

	DIN IEC 62055-41 (VDE 0418-5-41)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE

ICS 91.140.50

Einsprüche bis 2005-07-31

Entwurf

**Messung der elektrischen Energie –
Zählersysteme mit Inkassofunktion –
Teil 41: Standardtransferspezifikation – Protokoll der Anwendungsschicht für
Einweg-Tokenträgersysteme
(IEC 13/1333A/CD:2005)**

Electricity Metering –
Payment Systems –
Part 41: Standard Transfer Specification – Application layer protocol for one-way token carrier systems
(IEC 13/1333A/CD:2005)

Anwendungswarnvermerk

Dieser Norm-Entwurf wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an **dke@vde.com** in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter **www.dke.de/stellungnahme** abgerufen werden
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 229 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung des Internationalen Norm-Entwurfs [Committee Draft (CD)] IEC 13/1333A/CD:2005 „Electricity Metering – Payment Systems – Part 41: Standard Transfer Specification – Application layer protocol for one-way token carrier systems“.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den mit aufgenommenen englischen IEC-Text.

Der Internationale Entwurf wurde vom TC 13 „Equipment for electrical energy measurement and load control“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als CD herausgegeben. Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene entstandener Internationaler Norm-Entwurf im Schlusstadium [Final Draft International Standard (FDIS)] zeitgleich (parallel) bei IEC und CENELEC zur Abstimmung gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen.

Da der Abstimmungszeitraum für einen FDIS nur 2 Monate beträgt, und zum FDIS keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit noch vor der Abstimmung berücksichtigen zu können.

Für den vorliegenden Norm-Entwurf ist das nationale Arbeitsgremium K 461 „Elektrizitätszähler“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist nachstehend wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 62051:1999	–	–
	IEC 62055-31:200x	E DIN IEC 62055-31 (VDE 0418-5-31):2001-07	VDE 0418-5-31
–	IEC 62055-51:200x	E DIN IEC 62055-51 (VDE 0418-5-51):2005-06	VDE 0418-5-51

Nationaler Anhang NB (informativ)

Literaturhinweise

E DIN IEC 62055-31 (VDE 0418-5-31), *Messung der elektrischen Energie – Zählersysteme mit Inkassofunktion – Besondere Anforderungen – Elektronische Inkasso-Wirkverbrauchszähler (Klassen 1 und 2) (IEC 13/1226/CD:2000)*

E DIN IEC 62055-51 (VDE 0418-5-51), *Messung der elektrischen Energie – Zählersysteme mit Inkassofunktion – Teil 51: Standardtransferspezifikation – Protokoll der Bitübertragungsschicht für Einweg-Zahlwort- und Magnetkarten-Tokenträger (IEC 13/1334A/CD:2005)*

**Messung der elektrischen Energie
Zählersysteme mit Inkassofunktion
Teil 41: Standardtransferspezifikation – Protokoll der Anwendungsschicht für
Einweg-Tokenträgersysteme**

Inhalt

	Seite
Vorwort	12
Einleitung.....	15
1 Anwendungsbereich	17
2 Normative Verweisungen.....	17
3 Begriffe und Abkürzungen	18
3.1 Begriffe.....	18
3.2 Abkürzungen.....	19
3.3 Notation und Terminologie.....	22
4 Numerierungsvereinbarungen	23
5 Referenzmodell für die Standardtransferspezifikation.....	23
5.1 Funktionales Referenz-Blockdiagramm für Inkassozähler	23
5.2 OSI-Referenzmodell	25
5.3 Datenfluss vom Meter_Application_Process zum Token_Carrier	26
5.4 Datenfluss vom Token_Carrier zum Meter_Application_Process	27
5.5 Begleitspezifikation	27
5.6 ISO-Bezugsnummern für Transaktionen	28
6 POS_to-Token_Carrier_Interface: Protokoll der Anwendungsschicht.....	29
6.1 APDU: Dateneinheit der Anwendungsschicht	29
6.1.1 Meter_PAN: Meter_Primary_Account_Number.....	30
6.1.2 TCT: Token_Carrier_Type.....	31
6.1.3 DKGA: Decoder_Key_Generation_Algorithm.....	31
6.1.4 EA: Encryption_Algorithm.....	32
6.1.5 SGC: Supply_Group_Code	32
6.1.6 TI: Tariff_Index.....	33
6.1.7 KRN: Key_Revision_Number	33
6.1.8 KT: Key_Type	33
6.1.9 KEN: Key_Expiry_Number	33
6.1.10 ED: Expiration_Date	34
6.2 Token	34
6.2.1 Klasse 0: transfer_Credit	35
6.2.2 Klasse 1: Initiate_Meter_Test/Display	35
6.2.3 Klasse 2: set_Maximum_Power_Limit.....	35
6.2.4 Klasse 2: clear_Credit.....	35
6.2.5 Klasse 2: set_Tariff_Rate	36
6.2.6 Klasse 2: set_1st_Section_Decoder_Key (1. Abschnitt des Decoderschlüssels festlegen)	36

	Seite
6.2.7 Klasse 2: set_2nd_Section_Decoder_Key (2. Abschnitt des Decoderschlüssels festlegen).....	36
6.2.8 Klasse 2: clear_Tamper_Condition (Manipulationsbedingung löschen)	36
6.2.9 Klasse 2: set_Maximum_Phase_Power_Unbalance_Limit (oberen Grenzwert der unsymmetrischen Phasenbelastung festlegen)	36
6.2.10 Klasse 2: set_Water_Meter_Factor (Wasserzählerfaktor festlegen)	37
6.2.11 Klasse 2: Reserviert für STS-Anwendungen.....	37
6.2.12 Klasse 2: Reserviert für firmenspezifische Anwendung	37
6.2.13 Klasse 3: Reserviert für STS-Anwendungen.....	37
6.3 Tokendatenelemente	37
6.3.1 Klasse: Token_Class.....	38
6.3.2 Sub_Class: Token_Sub_Class.....	39
6.3.3 RND: Random_Number	39
6.3.4 TID: Token_Identifier	39
6.3.5 Betrag: Transfer_Amount	41
6.3.6 CRC: Cyclic_Redundancy_Code	42
6.3.7 Steuerung: initiate_Meter_Test/Display_control_field.....	42
6.3.8 MPL: Maximum_Power_Limit.....	43
6.3.9 MPUL: Maximum_Phase_Power_Unbalance_Limit	43
6.3.10 Rate: Tariff_Rate	43
6.3.11 WMfactor: Water_Meter_Factor	43
6.3.12 Register: Register_to_clear	44
6.3.13 NKHO: New_Key_High_Order	44
6.3.14 NKLO: New_Key_Low_Order	44
6.3.15 KexpNoHO: Key_Expiry_Number_High_Order	44
6.3.16 KexpNoLO: Key_Expiry_Number_Low_Order.....	44
6.3.17 RO: Rollover_Key_Change	44
6.4 TCDU_Generation-Funktionen.....	44
6.4.1 Transpositionen der Klassen-Bits.....	44
6.4.2 Funktion TCDU_Generation für die Token Klasse 0, 1 und 2.....	46
6.4.3 Funktion TCDU_Generation für Token set_1st_Section_Decoder_Key.....	47
6.4.4 Funktion TCDU_Generation für Token set_2nd_Section_Decoder_Key.....	49
6.5 Sicherheitsfunktionen	50
6.5.1 Schlüsselmerkmale und Schlüsseländerungen	50
6.5.2 Generierung des Decoder_Key.....	57
6.5.3 STA: Encryption_Algorithm_07	63
6.5.4 DEA: Encryption_Algorithm_09.....	66
7 Token_Carrier_to_Meter_Interface: Protokoll der Anwendungsschicht.....	67
7.1 APDU: Application_Protocol_Data_Unit.....	67
7.1.1 Token.....	67
7.1.2 Authentication_Result.....	67

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

	Seite
7.1.3 Validation_Result.....	68
7.1.4 Token_Result.....	68
7.2 APDU_Extraction-Funktionen.....	69
7.2.1 Auskoppeln der 2 Bits für die Klasse.....	69
7.2.2 APDU_Extraction-Funktion für die Token Klasse 0 und Klasse 2.....	70
7.2.3 APDU_Extraction-Funktion für Token Klasse 1.....	71
7.2.4 APDU_Extraction-Funktion für die Token set_1st_Section_Decoder_Key und set_2nd_Section_Decoder_Key.....	71
7.3 Sicherheitsfunktionen.....	72
7.3.1 Schlüsselattribute und Schlüsseländerungen.....	72
7.3.2 DKR: Decoder_Key_Register.....	72
7.3.3 STA: Decryption_Algorithm_07.....	73
7.3.4 DEA: Decryption_Algorithm_09.....	76
7.3.5 Token_Authentication.....	77
7.3.6 Token_Validation.....	77
7.3.7 Token_Cancellation.....	78
8 Anforderungen an den Meter_Application_Process.....	78
8.1 Tokenannahme/Tokenzurückweisung.....	78
8.2 Tokeneingabesperre.....	79
8.3 Anzeiger und Aufschriften an der Anzeige.....	79
8.4 Token transfer_Credit.....	80
8.5 Token initiate_Meter_Test/Display.....	80
8.6 Token set_Maximum_Power_Limit.....	80
8.7 Token clear_Credit.....	80
8.8 Token set_Tariff_Rate.....	80
8.9 Token set_1st_Section_Decoder_Key.....	81
8.10 Token set_2nd_Section_Decoder_Key.....	81
8.11 Token clear_Tamper_Condition.....	81
8.12 Token set_Maximum_Phase_Power_Unbalance_Limit.....	81
8.13 Klasse 2: Reserviert für STS-Token.....	81
8.14 Klasse 2: Reserviert für firmenspezifische Token.....	81
8.15 Klasse 3: Reserviert für STS-Token.....	81
9 Übergeordnete Meter_Function_Objects.....	82
9.1 VMFO: Virtual_Meter_Function_Object.....	83
9.2 CRFO: Configuration_Registry_Function_Object.....	84
9.3 ALFO: Application_Layer_Function_Object.....	85
9.4 PLFO: Physical_Layer_Function_Object.....	86
9.5 FOIN: Function_Object_Identification_Number.....	87
10 KMS: Key_Management_System – Übergeordnete Anforderungen.....	89
Anhang A (informativ) Leitfaden für ein Key_Management_System (KMS).....	90

	Seite
Anhang B (informativ) Entitäten und Kennungen in einem STS-System	93
Anhang C (informativ) Regeln für die Praxis	97
C.1 Wartungs- und Hilfsdienste der STS-Association	97
C.2 Schlüsselverwaltung	97
C.2.1 Verteilung von Supply_Group_Code und Vending_Key	97
C.2.2 Verteilung der Secure_Module	98
C.2.3 Schlüsselverfall	99
C.3 Meter_PAN	99
C.3.1 Issuer_Identification_Numbers	99
C.3.2 Manufacturer_Codes	100
C.3.3 Decoder_Serial_Numbers	100
C.4 Besondere reservierte Token_Identifier	100
C.5 Permutations- und Ersetzungstabellen für den STA Encryption_Algorithm_07	100
C.6 Encryption_Algorithms	101
C.7 Token_Carrier_Types	101
C.8 Function_Object_Identification_Numbers/Begleitspezifikationen	101
C.9 Tariff_Index	101
C.10 Zertifizierung der STS-Einhaltung	101
C.10.1 Produkte	101
C.10.2 Certification_Authority	102
C.11 Beschaffungsalternativen für Anwender von STS-Systemen	102
Anhang D (informativ) Beispiel einer Begleitspezifikation für ein Social_Credit_Function_Object (siehe auch Abschnitt 9)	107
D.1 Anwendungsbereich	107
D.2 Social_Credit_Function_Object	107
D.3 Attribute	109
D.3.1 FOIN	109
D.3.2 SC_Profile_Revision	109
D.3.3 Priorität	109
D.3.4 Verfügbarkeit	109
D.3.5 Accounting_Mode	110
D.3.6 SC_Accounting_Register	110
D.3.7 SC_Service_Delivery_Register	110
D.3.8 Date_Of_Last_Read	111
D.3.9 Activation_Criteria	111
D.3.10 SC_Quantity	111
D.3.11 SC_Cycle	111
D.3.12 Release_Quantity	111
D.3.13 Release_Cycle	112
D.3.14 Available_Service_Level	112

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

	Seite
D.3.15 Low_Credit_Warning_Level.....	112
D.3.16 Low_Credit_Warning	112
D.3.17 Credit_Expiry_Level.....	113
D.3.18 Credit_Expired	113
D.3.19 Interrupt_Service_On_Credit_Expiry	113
D.3.20 Restore_Service_On_Credit_Replenishment.....	113
D.4 Verfahren	114
D.4.1 set_SC_Profile(Profile_Data).....	114
D.4.2 get_SC_Profile()	114
D.4.3 display_SC_Profile(Attribute_Name).....	115
D.4.4 clear_SC_Service_Delivery_Register()	116
D.4.5 get_SC_Service_Delivery_Register()	116
D.4.6 display_SC_Service_Delivery_Register().....	116
D.4.7 clear_SC_Accounting_Register()	116
D.4.8 display_SC_Accounting_Register()	116
D.4.9 decrement_SC_Accounting_Register()	116
D.5 Operation	117
D.6 Verbindungen.....	117
D.6.1 Anzeigefunktionen	117
D.6.2 Aufzeichnungsfunktionen.....	118
D.6.3 Data_exchange-Funktionen.....	118
D.6.4 Sicherheitsfunktionen.....	118
D.6.5 Zeitfunktionen	118
D.6.6 Prüffunktionen.....	118
Literaturhinweise	118
Bild 1 – Funktionales Blockschaltbild eines einteiligen Inkassozählers.....	23
Bild 2 – Verdichtetes 2-Schichten-OSI-Referenzmodell für die STS	25
Bild 3 – Datenfluss vom Meter_Application_Process zum Token_Carrier	26
Bild 4 – Datenfluss vom Token_Carrier zum Meter_Application_Process	27
Bild 5 – Aufbau der ISO-Bezugsnummern für Transaktionen.....	28
Bild 6 – Transposition der 2 Klassen-Bits	45
Bild 7 – Funktion TCDU_Generation für die Token Klasse 0, 1 und 2	46
Bild 8 – Funktion TCDU_Generation für Token set_1st_Section_Decoder_Key	47
Bild 9 – Funktion TCDU_Generation für Token set_2nd_Section_Decoder_Key	49
Bild 10 – Änderungen des Decoder_Key – Zustandsdiagramm.....	55
Bild 11 – Decoder_Key_Generation_Algorithm_01	60
Bild 12 – Decoder_Key_Generation_Algorithm_02	61
Bild 13 – Decoder_Key_Generation_Algorithm_03	62
Bild 14 – STA: Encryption_Algorithm_07.....	63

Bild 15 – Ersetzungsprozess bei der STA-Verschlüsselung	64
Bild 16 – Permutationsprozess bei der STA-Verschlüsselung	64
Bild 17 – Rotationsprozess für des Decoder_Key bei der STA-Verschlüsselung	65
Bild 18 – STA-Verschlüsselung – Beispiel.....	66
Bild 19 – DEA-Encryption_Algorithm_09.....	66
Bild 20 – APDU_Extraction-Funktion.....	69
Bild 21 – Auskoppeln der 2 Bits für die Klasse	70
Bild 22 – STA Decryption_Algorithm_07	73
Bild 23 – Permutationsprozess bei der STA-Entschlüsselung	74
Bild 24 – Ersetzungsprozess bei der STA-Entschlüsselung.....	75
Bild 25 – Rotationsprozess für den Decoder_Key bei der STA-Entschlüsselung	75
Bild 26 – STA-Entschlüsselung – Beispiel.....	76
Bild 27 – DEA: Decryption_Algorithm_09.....	76
Bild 28 – Bezugsmodell der übergeordneten Meter_Function_Objects	82
Bild 29 – Key_Management_System und interaktive Beziehungen zwischen den Entitäten.....	90
Bild 30 – In einem STS-System verteilte Entitäten und Kennungen	93
Tabelle 1 – Datenelemente in der APDU.....	29
Tabelle 2 – Datenelemente im ID_Record.....	29
Tabelle 3 – Datenelemente in der Meter_PAN.....	30
Tabelle 4 – Datenelemente in der IAIN / DRN.....	30
Tabelle 5 – Typen von Tokenträgern.....	31
Tabelle 6 – DKGA-Kennzahlen.....	32
Tabelle 7 – EA-Kennzahlen	32
Tabelle 8 – SGC-Arten und Schlüsselarten.....	33
Tabelle 9 – Kodierte Formate für das Jahr des Expiration_Date	34
Tabelle 10 – Kodierte Formate für den Monat des Expiration_Date	34
Tabelle 11 – In Token angewendete Datenelemente.....	38
Tabelle 12 – Tokenklassen.....	38
Tabelle 13 – Unterklassen von Token	39
Tabelle 14 – Berechnungsbeispiel 1 für TID.....	40
Tabelle 15 – Berechnungsbeispiel 2 für TID.....	40
Tabelle 16 – Einheiten für elektrische Energie	41
Tabelle 17 – Einheiten für andere Anwendungen	41
Tabelle 18 – Bitzuweisungen für Transfer_Amount.....	41
Tabelle 19 – Maximaler Fehler durch Rundung	42
Tabelle 20 – Beispiele für Werte des Transfer_Amount.....	42
Tabelle 21 – Beispiel für eine CRC-Berechnung.....	42
Tabelle 22 – Zulässige Werte des Steuerfeldes.....	43
Tabelle 23 – Auswahl der zu löschenden Register	44

