

	DIN EN IEC 60839-11-5 (VDE 0830-8-11-5)	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
<p>ICS 13.320</p> <p>Alarmanlagen – Teil 11-5: Elektronische Zutrittskontrollanlagen – Open Supervised Device Protocol (OSDP) (IEC 60839-11-5:2020); Deutsche Fassung EN IEC 60839-11-5:2020</p> <p>Alarm and electronic security systems – Part 11-5: Electronic access control systems – Open Supervised Device Protocol (OSDP) (IEC 60839-11-5:2020); German version EN IEC 60839-11-5:2020</p> <p>Systèmes d'alarme et de sécurité électroniques – Partie 11-5: Systèmes de contrôle d'accès électronique – Protocole ouvert d'appareil supervisé (OSDP) (IEC 60839-11-5:2020); Version allemande EN IEC 60839-11-5:2020</p> <p style="text-align: right;">Gesamtumfang 93 Seiten</p> <p style="text-align: center;">DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE</p>		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2020-08-12 angenommene Europäische Norm als DIN-Norm ist 2021-11-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN IEC 60839-11-5 (VDE 0830-8-11-5):2019-10.

Für dieses Dokument ist das nationale Arbeitsgremium K 713 „Gefahrenmelde- und Überwachungsanlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Die enthaltene IEC-Publikation wurde vom TC 79 „Alarm and electronic security systems“ erarbeitet. und unterliegt dem Copyright der IEC .

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Nationaler Anhang NA (informativ)

Zusammenhang mit europäischen und internationalen Dokumenten

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

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

Eine Information über den Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ist nachstehend wiedergegeben.

Tabelle NA.1

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
–	ISO 7816	–	–
–	<i>ersetzt durch:</i> ISO/IEC 7816	–	–
	ISO/IEC 7816-4:2005 <i>ersetzt durch:</i> ISO/IEC 7816-4:2020		
–	ISO 8601	DIN ISO 8601	–
–	<i>ersetzt durch:</i> ISO 8601-1	<i>ersetzt durch:</i> DIN ISO 8601-1	–
–	ISO/IEC 10646:2017	–	–
–	<i>ersetzt durch:</i> ISO/IEC 10646:2020	–	–
EN 60839 (alle Teile)	IEC 60839 (alle Teile)	DIN EN 60839 (VDE 0830) (alle Teile)	VDE 0830
EN 60839-11-1:2013	IEC 60839-11-1:2013	DIN EN 60839-11-1 (VDE 0830-8-11-1):2013-12	VDE 0830-8-11-1
EN 60839-11-1:2013 + AC:2015	IEC 60839-11-1:2013	DIN EN 60839-11-1 Ber 2 (VDE 0830-8-11-1 Ber 2):2015-10	VDE 0830-8-11-1 Ber 2
EN 60839-11-2:2015	IEC 60839-11-2:2014	DIN EN 60839-11-2 (VDE 0830-8-11-2):2016-02	VDE 0830-8-11-2
EN 60839-11-2:2015 + AC:2015	IEC 60839-11-2:2014	DIN EN 60839-11-2 Ber 1 (VDE 0830-8-11-2 Ber 1):2016-04	VDE 0830-8-11-2 Ber 1

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN ISO 8601-1, *Datum und Uhrzeit – Darstellung für den Informationsaustausch – Teil 1: Grundlegende Regeln*

DIN EN 60839 (VDE 0830) (alle Teile), *Alarmanlagen*

DIN EN 60839-11-1 (VDE 0830-8-11-1):2013-12, *Alarmanlagen – Teil 11-1: Elektronische Zutrittskontrollanlagen – Anforderungen an Anlagen und Geräte (IEC 60839-11-1:2013); Deutsche Fassung EN 60839-11-1:2013*

DIN EN 60839-11-1 Berichtigung 2 (VDE 0830-8-11-1 Berichtigung 2):2015-10, *Alarmanlagen – Teil 11-1: Elektronische Zutrittskontrollanlagen – Anforderungen an Anlagen und Geräte (IEC 60839-11-1:2013); Deutsche Fassung EN 60839-11-1:2013, Berichtigung zu DIN EN 60839-11-1 (VDE 0830-8-11-1):2013-12; Deutsche Fassung EN 60839-11-1:2013/AC:2015*

