

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ...

Inhalt

	Seite
Vorwort.....	8
Einleitung	11
1 Anwendungsbereich	13
2 Normative Verweisungen	13
3 Begriffe und Abkürzungen	14
3.1 Begriffe	14
3.2 Abkürzungen	15
3.3 Notation und Terminologie	19
4 Numerierungsvereinbarungen	19
5 Referenzmodell für die Standardtransferspezifikation	20
5.1 Funktionales Referenz-Blockdiagramm für Inkassozähler	20
5.2 Referenzmodell für das STS-Protokoll	21
5.3 Datenfluss vom POSApplicationProcess zum TokenCarrier	22
5.4 Datenfluss vom TokenCarrier zum MeterApplicationProcess	23
5.5 MeterFunctionObjects/Begleitspezifikationen	24
5.6 ISO-Bezugsnummern für Transaktionen	24
6 POSToTokenCarrierInterface: Protokoll der Anwendungsschicht	25
6.1 APDU: Dateneinheit der Anwendungsschicht	25
6.2 Token	31
6.3 Tokendatenelemente	34
6.4 TCDUGeneration-Funktionen	42
6.5 Sicherheitsfunktionen	47
7 TokenCarrierToMeterInterface: Protokoll der Anwendungsschicht	64
7.1 APDU: ApplicationProtocolDataUnit	64
7.2 APDUExtraction-Funktionen	67
7.3 Sicherheitsfunktionen	70
8 Anforderungen an den MeterApplicationProcess	77
8.1 Allgemeine Anforderungen	77
8.2 Tokenannahme/Tokenzurückweisung	77
8.3 Anzeiger und Aufschriften an der Anzeige	78
8.4 Token TransferCredit	79
8.5 Token InitiateMeterTest/Display	79
8.6 Token SetMaximumPowerLimit	80
8.7 Token ClearCredit	80

	Seite
8.8 Token SetTariffRate	80
8.9 Token Set1stSectionDecoderKey	80
8.10 Token Set2ndSectionDecoderKey	80
8.11 Token ClearTamperCondition	81
8.12 Token SetMaximumPhasePowerUnbalanceLimit.....	81
8.13 SetWaterMeterFactor	81
8.14 Klasse 2: Reserviert für STS-Token.....	81
8.15 Klasse 2: Reserviert für firmenspezifische Token.....	81
8.16 Klasse 3: Reserviert für STS-Token.....	81
9 KMS: KeyManagementSystem – Übergeordnete Anforderungen	81
10 Aufrechterhaltung von STS-Entitäten und zugehörigen Diensten	82
10.1 Allgemeines	82
10.2 Ausführung	84
10.3 Normung.....	86
Anhang A (informativ) Leitfaden für ein KeyManagementSystem (KMS)	90
Anhang B (informativ) Entitäten und Kennungen in einem STS-konformen System.....	93
Anhang C (informativ) Regeln für die Praxis für die Realisierung STS-konformer Systeme	97
Literaturhinweise	112
Bild 1 – Funktionales Blockschaltbild eines einteiligen Inkassozählers	20
Bild 2 – Verdichtetes 2-Schichten-OSI-Referenzmodell für die STS	21
Bild 3 – Datenfluss vom POSApplicationProcess zum TokenCarrier	22
Bild 4 – Datenfluss vom TokenCarrier zum MeterApplicationProcess.....	23
Bild 5 – Aufbau der ISO-Bezugsnummern für Transaktionen	24
Bild 6 – Transposition der 2 Klassen-Bits.....	42
Bild 7 – Funktion TCDUGeneration für die Token Klasse 0, 1 und 2.....	43
Bild 8 – Funktion TCDUGeneration für Token Set1stSectionDecoderKey	44
Bild 9 – Funktion TCDUGeneration für Token Set2ndSectionDecoderKey	46
Bild 10 – Änderungen des DecoderKey – Zustandsdiagramm	52
Bild 11 – DecoderKeyGenerationAlgorithm01.....	57
Bild 12 – DecoderKeyGenerationAlgorithm02.....	58
Bild 13 – DecoderKeyGenerationAlgorithm03.....	59
Bild 14 – STA: EncryptionAlgorithm07	60
Bild 15 – Ersetzungsprozess bei der STA-Verschlüsselung.....	61
Bild 16 – Permutationsprozess bei der STA-Verschlüsselung.....	62
Bild 17 – Rotationsprozess für des DecoderKey bei der STA-Verschlüsselung.....	62
Bild 18 – Arbeitsbeispiel für ein TransferCredit-Token mit Anwendung der STA	63
Bild 19 – DEA: EncryptionAlgorithm09.....	64