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

Tabelle 24 – Einteilung der Decoderschlüssel.....	52
Tabelle 25 – Zulässige Beziehungen zwischen den Decoderschlüsseltypen	56
Tabelle 26 – Definition des PAN_Block	58
Tabelle 27 – Datenelemente im PAN_Block.....	58
Tabelle 28 – Definition des CONTROL_Block.....	58
Tabelle 29 – Datenelemente im CONTROL_Block.....	58
Tabelle 30 – Bereich der anwendbaren Decoderbezugsnummern	59
Tabelle 31 – Verzeichnis der anwendbaren Supply_Group_Codes	59
Tabelle 32 – Ersetzungstabelle (Beispiel).....	64
Tabelle 33 – Permutationstabelle (Beispiel)	65
Tabelle 34 – Datenelemente in der APDU.....	67
Tabelle 35 – Mögliche Werte für das Authentication_Result.....	67
Tabelle 36 – Mögliche Werte für das Validation_Result	68
Tabelle 37 – Mögliche Werte für das Token_Result.....	68
Tabelle 38 – Im DKR gespeicherte Werte	73
Tabelle 39 – Permutationstabelle (Beispiel)	74
Tabelle 40 – Ersetzungstabelle (Beispiel).....	75
Tabelle 41 – Übergeordnete Struktur für das Virtual_Meter_Function_Object.....	83
Tabelle 42 – Übergeordnete Struktur für das Configuration_Registry_Function_Object	84
Tabelle 43 – Übergeordnete Struktur für das Application_Layer_Function_Object	85
Tabelle 44 – Übergeordnete Struktur des Physical_Layer_Function_Object.....	86
Tabelle 45 – Datenelemente in der FOIN	87
Tabelle 46 – Codierung der Function_Class.....	88
Tabelle 47 – Codierung der Definition_ID.....	88
Tabelle 48 – Codierung der Definition_Version	89
Tabelle A.1 – Im KMS-Prozess beteiligte Entitäten	90
Tabelle A.2 – Zähler und Decoder_Key umgebende Prozesse.....	91
Tabelle A.3 – Secure_Module umgebende Prozesse	91
Tabelle A.4 – SGC und Vending_Key umgebende Prozesse	92
Tabelle B.1 – In einem STS-System verteilte Entitäten	93
Tabelle B.2 – Kennungen, die mit den Entitäten in einem STS-System in Verbindung stehen	95
Tabelle C.1 – Mit einer SGC verbundene Datenelemente	98
Tabelle C.2 – Mit dem Secure_Module verbundene Datenelemente	99
Tabelle C.3 – Bei Lieferaufträgen oder Lastenheften zu beachtende Einzelheiten.....	103
Tabelle D.1 – Definition des Social_Credit_Function_Object.....	107
Tabelle D.2 – Zusammensetzung der FOIN	109
Tabelle D.3 – Steuerbits für das Attribut Verfügbarkeit	110
Tabelle D.4 – Steuerwerte für das Attribut Accounting_Mode.....	110
Tabelle D.5 – Format des SC_Accounting_Register	110
Tabelle D.6 – Steuerwerte für das Attribut Activation_Criteria	111

Tabelle D.7 – Werte für das Attribut SC_Cycle	111
Tabelle D.8 – Häufigkeitswerte für das Attribut Release_Cycle	112
Tabelle D.9 – Anzeigewerte für das Attribut Low_Credit_Warning	113
Tabelle D.10 – Format für das Attribut Credit_Expiry_Level	113
Tabelle D.11 – Anzeigewerte für das Attribut Credit_Expired	113
Tabelle D.12 – Steuerwerte für das Attribut Interrupt_Service_On_Credit_Expiry	113
Tabelle D.13 – Steuerwerte für das Attribut Restore_Service_On_Credit_Replenishment	114
Tabelle D.14 – Attributwerte, die vom Token_Carrier übertragen werden	114
Tabelle D.15 – Attributwerte, die auf den Token_Carrier übertragen werden	115
Tabelle D.16 – Attribute, die an der Nutzerschnittstelle angezeigt werden	115
Tabelle D.17 – Attributwerte, die auf den Token_Carrier übertragen werden	116

Vorwort

- 1) Die IEC (Internationale Elektrotechnische Kommission) ist eine weltweite Normungsorganisation, die alle Nationalen Elektrotechnischen Komitees (Nationale Komitees der IEC) umfasst. Die IEC hat das Ziel, die internationale Zusammenarbeit in allen Fragen der Normung auf dem Gebiet der Elektrotechnik und Elektronik zu fördern. Zu diesem Zweck und neben anderen Aktivitäten veröffentlicht die IEC Internationale Normen, technische Spezifikationen, technische Berichte, öffentlich verfügbare Spezifikationen (PAS) und Leitfäden (im Folgenden als „Publikation(en) der IEC“ bezeichnet). Mit der Vorbereitung sind die Technischen Komitees beauftragt. Jedes Nationale Komitee der IEC, das an dem behandelten Thema interessiert ist, darf an dieser Vorbereitungsarbeit teilnehmen. Internationale, staatliche und nichtstaatliche Organisationen, die mit der IEC in Verbindung stehen, nehmen ebenfalls an diesen Vorbereitungsarbeiten teil. Die IEC arbeitet eng mit der Internationalen Organisation für Normung (ISO) nach den in der Vereinbarung zwischen beiden Organisationen festgelegten Bedingungen zusammen.
- 2) Die offiziellen Beschlüsse oder Vereinbarungen der IEC über technische Fragen, die in Technischen Komitees von Vertretern aller an dem behandelten Thema besonders interessierten Nationalen Komitees erarbeitet werden, bringen das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet zum Ausdruck.
- 3) Publikationen der IEC haben die Form von Empfehlungen zur internationalen Anwendung und werden von den Nationalen Komitees der IEC in diesem Sinne anerkannt. Obwohl alle möglichen Anstrengungen unternommen werden, um sicherzustellen, dass der fachliche Inhalt ihrer Publikationen korrekt ist, kann die IEC nicht für deren Art der Anwendung oder für eventuelle Fehlinterpretationen durch den Anwender verantwortlich gemacht werden.
- 4) Um die internationale Vereinheitlichung zu fördern, verpflichten sich die Nationalen Komitees der IEC, Publikationen der IEC möglichst unverändert in ihren nationalen und regionalen Normen anzuwenden. Jede Abweichung zwischen der Publikation der IEC und der entsprechenden nationalen oder regionalen Norm muss in dieser deutlich gekennzeichnet werden.
- 5) Die IEC hat kein Verfahren für die Kennzeichnung der Konformität festgelegt und übernimmt keine Verantwortung, wenn ein Gegenstand als konform mit einer ihrer Publikationen erklärt wird.
- 6) Alle Anwender sollten sicherstellen, dass sie über die neueste Ausgabe dieser Publikation verfügen.
- 7) Weder die IEC, deren Geschäftsführung, Angestellte oder sonstige Beteiligte oder Beauftragte der IEC noch einzelne Fachleute oder Mitglieder ihrer Technischen Komitees und Nationalen Komitees der IEC dürfen für Schäden an Personen, Sachen oder sonstige Schäden beliebiger Art, sei es direkt oder indirekt, oder für Kosten (einschließlich Gerichtskosten) oder Ausgaben, die sich aus der Veröffentlichung, Anwendung oder im Vertrauen auf diese oder jede andere Publikation der IEC ergeben, haftbar gemacht werden.
- 8) Zu beachten sind die in dieser Publikation zitierten normativen Verweisungen. Für die korrekte Anwendung dieser Publikation ist die Verwendung der zitierten Publikationen unerlässlich.
- 9) Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments hinsichtlich der in 6.3.4.1 angegebenen speziellen reservierten Token_Identifier Patentrechte berühren können.

Die IEC nimmt keine Stellung zur Rechtmäßigkeit, zur Gültigkeit und zum Anwendungsbereich dieser Patentrechte. Der Halter dieser Patentrechte hat der IEC zugesichert, dass er bereit ist, über Lizenzen zu vernünftigen und nicht diskriminierenden Geschäftsbedingungen mit Antragstellern in der ganzen Welt zu verhandeln. In diesem Zusammenhang ist die Erklärung des Halters dieser Patentrechte bei der IEC registriert. Informationen sind erhältlich bei:

Anschrift: Actaris Measurement and Systems, P.O. Box 4059, Tyger Valley 7536, Republic of South Africa

Tel: +27 21 914 3640

Fax: +27 21 914 3630

Website: <http://www.actaris.com>

Anschrift: Merlin Gerin SA (Pty) Ltd t/a Conlog, P.O. Box 2332, Durban 4000, Republic of South Africa

Tel: +27 31 268 1141

Fax: +27 31 208 7790

Website:

Es wird auf die Möglichkeit hingewiesen, dass einige Teile dieser Internationalen Norm Patentrechte berühren können, ohne dass diese vorstehend identifiziert wurden. Die IEC kann nicht zur Verantwortung gezogen werden, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

- 10) Die IEC weist darauf hin, dass einige Texte dieses Dokuments hinsichtlich der Wartung für die Verschlüsselungscodeverwaltung und die Ablage der Protokolle, auf denen die vorliegende Norm IEC 62055-41 beruht, Patentrechte berühren können. [Siehe Anhang C.] Die IEC nimmt keine Stellung zur Rechtmäßigkeit, zur Gültigkeit und zum Anwendungsbereich dieser Wartung.

Der Anbieter dieser Wartungsdienste hat der IEC zugesichert, dass er bereit ist, über Dienstleistungen zu vernünftigen und nicht diskriminierenden Geschäftsbedingungen mit Antragstellern in der ganzen Welt zu verhandeln. In diesem Zusammenhang ist die Erklärung des Anbieters dieser Wartungsdienste bei der IEC registriert. Informationen sind erhältlich bei:

Anschrift: The STS Association, P.O. Box 868, Ferndale 2160, Republic of South Africa

Tel: +27 11 789 1384

Fax: +27 11 789 1385

Email: email@sts.org.co.za

Website: <http://www.sts.org.za>

Hauptaufgabe der Technischen Komitees der IEC ist die Ausarbeitung Internationaler Normen. In Ausnahmefällen kann ein Technisches Komitee die Veröffentlichung eines Fachberichts vorschlagen, wenn:

- die erforderliche Unterstützung zur Veröffentlichung einer Internationalen Norm trotz wiederholter Bemühungen nicht gefunden werden kann, oder
- der Normungsgegenstand sich noch in der technischen Entwicklung befindet oder wenn aus einem anderen Grund erst in der Zukunft die Möglichkeit besteht, ein Einvernehmen über die Veröffentlichung einer Internationalen Norm zu erzielen.

Fachberichte unterliegen spätestens 3 Jahre nach ihrer Veröffentlichung einer Überprüfung, um festzustellen, ob sie in Internationale Normen umgewandelt werden können.

IEC 62055-41, die eine Technische Spezifikation ist, wurde von der Arbeitsgruppe 15 des Technischen Komitees 13 der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Der Text dieser Technischen Spezifikation basiert auf folgenden Schriftstücken:

Umfrageentwurf	Abstimmungsbericht
XX/XX/DTS	XX/XX/RVC

Vollständige Informationen über die Abstimmung zur Annahme dieser Technischen Spezifikation können dem in vorstehender Tabelle angeführten Abstimmungsbericht entnommen werden.

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

Die vorliegende Publikation wurde nach den ISO/IEC-Richtlinien, Teil 2, erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zum Jahr 200X unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- in eine Internationale Norm umgewandelt;
- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Einleitung

Die STS (Standardtransferspezifikation) ist ein gesichertes Nachrichtenprotokoll, welches die Übertragung von Informationen zwischen der Kasseneinrichtung und den Vorkassezählern zulässt und berücksichtigt mehrere Nachrichtentypen, wie Guthaben, Konfigurationssteuerung, Anzeige- und Prüfanweisungen. Ferner werden Einrichtungen und Regeln festgelegt, die eine sichere Verwaltung (Generierung, Speicherung, Wiedergewinnung und Transport) der innerhalb des Systems verwendeten kryptografischen Schlüssel ermöglicht.

Das nationale Elektrizitätsversorgungsunternehmen in Südafrika (Eskom) entwickelte zuerst und veröffentlichte 1993 die Standardtransferspezifikation und übertrug 1998 die Eigentumsrechte an die STS-Association zur Verwaltung und Weiterentwicklung. Es ist gegenwärtig das einzige offene Kommunikationssystem für Einweg-Vorkassezähler und zurzeit sind mehr als vier Millionen STS-Zähler im Einsatz, die von etwa 400 Unternehmen in 28 Ländern betrieben werden. Die Spezifikation ist seit 10 Jahren stabil und ist eine De-facto-Industrienorm auf nationaler und internationaler Ebene und wurde folglich als IEC-Norm mit der entsprechenden Neugestaltung zur Anpassung an die Arbeiten der WG 15 entwickelt. Die Hauptanwendung der STS ist für die Anwendung mit Zählern ohne Gebühren(erschaffung) mit energiebasierten Token, könnte jedoch auch für währungsbasierte Tokensysteme angewendet werden.

Vor der Entwicklung der STS wurden eine Vielzahl von firmenspezifischen Vorkassezählern und Verkaufssystemen entwickelt, die untereinander jedoch nicht kompatibel waren. Bei den Hauptanwendern entwickelte sich daraus ein bestimmter Bedarf, vereinheitlichte Lösungen anzustreben, indem die Betriebsprobleme angesprochen wurden, die bei den unterschiedlichen Typen der Vorkassezähler und Verkaufseinrichtungen gleichzeitig zu bearbeiten sind. Es wurde eine Standardtransferspezifikation (STS) entwickelt, die die Anwendung und Zusammenarbeit der Inkassozähler und Verkaufseinrichtungen von mehreren Herstellern in einer Installation aus Vorkassezählern und Verkaufseinrichtung zulassen sollte.

Obwohl die hauptsächliche Realisierung der STS in der Elektroversorgungsindustrie liegt, ist sie ebenso für die Verwaltung von anderen Versorgungsdienstleistungen, wie Wasser und Gas, geeignet. Zukünftige Überarbeitungen der STS können andere Tokenrögertechnologien, wie Smartcards und Speicherschlüssel mit Zweiweg-Funktionalität zulassen und eine Echtzeituhr und komplexe Tarife im Zähler berücksichtigen.

In dieser Norm werden zwei Encryption_Algorithms (Verschlüsselungsalgorithmen) unterstützt. In bestehenden Systemen wird STA angewendet, während für zukünftige Systeme DEA berücksichtigt werden kann.

Der Token_Carrier (Tokenrögter) ist die physikalische Einrichtung, die zur Übertragung der Information vom Verkaufssystem zum Vorkassezähler verwendet wird. In IEC 62055-51 wird die Anwendung von zwei Typen der Tokenrögter festgelegt, und zwar der Magnetkarte und des Zahlwort-Tokenrögters.

Die Normenreihe IEC 62055 behandelt Inkassosysteme, umfasst die Kundeninformationssysteme, Kassensysteme, Tokenrögter, Inkassozähler und die entsprechenden Schnittstellen, die zwischen diesen Entitäten existieren. Zum Zeitpunkt der Erarbeitung dieser Norm bestand IEC 62055 mit dem allgemeinen Titel *Messung der elektrischen Energie – Zählersysteme mit Inkassofunktion* aus den folgenden Teilen:

Teil 21: *Aufbau für die Normung*

Teil 31: *Besondere Anforderungen – Inkasso-Wirkverbrauchszähler (Genauigkeitsklassen 1 und 2)*

Teil 41: *Standardtransferspezifikation – Protokoll der Anwendungsschicht für Einweg-Tokenrögtersysteme*

Teil 51: *Standardtransferspezifikation – Protokoll der Bitübertragungsschicht für Einweg-Tokenrögter auf Magnetkarten und als Zahlwort*

In der Reihe *Teil 4x* werden Protokolle der Anwendungsschicht und in der Reihe *Teil 5x* werden Protokolle der Bitübertragungsschicht festgelegt.

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

Die STS-Association ist für die Erarbeitung von Normen für den Bereich der Standardtransferspezifikation eine Typ-D-Verbindung mit IEC/TC 13/WG 15 eingegangen und ist somit für die Pflege aller derartiger IEC-Normen verantwortlich, die im Ergebnis dieser Verbindung erarbeitet werden könnten.

Schlüsselwörter

Inkassosysteme, Vorauszahlung; Standardtransferspezifikation; Vorkassezähler; Token; Verschlüsselung, Entschlüsselung, Verwaltung kryptografischer Schlüssel.

1 Anwendungsbereich

In diesem Teil von IEC 62055 wird das Protokoll der Anwendungsschicht einer Standardtransferspezifikation (STS) für die Übertragung von Guthabeneinheiten und weiteren Verwaltungsinformationen von einem Kassensystem (POS-System) an einen STS-konformen Vorkassezähler in einem Einweg-Tokenträgersystem festgelegt. Er ist in erster Linie für die Anwendung mit Verbrauchszählern ohne eine Gebührenerfassung mit energiebasierten Token vorgesehen, kann jedoch auch bei währungsbasierten Tokensystemen und bei anderen Versorgungsleistungen als Elektrizität Anwendung finden.