DIN EN 60839-11-2 (VDE 0830-8-11-2):2016-02, *Alarmanlagen – Teil 11-2: Elektronische Zutrittskontrollanlagen – Anwendungsregeln (IEC 60839-11-2:2014); Deutsche Fassung EN 60839-11-2:2015*

DIN EN 60839-11-2 Ber 1 (VDE 0830-8-11-2 Ber 1):2016-04, *Alarmanlagen – Teil 11-2: Elektronische Zutrittskontrollanlagen – Anwendungsregeln (IEC 60839-11-2:2014); Deutsche Fassung EN 60839-11-2:2015, Berichtigung zu DIN EN 60839-11-2 (VDE 0830-8-11-2):2016-02; Deutsche Fassung EN 60839-11-2:2015/AC:2015*

Alarmanlagen –
Teil 11-5: Elektronische Zutrittskontrollanlagen –
Open Supervised Device Protocol (OSDP)
(IEC 60839-11-5:2020)

Alarm and electronic security systems –
Part 11-5: Electronic access control systems –
Open Supervised Device Protocol (OSDP)
(IEC 60839-11-5:2020)

Systèmes d'alarme et de sécurité
électroniques –
Partie 11-5: Systèmes de contrôle d'accès
électronique –
Protocole ouvert d'appareil supervisé (OSDP)
(IEC 60839-11-5:2020)

Diese Europäische Norm wurde von CENELEC am 2020-08-12 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brüssel

© 2020 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN IEC 60839-11-5:2020 D

Europäisches Vorwort

Der Text des Dokuments 79/634/FDIS, zukünftige 1. Ausgabe der IEC 60839-11-5, erarbeitet vom IEC/TC 79 „Alarm and electronic security systems“ wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN IEC 60839-11-5:2020 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2021-05-12
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2023-08-12

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 60839-11-5:2020 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Anhang ZA (normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ANMERKUNG 1 Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, gekennzeichnet durch (mod.), dann gilt die entsprechende EN oder das HD.

ANMERKUNG 2 Aktualisierte Informationen über die in diesem Anhang aufgeführten aktuellen Fassungen der Europäischen Normen sind hier verfügbar: www.cenelec.eu.

<u>Publikation</u>	<u>Jahr</u>	<u>Titel</u>	<u>EN/HD</u>	<u>Jahr</u>
IEC 60839-11-1	2013	Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements	EN 60839-11-1	2013
–	–		+ AC	2015
IEC 60839-11-2	2014	Alarm and electronic security systems – Part 11-2: Electronic access control systems – Application guidelines	EN 60839-11-2	2015
–	–		+ AC	2015

Inhalt

Seite

Europäisches Vorwort.....	2
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	3
Einleitung	11
1 Anwendungsbereich	12
2 Normative Verweisungen	12
3 Begriffe und Abkürzungen	12
3.1 Begriffe	12
3.2 Abkürzungen	13
4 Überblick.....	13
5 Kommunikationseinstellungen.....	14
5.1 Physikalische Schnittstelle	14
5.2 Signalgebung.....	14
5.3 Zeichenverschlüsselung	14
5.4 Kanalzugang.....	14
5.5 Datenverschlüsselung mit mehreren Bytes.....	14
5.6 Begrenzung der Paketgröße	15
5.7 Zeitanforderungen	15
5.8 Meldungssynchronisation	15
5.9 Paketformat	16
5.10 Mehrteilige Meldungen	18
5.10.1 Allgemeines	18
5.10.2 Regeln für die Verwendung mehrteiliger Meldungen	19
5.11 Handhabung von Smartcards.....	19
6 Befehle.....	20
6.1 Allgemeines	20
6.2 Abfrageanforderung (osdp_POLL)	21
6.3 Anforderung des ID-Berichts (osdp_ID)	21
6.4 Anforderung der Funktionen des Peripheriegeräts (osdp_CAP)	21
6.5 Anforderung des lokalen Statusberichts (osdp_LSTAT)	21
6.6 Anforderung des Eingangsstatusberichts (osdp_ISTAT)	22
6.7 Anforderung des Ausgangsstatusberichts (osdp_OSTAT)	22
6.8 Anforderung des Statusberichts des Lesegeräts (osdp_RSTAT)	22
6.9 Befehl zur Ausgangssteuerung (osdp_OUT)	23
6.10 Befehl zur Steuerung der Lesegerät-LEDs (osdp_LED)	23
6.11 Befehl zur Steuerung des Lesegerät-Summers (osdp_BUZ).....	26
6.12 Befehl zur Textausgabe am Lesegerät (osdp_TEXT).....	27
6.13 Befehl zur Konfiguration der Kommunikation (osdp_COMSET)	28

