

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



**Electricity metering – Payment systems –  
Part 42: Transaction Reference Numbers (TRN)**

**Comptage de l'électricité – Systèmes de paiement –  
Partie 42: Numéros de référence des transactions (TRN)**

<https://standards.iteh.ai/catalog/standards/sist/a0cbb879-c886-4a42-be7b-8d1a3f7d5dd0/iec-62055-42-2022>



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2022 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

### About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

### About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

#### IEC publications search - [webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: [sales@iec.ch](mailto:sales@iec.ch).

#### IEC Products & Services Portal - [products.iec.ch](http://products.iec.ch)

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

### A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

### A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

#### Recherche de publications IEC -

[webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

#### Service Clients - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: [sales@iec.ch](mailto:sales@iec.ch).

#### IEC Products & Services Portal - [products.iec.ch](http://products.iec.ch)

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



**Electricity metering – Payment systems –  
Part 42: Transaction Reference Numbers (TRN)**

**Comptage de l'électricité – Systèmes de paiement –  
Partie 42: Numéros de référence des transactions (TRN)**

<https://standards.iteh.ai/catalog/standards/sist/a0cbb879-c886-4a42-be7b-8d1a3f7d5dd0/iec-62055-42-2022>

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

ICS 17.220.20, ICS 35.100.70, ICS 91.140.50

ISBN 978-2-8322-3951-3

**Warning! Make sure that you obtained this publication from an authorized distributor.  
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

## CONTENTS

FOREWORD.....	7
INTRODUCTION.....	9
1 Scope.....	10
2 Normative references .....	10
3 Terms, definitions, abbreviated terms and notation.....	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms.....	12
3.3 Notation.....	13
4 Numbering conventions in this document.....	13
5 Reference smart meter model.....	13
5.1 Generic functional reference diagram.....	13
5.2 Token transfer protocol reference model.....	15
5.3 Dataflow from the POSApplicationProcess to the TokenCarrier.....	16
5.4 Dataflow from the TokenCarrier to the MeterApplicationProcess .....	16
5.5 MeterFunctionObjects / companion specifications .....	17
6 POSToTokenCarrierInterface application layer protocol.....	17
6.1 APDU: ApplicationProtocolDataUnit.....	17
6.1.1 Data elements in the APDU .....	17
6.1.2 SupplierID .....	19
6.1.3 MeterID .....	19
6.1.4 TokenOriginationID.....	19
6.1.5 MessageIdentifier .....	19
6.1.6 SequentialTokenNumber (STN).....	21
6.1.7 TruncatedSequentialTokenNumber (TSTN).....	21
6.1.8 Deducing the MS part of STN and validating TSTN.....	21
6.1.9 FunctionIndex.....	24
6.1.10 Relating the FunctionIndex and STN.....	25
6.1.11 SingleTokenPayload .....	27
6.1.12 SuperTokenPayload .....	27
6.1.13 MessageAuthenticationCode (MAC) and TruncatedMAC (TMAC).....	27
6.1.14 AdditionalAuthenticationData (AAD).....	30
6.1.15 SingleTokenPayload AAD preparation, TMAC derivation and APDU preparation .....	30
6.1.16 SuperTokenPayload AAD preparation, TMAC derivation and APDU preparation .....	31
6.1.17 Offset .....	34
6.2 Tokens.....	34
6.2.1 Token definition and format .....	34
6.2.2 Class 4: RESERVED FOR FUTURE ASSIGNMENT .....	35
6.2.3 Class 5 tokens.....	35
6.2.4 Class 5: Unencrypted tokens .....	39
6.2.5 Class 5: Encrypted tokens .....	41
6.3 Token data elements.....	47
6.4 TCDU Generation functions .....	47
6.5 Security functions .....	49
6.5.1 General requirements .....	49
6.5.2 Key management.....	49

