

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ...

Inhalt

	Seite
Nationales Vorwort.....	9
Einleitung	10
1 Anwendungsbereich	11
2 Normative Verweisungen	11
3 Begriffe und Abkürzungen	12
3.1 Begriffe	12
3.1.1 Allgemeines	12
3.2 Abkürzungen	13
4 Betroffene Kommunikationsumgebungen	14
5 Verwendung der Kommunikationsschicht für dieses Profil	15
5.1 Informationen zur Verwendung der Norm zur Festlegung der unteren Schichten.....	15
5.2 Die Struktur des Kommunikationsprofils	15
5.3 Untere Schichten und ihre Verwendung.....	16
5.3.1 Übersicht	16
5.3.2 Bitübertragungsschicht.....	16
5.3.3 Sicherungsschicht	16
5.3.4 Vermittlungsschicht	16
5.3.5 Transportschicht.....	17
5.4 Dienstzuordnung und Adaptionsschicht.....	17
5.4.1 Übersicht	17
5.4.2 Adaptionsschicht	17
5.5 Registrierungs- und Verbindungsverwaltung	22
5.5.1 Automatisierte Topologieverwaltung	22
5.5.2 Header der ADD-Nachricht	22
5.5.3 Anforderung der „ATM Query ID“	23
5.5.4 Antwort auf „ATM Query ID“	23
5.5.5 ATM Respond to query	24
5.5.6 Antwort auf „ATM Respond to Query“	24
6 Identifizierung und Adressierungsschemata	24
7 Besondere Überlegungen zu den Diensten der Anwendungsschicht.....	25
7.1 Übersicht	25
7.2 Erstellen und Freigeben von Anwendungsassoziationen: ACSE-Dienste	25
7.2.1 Aufbau von Anwendungsassoziationen	25
7.2.2 Freigabe von Anwendungsassoziationen	26
7.2.3 Parameter der Dienste COSEM-OPEN und COSEM-RELEASE	26

	Seite
7.3	xDLMS-Dienste 27
7.4	Sicherheitsmechanismen 27
7.4.1	DLMS/COSEM-Sicherheit..... 27
7.4.2	Sicherheit der Adaptionsschicht..... 27
7.4.3	Sicherheit der unteren Schichten..... 27
7.5	Übertragen von langen Anwendungsnachrichten 27
7.6	Überlegungen zu Medienzugriff, Bandbreite und Zeitverhalten..... 28
7.7	Sonstige Überlegungen..... 28
8	Kommunikationskonfiguration und Verwaltung 28
9	COSEM-Anwendungsprozess 28
10	Zusätzliche Überlegungen zur Verwendung dieses Profils 28
Anhang A (informativ) Beispiele 29	
A.1 29
Anhang B (normativ) Schnittstellenklassen..... 30	
B.1	Schnittstellenklassen..... 30
B.1.1	IEC 14908 Identification 30
B.1.2	IEC 14908 Physical Setup 30
B.1.3	IEC 14908 Physical status 31
B.1.4	IEC 14908 Diagnostic 32
B.2	Verbindung mit OBIS 34
Anhang C (normativ) Überlegungen zur Leistung 35	
C.1	Allgemeines..... 35
C.2	Vorgeschriebene DLMS/COSEM-Elemente 35
C.2.1	Übersicht 35
C.2.2	Logisches Gerät 35
C.2.3	Client 35
C.3	Anwendungsassoziationen 35
C.4	Kurznamendefinition 36
C.5	Überlegungen zum Client..... 38
C.6	Zugriff auf COSEM-Objekte 39
Anhang D (normativ) Sicherheits-Suite OSGP-AES-128-PSK 40	
D.1	Einleitung..... 40
D.2	Hintergrund..... 41
D.2.1	Übersicht 41
D.2.2	Systemannahmen 41
D.2.3	Bedrohungsmodell 41
D.2.4	Entwicklungsziele 42
D.2.5	Anregung..... 42
D.3	Begriffe und Notation 43