	Seite
Bild 20 – APDUExtraction-Funktion.....	67
Bild 21 – Auskoppeln der 2 Bits für die Klasse.....	68
Bild 22 – STA DecryptionAlgorithm07.....	71
Bild 23 – Permutationsprozess bei der STA-Entschlüsselung.....	72
Bild 24 – Ersetzungsprozess bei der STA-Entschlüsselung.....	73
Bild 25 – Rotationsprozess für den DecoderKey bei der STA-Entschlüsselung.....	74
Bild 26 – Arbeitsbeispiel für die Entschlüsselung eines TransferCredit-Tokens mit Anwendung der STA.....	74
Bild 27 – DEA: DecryptionAlgorithm09.....	75
Bild A.1 – KeyManagementSystem und interaktive Beziehungen zwischen den Entitäten.....	90
Bild B.1 – In einem STS-System verteilte Entitäten und Kennungen.....	93
Bild C.1 – Übersicht über das System.....	107
Tabelle 1 – Datenelemente in der APDU.....	25
Tabelle 2 – Datenelemente im IDRecord.....	25
Tabelle 3 – Datenelemente in der MeterPAN.....	26
Tabelle 4 – Datenelemente in der IAIN / DRN.....	26
Tabelle 5 – Typen von Tokenträgern.....	27
Tabelle 6 – DKGA-Kennzahlen.....	28
Tabelle 7 – EA-Kennzahlen.....	28
Tabelle 8 – SGC-Arten und Schlüsselarten.....	29
Tabelle 9 – DOE-Kodierungen für das Jahr.....	30
Tabelle 10 – DOE-Kodierungen für den Monat.....	30
Tabelle 11 – Festlegung des Formates für Token.....	31
Tabelle 12 – In Token angewendete Datenelemente.....	34
Tabelle 13 – Tokenklassen.....	35
Tabelle 14 – Unterklassen von Token.....	35
Tabelle 15 – Berechnungsbeispiele für TID.....	37
Tabelle 16 – Einheiten für elektrische Energie.....	38
Tabelle 17 – Einheiten für andere Anwendungen.....	38
Tabelle 18 – Bitzuweisungen für TransferAmount.....	38
Tabelle 19 – Maximaler Fehler durch Rundung.....	39
Tabelle 20 – Beispiele für Werte des TransferAmount.....	39
Tabelle 21 – Beispiel für eine CRC-Berechnung.....	40
Tabelle 22 – Zulässige Werte des Steuerfeldes.....	40
Tabelle 23 – Auswahl der zu löschenden Register.....	41
Tabelle 24 – Klassifizierung von Verkaufsschlüsseln.....	48
Tabelle 25 – Klassifizierung der Decoderschlüssel.....	49

	Seite
Tabelle 26 – Zulässige Beziehungen zwischen den Decoderschlüsseltypen.....	53
Tabelle 27 – Definition des PANBlock.....	55
Tabelle 28 – Datenelemente im PANBlock	55
Tabelle 29 – Definition des CONTROLBlock	56
Tabelle 30 – Datenelemente im CONTROLBlock.....	56
Tabelle 31 – Bereich der anwendbaren Decoderbezugsnummern.....	56
Tabelle 32 – Verzeichnis der anwendbaren Versorgungsgruppencodes	57
Tabelle 33 – Ersetzungstabelle (Beispiel).....	61
Tabelle 34 – Permutationstabelle (Beispiel).....	62
Tabelle 35 – Datenelemente in der APDU	64
Tabelle 36 – Mögliche Werte für das AuthenticationResult	65
Tabelle 37 – Mögliche Werte für das ValidationResult	65
Tabelle 38 – Mögliche Werte für das TokenResult	66
Tabelle 39 – Im DKR gespeicherte Werte.....	71
Tabelle 40 – Permutationstabelle (Beispiel).....	72
Tabelle 41 – Ersetzungstabelle (Beispiel).....	73
Tabelle 42 – Entitäten und Dienste, für die die Aufrechterhaltung erforderlich ist.....	82
Tabelle A.1 – Im KMS-Prozess beteiligte Entitäten	90
Tabelle A.2 – Inkassozähler und DecoderKey umgebende Prozesse	91
Tabelle A.3 – Das Verschlüsselungsmodul umgebende Prozesse.....	91
Tabelle A.4 – SGC und VendingKey umgebende Prozesse.....	92
Tabelle B.1 – In einem STS-konformen System verteilte Entitäten (1 von 2).....	94
Tabelle B.1 – In einem STS-konformen System verteilte Entitäten (2 von 2).....	95
Tabelle B.2 – Kennungen, die mit den Entitäten in einem STS-konformen System in Verbindung stehen (1 von 2)	95
Tabelle B.2 – Kennungen, die mit den Entitäten in einem STS-konformen System in Verbindung stehen (2 von 2)	96
Tabelle C.1 – Mit einer SGC verbundene Datenelemente	98
Tabelle C.2 – Mit dem CryptographicModule verbundene Datenelemente	99
Tabelle C.3 – Bei Lieferaufträgen oder Lastenheften zu beachtende Einzelheiten (1 von 4).....	102
Tabelle C.3 – Bei Lieferaufträgen oder Lastenheften zu beachtende Einzelheiten (2 von 4).....	103
Tabelle C.3 – Bei Lieferaufträgen oder Lastenheften zu beachtende Einzelheiten (3 von 4).....	104
Tabelle C.3 – Bei Lieferaufträgen oder Lastenheften zu beachtende Einzelheiten (4 von 4).....	105