

**Alarmanlagen –
Teil 11-5: Elektronische Zutrittskontrollanlagen - Open Supervised Device Protocol
(OSDP)**

Inhalt

	Seite
Einleitung	8
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe und Abkürzungen	9
3.1 Begriffe	9
3.2 Abkürzungen	10
4 Überblick	10
4.1 Allgemeines	10
5 Kommunikationseinstellungen	11
5.1 Physikalische Schnittstelle	11
5.2 Signalgebung	11
5.3 Zeichenverschlüsselung	11
5.4 Kanalzugang	11
5.5 Datenverschlüsselung mit mehreren Bytes	12
5.6 Begrenzung der Paketgröße	12
5.7 Zeitanforderungen	12
5.8 Nachrichtensynchronisation	13
5.9 Paketformat	13
5.10 Mehrteilige Nachrichten	16
5.10.1 Regeln für die Verwendung mehrteiliger Nachrichten	16
5.11 Handhabung von Smartcards	17
6 Befehle	17
6.1 Abfrageanforderung (osdp_POLL)	18
6.2 Anforderung des ID-Berichts (osdp_ID)	18
6.3 Anforderung der Funktionen des Peripheriegeräts (osdp_CAP)	19
6.4 Anforderung des lokalen Statusberichts (osdp_LSTAT)	19
6.5 Anforderung des Eingangstatusberichts (osdp_ISTAT)	19
6.6 Anforderung des Ausgangsstatusberichts (osdp_OSTAT)	19
6.7 Anforderung des Statusberichts des Lesegeräts (osdp_RSTAT)	20
6.8 Befehl zur Ausgangssteuerung (osdp_OUT)	20
6.9 Befehl zur Steuerung der Lesegerät-LEDs (osdp_LED)	21
6.10 Befehl zur Steuerung des Lesegerät-Summers (osdp_BUZ)	23
6.11 Befehl zur Textausgabe am Lesegerät (osdp_TEXT)	24
6.12 Befehl zur Konfiguration der Kommunikation (osdp_COMSET)	25

	Seite
6.13 Scannen und Senden biometrischer Daten (osdp_BIOREAD).....	26
6.14 Scannen und Abgleichen mit biometrischem Template (osdp_BIOMATCH).....	27
6.15 Setzen des Codierungsschlüssels (osdp_KEYSET).....	28
6.16 Challenge und Anforderung der Initialisierung einer sicheren Sitzung (osdp_CHLNG)	28
6.17 Zufällige Nummer und Kryptogramm des Servers (osdp_SCRYPT).....	28
6.18 Herstellerspezifischer Befehl (osdp_MFG).....	28
6.19 Empfangsgröße der ACU (osdp_ACURXSIZE)	28
6.20 Lesegerät aktiv halten (osdp_KEEPACTIVE)	29
6.21 Abbruch des aktuellen Vorgangs (osdp_ABORT).....	29
6.22 Abruf der PIV-Daten (osdp_PIVDATA)	29
6.23 Allgemeine Authentifizierung (osdp_GENAUTH).....	29
6.24 Authentifizierungs-Challenge (osdp_CRAUTH)	30
6.25 Befehl zur Dateiübertragung (osdp_FILETRANSFER).....	31
6.26 Erweiterter Schreibmodus (osdp_XWR)	31
6.26.1 Modusspezifische Befehlscodes für XRW_MODE=0	32
6.26.2 Leseanforderung der Moduseinstellung (osdp_PR00REQ).....	32
6.26.3 Befehl zum Setzen des Modus (osdp_PR00SET)	32
6.26.4 Modusspezifische Befehlscodes für XRW_MODE=1	33
6.26.5 Anforderung zum Senden transparenten Inhalts (osdp_PR01XMIT)	33
5.26.6 Smartcard-Verbindung trennen (osdp_PR01SCDONE)	34
6.26.7 Befehl zur Anforderung der sicheren PIN-Eingabe (osdp_PR01SPE)	34
6.26.8 Smartcard-Scan (osdp_PR01SCSCAN)	36
7 Antworten	36
7.1 Allgemeine Bestätigung, kein Bericht (osdp_ACK).....	36
7.2 Negative Bestätigung – Fehler-Response des Handlers der SIO-Kommunikation (osdp_NAK).....	37
7.3 Geräteidentifikationsbericht (osdp_PDID).....	37
7.4 Bericht über Gerätefunktionen (osdp_PDCAP).....	38
7.5 Lokaler Statusbericht (osdp_LSTATR).....	39
7.6 Eingangstatusbericht (osdp_ISTATR).....	39
7.7 Ausgangsstatusbericht (osdp_OSTATR)	40
7.8 Bericht über Sabotagestatus des Lesegeräts (osdp_RSTATR).....	40
7.9 Bericht über Kartendaten, Rohbitfeld (osdp_RAW)	41
7.10 Bericht über Kartendaten, Zeichenfeld (osdp_FMT)	41
7.11 Tastaturdatenbericht (osdp_KEYPAD).....	42
7.12 Bericht über Konfiguration der Kommunikation (osdp_COM).....	43
7.13 Scannen und Senden biometrischer Daten (osdp_BIOREADR)	43
7.14 Scannen und Abgleichen mit biometrischem Template (osdp_BIOMATCHR).....	44
7.15 ID und zufällige Nummer des Clients (osdp_CCRYPT).....	44