Festgelegt werden:

- POS_to_Token_Carrier_Interface (POS-Tokenträger-Schnittstelle), strukturiert nach dem OSI-Referenzmodell mit einem Protokoll der Anwendungsschicht und einem Protokoll der Bitübertragungsschicht;
- ein Token für das Protokoll der Anwendungsschicht für die Übertragung verschiedener Nachrichten vom POS zum Inkassozähler;
- Sicherheitsfunktionen und Prozesse im Protokoll der Anwendungsschicht, wie Standardtransferalgorithmus und Datenverschlüsselungsalgorithmus, einschließlich Generierung und Verteilung der zugehörigen kryptografischen Schlüssel;
- Sicherheitsfunktionen und Prozesse im Protokoll der Anwendungsschicht am Zähler, wie Entschlüsselungsalgorithmen, Token-Authentifikation, Überprüfung und Entwertung;
- spezifische Anforderungen an den Meter_Application_Process (Zähler-Anwendungs-Prozess) als Antwort auf empfangene Tokens;
- einem System für die Behandlung der Zählerfunktionalität im Meter_Application_Process und zugehörigen Begleitspezifikationen;
- allgemeine Anforderungen an ein STS-konformes Key_Management_System (Schlüsselverwaltungssystem);
- Leitlinien für ein Key_Management_System;
- in einem STS-System verwendete Entitäten und Kennungen;
- Regeln und Nebenleistungen der STS-Association.

Dieser Teil ist für die Anwendung von Herstellern von Vorkassezählern vorgesehen, welche Token akzeptieren sollen, die der STS entsprechen, sowie für die Hersteller von POS-Systemen, die STS-konforme Token herzustellen haben und ist in Verbindung mit Normen der Reihe IEC 62055-5x zu lesen.

ANMERKUNG 1 Obwohl sie für Inkassosysteme in der Elektrizitätsversorgung entwickelt worden ist, enthält diese Norm auch Bestimmungen für Token, die bei anderen Versorgungsdienstleistungen, wie Wasser und Gas, angewendet werden.

ANMERKUNG 2 STS-konforme Produkte sind nur erforderlich, um ausgewählten Teilen dieser Norm zu entsprechen, die allerdings einem Kaufvertrag unterliegen.

2 Normative Verweisungen

Die folgenden normativen Dokumente enthalten Festlegungen, die durch Verweisung in diesem Text Bestandteil dieser Internationalen Norm sind. Bei datierten Verweisungen gelten spätere Änderungen oder Überarbeitungen dieser Publikationen nicht. Anwender dieser Internationalen Norm werden jedoch gebeten, die Möglichkeit zu prüfen, die jeweils neuesten Ausgaben der nachfolgend angegebenen normativen Dokumente anzuwenden. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen normativen Dokuments. Mitglieder von ISO und IEC führen Verzeichnisse der gültigen Internationalen Normen.

IEC 62051, *Electricity metering – Glossary of terms*

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

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieser Norm gelten die Begriffe aus IEC 62051 und die folgenden.

Der Begriff „Zähler“ wird austauschbar mit „Inkassozähler“, „Vorkassezähler“ und „Decoder“ verwendet, wobei der Decoder ein Teil eines Inkassozählers ist.

Der Begriff „POS“ wird synonym mit „CIS“, „MIS“ und „HHU“ in dem Sinne verwendet, dass Token auch von diesen Entitäten generiert und zwischen ihnen und dem Inkassozähler übertragen werden können.

Der Begriff „Unternehmen“ wird zur Kennzeichnung eines Lieferers der Dienstleistung in einem allgemeinen Sinn verwendet. Es sollte beachtet werden, dass in liberalisierten Märkten die eigentliche Vertragspartei als „Lieferant“ der Dienstleistung an den Kunden nicht das traditionelle Unternehmen als solches zu sein braucht, sondern ein dazwischenliegender Dritter sein kann.

3.1.1

Begleitspezifikation

eine Spezifikation, die von der STS-Association koordiniert wird, in der eine spezifische Instanz eines Meter_Function_Object (siehe Abschnitt 9) festgelegt ist

3.1.2

Decoder

der Teil des Token_Carrier_to_Meter_Interface (Tokenträger-Zähler-Schnittstelle) eines Inkassozählers, der die Funktionen des Protokolls der Anwendungsschicht ausführt und der tokenbasierte Transaktionen ermöglicht, die zwischen einem POS und dem Inkassozähler ablaufen. Ein Inkassozähler darf nur einen Decoder haben

3.1.3

Zählerseriennummer

die Nummer, die dem messtechnischen Teil des Inkassozählers zugeordnet ist. In einem einteiligen Inkassozähler können die DRN und die Zählerseriennummer gleichbedeutend sein, während sie in einem mehrteiligen Inkassozähler verschieden sein kann

3.1.4

Token

die Untergruppe von Datenelementen, die eine Anweisung und Information enthält, die in der APDU der Anwendungsschicht des POS_to-Token_Carrier_Interface vorhanden ist und die auch mit einem Tokenträger an den Zähler übertragen wird. Das Gegenteil ist auch richtig für den Fall, dass ein Token vom Zähler zur POS gesendet wird

3.1.5

Tokenträger

das Medium, welches in der Bitübertragungsschicht des POS_to-Token_Carrier_Interface verwendet wird, und auf dem ein Token moduliert oder verschlüsselt ist und welches dazu dient, das Token von dem Punkt, an dem es generiert wird, bis zum entfernten Zähler zu tragen, wo es empfangen wird

3.1.6

Einweg-Tokenträgersystem

ein Inkassozählersystem, in dem Tokenträger verwendet werden, die die Information nur in einer Richtung übertragen – vom POS zum Inkassozähler

3.1.7

Zweiweg-Tokenträgersystem

ein Inkassozählersystem, in dem Tokenträger verwendet werden, die die Information in beiden Richtungen übertragen – vom POS zum Inkassozähler und auch vom Inkassozähler zum POS

3.1.8

tokenbasierte Transaktion

Verarbeitung jedes Tokens durch den Inkassozähler, welches wesentliche Auswirkungen auf die Menge, den Wert oder die Qualität der an den Kunden zu liefernden Dienstleistung hat und die vom Inkassozähler kontrolliert wird. Hinsichtlich der gegenwärtigen Praxis bedeutet dies Token der Klasse 0 und Klasse 2

3.2 Abkürzungen

3DES (Triple DES encryption or decryption)

dreifach DES-Verschlüsselung oder -Entschlüsselung

ALFO (Application_Layer_Function_Object)

Funktionsobjekt der Anwendungsschicht

ANSI (American National Standards Institute)

Nationales Normungsinstitut der USA

APDU (Application_Protocol_Data_Unit)

Dateneinheit des Anwendungsprotokolls

BCD (Binary Coded Digit)

binär codierte Dezimalzahl

CC (Country_Code)

Landescode

CIS (Customer Information System)

Kundeninformationssystem

COP (Code Of Practice)

Regeln (für die Praxis)

CRC (Cyclic_Redundancy_Code)

zyklisch redundanter Code

CRFO (Configuration_Registry_Function_Object)

Funktionsobjekt der Konfigurationsregistrierdatenbank

DAC (Device_Authentication_Code)

Geräteauthentifikationscode

DCTK (Decoder_Common_Transfer_Key)

einheitlicher Transferschlüssel für Decoder

DD (Discretionary Data)

benutzerbestimmbare Daten

DDTK (Decoder_Default_Transfer_Key)

vorgegebener Transferschlüssel für Decoder

DEA (Data Encryption Algorithm)

Datenverschlüsselungsalgorithmus

DES (Data Encryption Standard)

Norm für die Datenverschlüsselung

DITK (Decoder_Initialization_Transfer_Key)

Initialisierungstransferschlüssel für Decoder

DK (Decoder_Key)

Decoderschlüssel

DKGA (Decoder_Key_Generation_Algorithm)

Generierungsalgorithmus für Decoderschlüssel

DKR (Decoder_Key_Register)

Register für Decoderschlüssel

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

DRN (Decoder_Reference_Number)

Decoderbezugsnummer (bekannt als „Zählernummer“ in den Systemen, die vor der Erarbeitung dieser Norm angewendet wurden)

DSN (Decoder_Serial_Number)

Decoderseriennummer

DUTK (Decoder_Unique_Transfer_Key)

eindeutiger Transferschlüssel für Decoder

EA (Encryption_Algorithm)

Verschlüsselungsalgorithmus

ECB (Electronic Code Book)

elektronisches Code-Lexikon

ED (Expiration_Date)

Verfallsdatum

ETX (End_Sentinel)

Endemarkierung

FAC (Firmware_Authentication_Code)

Firmware-Authentifizierungscode

FOIN (Function_Object_Identification_Number)

Kennzeichnungsnummer des Funktionsobjektes

FS (Field_Separator)

Feldtrennzeichen

GPRS (General Packet Radio Service)

Allgemeiner Paketfunkdienst

GSM (Global System For Mobile Communication)

Europäisches System für digitale Mobilfunkdienste

HHU (Hand-held Unit)

tragbare Einheit

IAIN (Individual_Account_Identification_Number)

Kennzeichnungsnummer für Einzelrechnung

ID (Identification, Identifier)

Kennzeichnung, Kennung

IIN (Issuer_Identification_Number)

Aussteller-Kennzeichnungsnummer

ISDN (Integrated Services Digital Network)

Diensteintegrierendes Digitalnetz

ISO (International Standards Organisation)

Internationale Normungsorganisation

ISO BIN

Ersetzt durch IIN

KCT (Key_Change-Token)

Token für Schlüsselwechsel

KEK (Key_Exchange_Key)

Schlüssel für Schlüsselaustausch

KEN (Key_Expiry_Number)

Schlüsselverfallsnummer

KLF (Key_Load_File)

Schlüsselladefile

KMC (Key_Management_Centre)

Schlüsselverwaltungszentrale

KMI (Key Management Infrastructure)

Infrastruktur für die Schlüsselverwaltung

KMS (Key_Management_System)
Schlüsselverwaltungssystem

KRN (Key_Revision_Number)
Schlüsselrevisionsnummer

KT (Key Type)
Schlüsseltyp

LAN (Local Area Network)
lokales Netz

LRC (Longitudinal_Redundancy_Check)
Blockprüfung

MFO (Meter_Function_Object)
Zähler-Funktionsobjekt

MII (Major_Industry_Identifier)
Hauptbranchenkennung

MIS (Management Information System)
Verwaltungsinformationssystem

MPL (Maximum_Power_Limit)
Oberer Leistungsgrenzwert

MPPUL (Maximum_Phase_Power_Unbalance_Limit)
Oberer Grenzwert der Phasenbelastungsunsymmetrie

NKHO (New_Key_High_Order bits)
höherwertige Bits des neuen Schlüssels

NKLO (New_Key_Low_Order bits)
niederwertige Bits des neuen Schlüssels

NWIP (New Work Item Proposal)
Vorschlag für neues Arbeitsthema

OSI (Open Systems Interconnect)
Kommunikation offener Systeme

PAN (Primary_Account_Number)
Hauptabrechnungsnummer

PLC (Power Line Carrier)
Träger auf Hochspannungsleitungen

PLFO (Physical_Layer_Function_Object)
Funktionsobjekt der Bitübertragungsschicht

POS (Point_Of_Sale)
Kassenplatz

PRN (Printer)
Drucker

PSTN (Public Switched Telephone Network)
öffentliches Fernsprechwählnetz

RND (Random_Number)
Zufallszahl

RO (Rollover)
Überlappung

SG (Supply_Group)
Versorgungsgruppe

SGC (Supply_Group_Code)
Versorgungsgruppencode

SM (Secure_Module)
Sicherheitsmodul

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

SM_AC (Secure_Module_Authentication_Code)
Authentifikationscode des Sicherheitsmoduls

SM_ID (Secure_Module_Identifier)
Kennung des Sicherheitsmoduls; Sicherheitsmodulkennung

STA (Standard Transfer Algorithm)
Standardtransferalgorithmus

STS (Standard Transfer Specification)
Standardtransferspezifikation

STSA (Standard Transfer Specification Association)
STS-Association

STX (Start_Sentinel)
Startmarkierung

TCDU (Token_Carrier_Data_Unit)
Dateneinheit des Tokenträgers

TCT (Token_Carrier_Type)
Typ des Tokenträgers

TI (Tariff Index)
Tarif

TID (Token_Identifier)
Tokenkennung

UC (Utility_Code)
Unternehmenskennzahl

VCDK (Vending_Common_DES_Key)
gemeinsamer DES-Verkaufsschlüssel

VDDK (Vending_Default_DES_Key)
vorgegebener DES-Verkaufsschlüssel

VK (Vending_Key)
Verkaufsschlüssel

VMFO (Virtual_Meter_Function_Object)
Funktionsobjekt des virtuellen Zählers

VDK (Vending_Unique_DES_Key)
eindeutiger DES-Verkaufsschlüssel

WAN (Wide Area Network)
Weitverkehrsnetz

XOR (Exclusive Or (logical))
logisches ausschließendes ODER

3.3 Notation und Terminologie

In dieser Norm gelten die folgenden Regeln für Benennungsvereinbarungen:

- Entitätennamen, Datenelementnamen, Namen für Funktionen und Prozesse werden als übergeordnete Objektklassen behandelt und erhalten Namen in Hinsicht auf Substantive, die mit einem Großbuchstaben beginnen und mit einem Unterstrich verbunden werden, um sie als einzelne Entität kenntlich zu machen. Beispiele sind: Supply_Group_Code als Datenelementname, Encryption_Algorithm als Name für eine Funktion und Meter_Installation als Name für einen Prozess.
- Direkte (spezifische) Verweisung auf eine benannte Objektklasse verwendet die Form mit Großbuchstaben, während eine allgemeine (nicht-spezifische) Verweisung Kleinbuchstaben ohne verbindenden Unterstrich verwendet. Ein Beispiel für eine direkte Verweisung ist: „Der Supply_Group_Code steht mit einer Gruppe von Zählern in Verbindung“, während ein Beispiel für eine indirekte Verweisung ist: „Ein Versorgungsgruppencode steht im Zusammenhang mit einem Verkaufsschlüssel“.
- Für weitere Begriffe werden die allgemein akzeptierten Formen, wie PSTN für Public Switched Telephone Network verwendet.

4 Numerierungsvereinbarungen

In dieser Norm erfolgt die Darstellung der Zahlen in Binärzeichenfolgen nach der Vereinbarung, dass das niederwertigste Bit rechts und das hochwertigste Bit links steht.

Die Numerierung der Binärstellen beginnt an der Binärstelle 0, die dem niederwertigsten Bit in einer Binärzahl entspricht.

Zahlen werden üblicherweise im Dezimalformat angegeben, sofern nicht anders dargestellt.

Die Werte von Binärziffern sind 0 oder 1.

Die Werte von Dezimalziffern reichen von 0 bis 9.

Die Werte von Hexadezimalziffern reichen von 0 bis 9 und A bis F und werden üblicherweise mit einem „hex“ oder „h“ gekennzeichnet.

5 Referenzmodell für die Standardtransferspezifikation

5.1 Funktionales Referenz-Blockdiagramm für Inkassozähler

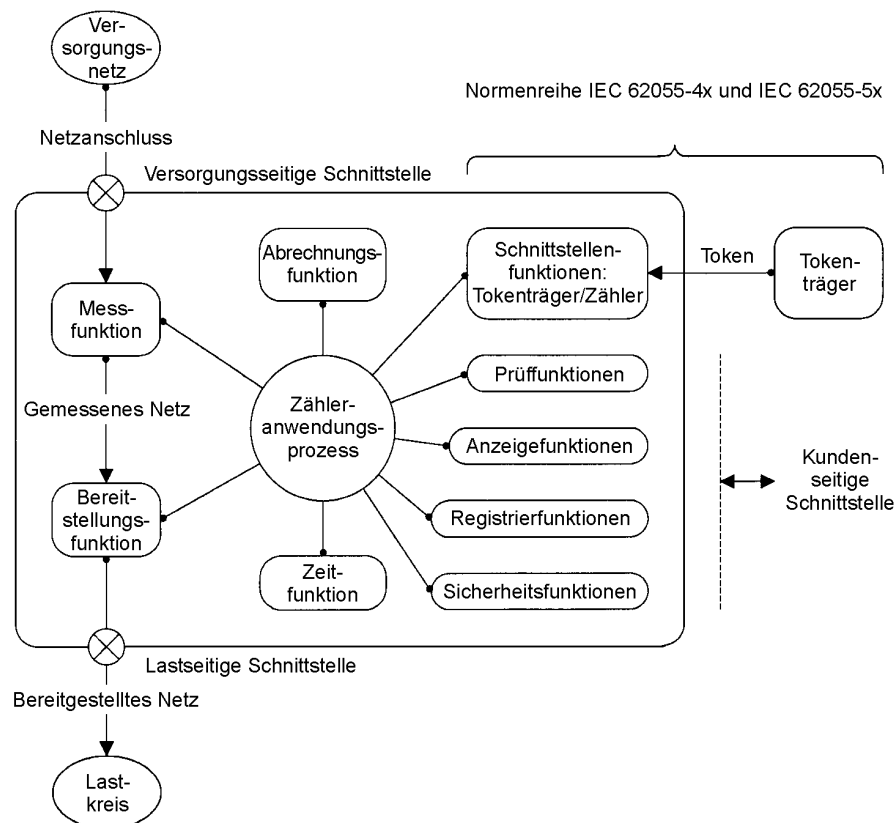


Bild 1 – Funktionales Blockschaltbild eines einteiligen Inkassozählers

Die Normenreihe IEC 62055-4x befasst sich mit dem Protokoll der Anwendungsschicht und die Normenreihe IEC 62055-5x befasst sich mit dem Protokoll der Bitübertragungsschicht der Token_Carrier_to_Meter_Interface (Tokenträger-Zähler-Schnittstelle). Der Tokenträger wird von der Bitübertragungsschicht eingeschlossen. In dieser Spezifikation ist der Decoder (siehe Abschnitt 3) als der Teil des Inkassozählers definiert, in dem die Funktionen der Anwendungsschicht der Tokenträger-Zähler-

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

Schnittstelle untergebracht sind und ihm deshalb eine Decoder_Reference_Number zugeordnet ist (siehe 6.1.1.2).