	Seite
D.3.1 Begriffe	43
D.3.2 Notation	44
D.3.3 Weitere Konventionen:	44
D.4 Verschlüsselungselemente	44
D.4.1 Allgemeines	44
D.4.2 CMAC	45
D.4.3 CCM.....	45
D.5 Verschlüsselungsfunktionen.....	46
D.5.1 Übersicht	46
D.5.2 OSGP_KDF: Funktion zur Schlüsselableitung	46
D.5.3 OSGP_MAC: Nachrichtenauthentifizierungscode-Funktion.....	46
D.5.4 OSGP_MAC_VERIFY: Funktion zur Überprüfung des Nachrichtenauthentifizierungscodes	47
D.5.5 OSGP_AE/OSGP_AD: Funktion zur authentifizierten Verschlüsselung/Entschlüsselung	48
D.5.5.1 Übersicht	48
D.5.5.2 OSGP_AE	48
D.5.5.3 OSGP_AD	48
D.5.6 OSGP_CSPRNG: Kryptografisch starker Pseudozufallszahlengenerator	49
D.6 Schlüssel	50
D.7 Initialisierung des sicheren Kanals	52
D.7.1 Übersicht	52
D.7.2 Zustand des sicheren Kanals (CryptoContext)	52
D.7.3 Ablauf.....	53
D.7.4 Aushandeln der Sicherheits-Suite	58
D.7.5 Inbetriebnahme der Zählerendgeräte.....	58
D.7.6 Fehlerbehandlung und Intrusion Detection	58
D.7.7 Nachrichten	59
D.7.7.1 Übersicht	59
D.7.7.2 ChallengeRequest.....	59
D.7.7.3 ChallengeResponse	59
D.7.7.4 CommissionRequest	60
D.7.7.5 CommissionResponse	60
D.8 Kommunikation über einen sicheren Kanal.....	61
D.8.1 Allgemeines	61
D.8.2 Allgemeiner Prozess.....	62
D.8.2.1 Übersicht	62
D.8.2.2 Schützen und Senden einer Nachricht.....	62
D.8.2.3 Verarbeiten einer geschützten Nachricht	62
D.8.3 Unicast-Kommunikation.....	63
D.8.3.1 Übersicht	63

	Seite
D.8.3.2 Aufbau der Nachrichten	63
D.8.3.3 Erstellen der Unicast-Nonce	64
D.8.3.4 Erstellen der zugeordneten Unicast-Daten	65
D.8.3.5 Schutz vor erneuten Übertragungen	65
D.8.3.6 Ablauf	65
D.8.3.7 Fehlerbehandlung und Intrusion Detection	67
D.8.4 Broadcast-Kommunikation	67
D.8.4.1 Übersicht	67
D.8.4.2 Aufbau der Nachrichten	68
D.8.4.3 Erstellen der Broadcast-Nonce	68
D.8.4.4 Erstellen der zugeordneten Broadcast-Daten	68
D.8.4.5 Vermeidung von erneuten Übertragungen	69
D.8.4.6 Ablauf	69
D.9 Herunterladen der Firmware	70
D.10 Schlüsselverwaltung	70
D.10.1 Aktualisierung von Zähler-eindeutigen Kurzzeitschlüsseln	70
D.10.2 Aktualisierung von Domain-eindeutigen Kurzzeitschlüsseln	70
D.10.3 UpdateDomainKeysRequest	71
D.10.4 UpdateDomainKeysResponse	71
D.11 Aktualisierung von Zähler-eindeutigen Langzeitschlüsseln	72
D.11.1 Allgemeines	72
D.11.2 Gültigkeitsdauer der Schlüssel	72
D.12 Fehlermeldungen	72
D.12.1 Übersicht	72
D.12.2 AuthenticationFailure	72
D.12.3 SequenceError	73
D.13 Überlegungen zur Sicherheit	73
D.13.1 Zugrunde liegende Überlegungen	73
D.13.1.1 Auswahl der Verschlüsselungselemente	73
D.13.1.2 Aufbau des Ablaufs der Initialisierung eines sicheren Kanals	75
D.13.1.3 Auswahl der Länge des CCM-MAC	75
D.13.2 Empfehlungen und Hilfestellung für Implementierer	76
D.13.2.1 Übersicht	76
D.13.2.2 Gültigkeitsdauer von Kurzzeitschlüsseln	76
D.13.3 Fragen und Antworten	77
Anhang E (normativ) Weiterleitungsdaten	79
E.1 Übersicht	79
E.2 Einheiten	79
E.2.1 Proxy-Ziel	79