	Seite
7.16 Paket mit Client-Kryptogramm und initialer R-MAC (osdp_RMAC_I).....	45
7.17 Herstellerspezifische Antwort (osdp_MFGREP).....	45
7.18 Antwort „PD beschäftigt“ (osdp_BUSY).....	45
7.19 Antwort auf Anforderung von PIV-Daten (osdp_PIVDATAR).....	46
7.20 osdp_GENAUTHR.....	46
7.21 Response auf Challenge (osdp_CRAUTHR).....	47
7.22 Antwort auf Anforderung eines herstellerepezifischen Status (osdp_MFGSTATR).....	47
7.23 Antwort auf Anforderung eines herstellerepezifischen Fehlers (osdp_MFGERRR).....	47
7.24 Status der Dateiübertragung (osdp_FTSTAT).....	47
7.25 Antwort auf Anforderung des erweiterten Lesemodus (osdp_XRD).....	48
7.25.1 Modusspezifische Antwortcodes für XRW_MODE=0.....	49
7.25.2 Antwort mit Mode-00-Fehler (osdp_PR00ERROR).....	49
7.25.3 Bericht über Moduseinstellung (osdp_PR00REQR).....	49
7.25.4 Bericht über Karteninformationen (osdp_PR00CIRR).....	50
7.25.5 Modusspezifische Antwortcodes für XRW_MODE=1.....	50
7.25.6 Antwort mit Mode-01-NAK oder Fehler (osdp_PR01ERROR).....	51
7.25.7 Antwort mit Benachrichtigung „Karte vorhanden“ (osdp_PR01PRES).....	51
7.25.8 Antwort mit transparenten Kartendaten (osdp_PR01SCREP).....	51
7.25.9 Antwort „Sichere PIN-Eingabe abgeschlossen“ (osdp_PR01SPER).....	52
Anhang A (normativ) Codenummern für Befehle und Antworten.....	53
A.1 Befehle.....	53
A.2 Antworten.....	54
Anhang B (normativ) Liste von Definitionen der Funktionscodes.....	56
B.1 Funktionscode 1 – Überwachung des Kontaktstatus.....	56
B.2 Funktionscode 2 – Ausgangssteuerung.....	56
B.3 Funktionscode 3 – Kartendatenformat.....	57
B.4 Funktionscode 4 – Steuerung der Lesegerät-LEDs.....	57
B.5 Funktionscode 5 – Akustische Ausgabe des Lesegeräts.....	57
B.6 Funktionscode 6 – Textausgabe des Lesegeräts.....	58
B.7 Funktionscode 7 – Aufrechterhaltung der Zeit.....	58
B.8 Funktionscode 8 – Unterstützung der Zeichenprüfung.....	58
B.9 Funktionscode 9 – Kommunikationssicherheit.....	58
B.10 Funktionscode 10 – Größe des Empfangspuffers.....	59
B.11 Funktionscode 11 – Maximale Größe kombinierter Nachrichten.....	59
B.12 Funktionscode 12 – Smartcard-Unterstützung.....	59
B.13 Funktionscode 13 – Lesegeräte.....	59
B.14 Funktionscode 14 – Biometrik.....	59
B.15 Funktionscode 15 – Unterstützung der sicheren PIN-Eingabe.....	60