ANMERKUNG In IEC 62055-41 sind auch Meter_Function_Objects (Zähler-Funktionsobjekte) definiert, die weiter in 5.5 diskutiert werden.

In einem einteiligen Inkassozähler sind alle wesentlichen Funktionen in einem einzigen Gehäuse untergebracht, wie in Bild 1 dargestellt, wobei der Decoder mit der Zählerfunktion ein Ganzes bildet und die Decoder_Reference_Number könnte wahlweise mit der Seriennummer des Zählers übereinstimmen.

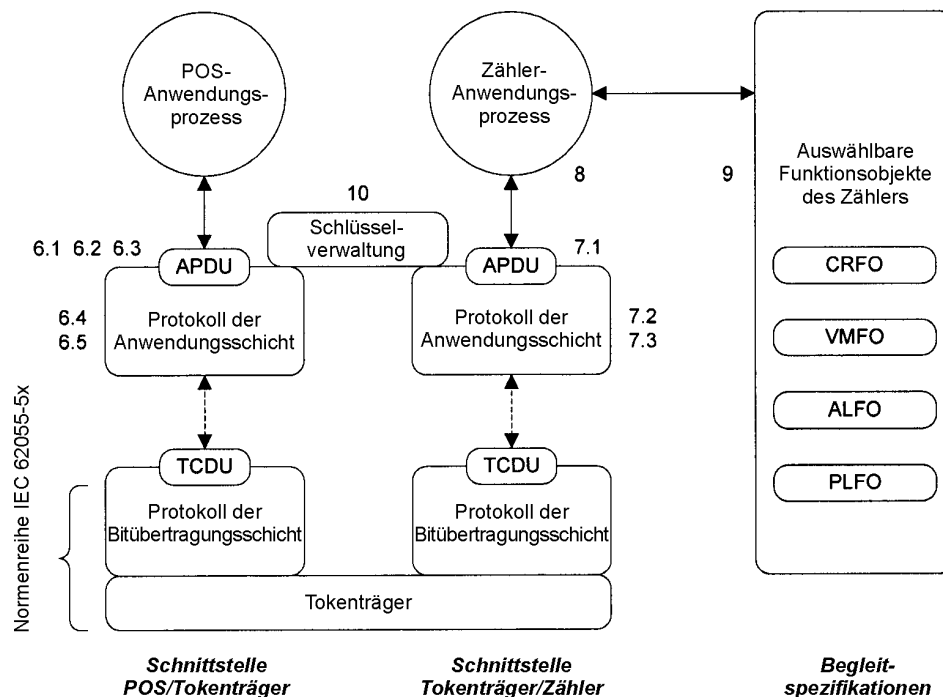
Bei einem mehrteiligen Inkassozähler ist es für das Token_Carrier_to_Meter_Interface möglich, dass es in einem gesonderten Gehäuse, beispielsweise getrennt untergebracht ist von der Zählerfunktion, und kann durchaus ein eigenständiger Zähler sein und seine eigene Zähler-Seriennummer haben. In diesem Fall wäre die Decoder_Reference_Number nicht dieselbe wie die Zähler-Seriennummer, sondern würde deutlich anders sein und würde somit auf dem Gehäuse angegeben werden, welches die Funktionen der Anwendungsschicht des Token_Carrier_to_Meter_Interface enthält.

In allen Fällen würde es nur eine Realisierung der Anwendungsschicht geben und somit auch nur eine Decoder_Reference_Number, die mit dem Inkassozähler verbunden ist, und zwar unabhängig davon, ob es ein einteiliger oder mehrteiliger Zähler ist, selbst wenn es mehr als eine Realisierung der Bitübertragungsschicht in demselben Inkassozähler gibt (siehe Abschnitt 9).

Es ist auch möglich, dass die Funktionen der Anwendungsschicht und die Funktionen der Bitübertragungsschicht in gesonderten Gehäusen untergebracht werden, wobei in diesem Fall die Kennzeichnung (siehe 8.3) der Decoder_Reference_Number und des Encryption_Algorithm (Verschlüsselungsalgorithmus) auf dem Teil angebracht werden, in dem der physikalische Anschlusspunkt für den Token_Carrier (Tokenträger) enthalten ist. Dies kann beispielsweise ein Kabel- oder Modemsteckverbinder für einen virtuellen Tokenträger, ein Tastenfeld für einen Zahlwort-Tokenträger oder ein Magnetkartenlesegerät für einen Tokenträger als Magnetkarte sein (siehe auch 5.2).

Eine umfangreichere Beschreibung der Inkassozähler-Funktionsklassen enthält IEC 62055-21.

5.2 OSI-Referenzmodell



Legende:

- APDU Dateneinheit des Anwendungsprotokolls; Datenschnittstelle zum Protokoll der Anwendungsschicht.
- TCDU Dateneinheit des Tokenträgers; Datenschnittstelle zum Protokoll der Bitübertragungsschicht.
- CRFO Funktionsobjekt der Konfigurationsregistrierdatenbank.
- VMFO Funktionsobjekt des virtuellen Zählers.
- ALFO Funktionsobjekt der Anwendungsschicht.
- PLFO Funktionsobjekt der Bitübertragungsschicht.

Die Verweisungen auf die betreffenden Abschnittsnummer in dieser Spezifikation sind neben jedem Kästchen angegeben.

Bild 2 – Verdichtetes 2-Schichten-OSI-Referenzmodell für die STS

Die Standardtransferspezifikation ist ein gesichertes Datenübertragungsprotokoll zwischen einem POS und einem Zähler mit einem Tokenträger als Übertragungsmedium. Das Protokoll der Anwendungsschicht befasst sich mit den Token, den Verschlüsselungsprozessen und Funktionen, während sich das Protokoll der Bitübertragungsschicht mit der eigentlichen Codierung der Tokendaten auf einen Tokenträger befasst.

Beispiele für gegenständlich transportable Tokenträger sind: Karten mit Zahlenkombination, Magnetkarten, Speicherkarten und Speicherschlüssel. Beispiele für virtuelle Tokenträger sind: PSTN-Modem, ISDN-Modem, GSM-Modem, GPRS-Modem, Funkmodem, PLC-Modem, Infrarot-, LAN- und WAN-Verbindungen und direkter lokaler Anschluss.

Obwohl das Modell in erster Linie ein Protokoll „POS zum Tokenträger zum Zähler“ angibt, ist zu beachten, dass das gleiche Protokoll ebenso für jede andere Einrichtung anwendbar ist, die eine Kommunikation mit dem Zähler erfordert, z. B. CIS, MIS oder transportable HHUs.

Obwohl in dieser Spezifikation eine verdichtete 2-schichtige OSI-Architektur befolgt wird, sind zukünftige Erweiterungen zur Aufnahme weiterer Schichten nicht ausgeschlossen, sofern sich dieser Bedarf ergeben sollte oder wenn es für den Realisierenden notwendig ist, zwischen den beiden im Modell gezeigten Schichten noch zusätzliche Schichten einzufügen.

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

Die APDU ist die Datenschnittstelle zum Protokoll der Anwendungsschicht und die TCDU ist die Datenschnittstelle zum Protokoll der Bitübertragungsschicht, welche in der Normenreihe IEC 62055-5x festgelegt sind.

In dieser Norm legt die STS ein Einweg-Datentransferprotokoll fest (d. h., vom POS zum Zähler), obwohl das Referenzmodell gleichermaßen ein Zweiweg-Transferprotokoll zulässt, welches bei einer zukünftigen Überarbeitung der Norm eine Anforderung sein kann.

5.3 Datenfluss vom Meter_Application_Process zum Token_Carrier

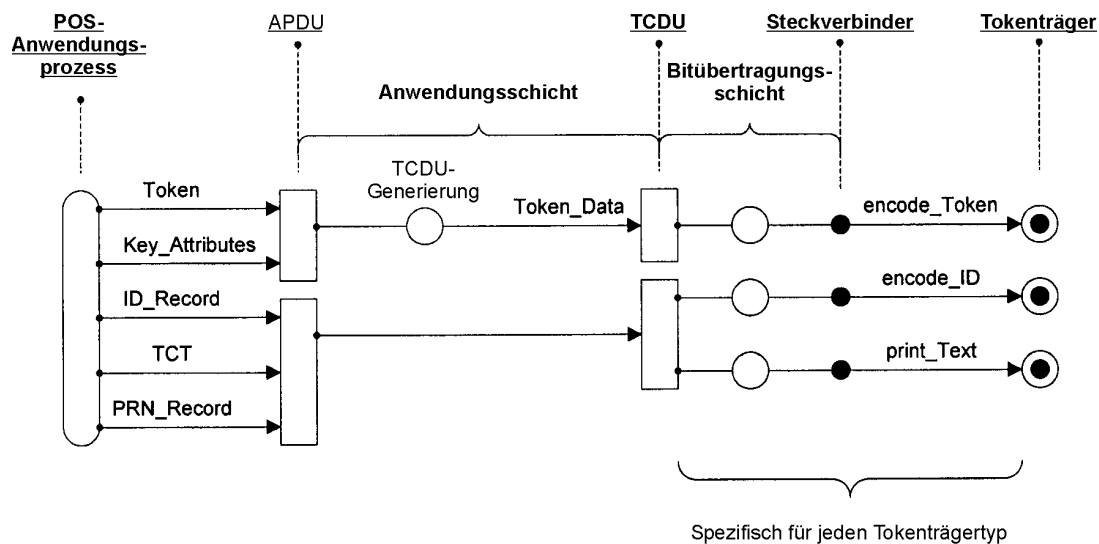


Bild 3 – Datenfluss vom Meter_Application_Process zum Token_Carrier

Der Meter_Application_Process präsentiert der APDU das Token gemeinsam mit den Attributen des Decoder_Key, der für die Verschlüsselung des Token anzuwenden ist. Das Protokoll der Anwendungsschicht generiert den Decoder_Key, verschlüsselt das Token und präsentiert die sich ergebenden Token_Data in der TCDU. Das Protokoll der Bitübertragungsschicht verschlüsselt die Token_Data auf dem Token_Carrier. Kennzeichnungsdaten des Zählers können wahlfrei sowohl auf dem Token_Carrier verschlüsselt sein (siehe Beispiel in IEC 62055-51, 5.2.3) als auch auf die Oberfläche als Text aufgedruckt werden (siehe Beispiel in IEC 62055-51, 5.1.4). Dieser Teil des Prozesses endet im Wesentlichen mit der Verschlüsselung der Daten auf dem Token_Carrier und anschließend wird das Token zum Zähler transportiert (üblicherweise vom Kunden), wo es über das Token_Carrier_Interface in den Zähler eingegeben wird.

5.4 Datenfluss vom Token_Carrier zum Meter_Application_Process

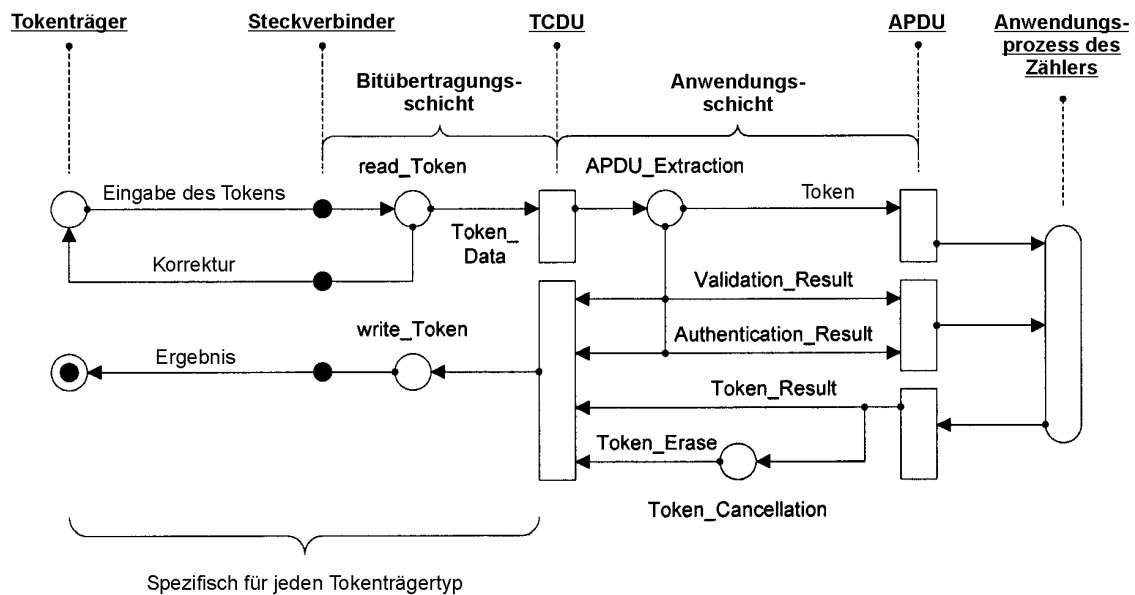


Bild 4 – Datenfluss vom Token_Carrier zum Meter_Application_Process

Der Prozess der Eingabe des Tokens vom Token_Carrier ist entsprechend der Art des Token_Carrier_Type (Bauart des Tokenträger) unterschiedlich. Die Beschaffenheit des Steckverbinders unterscheidet sich gleichermaßen entsprechend dem Token_Carrier_Type; ein Beispiel ist entweder ein Tastenblock oder ein Magnetkartenlesegerät, welches Einweg-Tokenträger entsprechend der Festlegung in IEC 62055-51 unterstützt.

ANMERKUNG Es würden andere Steckverbinderarten erforderlich sein, um andere Tokenträgertypen, wie Speicherschlüssellesegeräte oder Stecker einer tragbaren Einheit, die als virtueller Tokenträger arbeitet, zu unterstützen. Derartige Tokenträger können in der Zukunft in zusätzlichen Teilen von IEC 62055-5x festgelegt sein.

Das Protokoll der Bitübertragungsschicht liest die eingegebenen Tokendaten und liefert unverzüglich eine Korrekturantwort an den Benutzer (siehe Beispiel in IEC 62055-51, 6.3). Die eingegebenen Tokendaten werden in der TCDU dargestellt, von wo aus das Protokoll der Anwendungsschicht durch entsprechende Entschlüsselung, Berechtigungsprüfung und Authentifikation das Token entnimmt und die Ergebnisse für den Meter_Application_Process in der APDU darstellt. Nach der Verarbeitung und Ausführung der Anweisung vom Token wird für weitere Aktionen das Ergebnis vom Meter_Application_Process in der APDU für das Protokoll der Anwendungsschicht angezeigt. Üblicherweise hat dies die Löschung des Token_Identifier zur Folge und über die TCDU wird an das Protokoll der Bitübertragungsschicht die Anweisung erteilt, den Tokeneingabeprozess durch Löschen der Tokendaten (sofern zutreffend) oder gegebenenfalls durch Schreiben von anderen zutreffenden Daten auf den Token_Carrier fertigzustellen.

5.5 Begleitspezifikation

Unter Bezugnahme auf Bild 1 ist zu sehen, dass in IEC 62055-4x und IEC 62055-5x in erster Linie das Token_Carrier_to_Meter_Interface behandelt wird und auch der Token_Carrier eingeschlossen ist. Entsprechend diesem Diagramm werden die verbleibenden Funktionen in Begleitspezifikationen behandelt, für die die übergeordneten Strukturen als Meter_Function_Objects in Abschnitt 9 festgelegt werden.

Die besonderen Meter_Function_Objects in Abschnitt 9 sind somit Blaupausen für die Festlegung der Funktionalität von Inkassozählern. Die spezifischen Instanzen derartiger Meter_Function_Objects sind in den Begleitspezifikationen definiert (siehe auch Anhang D), und jeder ist eine nur einmal existierende Function_Object_Identification_Number (siehe 9.5) zugewiesen, die von der STS-Association verwaltet wird (siehe C.8).

In dieser Norm werden die folgenden vier übergeordneten Meter_Function_Objects definiert:

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

- CRFO: Configuration_Registry_Function_Object; enthält eine Liste registrierter Function_Objects, die im Zähler vorhanden sind, sowie allgemeine Konfigurationsparameter des Zählers.
- VMFO: Virtual_Meter_Function_Object; eine oder mehr Instanzen von Sonderfunktionen, die im Zähler realisiert sind.
- ALFO: Application_Layer_Function_Object; enthält veränderbare Konfigurationsdaten für Sicherheitsfunktionen der Anwendungsschicht und eine Registrierdatenbank von Physical_Layer_Function_Objects, die im Zähler vorhanden sind.
- PLFO: Physical_Layer_Function_Object, enthält veränderbare Protokollkonfigurationsdaten für jede ihrer Tokenträgerschnittstellen der Bitübertragungsschicht, die im Zähler realisiert sind.