6.5.3	Key derivation.....	50
6.5.4	Encryption process .....	50
7	TokenCarrierToMeterInterface application layer protocol .....	50
7.1	APDU: ApplicationProtocolDataUnit .....	50
7.1.1	Data elements in the APDU .....	50
7.1.2	TokenData .....	50
7.1.3	AuthenticationResult.....	50
7.1.4	ValidationResult .....	51
7.1.5	TokenResult .....	51
7.2	APDU Extraction processes .....	52
7.2.1	APDU Extraction process for Class 5 tokens.....	52
7.2.2	APDU Extraction process for SubClass 0 unencrypted token .....	53
7.2.3	APDU Extraction process for SubClass 8 encrypted token .....	53
7.3	Security functions .....	54
7.3.1	Key attributes and key changes .....	54
7.3.2	Decryption algorithm.....	55
7.3.3	TokenAuthentication .....	55
7.3.4	TokenValidation.....	55
7.3.5	TokenResult .....	55
8	MeterApplicationProcess requirements .....	56
8.1	General requirements .....	56
8.2	Token acceptance/rejection .....	56
8.3	Display indicators and markings.....	57
8.4	TransferCredit tokens .....	57
8.5	Engineering/SpecialFunction tokens .....	57
9	KMS: KeyManagementSystem generic requirements .....	58
10	Maintenance of unassigned entities .....	58
	Annex A (informative) Verhoeff code implementation example .....	59
A.1	Sample code .....	59
	Annex B (informative) Example of ExtendedTransferCredit .....	61
B.1	Class 5: SubClass 10: TransferCredit + Tariff .....	61
B.1.1	General .....	61
B.1.2	Block sequence/SuperTokenBlockToFollow .....	61
B.1.3	Complete tariff.....	62
B.1.4	Tariff sub-information.....	62
B.1.5	Tariff activation month .....	62
B.1.6	Tariff data .....	63
B.1.7	Tariff types .....	63
B.1.8	Tariff sub-information.....	63
B.2	Class 5, SubClass 10, tariff type 0: TransferCredit + slab or time-of-use tariff.....	64
B.2.1	Class 5, SubClass 10, tariff type 0, sub-type 0: TransferCredit + slab tariff.....	64
B.2.2	Number of slab boundaries .....	65
B.2.3	Slab scaling.....	65
B.2.4	Slab field size .....	65
B.2.5	Slab value .....	66
B.2.6	Class 5, SubClass 10, tariff type 0, sub-type 1: TransferCredit + time of use (TOU) tariff .....	66
B.2.7	Week definition.....	66

B.2.8	Time period definitions .....	67
B.2.9	Register definitions .....	68
B.3	Class 5, SubClass 10, tariff type 1: TransferCredit + rate prices or fixed charge price token format .....	68
B.3.1	Class 5, SubClass 10, tariff type 1: tariff sub-information .....	68
B.3.2	Class 5, SubClass 10, tariff type 1, sub-type 0: TransferCredit + rate prices .....	68
B.3.3	Class 5, SubClass 10, tariff type 1: tariff sub-information .....	69
B.3.4	Number of rate prices .....	69
B.3.5	Rate price multiplier .....	70
B.3.6	Rate price field size .....	70
B.3.7	Rate price value .....	70
B.3.8	Class 5, SubClass 10, tariff type 1, sub type 1: TransferCredit + fixed charge prices .....	71
B.3.9	Number of fixed charge prices .....	71
B.3.10	Fixed charge price multiplier .....	72
B.3.11	Fixed charge price field size .....	72
B.3.12	Fixed charge application .....	72
B.3.13	Fixed charge price value .....	72
B.4	Class 5, SubClass 10, tariff type 2: TransferCredit + electricity duty (ED) token format .....	72
B.4.1	Electricity duty (ED) .....	72
B.4.2	Electricity duty on energy charges .....	73
B.4.3	Electricity duty on fixed charges .....	73
B.4.4	Number of electricity duty slabs .....	73
B.4.5	Electricity duty rate .....	73
B.4.6	Electricity duty slab size .....	74
B.5	SubClass 0 TCDU generation detailed process .....	75
B.6	SubClass 8 TCDU generation detailed process .....	75
B.7	SubClass 10 TCDU generation detailed process .....	76
B.8	SubClass 10 APDU extraction detailed process .....	77
	Bibliography .....	80
	Figure 1 – Functional block diagram of a generic payment meter .....	14
	Figure 2 – Reference model as a 2-layer collapsed OSI protocol stack .....	15
	Figure 3 – Generic model of POSApplicationProcess to TokenCarrier .....	16
	Figure 4 – Dataflow from the TokenCarrier to the MeterApplicationProcess .....	16
	Figure 5 – Generic data elements for AAD payload construction for SingleTokenPayload .....	28
	Figure 6 – Generic data elements for AAD payload construction for SuperTokenPayload .....	29
	Figure 7 – InitializationVector (IV) construction .....	29
	Figure 8 – GMAC construction .....	30
	Figure 9 – Class 5 SubClass 8 TMAC derivation and full APDU preparation example .....	31
	Figure 10 – Class 5 SubClass 10 TMAC derivation and full APDU preparation example .....	33
	Figure 11 – TCDU generation for SubClass 0 unencrypted tokens .....	48
	Figure 12 – TCDU generation for SubClass 8 encrypted tokens .....	49
	Figure 13 – APDU extraction process for SubClass 0 tokens .....	53

