SubClass pour l'APDU de Class 5 avant chiffrement.....	118
Tableau 13 – Limites de SubClass pour les jetons de Class 5, TCDU après chiffrement (si applicable) et ajout du décalage (sans CheckDigit)	118
Tableau 14 – Limites de SubClass de la Class 5 pour la TCDU (espace réservé)	119
Tableau 15 – FunctionalClass liée à la SubClass et cas d'utilisation associés	120
Tableau 16 – SubClass 0: jeton TransferCredit	121
Tableau 17 – SubClass 8: jeton TransferCredit	122
Tableau 18 – Class 5, SubClass 9: Jeton SpecialFunction	122
Tableau 19 – Types de service	123
Tableau 20 – Bloc 1 du jeton TransferCredit + Function	124
Tableau 21 – Bloc 2 à $N-1$ du jeton TransferCredit + Function N ($N > 2$).....	125
Tableau 22 – Dernier bloc du jeton TransferCredit + Function.....	125
Tableau 23 – Bloc 1 pour la structure du jeton de SubClass 11 de Class 5 généré par le compteur.....	126
Tableau 24 – Bloc 2 pour la structure du jeton de SubClass 11 de Class 5 généré par le compteur.....	126
Tableau 25 – Eléments de données des jetons	129
Tableau 26 – Eléments de données dans l'APDU.....	132
Tableau 27 – Valeurs possibles pour AuthenticationResult	133
Tableau 28 – Valeurs possibles pour ValidationResult	133
Tableau 29 – Valeurs possibles pour TokenResult.....	134

Tableau B.1 – Bloc 1 du jeton TransferCredit + Tariff.....	143
Tableau B.2 – Bloc 2 du jeton TransferCredit + Tariff.....	143
Tableau B.3 – Bloc 3 du jeton TransferCredit + Tariff.....	145
Tableau B.4 – Bloc 4 du jeton TransferCredit + Tariff.....	145
Tableau B.5 – Types de tarif.....	145
Tableau B.6 – Détails des sous-informations tarifaires.....	146
Tableau B.7 – Bloc 2 pour la Class 5, SubClass 10, type de tarif 0, sous-type 0 (TransferCredit + tarif par tranche)	147
Tableau B.8 – Bloc 2 pour la Class 5, SubClass 10, type de tarif 0, sous-type 0 (TransferCredit + tarif par tranche) – partie des données tarifaires	147
Tableau B.9 – Bloc 3 pour la Class 5, SubClass 10, type de tarif 0, sous-type 0 (TransferCredit + tarif par tranche)	148
Tableau B.10 – Bloc 2 pour la Class 5, SubClass 10, type de tarif 0, sous-type 1 (TransferCredit + tarif basé sur la période d'utilisation)	149
Tableau B.11 – Bloc 3 pour la Class 5, SubClass 10, type de tarif 0, sous-type 1 (TransferCredit + tarif basé sur la période d'utilisation)	150
Tableau B.12 – Bloc 4 pour la Class 5, SubClass 10, type de tarif 0, sous-type 1 (TransferCredit + tarif basé sur la période d'utilisation)	150
Tableau B.13 – Bloc 2 pour la Class 5, SubClass 10, type de tarif 1, sous-type 0 (TransferCredit + prix par tarif)	151
Tableau B.14 – Bloc 2 pour la Class 5, SubClass 10, type de tarif 1, sous-type 0 (TransferCredit + prix par tarif) – Données tarifaires	152
Tableau B.15 – Bloc 3 pour la Class 5, SubClass 10, type de tarif 1, sous-type 0 (TransferCredit + prix par tarif)	153
Tableau B.16 – Bloc 4 pour la Class 5, SubClass 10, type de tarif 1, sous-type 0 (TransferCredit + prix par tarif)	153
Tableau B.17 – Bloc 2 pour la Class 5, SubClass 10, type de tarif 1, sous-type 1 (TransferCredit + prix des charges fixes)	154
Tableau B.18 – Bloc 2 pour la Class 5, SubClass 10, type de tarif 1, sous-type 1 (TransferCredit + prix des charges fixes) – Données tarifaires	154
Tableau B.19 – Bloc 2 pour la Class 5, SubClass 10, type de tarif 2, sous-type 0 (TransferCredit + taxe sur l'électricité)	155
Tableau B.20 – Bloc 2 pour la Class 5, SubClass 10, type de tarif 2, sous-type 0 (TransferCredit + taxe sur l'électricité) – Champs de données	156
Tableau B.21 – Codage de la valeur des tranches de la taxe sur l'électricité	157
Tableau B.22 – Bloc 3 pour la Class 5, SubClass 10, type de tarif 2, sous-type 0 (TransferCredit + taxe sur l'électricité)	158