5.6 ISO-Bezugsnummern für Transaktionen

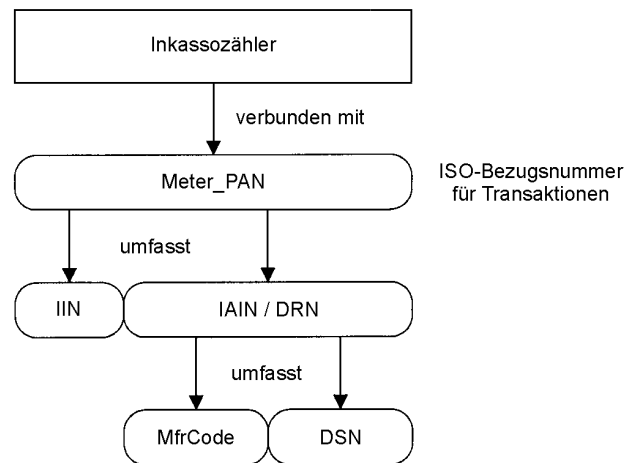


Bild 5 – Aufbau der ISO-Bezugsnummern für Transaktionen

Eine auf Token basierende Transaktion (siehe Abschnitt 3) stellt eine finanzielle Aktivität dar, die entsprechend den genormten Finanzpraktiken zu behandeln ist.

Die in ISO/IEC 7812-1 definierte Primary_Account_Number (PAN) dient zur Kennzeichnung der Aufzeichnungen, Nachrichten, Aufforderungen, Berechtigungen und Benachrichtigungen der Transaktion, durch die beide an der Transaktion beteiligten Parteien eindeutig identifizierbar sind.

Ein Inkassozähler ist somit eindeutig mit einer Meter_PAN verbunden, die eine zusammengesetzte Zahl ist, bestehend aus IIN und IAIN / DRN, die wiederum MfrCode und DSN umfasst (siehe 6.1.1).

6 POS_to-Token_Carrier_Interface: Protokoll der Anwendungsschicht

6.1 APDU: Dateneinheit der Anwendungsschicht

Die APDU ist die Datenschnittstelle zwischen dem Meter_Application_Process und dem Protokoll der Anwendungsschicht und besteht aus den folgenden Datenelementen.

Tabelle 1 – Datenelemente in der APDU

Element	Beschreibung	Format	Bezug
Meter_PAN	ISO-konforme Kennzeichnung Meter_Primary_Account_Number für den Zähler.	18 Ziffern	6.1.1
TCT	Anweisungen, welcher Token_Carrier_Type für das Protokoll der Bitübertragungsschicht verwendet werden sollte, um das Token an den Zähler zu überbringen.	2 Ziffern	6.1.2
DKGA	Anweisungen, welcher Decoder_Key_Generation_Algorithm für die Generierung des Decoder_Key anzuwenden ist.	2 Ziffern	6.1.3
EA	Anweisungen, welcher Encryption_Algorithm für die Verschlüsselung der Tokendaten anzuwenden ist.	2 Ziffern	6.1.4
SGC	Anweisungen, welcher Supply_Group_Code dem Zähler zugewiesen ist.	6 Ziffern	6.1.5
TI	Anweisungen, mit welchem Tariff_Index der Zähler verbunden ist.	2 Ziffern	6.1.6
KRN	Anweisungen, welche Key_Revision_Number der Decoder_Key ist.	1 Ziffer	6.1.7
KT	Anweisungen, welcher Key_Type der Decoder_Key ist.	1 Ziffer	6.1.8
Key_Expiry_Number	Eine mit dem Vending_Key und einem Decoder_Key in Verbindung stehende Nummer, welche die Gültigkeitsdauer des Schlüssels bestimmt.	8 Bit	6.1.9
Token	Die tatsächlichen Tokendaten, die vor der Verschlüsselung und Verarbeitung an den Zähler zu übertragen sind.	66 Bit	6.2
ID-Record	Freigestellte Identifikationsdaten, die dazu vorgesehen sind, dass sie auf einer Zähleridentifikationskarte oder auf einem Tokenträger gemeinsam mit dem Token verschlüsselt werden.	35/32 Ziffern	Tabelle 2
PRN_Record	Freigestellte Daten für einen Ausdruck, die gleichzeitig mit der Codierung des Tokens auf dem Token_Carrier ausgedruckt werden sollen. Bestimmte Tokenträger, wie Magnetstreifenkarten auf Papierbasis, lassen den Ausdruck auf die Kartenoberfläche selbst zu und dieser Vorgang kann mit in der Verschlüsselungseinrichtung für die Magnetkarte integriert sein. Der Inhalt und das Format ist nicht festgelegt und bleibt jedem System überlassen, um es entsprechend den besonderen Anforderungen festzulegen.	unbestimmter Text	

Der freigestellte ID_Record (Kennzeichnungssatz) enthält die folgenden Datenelemente.

Tabelle 2 – Datenelemente im ID_Record

Element	Beschreibung	Format	Bezug
Meter_PAN	ISO-konforme Kennzeichnung Meter_Primary_Account_Number für den Zähler	18 Ziffern	6.1.1
Expiration_Date	Freigestelltes Verfallsdatum für die Identifikationsdaten, wie sie auf der Zähleridentifikationskarte oder auf dem Tokenträger verschlüsselt sind (siehe auch IEC 62055-51, 5.2).	4 Ziffern oder 1 Ziffer	6.1.10
TCT	Gibt an, welcher Token_Carrier_Type mit dieser Meter_PAN verbunden ist.	2 Ziffern	6.1.2
EA	Gibt an, welcher Encryption_Algorithm mit dieser Meter_PAN verbunden ist.	2 Ziffern	6.1.4
SGC	Gibt an, welcher Supply_Group_Code mit dieser Meter_PAN verbunden ist.	6 Ziffern	6.1.5
TI	Gibt an, welcher Tariff_Index mit dieser Meter_PAN verbunden ist.	2 Ziffern	6.1.6
KRN	Gibt an, welche Key_Revision_Number mit dieser Meter_PAN verbunden ist.	1 Ziffer	6.1.7

6.1.1 Meter_PAN: Meter_Primary_Account_Number

Die Meter_PAN ist eine eindeutige Identifikationsnummer für jeden STS-konformen Zähler. Sie enthält die folgenden drei Teile und entspricht der Definition für die PAN (Primary_Account_Number) nach ISO/IEC 7812-1.

Tabelle 3 – Datenelemente in der Meter_PAN

Element	Beschreibung	Format	Bezug
IIN	Issuer_Identification_Number	6 Ziffern	6.1.1.1
IAIN / DRN	Individual_Account_Identification_Number / Decoder_Reference_Number	11 Ziffern	6.1.1.2
PAN_Check_Digit	Formel für die Überprüfung der Unversehrtheit der IIN und der IAIN.	1 Ziffer	6.1.1.3

ANMERKUNG Die Issuer_Identification_Number sind die sechs hochwertigsten Ziffern der 18-stelligen Meter_PAN und das PAN_Check_Digit ist die niederwertigste Ziffer.

Siehe auch C.3 hinsichtlich der Regeln zur Verwaltung dieses Datenelementes.

6.1.1.1 IIN: Issuer_Identification_Number

Die IIN ist eine eindeutige 6-stellige Zahl, die einen Bereich angibt, unter der weitere Individual_Account_Identification_Numbers (d. h. Decoder_Reference_Numbers) für die Anwendung innerhalb dieses definierten Bereiches erteilt werden können.

Die ursprüngliche Absicht und der Zweck der IIN bestand darin, finanzielle Transaktionen zu markieren, um sie eindeutig zu kennzeichnen und sie als entsprechende Konten finanzieller Transaktionen zu führen. Es war vorgesehen, dass die IIN von der ISO nach dem Registrierungssystem in ISO/IEC 7812-1 und ISO/IEC 7812-2 erteilt wird. Dies hat sich jedoch als ungeeignet herausgestellt und der Wert 600727 für die IIN ist seitdem der De-facto-Standard geworden, der weltweit für alle STS-Inkassozählersysteme angewendet wird. Die Fortsetzung dieser Praxis wird unterstützt.

Demzufolge muss für die Anwendung dieser Norm, sofern sie für STS-Energiemesssysteme gilt, die IIN den Wert 600727 besitzen.

Siehe auch C.3.1 hinsichtlich der Regeln zur Verwaltung dieses Datenelementes.

6.1.1.2 IAIN: Individual_Account_Identification_Number DRN: Decoder_Reference_Number

Der Einrichtung, die das Protokoll der Anwendungsschicht in einem STS-konformen Zähler ausführt, muss eine eindeutige DRN zugewiesen werden.

ANMERKUNG In vielen Systemen gehört der Decoderteil direkt zum Zählerteil und somit kann die Decoder_Reference_Number mit der Zählerseriennummer übereinstimmen.

Sie ist eine 11-stellige Zahl und umfasst die folgenden Datenelemente.

Tabelle 4 – Datenelemente in der IAIN / DRN

Element	Beschreibung	Format	Bezug
Manufacturer_Code	Manufacturer_Code (Herstellerkennzahl)	2 Ziffern	6.1.1.2.1
Decoder_Serial_Number	Eine vom Hersteller zugewiesene achtstellige Seriennummer	8 Ziffern	6.1.1.2.2
DRN_Check_Digit	Prüfziffer; Formel für die Überprüfung der Unversehrtheit der Manufacturer_Code und der Decoder_Serial_Number.	1 Ziffer	6.1.1.2.3

ANMERKUNG Der Manufacturer_Code sind die zwei hochwertigsten Ziffern der 11-stelligen Decoder_Reference_Number und die DRN_Check_Digit ist die niederwertigste Ziffer.

6.1.1.2.1 MfrCode: Manufacturer_Code

Der Manufacturer_Code ist eine zweistellige Zahl, die zur eindeutigen Kennzeichnung des Herstellers des Zählers zu verwenden ist.

Die STS stellt einen Dienst für die Zuweisung der Manufacturer_Codes bereit, um die Hersteller eindeutig zu identifizieren und die Kompatibilität der STS-konformen Einrichtungen zu sichern.

Siehe auch C.3.2 hinsichtlich der Regeln zur Verwaltung dieses Datenelementes.

6.1.1.2.2 DSN: Decoder_Serial_Number

Die DSN ist eine nur einmal existierende 8-stellige Seriennummer, die intern vom Hersteller generiert wird. Jeder Hersteller ist für die Einmaligkeit der DSN bezüglich seines Manufacturer_Codes verantwortlich.

Siehe auch C.3.3 hinsichtlich der Regeln zur Verwaltung dieses Datenelementes.

6.1.1.2.3 DRN_Check_Digit

Das DRN_Check_Digit ist eine einzelne Ziffer, die zur Gültigkeitsprüfung der Unversehrtheit der Werte von Manufacturer_Code und DRN verwendet wird, wenn diese von Hand eingegeben oder maschinell eingelesen werden. Dies ist eine Modulo-10-Prüfziffer, die nach der in ISO/IEC 7812-1, Anhang B, angegebenen Luhn-Gleichung berechnet wird. Sie wird aus den 10 Ziffern, die der DSN vorhergehen, berechnet und wird durch die Verkettung der Werte von Manufacturer_Code und der DSN generiert.

6.1.1.3 PAN_Check_Digit

Das PAN_Check_Digit ist eine einzelne Ziffer, die zur Gültigkeitsprüfung der Unversehrtheit der Werte von Issuer_Identification_Number und Individual_Account_Identification_Number verwendet wird, wenn diese von Hand eingegeben oder maschinell eingelesen werden. Das Verfahren für die Berechnung des Wertes von PAN_Check_Digit ist in ISO/IEC 7812-1 angegeben und sie wird aus den 17 vorhergehenden Ziffern der Meter_PAN berechnet und wird durch Verkettung der Werte von Issuer_Identification_Number und Individual_Account_Identification_Number generiert.

6.1.2 TCT: Token_Carrier_Type

Dies ist eine zweistellige Zahl, die verwendet wird zur eindeutigen Kennzeichnung des Typs des Tokenträgers, auf dem das Token für die Übertragung an den Zähler verschlüsselt sein sollte.

Tabelle 5 – Typen von Tokenträgern

Type	Token_Carrier	Bemerkungen
00	Reserviert	Für künftige Zuweisungen.
01	Magnetkarte	Wie in dieser Norm festgelegt.
02	Zahlwort	Wie in dieser Norm festgelegt.
03-06	Reserviert	Altsysteme mit firmenspezifischen Tokenträgertechniken.
07-99	Reserviert	Für künftige Zuweisungen.

Werte kleiner als 10 müssen rechts ausgerichtet und links mit einer Null aufgefüllt werden (z. B. 01, 02 ...09).

6.1.3 DKGA: Decoder_Key_Generation_Algorithm

Dies ist eine zweistellige Zahl, die zur eindeutigen Kennzeichnung des Algorithmus verwendet wird, welcher für die Generierung des Decoder_Key angewendet wird.

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

Tabelle 6 – DKGA-Kennzahlen

Kenn-zahl	DKG-Algorithmus	Bemerkungen	Bezug
00	Reserviert	Für künftige Zuweisungen.	
01	DKGA01	Begrenzte Anzahl von früheren alten STS-Zählern. Ersetzt durch DKGA02.	6.5.2.3
02	DKGA02	Systeme mit 56-Bit-Vending_Key-Diversifikation.	6.5.2.4
03	DKGA03	Systeme mit 112-Bit-Vending_Key-Diversifikation.	6.5.2.5
04-99	Reserviert	Für künftige Zuweisungen.	

ANMERKUNG 1 DKGA02 ist der Algorithmus, der für gegenwärtige Systeme anzuwenden ist, vorbehaltlich der Kriterien für DKGA01.

ANMERKUNG 2 DKGA03 ist der Algorithmus, der für zukünftige Systeme anzuwenden ist, die einen höheren Sicherheitsgrad hinsichtlich des Schutzes des Vending_Key durch „brute-force“-Angriff („Brechstangen“-Angriff) erforderlich machen.

ANMERKUNG 3 Die Einführung von DKGA03 sollte vorzugsweise mit dem Wechsel von STA zu DEA (EA-Code 07 auf EA-Code 09) zusammenfallen. Siehe auch 6.1.4.

Werte kleiner als 10 müssen rechts ausgerichtet und links mit einer Null aufgefüllt werden (z. B. 01, 02 ...09).

6.1.4 EA: Encryption_Algorithm

Dies ist eine zweistellige Zahl, die zur eindeutigen Kennzeichnung des Verschlüsselungsalgorithmus verwendet wird, welcher für die Verschlüsselung der Tokendaten angewendet wird.

Tabelle 7 – EA-Kennzahlen

Kenn-zahl	Verschlüsselungs-algorithmus	Bemerkungen	Bezug
00-06	Reserviert	Firmenspezifische Altsysteme.	
07	STA	Systeme, die den Standardtransferalgorithmus anwenden, wie er in dieser Norm festgelegt wird.	6.5.3
08	Reserviert	Firmenspezifische Altsysteme.	
09	DEA	Systeme, die den Datenverschlüsselungsalgorithmus anwenden, wie er in ANSI X3.92 festgelegt ist.	6.5.4
10	Reserviert	Firmenspezifische Altsysteme.	
10-99	Reserviert	Für künftige Zuweisungen.	

ANMERKUNG Der Wechsel von STA zu DEA sollte vorzugsweise mit der Einführung von DKGA03 zusammenfallen, um die Auswirkung auf bestehende Systeme im installierten Hauptbestandteil auf ein Minimum einzuschränken (siehe 6.1.3).

Werte kleiner als 10 müssen rechts ausgerichtet und links mit einer Null aufgefüllt werden (z. B. 01, 02 ...09).

6.1.5 SGC: Supply_Group_Code

Dies ist eine eindeutige 6-stellige Zahl, die einem Unternehmen zugewiesen wird, welches innerhalb der KMS registriert ist. Es wird zur eindeutigen Kennzeichnung einer Untergruppe von Zählern in einem Versorgungs-

oder Verteilungsbereich des Unternehmens verwendet. Jede Supply_Group hat einen Vending_Key, der mit ihm und folglich jedem Zähler in der Supply_Group einen abgeleiteten Decoder_Key hat, der damit in Verbindung steht. Die Befugnis zum Verkauf von Token wird somit durch die selektive Verteilung eines derartigen Vending_key und Supply_Group_Code an autorisierte Verkäufer gesteuert, die POS-Dienste im Auftrag der Unternehmen ausführen.

Die Verwaltung des Supply_Group_Code und die Verwaltung des Vending_Key steht vollständig unter der Kontrolle der KMS und unterliegt dessen Regeln.

Werte kleiner als 6 Dezimalstellen müssen rechts ausgerichtet und links mit Null aufgefüllt werden (z. B. 000001, 000002 ... 000009).

Der Supply_Group_Code bekommt den Type vom Verkaufsmerkmal Key_Type (siehe 6.5.1.1) mit dem er nach der folgenden Tabelle verbunden ist.

Tabelle 8 – SGC-Arten und Schlüsselarten

SGC-Art	Verkaufs-Schlüsselart (siehe 6.5.1.1)	Decoder-Schlüsselart (siehe 6.5.1.2)
Initialisierung	Nicht festgelegt.	DITK
Stabdard	VDDK	DDTK
Eindeutig	VUDK	DUTK
Gemeinsam	VCDK	DCTK

Siehe auch Anhang C hinsichtlich der Regeln zur Verwaltung dieses Datenelementes.

6.1.6 TI: Tariff_Index

Eine zweistellige Zahl, die mit einem besonderen Tarif verbunden ist, der einem speziellen Kunden zugeordnet worden ist. Die Pflege und der Inhalt der Tariftabellen liegt in der Verantwortung des Unternehmens.

Werte kleiner als 10 müssen rechts ausgerichtet und links mit einer Null aufgefüllt werden (z. B. 01, 02 ...09).

Der Tariff_Index wird auch im Decoder_Key verschlüsselt, was bedeutet, dass bei einer Umstellung eines Kunden von einem Tariff_Index auf einen anderen auch dessen Decoder_Key zu verändern ist (siehe 6.5.1).

Siehe auch Anhang C hinsichtlich der Regeln zur Verwaltung dieses Datenelementes.