	Seite
B.16 Funktionscode 16 – OSDP-Version	60
Anhang C (normativ) CRC-Definition.....	61
Anhang D (normativ) Verschlüsselung	63
D.1 Befehle.....	63
D.1.1 Setzen des Codierungsschlüssels (osdp_KEYSET).....	63
D.1.2 Challenge und Anforderung der Initialisierung einer sicheren Sitzung (osdp_CHLNG)	63
D.1.3 Zufällige Nummer und Kryptogramm des Servers (osdp_SCRYPT)	64
D.2 Antworten	64
D.2.1 ID und zufällige Nummer des Clients (osdp_CCRYPT).....	64
D.2.2 Paket mit Client-Kryptogramm und initialer R-MAC (osdp_RMAC_I)	64
D.3 Verschlüsselungsverfahren: OSDP-SC.....	64
D.3.1 Allgemeiner Überblick.....	65
D.3.2 Der Prozess	66
D.3.3 Verbindungssequenz der sicheren Kanalsitzung (SCS-CS).....	66
D.3.4 SCS_11 ACU → PD	66
D.3.5 SCS_12 PD → ACU	66
D.3.6 SCS_13 ACU → PD	67
D.3.7 SCS_14 PD → ACU	67
D.3.8 Kommunikation während einer sicheren Kanalsitzung	67
D.3.9 SCS_15 ACU → PD	67
D.3.10 SCS_16 PD → ACU	68
D.3.11 SCS_17 ACU → PD:	68
D.3.12 SCS_18 PD → ACU	68
D.4 Algorithmen und Unterstützungsfunktionen	68
D.4.1 Diversifizierung von Schlüsseln.....	68
D.4.2 Ableitung von Sitzungsschlüsseln	68
D.4.3 Client-Kryptogramm.....	69
D.4.4 Server-Kryptogramm	69
D.4.5 Auffüllen.....	69
D.5 Generierung des Nachrichtenauthentifizierungscodes (MAC).....	69
D.5.1 Packvorgang für Sicherheitsblocktypen SCS_15, SCS-16, SCS_17 und SCS_18.....	70
D.5.2 Entpackvorgang.....	71
D.5.3 Feldentwicklung und Konfiguration	71
Anhang E (normativ) Prüfvektoren	73
Anhang F (informativ) Vergleichende Darstellung der in IEC 60839-11-1 verbindlich vorgeschriebenen Funktionen	75
Literaturverzeichnis.....	87
Bilder	
Bild 1 – Schematischer Überblick über eine OSDP-Verbindung.....	11

	Seite
Bild D.1 – MAC-Algorithmus.....	70
Tabellen	
Tabelle 1 – Paketformat	13
Tabelle 2 – Nachrichtensteuerinformationen.....	15
Tabelle 3 – Sicherheitsblock (SB)	15
Tabelle 4 – Struktur einer mehrteiligen Nachricht	16
Tabelle 5 – Verhaltensmodi.....	17
Tabelle 6 – Abfrageanforderung.....	18
Tabelle 7 – Anforderung des ID-Berichts	18
Tabelle 8 – Anforderung der Funktionen des Peripheriegeräts	19
Tabelle 9 – Anforderung des lokalen Statusberichts.....	19
Tabelle 10 – Anforderung des Eingangsstatusberichts.....	19
Tabelle 11 – Anforderung des Ausgangsstatusberichts.....	20
Tabelle 12 – Anforderung des Statusberichts des Lesegeräts	20
Tabelle 13 – Befehl zur Ausgangssteuerung	20
Tabelle 14 – Werte des Steuercodes	21
Tabelle 15 – Befehl zur Steuerung der Lesegerät-LEDs	22
Tabelle 16 – Temporäre Steuercodewerte.....	22
Tabelle 17 – Permanente Steuercodewerte.....	23
Tabelle 17 – Farbwerte.....	23
Tabelle 18 – Befehl zur Steuerung des Lesegerät-Summers (osdp_BUZ).....	24
Tabelle 19 – Befehl zur Textausgabe am Lesegerät (osdp_TEXT).....	25
Tabelle 20 – Textbefehlswerte	25
Tabelle 21 – Befehl zur Konfiguration der Kommunikation (osdp_COMSET)	26
Tabelle 22 – Scannen und Senden biometrischer Daten (osdp_BIOREAD).....	26
Tabelle 23 – Biometrische Typen.....	26
Tabelle 24 – Fingerabdruckformate	27
Tabelle 25 – Befehlsstruktur: Header aus 6 Bytes, gefolgt von einem Template variabler Länge	27
Tabelle 26 – Herstellerspezifische Befehle (osdp_MFG).....	28
Tabelle 27 – Empfangsgröße der ACU (osdp_ACURXSIZE)	29
Tabelle 28 – Lesegerät aktiv halten (osdp_KEEPACTIVE)	29
Tabelle 29 – Abruf der PIV-Daten (osdp_PIVDATA)	29
Tabelle 30 – Fragment der allgemeinen Authentifizierung (osdp_GENAUTH).....	30
Tabelle 31 – Fragment der Authentifizierungs-Challenge (osdp_CRAUTH)	30
Tabelle 32 – Befehl zur Dateiübertragung.....	31
Tabelle 33 – Befehlsstruktur für erweiterten Schreibmodus	31
Tabelle 34 – Modusspezifische Befehlscodes	32
Tabelle 35 – Leseanforderung der Moduseinstellung	32