6.14	Scannen und Senden biometrischer Daten (osdp_BIOREAD).....	29
6.15	Scannen und Abgleichen mit biometrischem Template (osdp_BIOMATCH)	30
6.16	Setzen des Codierungsschlüssels (osdp_KEYSET).....	31
6.17	Challenge und Anforderung der Initialisierung einer sicheren Sitzung (osdp_CHLNG).....	31
6.18	Zufallszahl und Kryptogramm des Servers (osdp_SCRIPT)	31
6.19	Herstellerspezifischer Befehl (osdp_MFG)	31
6.20	Empfangsgröße der ACU (osdp_ACURXSIZE).....	32
6.21	Lesegerät aktiv halten (osdp_KEEPACTIVE)	32
6.22	Abbruch des aktuellen Vorgangs (osdp_ABORT)	33
6.23	Abruf der PIV-Daten (osdp_PIVDATA)	33
6.24	Allgemeine Authentifikation (osdp_GENAUTH).....	33
6.25	Authentifikations-Challenge (osdp_CRAUTH).....	34
6.26	Befehl zur Dateiübertragung (osdp_FILETRANSFER).....	35
6.27	Erweiterter Schreibmodus (osdp_XWR)	35
6.27.1	Allgemeines.....	35
6.27.2	Befehl zum Setzen des Modus	36
6.27.3	Modus-00-Befehl zum Lesen der Einstellung	37
6.27.4	Modusspezifische Befehlscodes für XRW_MODE=1	37
6.27.5	Modus-01-Befehl mit Anforderung zum Senden transparenten Inhalts.....	37
6.27.6	Modus-01-Befehl zum Trennen der Verbindung.....	38
6.27.7	Modus-01-Befehl zur Anforderung der sicheren PIN-Eingabe	38
6.27.8	Modus-01-Befehl zum Scannen der Smartcard.....	40
7	Antworten	40
7.1	Allgemeines.....	40
7.2	Allgemeine Quittierung – Kein Bericht (osdp_ACK).....	41
7.3	Negative Quittierung – Fehlerantwort (osdp_NAK).....	41
7.4	Geräteidentifikationsbericht (osdp_PDID).....	42
7.5	Bericht über Gerätefunktionen (osdp_PDCAP)	43
7.6	Lokaler Statusbericht (osdp_LSTATR)	44
7.7	Eingangstatusbericht (osdp_ISTATR).....	44
7.8	Ausgangsstatusbericht (osdp_OSTATR).....	45
7.9	Bericht über den Sabotagestatus des Lesegeräts (osdp_RSTATR)	45
7.10	Bericht über Kartendaten, Rohbitfeld (osdp_RAW)	45
7.11	Bericht über Kartendaten, Zeichenfeld (osdp_FMT).....	46
7.12	Tastaturdatenbericht (osdp_KEYPAD)	46
7.13	Bericht über die Konfiguration der Kommunikation (osdp_COM).....	47
7.14	Scannen und Senden biometrischer Daten (osdp_BIOREADR).....	47
7.15	Scannen und Abgleichen mit biometrischem Template (osdp_BIOMATCHR).....	48
7.16	ID und Zufallszahl des Clients (osdp_CCRYPT)	49