6.1.7 KRN: Key_Revision_Number

Dies ist eine einstellige Zahl im Bereich von 1 bis 9, die mit einer Version des Vending_Key und mit dem entsprechenden Decoder_Key verbunden ist.

Zu ausführlichen Festlegungen für dieses Datenelement siehe 6.5.1.4.

6.1.8 KT: Key_Type

Dies ist eine einstellige Zahl im Bereich von 0 bis 3, die mit einer Eigenschaft des Vending_Key und somit auch mit dem entsprechenden Decoder_Key verbunden ist, welche aus dem Vending_Key abgeleitet wird.

Zu ausführlichen Festlegungen für dieses Datenelement siehe 6.5.1.

6.1.9 KEN: Key_Expiry_Number

Eine Key-Expiry_Number ist durch die KMS mit jedem Vending_Key verbunden und bestimmt die Zeit, wann ein Vending_Key und jeder entsprechende Decoder_Key abläuft, nach der er für die weitere Verwendung vorbehaltlich bestimmter Bewilligungen ungültig wird.

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

Die Key_Expiry_Number entspricht den hochwertigsten 8 Bit des 24-Bit-Token_Identifier. Jede Tokenkennung, deren höchstwertigste 8 Bit größer die Key_Expiry_Number des Schlüssels ist, kann mit diesem Schlüssel nicht verschlüsselt oder entschlüsselt werden.

Zu ausführlichen Festlegungen für dieses Datenelement siehe 6.5.1.5.

Siehe auch Anhang C hinsichtlich der Regeln zur Verwaltung dieses Datenelementes.

6.1.10 ED: Expiration_Date

Dieses Datum ist mit der Gültigkeitsdauer für identitätsbezogene Daten verbunden, die verschlüsselt auf einer identitätstragenden Einrichtung vorliegen. Beispielsweise eine Zähleridentifizierungskarte oder eine zweite Aufzeichnung, die auf dem Token_Carrier gemeinsam mit den Tokendaten verschlüsselt ist. Bei einigen Realisierungen hat es sich als nützlich erwiesen, dass der Kunde einen benutzten Tokenträger wieder zurückbringt, weil dies beim Kauf des nächsten Tokens als seine Decoderidentifizierung für die Kasse dient. (siehe auch IEC 62055-51, 5.1.3)

Dieses Datum kann beispielsweise auch in Fällen verwendet werden, in denen einem Verbraucher ein Ermäßigungstarif für eine beschränkte Dauer zugeteilt worden ist. Das verschlüsselte Datum ist der letzte Monat, in dem die Karte gültig ist.

Das Format für das Expiration_Date ist: YYMM und muss immer vier Stellen enthalten. Wenn YY oder MM kleiner als 10 sind, muss die Zahl rechtsbündig stehen und links mit einer 0 aufgefüllt werden.

Tabelle 9 – Kodierte Formate für das Jahr des Expiration_Date

YY	Gibt an
00 bis 99	2000 bis 2099

Tabelle 10 – Kodierte Formate für den Monat des Expiration_Date

MM	Gibt an
00	Expiration_Date ist nicht erforderlich
01 bis 12	Januar bis Dezember
13 bis 99	Ungültig

Das Expiration_Date ist freigestellt und wenn es nicht verlangt ist, dann muss der MM-Wert gegen 00 ausgetauscht werden und das YY-Feld kann einen beliebigen Wert haben.

6.2 Token

Das Element Token_Data in der APDU ist eine 66-Bit-Binärzahl, die aus mehreren Feldern kleinerer Datenelemente besteht, mit denen verschiedene Prozesse im Meter_Application_Process ausgelöst und verschiedene Informationsbits an die Zählerregister übertragen werden.

6.2.1 Klasse 0: transfer_Credit

Klasse	Unterklasse (Sub_Class)	RND	TID	Betrag	CRC
2 Bits	4 Bit	4 Bit	24 Bit	16 Bit	16 Bit
0	0 = Elektrizität <u>Reserviert:</u> 1 = Wasser 2 = Gas 3 = Zeit 4 = Währung 5 bis 15 = künftige Zuweisungen				

Das Guthaben wird an den Zähler übertragen mit dem Wert, der im Feld Betrag bestimmt ist, und für die Dienstart, die im Feld Sub_Class bestimmt ist.

ANMERKUNG Die Sub_Class-Werte 1 bis 4 sind von der STS-Association für andere Anwendungen und die Werte 5 bis 15 für künftige Zuweisungen reserviert.

6.2.2 Klasse 1: Initiate_Meter_Test/Display

Klasse	Unterklasse (Sub_Class)	Steuerung	MfrCode	CRC
2 Bit	4 Bit	36 Bit	8 Bit	16 Bit
1	0 = STS definiert	Bitpositionssteuerung von Prüfung/Anzeigenummer	0	
1	1 - 10 = reserviert von STS-Association für künftige Zuweisungen	Reserviert	0	
1	11 - 15 = firmenspezifische Anwendung	Auf Null setzen, falls nicht benutzt	0 - 99	

Die Prüf- oder Anzeigefunktion im Zähler wird entsprechend dem Bitmuster ausgelöst, welches im Feld Steuerung festgelegt ist.

6.2.3 Klasse 2: set_Maximum_Power_Limit

Klasse	Unterklasse (Sub_Class)	RND	TID	MPL	CRC
2 Bit	4 Bit	4 Bit	24 Bit	16 Bit	16 Bit
2	0				

Das Register maximale Leistungsgrenze im Zähler ist mit dem Wert zu laden, der im Feld MPL angegeben ist.

6.2.4 Klasse 2: clear_Credit

Klasse	Unterklasse (Sub_Class)	RND	TID	Register	CRC
2 Bit	4 Bit	4 Bit	24 Bit	16 Bit	16 Bit
2	1				

Das entsprechende Guthabenregister (wie im Registerfeld angegeben) im Zähler ist zu löschen (auf Null zu setzen).

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

6.2.5 Klasse 2: set_Tariff_Rate

Klasse	Unterklasse (Sub_Class)	RND	TID	Rate	CRC
2 Bit	4 Bit	4 Bit	24 Bit	16 Bit	16 Bit
2	2				

Das Tarifregister im Zähler ist mit dem Wert zu laden, der im Feld Rate angegeben ist.

Dieses Token ist von der STS-Association für künftige Festlegungen reserviert.

6.2.6 Klasse 2: set_1st_Section_Decoder_Key (1. Abschnitt des Decoderschlüssels festlegen)

Klasse	Unterklasse (Sub_Class)	KexpNoHO	KRN	RO	Res	KT	NKHO	CRC
2 Bit	4 Bit	4 Bit	4 Bit	1 Bit	1 Bit	2 Bit	32 Bit	16 Bit
2	3		1 - 9	0 - 1	x	0 - 3		

Das Decoder_Key_Register ist mit der 1. Hälfte des neuen Decoder_Key zu laden, abhängig von einem authentifizierten Laden eines set_2nd_Section_Decoder_Key-Token.

6.2.7 Klasse 2: set_2nd_Section_Decoder_Key (2. Abschnitt des Decoderschlüssels festlegen)

Klasse	Unterklasse (Sub_Class)	KexpNoLO	TI	NKLO	CRC
2 Bit	4 Bit	4 Bit	8 Bit	32 Bit	16 Bit
2	4		0 - 99		

Das Decoder_Key_Register ist mit der 2. Hälfte des neuen Decoder_Key zu laden, abhängig von einem authentifizierten Laden eines set_1st_Section_Decoder_Key-Token.

6.2.8 Klasse 2: clear_Tamper_Condition (Manipulationsbedingung löschen)

Klasse	Unterklasse (Sub_Class)	RND	TID	Pad	CRC
2 Bit	4 Bit	4 Bit	24 Bit	16 Bit	16 Bit
2	5			0	

Das Manipulationsstatusregister im Zähler ist zu löschen und alle sich ergebenden Steuerprozesse, die momentan ablaufen können, sind abzuberechnen.

6.2.9 Klasse 2: set_Maximum_Phase_Power_Unbalance_Limit (oberen Grenzwert der unsymmetrischen Phasenbelastung festlegen)

Klasse	Unterklasse (Sub_Class)	RND	TID	MPPUL	CRC
2 Bit	4 Bit	4 Bit	24 Bit	16 Bit	16 Bit
2	6				

Das Register für den Grenzwert der Phasenunsymmetrie im Zähler ist mit dem Wert zu laden, der im MPPUL-Feld angegeben ist.

6.2.10 Klasse 2: set_Water_Meter_Factor (Wasserzählerfaktor festlegen)

Klasse	Unterklasse (Sub_Class)	RND	TID	WMfactor	CRC
2 Bit	4 Bit	4 Bit	24 Bit	16 Bit	16 Bit
2	7				

Das Register Wasserzählerfaktor im Zähler ist mit dem Wert zu laden, der im Feld WMfactor angegeben ist.

Dieses Token ist von der STS-Association für Anwendungen mit Wasserzählern reserviert.

6.2.11 Klasse 2: Reserviert für STS-Anwendungen

Klasse	Unterklasse (Sub_Class)	RND	TID	ResData	CRC
2 Bit	4 Bit	4 Bit	24 Bit	16 Bit	16 Bit
2	8 - 10				

Dieser Tokenbereich ist von der STS-Association für künftige Festlegungen reserviert.

6.2.12 Klasse 2: Reserviert für firmenspezifische Anwendung

Klasse	Unterklasse (Sub_Class)	RND	TID	PropData	CRC
2 Bit	4 Bit	4 Bit	24 Bit	16 Bit	16 Bit
2	11 - 15				

Dieser Tokenbereich ist für firmenspezifische Festlegungen und Anwendungen reserviert.

ANMERKUNG Diese Norm bietet keinen Schutz gegen Konflikte zwischen Herstellern, die diesen Tokenbereich verwenden. Generierung und Steuerung dieser Token muss deshalb stets unter der direkten Verwaltung der betreffenden Hersteller stehen und darf niemals in Vertriebssystemen für die allgemeine Anwendung innerhalb von STS-Inkassozählernsystemen verfügbar sein.

6.2.13 Klasse 3: Reserviert für STS-Anwendungen

Klasse	Unterklasse (Sub_Class)	Res
2 Bit	4 Bit	60 Bit
3	0 - 15	

Dieser Tokenbereich ist von der STS-Association für künftige Festlegungen reserviert.

6.3 Tokendatenelemente

Die folgenden Datenelemente werden in verschiedenen Kombinationen in Token angewendet.

Tabelle 11 – In Token angewendete Datenelemente

Element	Name	Format	Bezug
Amount	Transfer_Amount	16 Bit	6.3.5
Class	Token_Class	2 Bit	6.3.1
Control	initiate_meter_Test/Display control field	36 Bit	6.3.7
CRC	Cyclic_Redundancy_Code	16 Bit	6.3.6
KexpNoHO	Key_Expiry_Number_High_Order	4 Bit	6.3.15
KexpNoLO	Key_Expiry_Number_Low_Order	4 Bit	6.3.16
KRN	Key_Revision_Number	4 Bit	6.1.7
KT	Key_Type	2 Bit	6.1.8
MfrCode	Manufacturer_Code	8 Bit	6.1.1.2.1
MPL	Maximum_Power_Limit	16 Bit	6.3.8
MPPUL	Maximum_Phase_Power_Unbalance_Limit	16 Bit	6.3.9
NKHO	New_Key_High_Order	32 Bit	6.3.13
NKLO	New_Key_Low_Order	32 Bit	6.3.14
Pad	Auffüllwert mit 0	16 Bit	X
PropData	Firmenspezifisches Datenfeld	16 Bit	X
Rate	[Tarif] Für künftige Festlegungen	16 Bit	6.3.10
Register	Register_to_clear	16 Bit	6.3.12
Res	Reserviert	1 Bit	X
ResData	Reservierte Daten für künftige Festlegungen	16 Bit	X
RND	Zufallszahl	4 Bit	6.3.3
RO	Rollover_Key_Change	1 Bit	6.3.17
Sub_Class	Token_Sub_Class	4 Bit	6.3.2
TI	Tariff_Index	8 Bit	6.1.6
TID	Token_Identifier	24 Bit	6.3.4
WMfactor	[Water_Meter_Factor] Von der STS-Association für Anwendungen mit Wasserzählern reserviert.	16 Bit	6.3.11

6.3.1 Klasse: Token_Class

Tokens werden in 4 Hauptfunktionsbereiche eingeteilt:

Tabelle 12 – Tokenklassen

Token_Class	Funktion
0	Guthabentransfer
1	Nicht zählerspezifische Verwaltung
2	Zählerspezifische Verwaltung
3	Für künftige Festlegungen reserviert.

Token der Klasse 0 und der Klasse 2 werden mit dem Decoder_Key verschlüsselt, während Token der Klasse 1 nicht verschlüsselt werden und somit für jeden STS-konformen Zähler angewendet werden können.

6.3.2 Sub_Class: Token_Sub_Class

Weitere Unterklassifizierung der Token_Class wie folgt:

Tabelle 13 – Unterklassen von Token

Token_Sub_Class	Token_Class			
	0	1	2	3
0	Guthaben für Elektrizität	Zählerprüfung einleiten	oberen Leistungsgrenzwert festlegen	Von der STS-Association für künftige Festlegungen reserviert
1	Von der STS-Association für Guthaben für Wasser reserviert	Von der STS-Association für künftige Festlegungen reserviert	Guthabenregister löschen	
2	Von der STS-Association für Guthaben für Gas reserviert		Tarif einstellen	
3	Von der STS-Association für Guthaben für Verbindungszeit reserviert		1. Abschnitt des Decoder-schlüssels festlegen	
4	Von der STS-Association für Guthaben in Währungseinheiten reserviert		2. Abschnitt des Decoder-schlüssels festlegen	
5	Von der STS-Association für künftige Festlegungen reserviert		Manipulationsbedingung löschen	
6			Oberen Grenzwert der unsymmetrischen Phasenbelastung festlegen	
7			Von der STS-Association für Einstellung des Wasserzählerfaktors reserviert.	
8			Von der STS-Association für künftige Festlegungen reserviert	
9				
10				
11				
12		Für firmenspezifische Anwendungen reserviert.	Für firmenspezifische Anwendungen reserviert.	
13				
14				
15				

6.3.3 RND: Random_Number

Die Generierung dieser 4-Bit-Zahl sind ein Schnappschuss der vier niederwertigsten Bit eines Zählers, der mindestens Millisekunden zählt. Die Einbeziehung einer Zufallszahl in die zu übertragenden Daten erhöht die Sicherheit des Tokentransfers, weil eine Wahrscheinlichkeit von 16:1 vorgesehen wird, dass zwei Token, die identische zu übertragende Daten enthalten, nicht dasselbe Binärmuster enthalten werden.

6.3.4 TID: Token_Identifier

Das Feld Token_Identifier wird aus dem Datum und der Zeit der Ausgabe abgeleitet und gibt die Anzahl der Minuten an, die seit einem STS-Grunddatum und -zeit vergangen sind. STS-Grunddatum und -zeit sind der

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

01. Januar 1993, 00:00:00. Bei der Berechnung der vergangenen Minuten müssen Schaltjahre berücksichtigt werden. Dieses Feld ist eine 24-Bit-Binärdarstellung der vergangenen Minuten, das am weitesten links stehende Bit ist das höchstwertigste Bit.

Für ein Datums- und Zeitformat, wie YYYY:MM:DD:hh:mm:ss entsprechen STS-Grunddatum und -zeit von 1993:01:01:00:00:00 einem Token_Identifier von 0.

Bei der Berechnung des Token_Identifiers wird der Wert „:ss“ vom Istwert der Zeit abgeschnitten.

Tabelle 14 – Berechnungsbeispiel 1 für TID

Ausgabedatum:	25. März 1993
Ausgabezeit:	13:55:22
Vergangene Minuten	120 355
Ergebnis: 24-Bit-Token_ID	0000 0001 1101 0110 0010 0011

Tabelle 15 – Berechnungsbeispiel 2 für TID

Ausgabedatum:	25. März 1996
Ausgabezeit:	13:55:22
Vergangene Minuten	1 698 595
Ergebnis: 24-Bit-Token_ID	0001 1001 1110 1011 0010 0011

6.3.4.1 Besonderer reservierter Token_Identifier

Der Token_Identifier, der 00h01 eines jeden Tages entspricht, ist für Token für Sonderanwendungen reserviert und darf nicht für beliebige andere Token verwendet werden.

Mit dem Datums- und Zeitformat von YYYY:MM:DD:hh:mm:ss entsprechen die reservierten Token_Identifier xxxx:xx:xx:00:01:xx.

Wenn ein Token, ausgenommen ein Token für eine Sonderanwendung, zu einem Zeitpunkt zu generieren ist, der diesem reservierten Token_Identifier entspricht, dann muss eine Minute zum Token_Identifier addiert werden.

Siehe auch Regeln für die Verwaltung dieses besonderen reservierten Token_Identifiers in Anhang C.

6.3.4.2 Mehrere Token, die innerhalb derselben Minute zu generieren sind

Der Kassenplatz muss sicherstellen, dass kein rechtmäßig gekauftes Token denselben Token_Identifier wie der eines anderen rechtmäßig gekauften Tokens für denselben Zähler tragen darf, selbst wenn mehr als ein Token innerhalb derselben Minute an demselben Kassenplatz gekauft wird.

Wenn es erforderlich ist, innerhalb derselben Minute für denselben Zähler mehrere Tokens zu generieren, dann muss zu jedem aufeinanderfolgenden Token in dieser Reihe eine Minute zum Token_Identifier addiert werden. Am Ende des Tokengenerierungsprozesses muss der Kassenplatz wieder zur Echtzeit zurückkehren.