	Seite
E.2.2 Proxy-Quelle	79
E.2.3 Proxy-Repeater	79
E.2.4 Proxy-Agent.....	79
E.3 Festlegung des Protokolls	79
E.4 Multicasting (Gruppenaufruf).....	81
E.5 Adressierung	81
E.6 Format des Aufwärtsstrecken-Datenblocks.....	81
E.6.1 Übersicht	81
E.6.2 Proxy-Anforderungs-Datenblock	82
E.6.2.1 ProxyHeader.....	82
E.6.2.2 Proxy-Adresse	82
E.6.2.3 Proxy-Steuerung.....	83
E.6.2.4 ProxyTrailer	83
E.7 Format des Abwärtsstrecken-Datenblocks.....	86
E.7.1 Übersicht	86
E.7.2 Acknowledged Service Success	86
E.7.3 Repeating Failure	86
E.7.4 Authentication Failure.....	86
Bilder	
Bild 1 – Funktionale Referenzarchitektur.....	14
Bild 2 – Struktur des Kommunikationsprofils	15
Bild 3 – Struktur einer PDU der Adaptionsschicht.....	18
Bild 4 – Struktur der geschützten Adaptionsschicht-PDU	19
Bild 5 – Zusammenfassung der Dienste der Adaptionsschicht	19
Bild D.1 – Diagramm der Schlüsselhierarchie	50
Bild D.2 – Einrichtung des sicheren Kanals.....	53
Bild D.3 – Challenge-Anforderung (ChallengeRequest).....	54
Bild D.4 – Challenge-Antwort (ChallengeResponse).....	54
Bild D.5 – Inbetriebnahmeanforderung (CommissionRequest).....	55
Bild D.6 – Inbetriebnahmeantwort (CommissionResponse).....	56
Bild D.7 – Einrichtung eines CryptoContext	61
Bild D.8 – Mechanismus der authentifizierten Verschlüsselung.....	62
Bild D.9 – Authentifizierte Entschlüsselung	63
Bild E.1 – Austausch einer unbestätigten Nachricht.....	80
Bild E.2 – Anforderungs-/Antwortnachricht.....	80
Bild E.3 – Fehler bei Übertragung der Anforderung	80
Bild E.4 – Fehler bei Übertragung der Antwort.....	81
Bild E.5 – Proxy-Agent-PDU	81
Bild E.6 – Proxy-Repeater-PDU	81

	Seite
Bild E.7 – Normaler ProxyTrailer	83
Bild E.8 – ProxyTrailer mit alternativem Schlüssel.....	84
Bild E.9 – Struktur des SICB-Feldes	84
Bild E.10 – Format mit alternativem Schlüssel.....	85
Bild E.11 – ProxySubnetNode-Adresse (Typ 1).....	85
Bild E.12 – ProxyBroadcast-Adresse (Typ 3).....	85
Bild E.13 – Kompakte ProxySubnetNode-Adresse (Typ 5 und 7).....	85
Bild E.14 – ProxyUniqueNodeId-Adresse (Typ 6).....	85
 Tabellen	
Tabelle 1 – Steuerfeld	18
Tabelle 2 – Header-Struktur der ATM-Nachricht.....	23
Tabelle 3 – Struktur der ATM-Anforderung	23
Tabelle 4 – Struktur der ATM-Antwort.....	23
Tabelle 5 – Struktur von „ATM Respond to Query“	24
Tabelle 6 – Struktur der Antwort auf „ATM Respond to Query“	24
Tabelle 7 – Client- und Server-SAPs	25
Tabelle 8 – Anwendungsassoziationen und Datenaustausch im OSGP-DLMS/COSEM-Profil	26
Tabelle C.1 – Standardkurznamen.....	36
Tabelle C.2 – Tabellenkategorie	36
Tabelle C.3 – Standardtabellen	37
Tabelle C.4 – Parameter für voraufgebaute Assoziationen	39
Tabelle D. 1 – Sicherheitsschichten	40
Tabelle D.2 – Schlüsseltyp und Geltungsbereich.....	51
Tabelle D.3 – ChallengeRequest	59
Tabelle D.4 – ChallengeResponse.....	59
Tabelle D.5 – CommissionRequest.....	60
Tabelle D.6 – Struktur der CommissionResponse	61
Tabelle D.7 – Anforderungsnachricht.....	64
Tabelle D.8 – Struktur der Antwortnachricht	64
Tabelle D.9 – Erstellung der Nonce	64
Tabelle D.10 – Erstellung der zugeordneten Daten	65
Tabelle D.11 – Broadcast-Nachricht	68
Tabelle D.12 – Broadcast-Nonce	68
Tabelle D.13 – Zugeordnete Daten von Broadcast-Nachrichten	68
Tabelle D.14 – UpdateDomainKeysRequest.....	71
Tabelle D.15 – UpdateDomainKeysResponse	72
Tabelle D.16 – AuthenticationFailure	72
Tabelle D.17 – SequenceError	73
Tabelle D.18 – Beispiele für Risk	77

	Seite
Tabelle E.1 – ProxyHeader-Format	82
Tabelle E.2 – Format der Proxy-Adresse	83
Tabelle E.3 – Format einheitlicher Proxy-Adressen	83
Tabelle E.4 – Format der ProxyTx-Steuerung	83
Tabelle E.5 – Adresstypwerte	84
Tabelle E.6 – „Mode“-Typen	84
Tabelle E.7 – Fehlgeschlagene Weiterleitung	86
Tabelle E.8 – Code für fehlgeschlagene Authentifizierung	86