	Seite
7.17 Paket mit Client-Kryptogramm und initialer R-MAC (osdp_RMAC_I)	49
7.18 Herstellerspezifische Antwort (osdp_MFGREP)	49
7.19 Antwort „PD beschäftigt“ (osdp_BUSY)	49
7.20 Antwort auf die Anforderung von PIV-Daten (osdp_PIVDATAR).....	50
7.21 osdp_GENAUTHR.....	50
7.22 Reaktion auf Challenge (osdp_CRAUTHR)	50
7.23 Herstellerspezifische Antwort auf einen Status (osdp_MFGSTATR).....	51
7.24 Herstellerspezifische Antwort auf einen Fehler (osdp_MFGERRR)	51
7.25 Status der Dateiübertragung (osdp_FTSTAT)	51
7.26 Antwort auf die Anforderung des erweiterten Lesemodus (osdp_XRD)	53
7.26.1 Allgemeines	53
7.26.2 Modusspezifische Antwortcodes für XRW_MODE=0	53
7.26.3 Modus-00-Fehlerantwort (osdp_PR00ERROR).....	53
7.26.4 Bericht über die Moduseinstellungen (osdp_PR00REQR)	54
7.26.5 Bericht über Karteninformationen (osdp_PR00CIRR)	54
7.26.6 Modusspezifische Antwortcodes für XRW_MODE=1	55
7.26.7 Antwort mit Modus-01-NAK oder Fehler (osdp_PR01ERROR).....	55
7.26.8 Antwort mit Benachrichtigung „Karte vorhanden“ (osdp_PR01PRES)	55
7.26.9 Antwort mit transparenten Kartendaten (osdp_PR01SCREP).....	56
7.26.10 Antwort „Sichere PIN-Eingabe abgeschlossen“ (osdp_PR01SPER).....	56
Anhang A (normativ) Codenummern für Befehle und Antworten	57
A.1 Befehle.....	57
A.2 Antworten	58
Anhang B (normativ) Liste von Definitionen der Funktionscodes.....	59
B.1 Allgemeines	59
B.2 Funktionscode 1 – Überwachung des Kontaktzustands	59
B.3 Funktionscode 2 – Ausgangssteuerung	60
B.4 Funktionscode 3 – Kartendatenformat	60
B.5 Funktionscode 4 – Steuerung der Lesegerät-LEDs	60
B.6 Funktionscode 5 – Akustische Ausgabe des Lesegeräts.....	61
B.7 Funktionscode 6 – Textausgabe des Lesegeräts	61
B.8 Funktionscode 7 – Aufrechterhaltung der Zeit	61
B.9 Funktionscode 8 – Unterstützung der Zeichenprüfung	61
B.10 Funktionscode 9 – Kommunikationssicherheit.....	62
B.11 Funktionscode 10 – Größe des Empfangspuffers.....	62
B.12 Funktionscode 11 – Maximale Größe kombinierter Meldungen.....	62
B.13 Funktionscode 12 – Smartcard-Unterstützung.....	62
B.14 Funktionscode 13 – Lesegeräte	63
B.15 Funktionscode 14 – Biometrik	63

B.16	Funktionscode 15 – Unterstützung der sicheren PIN-Eingabe	63
B.17	Funktionscode 16 – OSDP-Version	63
Anhang C (normativ)	CRC-Definition	64
Anhang D (normativ)	Verschlüsselung	66
D.1	Verschlüsselungsverfahren: OSDP-SC	66
D.1.1	Allgemeines	66
D.1.2	Überblick	67
D.1.3	Der Prozess	67
D.1.4	Verbindungssequenz der sicheren Kanalsitzung (SCS-CS)	67
D.1.5	Kommunikation während einer sicheren Kanalsitzung	69
D.1.6	SCS_16 PD -> ACU	69
D.1.7	SCS_17 ACU -> PD	69
D.1.8	SCS_18 PD -> ACU	69
D.2	Befehle	69
D.2.1	Setzen des Codierungsschlüssels (osdp_KEYSET)	69
D.2.2	Challenge und Anforderung der Initialisierung einer sicheren Sitzung (osdp_CHLNG)	70
D.2.3	Zufallszahl und Kryptogramm des Servers (osdp_SCRYPT)	70
D.3	Antworten	71
D.3.1	ID und Zufallszahl des Clients (osdp_CCrypt)	71
D.3.2	Paket mit Client-Kryptogramm und initialer R-MAC (osdp_RMAC_I)	71
D.4	Algorithmen und Unterstützungsfunktionen	71
D.4.1	Ableitung von Sitzungsschlüsseln	71
D.4.2	Diversifizierung von Schlüsseln	72
D.4.3	Client-Kryptogramm	72
D.4.4	Server-Kryptogramm	72
D.4.5	Auffüllen	72
D.5	Generierung des Nachrichtenauthentifizierungscodes (MAC)	73
D.5.1	Allgemeines	73
D.5.2	Packvorgang für die Sicherheitsblocktypen SCS_15, SCS_16, SCS_17 und SCS_18	74
D.5.3	Der Entpackvorgang	74
D.6	Widerherstellung im Fehlerfall	74
D.7	Feldentwicklung und Konfiguration	75
Anhang E (normativ)	Prüfvektoren	76
Anhang F (informativ)	Vergleichende Darstellung der in IEC 60839-11-1 verbindlich vorgeschriebenen Funktionen	78
Literaturhinweise		89
Bilder		
Bild 1	– Schematischer Überblick über eine OSDP-Verbindung	13
Bild D.1	– MAC-Algorithmus	73