Beispiel: Wenn 3 Guthabentokens A, B und C innerhalb derselben Minute um 13h23 und in der Reihenfolge A, B und C generiert werden, dann müssen die Token_Identifier von A die Zeitmarke 13h23, von B die Zeitmarke 13h24 und von C 13h25 tragen.

6.3.5 Betrag: Transfer_Amount

Für den Transfer des Betrages sind die zugehörigen Einheiten wie folgt definiert:

Tabelle 16 – Einheiten für elektrische Energie

Typ des Transfers	Einheiten
Elektrische Energie	Wattstunden × 100

Für andere Anwendungen sieht die STS-Association die Folgenden vor:

Tabelle 17 – Einheiten für andere Anwendungen

Typ des Transfers	Einheiten
Wasser	Liter × 100
Gas	Ist festzulegen.
Zeit	Minuten
Währung	Ist festzulegen.

ANMERKUNG Für andere Versorgungsdienste bestimmt die STS-Association weitere künftige Transfertypen.

Die 16 Bit des Feldes Transferbetrag sind in zwei Abschnitte unterteilt, in einen Exponenten aus zwei Bit zur Basis 10 und eine Mantisse von 14 Bit. Die Bit sind beginnend bei 0 von rechts nach links nummeriert. Bit 15 ist das höchstwertigste Bit des Exponenten und Bit 13 ist das höchstwertigste Bit der Mantisse. Die Bitzuweisungen innerhalb dieses Feldes sind nachfolgend dargestellt

Tabelle 18 – Bitzuweisungen für Transfer_Amount

Position	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Wert	e	e	m	m	m	m	m	m	m	m	m	m	m	m	m	m

Die Gleichung für die Umrechnung des Transferbetrages lautet:

$$t = 10^e \times m, \text{ für } e = 0; \text{ oder}$$

$$t = (10^e \times m) + \sum_{n=1}^e (2^{14} \times 10^{(n-1)}), \text{ für } e > 0$$

Dabei ist:

t der Transferbetrag;

e der Exponent zur Basis 10;

m die Mantisse und

n ist eine ganze Zahl im Bereich von 1 bis einschließlich e .

Alle Umrechnungen des Transferbetrages müssen zugunsten des Kunden aufgerundet werden. In der folgenden Tabelle sind die möglichen Bereiche der Transferbeträge und die zugehörigen maximalen Fehler angegeben.

Tabelle 19 – Maximaler Fehler durch Rundung

Wert des Exponenten	Bereich des Transferbetrages	Maximaler Fehler
0	0000000 bis 00016383	0,000
1	0016384 bis 00180214	0,061 %
2	0180224 bis 01818524	0,055 %
3	1818624 bis 18201624	0,055 %

Tabelle 20 – Beispiele für Werte des Transfer_Amount

	Gekaufte Einheiten	16-Bit Feld für den Transferbetrag
1	0,1 kWh	0000 0000 0000 0001
2	25,6 kWh	0000 0001 0000 0000
3	1 638,3 kWh	0011 1111 1111 1111
4	1 638,4 kWh	0100 1111 1111 1111
5	18 022,3 kWh	0111 1111 1111 1111
6	10 022,4 kWh	1000 0000 0000 0000
7	181 862,3 kWh	1011 1111 1111 1111
8	181 862,4 kWh	1100 0000 0000 0000
9	1 820 162,4 kWh	1111 1111 1111 1111

6.3.6 CRC: Cyclic_Redundancy_Code

Der CRC ist ein Prüfsummenfeld, welches zur Prüfung der Unversehrtheit der übertragenen Daten verwendet wird. Die Prüfsumme wird aus dem folgenden CRC-Generierungspolynom abgeleitet:

$$X^{16} + X^{15} + X^2 = 1$$

Die Gesamtlänge der über das Token übertragenen Daten ist 66 Bit. Die letzten 16 Bit enthalten die CRC-Prüfsumme, die aus den vorangegangenen 50 Bit abgeleitet worden ist. Diese 50 Bit werden links mit 6 Binärnullen aufgefüllt, um 56 Bit zu erhalten. Vor der Berechnung wird die CRC-Prüfsumme mit FFFFhex initialisiert (siehe folgendes Beispiel).

Tabelle 21 – Beispiel für eine CRC-Berechnung

Original 50 Bit	0 00 4A 2D 90 0F F2 hex
Links aufgefüllt, um 7 Byte zu erhalten	00 00 4A 2D 90 0F F2 hex
Berechnete Prüfsumme	0F FA hex

6.3.7 Steuerung: initiate_Meter_Test/Display_control_field

Das Datenfeld „initialisiere Zählerprüfung“ ist 36 Bit lang und wird zur Anzeige des Typs der durchzuführenden Prüfung angewendet. Die einzelne Prüfung wird ausgewählt, indem das betreffende Bit auf eine logische Eins gesetzt wird. Die zulässigen Werte des Feldes sind in der nachstehenden Tabelle festgelegt.

Tabelle 22 – Zulässige Werte des Steuerfeldes

LSB Nr. = 1	Nr. der Prüfung	Wirkung	Bedingung
Alle Bit = 1	0	Prüfungen Nr. 1 bis 5 durchführen, wahlfrei jede weitere	Verbindlich
1	1	Prüfung des Lastschalters	Verbindlich
2	2	Prüfung der Einrichtungen für die Informationsanzeige des Zählers	Verbindlich
3	3	Anzeige der Register für den kumulativen Gesamtverbrauch	Verbindlich
4	4	Anzeige der Key_Revision_Number	Verbindlich
5	5	Anzeige des Tariff_Index	Verbindlich
6	6	Prüfung der Tokenleseeinrichtung	Wahlfrei
7	7	Anzeige der Obergrenze der Leistung	Wahlfrei
8	8	Anzeige des Manipulationsstatus	Wahlfrei
9	9	Anzeige der Leistungsaufnahme	Wahlfrei
10	10	Anzeige der Softwareversion	Wahlfrei
11	11	Anzeige des Grenzwertes der Phasenunsymmetrie	Wahlfrei
12	12	Von der STS-Association reserviert für: Anzeige des Wasserzählerfaktors	Verbindlich für Wasserzähler
13	13	Anzeige des Tarifs	Verbindlich für währungsbasierte Zähler
14 - 36	Reserviert	Von der STS-Association reserviert für künftige Festlegungen	Reserviert

Alle Zähler müssen die Prüfung Nr. 5 unterstützen; wird eine der dazugehörigen Prüfungen nicht vom Zähler unterstützt, muss die Untergruppe der Prüfungen durchgeführt werden, die unterstützt wird.

6.3.8 MPL: Maximum_Power_Limit

Das Feld für die Obergrenze der Leistung ist ein 16-Bit-Feld, welches die maximale Leistung in Watt angibt, die die Last aufnehmen darf. Die Berechnung dieses Feldes ist identisch wie die des Feldes für den Transferbetrag (siehe 6.3.5). Zu Funktionsanforderungen des Meter_Application_Process siehe auch Anmerkung in 8.6.

6.3.9 MPUL: Maximum_Phase_Power_Unbalance_Limit

Das Feld für den oberen Grenzwert der unsymmetrischen Phasenbelastung ist ein 16-Bit-Feld, welches die maximale Leistungsdifferenz zwischen den Phasenbelastungen in Watt angibt. Die Berechnung dieses Feldes ist identisch wie die des Feldes für den Transferbetrag (siehe 6.3.5).

6.3.10 Rate: Tariff_Rate

Das Feld Tariff_Rate ist ein 16-Bit-Feld, welches den Tarif oder den Preis je Einheit angibt. Das Format ist noch festzulegen. Dieses Token ist für künftige Anwendungen mit währungsbasierten kontoführenden Zählern vorgesehen, aber bis dahin ist es von der STS-Association für eine künftige Festlegung reserviert.

6.3.11 WMfactor: Water_Meter_Factor

Von der STS-Association für Anwendung mit Wasserzählern reserviert.

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

6.3.12 Register: Register_to_clear

Ein nur einmal vorkommender 16-Bit-Binärwert im Bereich von 0 bis FFFFh; zum Auswählen des besonderen Registers, welches mit dem clear_Credit-Token gelöscht werden sollte.

Tabelle 23 – Auswahl der zu löschenden Register

Wert	Wirkung
0	Register des Guthabens für elektrische Energie
1	Von der STS-Association reserviert für Guthaben-Register für Wasser
2	Von der STS-Association reserviert für Guthaben-Register für Gas
3	Von der STS-Association reserviert für Guthaben-Register für Zeit
4	Von der STS-Association reserviert für Guthaben-Register für Währung
5 bis FFFEh	Für künftige Festlegungen reserviert
FFFFh	Löschen aller Guthaben-Register im Zähler

6.3.13 NKHO: New_Key_High_Order

Die höherwertigen 32 Bit des neuen Decoder_Key, der generiert wird (siehe 6.4.3) und die mit dem Token an den Zähler zu übertragen sind.

6.3.14 NKLO: New_Key_Low_Order

Die niederwertigen 32 Bit des neuen Decoder_Key, der generiert wird (siehe 6.4.4) und die mit dem Token an den Zähler zu übertragen sind.

6.3.15 KexpNoHO: Key_Expiry_Number_High_Order

Dies sind die höherwertigen 4 Bit der Key_Expiry_Number (siehe 6.1.9).

6.3.16 KexpNoLO: Key_Expiry_Number_Low_Order

Dies sind die niederwertigen 4 Bit der Key_Expiry_Number (siehe 6.1.9).

6.3.17 RO: Rollover_Key_Change

Wenn das Rollover_Key_Change-Bit auf Eins gesetzt ist, muss der Zähler einen überlappenden Schlüsselwechsel ausführen. Dieser Vorgang ist identisch mit dem eines normalen Schlüsselwechsels, außer dass der Token_Identifizier-Speicher im Zähler mit Tokenkennungen des Wertes 0 (Null) aufgefüllt wird.

6.4 TCDU_Generation-Funktionen

Zu ausführlichen Festlegungen für die TCDU siehe Normenreihe IEC 62055-5x, 5.1.

6.4.1 Transpositionen der Klassen-Bits

Diese Funktion wird von anderen TCDU_Generation-Funktionen angewendet (Siehe 6.4.2 bis 6.4.4). Hierbei werden die zwei Klassen-Bits in den Datenstrom aus 64 Bit eingefügt, um eine 66-Bit-Zahl entsprechend dem nachfolgend beschriebenen Verfahren zu erzeugen.

Die 64-Bit-Zahl hat ihr niederwertigstes Bit an der Bitposition 0 und ihr höchstwertigstes Bit an der Bitposition 63. Die binäre Zahlenkette aus 64 Bit wird verändert, um das nicht verschlüsselte Token Klasse

aufzunehmen (siehe nachfolgende Anmerkung). Der Wert des 2-Bit-Tokens Klasse wird so eingefügt, dass er die Bitpositionen 28 und 27 belegt. Die ursprünglichen Werte der Bitpositionen 28 und 27 werden an die Bitpositionen 65 und 64 verlagert. Das höherwertige Bit des Tokens Klasse belegt nun die Bitposition 28.

ANMERKUNG Weil das Token Klasse nicht verschlüsselt ist, könnte ein einheitliches Muster eingeführt werden, indem es an den Anfang oder das Ende der 64-Bit-Binärzeichenkette gestellt wird, wodurch aber einige der Sicherheitsaspekte der Verschlüsselungsmethodik verneint werden würden. Deshalb wird das Token Klasse in den Rumpf der Binärziffernfolge eingefügt.

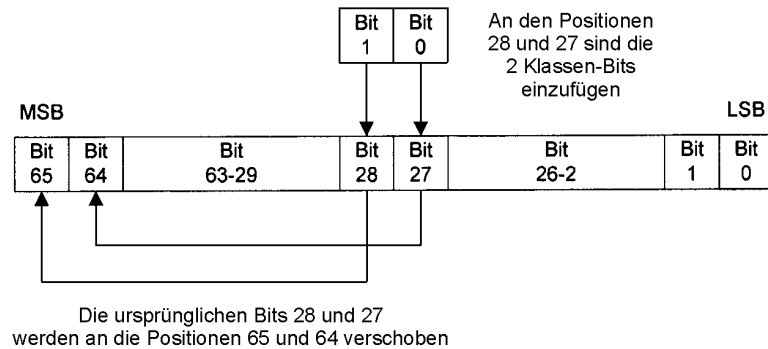


Bild 6 – Transposition der 2 Klassen-Bits

Beispiel: Einfügen der Zeichenfolge Klasse = 01 (binär)

Die 64-Bit-Binärzahl ist in Halbbytes angeordnet: (Bits 27 und 28 sind hervorgehoben)

0110 0101 0100 0011 0010 0001 0000 1001 1000 **01**11 0110 0101 0100 0011 0010 0001

Die Bits 28 und 27 werden an die Bitpositionen 65 und 64 kopiert, so dass eine 66-Bit-Zahl entsteht:

00 0110 0101 0100 0011 0010 0001 0000 1001 1000 0111 0110 0101 0100 0011 0010 0001

Die Bits 28 und 27 werden durch die 2 Klassen-Bits ersetzt:

00 0110 0101 0100 0011 0010 0001 0000 1001 1000 **11**11 0110 0101 0100 0011 0010 0001

6.4.2 Funktion TCDU_Generation für die Token Klasse 0, 1 und 2

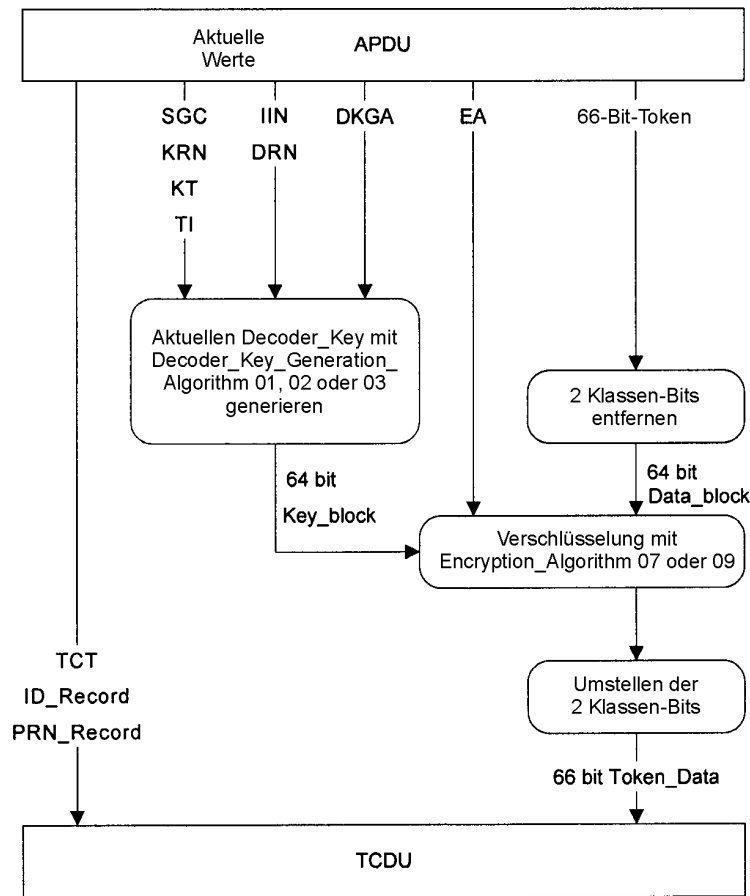


Bild 7 – Funktion TCDU_Generation für die Token Klasse 0, 1 und 2

Dies ist eine Transferfunktion von der APDU zur TCDU und gilt für alle Token der Klasse 0, Klasse 1 und Klasse 2, ausgenommen für die Token `set_1st_Section_Decoder_Key` und `set_2nd_Section_Decoder_Key` (siehe 6.4.3 und 6.4.4).

Zu den Definitionen der Datenelemente siehe IEC 62055-51, 6.1 und 5.1.

Im Folgenden wird die Transferfunktion für die Token Klasse 0 und Klasse 2 beschrieben:

- Die 2 Klassen-Bits werden aus dem 66-Bit-Token herausgenommen und führen zu einem 64-Bit-Ergebnis, welches anschließend dem `Encryption_Algorithm` als seine `Data_block`-Eingabe angeboten wird. Der spezifische anzuwendende `Encryption_Algorithm` richtet sich nach dem `EA`-Wert in der APDU.
- Die `Key_block`-Eingabe für den `Encryption_Algorithm` wird vom `Decoder_Key_Generation_Algorithm` erhalten, der den aktuellen `Decoder_Key` mit den aktuellen Werten von `SGC`, `KRN`, `KT`, `TI`, `IIN` und `DRN` aus der APDU wie angegeben generiert. Der spezifische anzuwendende `Decoder_Key_Generation_Algorithm` richtet sich nach dem Wert von `DKGA` in der APDU.
- Nach der Verschlüsselung werden die 2 Klassen-Bits nach dem in 6.4.1 festgelegten Verfahren wieder in die 64-Bit-Zahl eingefügt und führen zu einem 66-Bit-Ergebnis, das in das Feld `Token_Data` der TCDU nach IEC 62055-51, 5.1, übergeben wird.
- In ähnlicher Weise werden die Datenelemente `TCT`, `ID_Record` und `PRN_Record` aus der APDU wie angegeben an die TCDU in deren entsprechende Felder nach IEC 62055-51, 5.1, übertragen.