	Seite
Tabelle 36 – Befehl zum Setzen des Modus	32
Tabelle 37 – Konfiguration von Modus 0	33
Tabelle 38 – Konfiguration von Modus 1	33
Tabelle 39 – Modusspezifische Befehlscodes.....	33
Tabelle 40 – Anforderung zum Senden transparenten Inhalts.....	33
Tabelle 41 – Smartcard-Verbindung trennen	34
Tabelle 42 – Befehl zur Anforderung der sicheren PIN-Eingabe	34
Tabelle 43 – Smartcard-Scan	36
Tabelle 44 – Negative Bestätigung (osdp_NAK).....	37
Tabelle 45 – Fehlercodes	37
Tabelle 46 – Geräteidentifikationsbericht (osdp_PDID)	38
Tabelle 47 – Bericht über Gerätefunktionen (osdp_PDCAP).....	39
Tabelle 48 – Lokaler Statusberichts (osdp_LSTATR).....	39
Tabelle 49 – Eingangstatusbericht (osdp_ISTATR)	40
Tabelle 50 – Ausgangsstatusbericht (osdp_OSTATR).....	40
Tabelle 51 – Bericht über Sabotagestatus des Lesegeräts (osdp_RSTATR).....	41
Tabelle 52 – Bericht über Kartendaten, Rohbitfeld (osdp_RAW).....	41
Tabelle 53 – Bericht über Kartendaten, Zeichenfeld (osdp_FMT)	42
Tabelle 54 – Tastaturdatenbericht (osdp_KEYPAD).....	42
Tabelle 55 – Bericht über Konfiguration der Kommunikation (osdp_COM)	43
Tabelle 56 – Scannen und Senden biometrischer Daten (osdp_BIOREADR).....	43
Tabelle 57 – Scannen und Abgleichen mit biometrischem Template (osdp_BIOMATCHR)	44
Tabelle 58 – Herstellerspezifische Antwort (osdp_MFGREP).....	45
Tabelle 59 – Antwort „PD beschäftigt“ (osdp_BUSY).....	45
Tabelle 60 – Antwort auf Anforderung von PIV-Daten (osdp_PIVDATAR).....	46
Tabelle 61 – Response auf Anforderung zur allgemeinen Authentifizierung (osdp_GENAUTHR).....	46
Tabelle 62 – Response auf Challenge (osdp_CRAUTHR)	47
Tabelle 63 – Antwort auf Anforderung eines herstellereigenen Status (osdp_MFGSTATR).....	47
Tabelle 64 – Antwort auf Anforderung eines herstellereigenen Fehlers (osdp_MFGERRR).....	47
Tabelle 65 – Status der Dateiübertragung (osdp_FTSTAT).....	48
Tabelle 66 – Antwort auf Anforderung des erweiterten Lesemodus	49
Tabelle 67 – Modusspezifische Antwortcodes	49
Tabelle 68 – Fehlerantwort.....	49
Tabelle 69 – Bericht über Moduseinstellung	50
Tabelle 70 – Bericht über Karteninformationen	50
Tabelle 71 – Modusspezifische Antwortcodes	51
Tabelle 72 – Fehlerantwort.....	51
Tabelle 73 – Antwort mit Benachrichtigung „Karte vorhanden“	51

	Seite
Tabelle 74 – Antwort mit transparenten Kartendaten.....	52
Tabelle 75 – Antwort mit transparenten Kartendaten.....	52
Tabelle A.1 – Befehls Codenummern	53
Tabelle A.2 – Codenummern für Antworten	54
Tabelle B.1 – Funktionscodes	56
Tabelle D.1 – Befehlsstruktur: 2 Byte langer Header, gefolgt von Daten variabler Länge	63
Tabelle D.2 – Befehlsstruktur: 8 Byte lange zufällige Nummer als „Challenge“	63
Tabelle D.3 – Befehlsstruktur: 16 Byte langes Kryptogramm des Servers	64
Tabelle D.4 – Befehlsstruktur: Struktur mit 32 Bytes	64
Tabelle D.5 – Befehlsstruktur: Struktur mit 16 Bytes	64
Tabelle D.6 – Zuweisung von Werten für SEC_BLK_TYPE	65
Tabelle F.1 – Anforderungen an die Zutrittspunkt-Schnittstelle	75
Tabelle F.2 – Anforderungen an Anzeige/Meldung/Hinweise/Signalisierung	76
Tabelle F.3 – Anforderungen an die Erkennung	81
Tabelle F.4 – Anforderungen an die Bedrohungssignalisierung	83
Tabelle F.5 – Anforderungen an die Vorrangschaltung	83
Tabelle F.6 – Anforderungen an den Selbstschutz der Anlage.....	84