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

COMPTAGE DE L'ÉLECTRICITÉ – SYSTÈMES DE PAIEMENT –

Partie 42: Numéros de référence des transactions (TRN)

AVANT-PROPOS

- 1) La Commission Electrotechnique 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. A 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 propriété et averti de leur existence.

L'IEC 62055-42 a été établie par le comité d'études 13 de l'IEC: Comptage et pilotage de l'énergie électrique. Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
13/1843/CDV	13/1860/RVC

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 62055, publiées sous le titre général *Comptage de l'électricité – Systèmes de paiement*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de ce document 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.

INTRODUCTION

La série IEC 62055 identifie et applique le concept d'interopérabilité entre les couches dans les domaines du comptage intelligent et des réseaux intelligents.

Elle assure également l'interopérabilité des éléments du système au-dessus de la couche sémantique afin d'intégrer les couches d'interopérabilité des fonctions et processus métier au sein d'un système de comptage de l'électricité, en assurant ainsi la compatibilité globale à tous ces niveaux.

Le présent document est fondé sur les principes des normes IEC 62055 et établit les règles qui assureront la cohérence des futures extensions, en fournissant ainsi aux entreprises de distribution un vocabulaire commun pour formuler des exigences dans le cadre d'appels d'offres, et aux vendeurs une base de connaissances unifiée pour l'interprétation des exigences relatives aux appels d'offres.

Le présent document fait partie de la série IEC 62055 et partage plusieurs références avec l'IEC 62055-41, les deux normes représentant les jetons TransferCredit en utilisant des supports de jetons à 20 chiffres. En revanche, l'IEC 62055-41 et l'IEC 62055-42 présentent de nettes différences pour ce qui est du codage, du mécanisme de sécurité et des cas d'utilisation prévue. L'IEC 62055-41 porte essentiellement sur les systèmes hors ligne, alors que l'IEC 62055-42 est principalement destinée aux systèmes en ligne dans lesquels le support de jeton décimal fait office de mécanisme de secours pour la vente lorsque les compteurs sont hors ligne par intermittence.

L'IEC TC13 a spécifiquement développé la série IEC 62055 pour les systèmes de comptage de l'électricité, mais cette série peut également s'appliquer à d'autres services d'utilité publique tels que l'eau et le gaz.

COMPTAGE DE L'ÉLECTRICITÉ – SYSTÈMES DE PAIEMENT –

Partie 42: Numéros de référence des transactions (TRN)

1 Domaine d'application

Le présent document spécifie un mécanisme de génération de jetons ainsi que la structure de jetons associée à la fonctionnalité de prépaiement intelligent, destinée aux marchés où les systèmes conformes à l'IEC 62055-41 ne sont pas utilisés et lorsque les exigences nationales ou spécifiques à un projet imposent l'utilisation d'un autre mécanisme de sécurité. Le présent document spécifie la structure des jetons, leur authentification, un mécanisme antirediffusion, le modèle d'exploitation des jetons et le protocole associé.