Figure 14 – APDU extraction process for SubClass 8 tokens .....	54
Figure B.1 – TCDU generation process for SubClass 0 .....	75
Figure B.2 – TCDU generation process for SubClass 8 .....	76
Figure B.3 – TCDU generation process for SubClass 10 .....	77
Figure B.4 – APDU extraction process for SubClass 10 .....	78
Table 1 – Basic and derived elements of APDU and TCDU construction .....	17
Table 2 – SubClass-wise MessageIdentifier detail and SubClass Functional Class .....	20
Table 3 – Example of defining $L_N$ and $U_N$ for each SubClass .....	22
Table 4 – Process of validating STN and deducing MS(N) .....	23
Table 5 – Last accepted token example(a) .....	23
Table 6 – Last accepted token example(b) .....	23
Table 7 – Last accepted token example(c) .....	24
Table 8 – Last accepted token example(d) .....	24
Table 9 – Numeric constants and their purpose .....	34
Table 10 – Token definition and format .....	35
Table 11 – Class 5 SubClass assignment .....	36
Table 12 – SubClass-wise boundaries for Class 5 APDU before encryption .....	37
Table 13 – SubClass-wise boundaries for Class 5 tokens, TCDU after encryption (if applicable) and adding offset (without CheckDigit) .....	37
Table 14 – Class 5 SubClass boundaries for TCDU (reserved space) .....	38
Table 15 – SubClass related FunctionalClass and associated use cases .....	39
Table 16 – SubClass 0: TransferCredit token .....	40
Table 17 – SubClass 8: TransferCredit token .....	41
Table 18 – Class 5, SubClass 9: SpecialFunction token .....	41
Table 19 – Service types .....	42
Table 20 – Block 1 of TransferCredit + Function token .....	43
Table 21 – Block 2 to $N-1$ of $N$ ( $N > 2$ ) TransferCredit + Function token .....	44
Table 22 – Last block TransferCredit + Function token .....	44
Table 23 – Block 1 for Class 5 SubClass 11 meter generated token structure .....	45
Table 24 – Block 2 for Class 5 SubClass 11 meter generated token structure .....	45
Table 25 – Token data elements .....	47
Table 26 – Data elements in the APDU .....	50
Table 27 – Possible values for AuthenticationResult .....	51
Table 28 – Possible values for ValidationResult .....	51
Table 29 – Possible values for TokenResult .....	52
Table B.1 – Block 1 of TransferCredit + tariff token .....	61
Table B.2 – Block 2 of TransferCredit + Tariff token .....	61
Table B.3 – Block 3 of TransferCredit + Tariff token .....	63
Table B.4 – Block 4 of TransferCredit + Tariff token .....	63
Table B.5 – Tariff types .....	63
Table B.6 – Details of tariff sub-information .....	64
Table B.7 – Block 2 for class 5, SubClass 10, tariff type 0, sub-type 0 (TransferCredit + slab tariff) .....	64



Table B.8 – Block 2 for Class 5, SubClass 10, tariff type 0, sub-type 0 (TransferCredit + slab tariff) – tariff data part .....	65
Table B.9 – Block 3 for class 5, SubClass 10, tariff type 0, sub-type 0 (TransferCredit + slab tariff).....	66
Table B.10 – Block 2 for class 5, SubClass 10, tariff type 0, sub-type 1 (TransferCredit + time of use tariff) .....	66
Table B.11 – Block 3 for class 5, SubClass 10, tariff type 0, sub-type 1 (TransferCredit + time of use tariff) .....	68
Table B.12 – Block 4 for class 5, SubClass 10, tariff type 0, sub-type 1 (TransferCredit + time of use tariff) .....	68
Table B.13 – Block 2 for class 5, SubClass 10, tariff type 1, sub-type 0 (TransferCredit + rate prices).....	69
Table B.14 – Block 2 for class 5, SubClass 10, tariff type 1, sub-type 0 (TransferCredit + rate prices) – tariff data .....	69
Table B.15 – Block 3 for class 5, SubClass 10, tariff type 1, sub-type 0 (TransferCredit + rate prices).....	70
Table B.16 – Block 4 for class 5, SubClass 10, tariff type 1, sub-type 0 (TransferCredit + rate prices).....	71
Table B.17 – Block 2 for class 5, SubClass 10, tariff type 1, sub-type 1 (TransferCredit + fixed charge prices).....	71
Table B.18 – Block 2 for class 5, SubClass 10, tariff type 1, sub-type 1 (TransferCredit + fixed charge prices) – tariff data .....	71
Table B.19 – Block 2 for class 5, SubClass 10, tariff type 2, sub-type 0 (TransferCredit + electricity duty).....	73
Table B.20 – Block 2 for class 5, SubClass 10, tariff type 2, sub-type 0 (TransferCredit + electricity duty) – data field.....	73
Table B.21 – Electricity duty slab value encoding.....	74
Table B.22 – Block 3 for class 5, SubClass 10, tariff type 2, sub-type 0 (TransferCredit + electricity duty).....	75