Die Transferfunktion für Token Klasse 1 ist identisch mit der `TCDU_Generation`-Funktion für Token Klasse 0 und Klasse 2, mit der Ausnahme, dass das Token nicht verschlüsselt wird. Die Funktion wird im Folgenden beschrieben:

- Die 2 Klassen-Bits werden aus dem 66-Bit-Token herausgenommen und nach dem in 6.4.1 festgelegten Verfahren umgesetzt und führen zu einem 66-Bit-Ergebnis, das an das Feld Token_Data der TCDU nach IEC 62055-51, 5.1, übergeben wird.
- In ähnlicher Weise werden die Datenelemente TCT, ID_Record und PRN_Record aus der APDU wie angegeben an die TCDU in deren entsprechende Felder nach IEC 62055-51, 5.1, übertragen.

6.4.3 Funktion TCDU_Generation für Token set_1st_Section_Decoder_Key

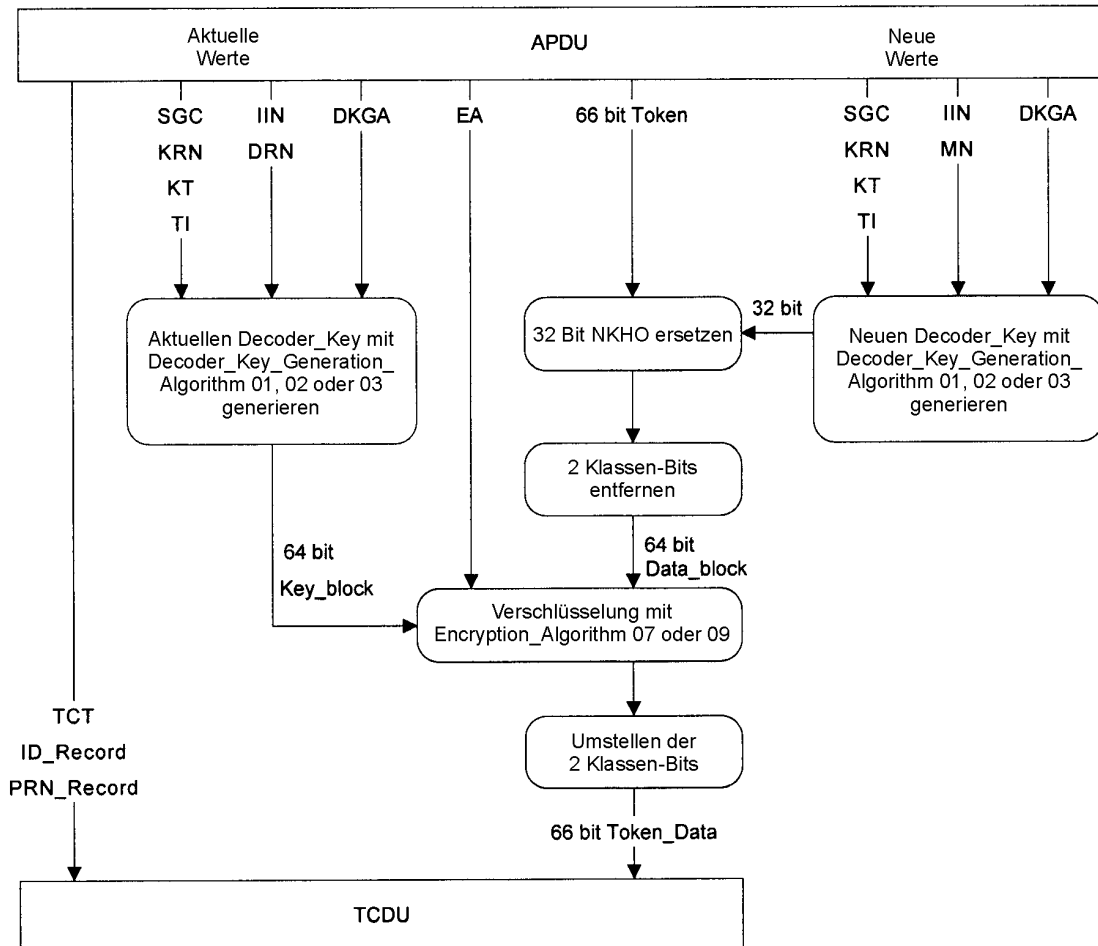


Bild 8 – Funktion TCDU_Generation für Token set_1st_Section_Decoder_Key

Dies ist die Transferfunktion von der APDU zur TCDU und ist nur für das Token set_1st_Section_Decoder_Key anwendbar.

Die Funktion TCDU_Generation set_1st_Section_Decoder_Key wird hier als getrennt von der Funktion TCDU_Generation set_2nd_Section_Decoder_Key dargestellt, jedoch können in der Praxis die beiden in eine gemischt werden, um Verarbeitungsressourcen zu sparen und weil es zwckmäßig ist. In einem derartigen Fall braucht die Generierung des neuen Decoder_Key beispielsweise nur einmal zu erfolgen, obwohl das Endergebnis immer noch das gleiche ist. Dadurch werden immer zwei getrennte TCDU-Instanzen erzeugt: eine für das Token set_1st_Section_Decoder_Key und ein zweites Token set_2nd_Section_Decoder_Key.

Es ist zu beachten, dass die APDU zwei Datengruppen für den PAN_Block und CONTROL_Block im Decoder_Key_Generation_Algorithm bereitzustellen hat: eine Gruppe mit den neuen Daten für den neuen Decoder_Key und eine zweite Gruppe mit den aktuellen Daten für den aktuellen Decoder_Key. Der DKGA-Wert ist für beide Gruppen derselbe.

– Entwurf –

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

Zu den Festlegungen der Datenelemente siehe IEC 62055-51, 6.1 und 5.1.

Die Transferfunktion wird wie folgt beschrieben:

- Der neue Decoder_Key wird mit den neuen Werten von SGC, KRN, KT, TI, IIN und DRN generiert. Der spezifische anzuwendende Decoder_Generation_Key_Algorithm richtet sich nach dem Wert von DKGA in der APDU.
- Die sich ergebenden höherwertigen 32 Bit des neuen Wertes des Decoder_Key werden anschließend dazu verwendet, das NKHO-Feld des Token set_1st_Section_Decoder_Key (siehe 6.2.6) zu ersetzen, wie es von der APDU bereitgestellt wird.
- Die 2 Klassen-Bits werden aus dem 66-Bit-Token entfernt und führen zu einem 64-Bit-Ergebnis, welches anschließend dem Encryption_Algorithm als seine Data_block-Eingabe angeboten wird. Der spezifische anzuwendende Encryption_Algorithm richtet sich nach dem EA-Wert in der APDU.
- Die Key_block-Eingabe für den Encryption_Algorithm wird vom Decoder_Key_Generation_Algorithm erhalten, der den aktuellen Decoder_Key mit den aktuellen Werten von SGC, KRN, KT, TI, IIN und DRN aus der APDU wie angegeben generiert. Der spezifische anzuwendende Decoder_Key_Generation_Algorithm richtet sich nach dem Wert von DKGA in der APDU.
- Nach der Verschlüsselung werden die 2 Klassen-Bits nach dem in 6.4.1 festgelegten Verfahren wieder in die 64-Bit-Zahl eingefügt und führen zu einem 66-Bit-Ergebnis, das in das Feld Token_Data der TCDU nach IEC 62055-51, 5.1, übergeben wird.
- In ähnlicher Weise werden die Datenelemente TCT, ID_Record und PRN_Record aus der APDU wie angegeben an die TCDU in deren entsprechende Felder nach IEC 62055-51, 5.1, übertragen.

6.4.4 Funktion TCDU_Generation für Token set_2nd_Section_Decoder_Key

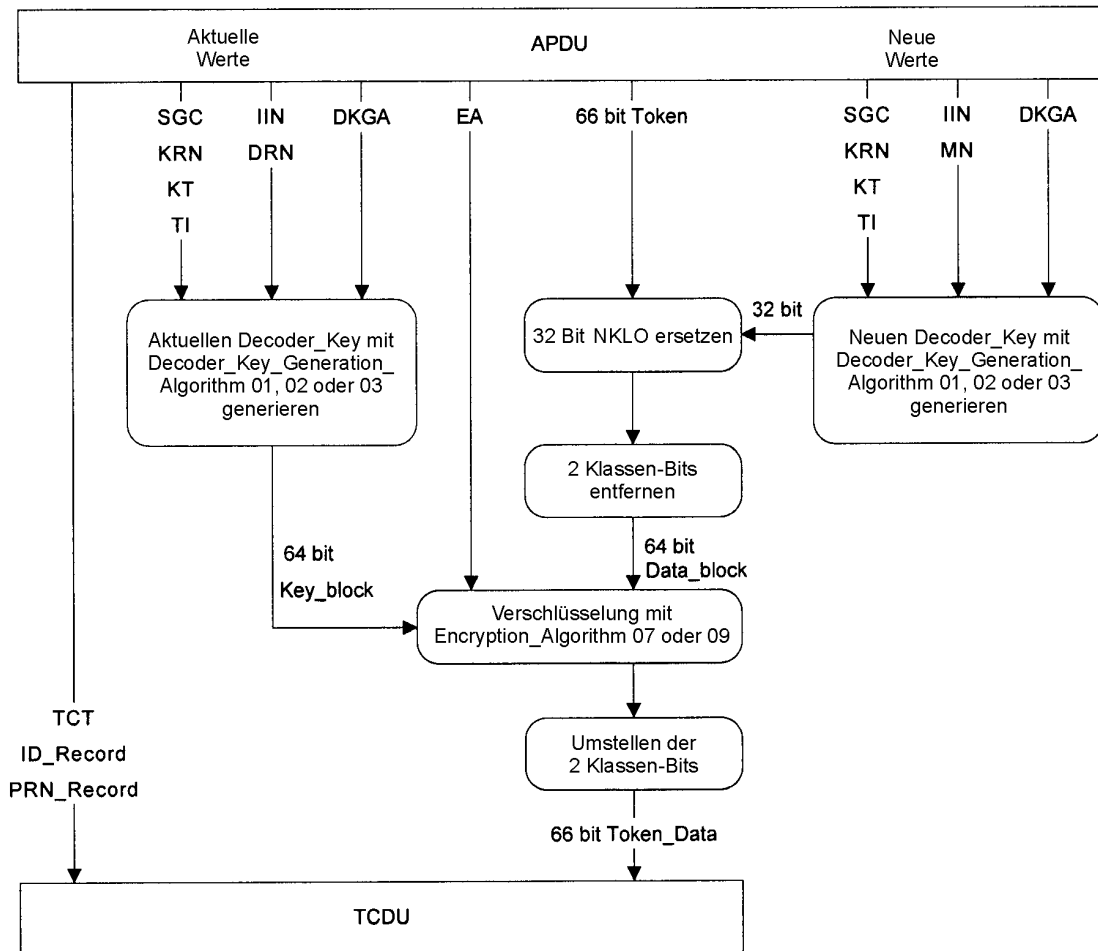


Bild 9 – Funktion TCDU_Generation für Token set_2nd_Section_Decoder_Key

Dies ist die Transferfunktion von der APDU zur TCDU und ist nur für das Token set_2nd_Section_Decoder_Key anwendbar.

Die Funktion TCDU_Generation set_2nd_Section_Decoder_Key wird hier als getrennt von der Funktion TCDU_Generation set_1st_Section_Decoder_Key dargestellt, jedoch können in der Praxis die beiden in eine gemischt werden, um Verarbeitungsressourcen zu sparen und weil es zweckmäßig ist. In einem derartigen Fall braucht die Generierung des neuen Decoder_Key beispielsweise nur einmal zu erfolgen, obwohl das Endergebnis immer noch das gleiche ist. Dadurch werden immer zwei getrennte TCDU-Instanzen erzeugt: eine für das Token set_1st_Section_Decoder_Key und eine zweite für das Token set_2nd_Section_Decoder_Key.

Es ist zu beachten, dass die APDU zwei Datengruppen für den PAN_Block und CONTROL_Block im Decoder_Key_Generation_Algorithm bereitzustellen hat: eine Gruppe mit den neuen Daten für den neuen Decoder_Key und eine zweite Gruppe mit den aktuellen Daten für den aktuellen Decoder_Key. Der DKGA-Wert ist für beide Gruppen derselbe.

Zu den Festlegungen der Datenelemente siehe IEC 62055-51, 6.1 und 5.1.

Die Transferfunktion wird wie folgt beschrieben:

- Der neue Decoder_Key wird mit den neuen Werten von SGC, KRN, KT, TI, IIN und DRN generiert. Der spezifische anzuwendende Decoder_Generation_Key_Algorithm richtet sich nach dem Wert von DKGA in der APDU.

E DIN IEC 62055-41 (VDE 0418-5-41):2005-06

- Die sich ergebenden niederwertigen 32 Bit des neuen Wertes des Decoder_Key werden anschließend dazu verwendet, das NKLO-Feld des Token set_2nd_Section_Decoder_Key (siehe 6.2.7) zu ersetzen, wie es von der APDU bereitgestellt wird.
- Die 2 Klassen-Bits werden aus dem 66-Bit-Token entfernt und führen zu einem 64-Bit-Ergebnis, welches anschließend dem Encryption_Algorithm als seine Data_block-Eingabe angeboten wird. Der spezifische anzuwendende Encryption_Algorithm richtet sich nach dem EA-Wert in der APDU.
- Die Key_block-Eingabe für den Encryption_Algorithm wird vom Decoder_Key_Generation_Algorithm erhalten, der den aktuellen Decoder_Key mit den aktuellen Werten von SGC, KRN, KT, TI, IIN und DRN aus der APDU wie angegeben generiert. Der spezifische anzuwendende Decoder_Key_Generation_Algorithm richtet sich nach dem Wert von DKGa in der APDU.
- Nach der Verschlüsselung werden die 2 Klassen-Bits nach dem in 6.4.1 festgelegten Verfahren wieder in die 64-Bit-Zahl eingefügt und führen zu einem 66-Bit-Ergebnis, das in das Feld Token_Data der TCDU nach IEC 62055-51, 5.1, übergeben wird.
- In ähnlicher Weise werden die Datenelemente TCT, ID_Record und PRN_Record aus der APDU wie angegeben an die TCDU in deren entsprechende Felder nach IEC 62055-51, 5.1, übertragen.

6.5 Sicherheitsfunktionen

Mit Ausnahme der Schlüsselwerte Typ 0 dürfen die Werte für Vending_Key und Decoder_Key nur von einer Einrichtung generiert werden, die für die Tokengenerierung verantwortlich ist, wie einem Kassenplatz, der als STS-konform zertifiziert ist und der von einem STS-zertifizierten Key_Management_System (siehe Abschnitt 10) abhängig ist. In diesem Abschnitt 6.5 werden die Verfahren für die Schlüsselgenerierung beschrieben, die von derartigen Einrichtungen angewendet werden und gilt für die Hersteller derartiger Einrichtungen.

6.5.1 Schlüsselmerkmale und Schlüsseländerungen

Mit Ausnahme der DITK-Werte Typ 0, dürfen STS-Schlüsselwerte in einen Zähler nur von einer Einrichtung eingegeben oder verändert werden, die für die Schlüsselverwaltung verantwortlich ist, wie einem Kassenplatz, der als STS-konform zertifiziert ist und der von einer STS-Schlüsselverwaltung abhängig ist. In diesem Abschnitt wird das Verfahren für die STS-Schlüsselveränderung beschrieben, dass zwischen derartigen Einrichtungen und Zählern angewendet wird und gilt für die Hersteller derartiger Einrichtungen.

Eine STS-Schlüsseländerung liefert den Mechanismus für die Änderung des in einem Decoder vorhandenen Decoder_Key von seinem aktuellen Wert auf einen neuen Wert. Dieser Prozess kann von mehreren Ereignissen oder Umständen ausgelöst werden, einschließlich folgender:

- ein neuer oder reparierter Zähler, der einen DITK-Wert des Herstellers enthält, muss vor dem Verlassen der Produktionsstätte oder der Werkstatt verändert werden, damit er den entsprechenden Vorgabewert des Herstellers (DDTK) oder den Decoder_Key (DUTK oder DCTK) des Versorgungsunternehmens enthält, abhängig von der Supply_Group, der der Zähler zugeordnet wird;
- der Vending_Key einer Supply_Group ist entweder abgelaufen oder gefährdet, und wird durch eine neue Überarbeitung des Vending_Key ersetzt und als ein Ergebnis muss jeder Decoder_Key innerhalb einer Supply_Group von seinem aktuellen Wert des Decoder_Key auf den Wert des Decoder_Key geändert werden, der dem neuen Wert des Vending_Key entspricht;
- ein Zähler wird von einer Supply_Group in eine andere Supply_Group wieder zugeordnet und im Ergebnis dessen muss sein Decoder_Key von seinem aktuellen Wert, der vom Vending_Key der vorherigen Supply_Group generiert wurde, auf einen neuen Wert geändert werden, der von dessen Vending_Key der Supply_Group generiert wird; oder
- der Tariff_Index für einen Zähler wurde verändert und folglich muss dessen Decoder_Key von seinem aktuellen Wert (der dem vorherigen Tariff_Index entspricht) auf den neuen Wert verändert werden (der dem neuen Tariff_Index entspricht).

Die Tokenpaare set_1st_Section_Decoder_Key und der set_2nd_Section_Decoder_Key bewirken eine STS-Schlüsseländerung. Dieses zählerspezifische Verwaltungstokenpaar überträgt die folgenden Informationen vom Kassenplatz an den Zähler, verschlüsselt nach dem aktuellen Decoder_Key:

- den Wert des neuen Decoder_Key;