Le présent document est informé par les services de gestion de clés de la STS Association ainsi que par les mécanismes de gestion de clés utilisés dans le modèle de sécurité DLMS/COSEM spécifié dans l'IEC 62056-6-2. Une référence est faite aux normes internationales relatives aux jetons STS (IEC 62055-41, IEC 62055-51 et IEC 62055-52) pour les systèmes de comptage à paiement, et l'interconnexion a été envisagée le cas échéant en ce qui concerne les plages des supports de jetons dans le domaine décimal. Les jetons conformes à l'IEC 62055-41 et ceux décrits dans le présent document ne sont pas interopérables, mais leurs domaines sont conçus pour être mutuellement exclusifs afin d'assurer que les deux types de jetons n'interfèrent pas l'un avec l'autre.

Le traitement et la fonctionnalité des applications de comptage ainsi que les commandes et attributs des interfaces HAN et WAN ne relèvent pas du domaine d'application du présent document. Une référence est toutefois faite à d'autres normes traitant de ces aspects.

Le mécanisme d'audit et de récupération des données du compteur relatives à la tarification, des relevés de compteurs, des données sur les profils et autres informations métrologiques légales ne relève pas du domaine d'application du présent document. Il est cependant défini dans le cadre de toute solution de comptage globale. Il est permis de définir de telles interfaces pour la récupération des données d'un compteur en utilisant des protocoles adaptés, tels que DLMS/COSEM défini dans la série IEC 62056.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils 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).

IEC 60050-300:2001, *Vocabulaire Electrotechnique International (IEV) – Partie 300: Mesures et appareils de mesure électriques et électroniques – Partie 311: Termes généraux concernant les mesures – Partie 312: Termes généraux concernant les mesures électriques – Partie 313: Types d'appareils électriques de mesure – Partie 314: Termes spécifiques selon le type d'appareil*

IEC 60050-300:2001/AMD1:2015

IEC 60050-300:2001/AMD2:2016

IEC 60050-300:2001/AMD3:2017

IEC 60050-300:2001/AMD4:2020

IEC TR 62051:1999, *Electricity metering - Glossary of terms (disponible en anglais seulement)*

IEC TR 62055-21:2005, *Electricity metering – Payment systems – Part 21: Framework for standardization* (disponible en anglais seulement)

IEC 62055-31:2005, *Equipements de comptage de l'électricité – Systèmes à paiement – Partie 31: Exigences particulières – Compteurs statiques à paiement d'énergie active (classes 1 et 2)*

IEC 62055-41:2018, *Partie 41: Spécification de transfert normalisé (STS) – Protocole de couche application pour les systèmes de supports de jeton unidirectionnel*

IEC 62056-5-3:2017, *Echange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 5-3: Couche application DLMS/COSEM*

IEEE EUI-64, <https://standards.ieee.org/develop/regauth/tut/eui64.pdf>

Verhoeff, J., 1975, *Error Detecting Decimal Codes* (Mathematical Centre Tracts, 29)

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

3 Termes, définitions, termes abrégés et notation

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'IEC 60050-300:2001, l'IEC TR 62051:1999, l'IEC 62055-31:2005, l'IEC 62055-41:2018 et l'IEC TR 62055-21:2005, ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <http://www.iso.org/obp>

NOTE Lorsqu'il existe une différence entre les définitions du présent document et celles contenues dans d'autres normes IEC de référence, les définitions du présent document prévalent.

3.1.1 **spécification d'accompagnement**

ensemble d'exigences et de choix opérés à partir d'une norme de base, spécifique à une région, un consortium ou un fabricant, afin de faciliter un ensemble particulier de cas d'utilisation

3.1.2 **compteur**

instrument de mesure; synonyme de "compteur à paiement" et de "décodeur" lorsque le décodeur est une sous-partie d'une installation à dispositifs multiples

3.1.3 **POS**

point de vente; entité qui peut créer et transférer des jetons, synonyme de "SIC" (système d'information des consommateurs), "SIG" (système d'informations de gestion) et "TSP" (terminal de saisie portable)

3.1.4 **super jeton**

groupe de chiffres issus de plusieurs blocs de données de l'APDU, qui doivent être saisis les uns à la suite des autres pour former un message de plus grande taille