## INTERNATIONAL ELECTROTECHNICAL COMMISSION

**ELECTRICITY METERING – PAYMENT SYSTEMS –****Part 42: Transaction Reference Numbers (TRN)**

## FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62055-42 has been prepared by IEC technical committee 13: Electrical energy measurement and control. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
13/1843/CDV	13/1860/RVC

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs). The main document types developed by IEC are described in greater detail at [www.iec.ch/standardsdev/publications](http://www.iec.ch/standardsdev/publications).

A list of all parts in the IEC 62055 series, published under the general title *Electricity metering – Payment systems*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under [webstore.iec.ch](http://webstore.iec.ch) in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

**IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[IEC 62055-42:2022](https://standards.iteh.ai/catalog/standards/sist/a0cbb879-c886-4a42-be7b-8d1a3f7d5dd0/iec-62055-42-2022)

<https://standards.iteh.ai/catalog/standards/sist/a0cbb879-c886-4a42-be7b-8d1a3f7d5dd0/iec-62055-42-2022>

## INTRODUCTION

The IEC 62055 series recognizes and takes into account the concept of layered interoperability for use within the smart metering and smart grid domains.

It also ensures system element interoperability above the semantic layer to include business function and business process interoperability layers within an electricity metering system, thus ensuring overall compatibility at all these levels.

This document is based on the principles the IEC 62055 standards are built on and sets the rules for future extensions to guarantee consistency, thus providing a common vocabulary for use by utilities to express requirements in tenders and also by vendors to have a unified understanding for interpretation of the tender requirements.

This document forms part of the IEC 62055 series and shares some references with IEC 62055-41, in that both standards represent TransferCredit tokens utilising 20-digit token carriers. However, IEC 62055-41 and IEC 62055-42 differ greatly in their encoding, security mechanism and intended use cases. Whereas IEC 62055-41 is meant for predominantly offline systems, IEC 62055-42 is intended for mostly online systems where the decimal token carrier is used as a back-up mechanism for vending while meters are intermittently offline.

The IEC 62055 series has been developed by IEC TC13 specifically for electricity metering systems, but it is equally applicable in the domain of other utility services such as water and gas.

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

[IEC 62055-42:2022](https://standards.iteh.ai/catalog/standards/sist/a0cbb879-c886-4a42-be7b-8d1a3f7d5dd0/iec-62055-42-2022)

<https://standards.iteh.ai/catalog/standards/sist/a0cbb879-c886-4a42-be7b-8d1a3f7d5dd0/iec-62055-42-2022>

# ELECTRICITY METERING – PAYMENT SYSTEMS –

## Part 42: Transaction Reference Numbers (TRN)

### 1 Scope

This document specifies a token generation mechanism and token structure for smart prepayment functionality in markets where IEC 62055-41 compliant systems are not used, and where a different security mechanism is required by project-specific or national requirements. This document specifies token structure, authentication and an anti-replay mechanism, token operating model, and protocol.

This document is informed by the STS Association key management services, and by the key management mechanisms used within the DLMS/COSEM security model within IEC 62056-6-2. Reference is made to the international STS token standards (IEC 62055-41, IEC 62055-51 and IEC 62055-52) for payment metering systems, and interworking has been considered where appropriate in terms of token carrier ranges in the decimal domain. IEC 62055-41 tokens and those described in this document are not interoperable, however their domains are designed to be mutually exclusive to ensure the two kinds of tokens do not interfere with each other.

Metering application processing and functionality, HAN interface commands and attributes, WAN interface commands and attributes are outside the scope of this document; however, reference is made to other standards in this regard.

The mechanism for auditing and retrieving data from the meter relating to tariffication, meter readings, profile data and other legal metrology information is outside the scope of this document; however, this is defined as part of any overall metering solution. Such interfaces for retrieving data from a meter may be defined using suitable protocols such as DLMS/COSEM as defined in the IEC 62056 series.

### 2 Normative references

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

IEC 60050-300:2001, *International Electrotechnical Vocabulary (IEV) – Part 300: Electrical and electronic measurements and measuring instruments – Part 311: General terms relating to measurements – Part 312: General terms relating to electrical measurements – Part 313: Types of electrical measuring instruments – Part 314: Specific terms according to the type of instrument*

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*

IEC TR 62055-21:2005, *Electricity metering – Payment systems – Part 21: Framework for standardization*

IEC 62055-31:2005, *Electricity metering – Payment systems – Part 31: Particular requirements – Static payment meters for active energy (classes 1 and 2)*

IEC 62055-41:2018, *Electricity metering – Payment systems – Part 41: Standard transfer specification – Application layer protocol for one-way token carrier systems*

IEC 62056-5-3:2017, *Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer*

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

Verhoeff, J., 1975, *Error Detecting Decimal Codes*, (Tract 29)

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

### 3 Terms, definitions, abbreviated terms and notation

#### 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-300:2001, IEC TR 62051:1999, IEC 62055-31:2005, IEC 62055-41:2018, IEC 62055-21:2005 and the following apply.

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

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

NOTE Where there is a difference between the definitions in this document and those contained in other referenced IEC standards, then those defined in this document take precedence.

#### 3.1.1 companion specification

regional, consortia, or manufacturer-specific set of requirements and choices taken from a base standard, in order to facilitate a particular set of use cases

#### 3.1.2 meter

measuring instrument; synonymous with “payment meter” and “decoder” where the decoder is a sub-part of a multi-device installation

#### 3.1.3 POS

point of sale; entity that may create and transfer tokens, synonymous with “CIS”, “MIS” and “HHU”

#### 3.1.4 super token

group of digits derived from more than one data block of the APDU that shall be entered together in sequence to form a larger message

#### 3.1.5 utility

retailer or supplier of an energy or water commodity service

Note 1 to entry: In the liberalized markets the actual contracting party acting as the “supplier” of the service to the consumer may not be the traditional utility as such, but may be a third service provider party.

### 3.2 Abbreviated terms

AES	Advanced Encryption Standard
AAD	AdditionalAuthenticatedData
AMT	Amount
APDU	ApplicationProtocolDataUnit
CIS	Customer Information System
COSEM	Companion Specification for Electricity Metering
DLMS	Device Language Message Specification
EUI	Extended Unique Identifier
GMAC	Galois Message Authentication Code
HAN	Home Area Network
HES	Head End System
HHU	Hand Held Unit
HMI	Human to Machine Interface
ID	Identifier
IHD	In-Home Display
IEEE	Institute of Electrical and Electronics Engineers
KMS	Key Management System
LCS	Load Control Switch
LSB	Least Significant Byte
MAC	MessageAuthenticationCode
MIS	Management Information System
MOD	Modulo operation
MS	Most Significant
MSB	Most Significant Byte
NIST	National Institute of Standards and Technology
NSP	National Service Provider
PIN	Personal Identification Number
POS	Point Of Sale
RANDz	Reasonable And Non-Discriminatory with Zero royalty
RES	Reserved
SE	Smart Energy
SMS	Short Message Service
STN	SequentialTokenNumber
STS	Standard Transfer Specification
TC	Technical Committee
TCDU	TokenCarrierDataUnit
TMAC	Truncated Message Authentication Code
TOU	Time Of Use
TSTN	TruncatedSequentialTokenNumber
WAN	Wide Area Network
WG	Working Group

### 3.3 Notation

Entity names, data element names, function names and process names are treated as generic object classes and are given names in terms of phrases in which the words are capitalized and joined without spaces.

NOTE The notation used for naming of objects has been aligned with the so called "camel-notation" used in the common information model (CIM) standards prepared by IEC TC 57, in order to facilitate future harmonization and integration of payment system standards with the CIM standards.

The symbol "||" inserted between two expressions means that the resultant values of the two expressions are concatenated into a single string without separators.

## 4 Numbering conventions in this document

Numbers are in decimal format, unless otherwise indicated. Decimal digit values range from 0 to 9.

Binary digit values range from 0 to 1. Binary numbers are indicated by suffix "b". The representation of binary strings is such that the least significant bit is to the right of the string representation and the most significant bit is to the left of the string. Numbering of bit positions starts with bit position 0 which corresponds to the least significant bit of the binary number.

Hexadecimal digit values range from 0 to 9 and A to F and are indicated by prefix "0x" or suffix "hex".

## 5 Reference smart meter model

### 5.1 Generic functional reference diagram

In the general case any meter designed to be compliant with this document may contain some or all of the functions specified in Figure 1 and a minimum of 1 credit and 1 charge type (more are permitted). The diagram in Figure 1 is provided here for reference and context, but is outside the normative scope of this document.