Tabellen

Tabelle 1 – Paketformat	16
Tabelle 2 – Meldungssteuerinformationen	17
Tabelle 3 – Sicherheitsblock (SB)	18
Tabelle 4 – Struktur einer mehrteiligen Meldung	19
Tabelle 5 – Verhaltensmodi	20
Tabelle 6 – Abfrageanforderung	21
Tabelle 7 – Anforderung des ID-Berichts	21
Tabelle 8 – Anforderung der Funktionen des Peripheriegeräts	21
Tabelle 9 – Anforderung des lokalen Statusberichts	22
Tabelle 10 – Anforderung des Eingangsstatusberichts	22
Tabelle 11 – Anforderung des Ausgangsstatusberichts	22
Tabelle 12 – Anforderung des Statusberichts des Lesegeräts	22
Tabelle 13 – Befehl zur Ausgangssteuerung	23
Tabelle 14 – Werte des Steuercodes	23
Tabelle 15 – Befehl zur Steuerung der Lesegerät-LEDs	25
Tabelle 16 – Temporäre Steuercodewerte	26
Tabelle 17 – Permanente Steuercodewerte	26
Tabelle 18 – Farbwerte	26
Tabelle 19 – Befehl zur Steuerung des Lesegerät-Summers (osdp_BUZ)	27
Tabelle 20 – Befehl zur Textausgabe am Lesegerät (osdp_TEXT)	28
Tabelle 21 – Textbefehlswerte	28
Tabelle 22 – Befehl zur Konfiguration der Kommunikation (osdp_COMSET)	29
Tabelle 23 – Scannen und Senden biometrischer Daten (osdp_BIOREAD)	29
Tabelle 24 – Biometrische Typen	30
Tabelle 25 – Fingerabdruckformate	30
Tabelle 26 – Befehlsstruktur: Header aus 6 Bytes, gefolgt von einem Template variabler Länge	31
Tabelle 27 – Herstellerspezifische Befehle (osdp_MFG)	32
Tabelle 28 – Empfangsgröße der ACU (osdp_ACURXSIZE)	32
Tabelle 29 – Lesegerät aktiv halten (osdp_KEEPACTIVE)	32
Tabelle 30 – Abbruch des aktuellen Vorgangs (osdp_ABORT)	33
Tabelle 31 – Abruf der PIV-Daten (osdp_PIVDATA)	33
Tabelle 32 – Fragment der allgemeinen Authentifikation (osdp_GENAUTH)	34
Tabelle 33 – Fragment der Authentifikations-Challenge (osdp_CRAUTH)	34
Tabelle 34 – Befehl zur Dateiübertragung	35
Tabelle 35 – Befehlsstruktur für erweiterten Schreibmodus	36
Tabelle 36 – Befehl zum Setzen des Modus	36
Tabelle 37 – Konfiguration von Modus 0	36
Tabelle 38 – Konfiguration von Modus 1	37

Tabelle 39 – Leseanforderung der Einstellung	37
Tabelle 40 – Modusspezifische Befehlscodes	37
Tabelle 41 – Anforderung zum Senden transparenten Inhalts.....	38
Tabelle 42 – Smartcard-Verbindung trennen	38
Tabelle 43 – Befehl zur Anforderung der sicheren PIN-Eingabe	39
Tabelle 44 – Scannen der Smartcard.....	40
Tabelle 45 – Allgemeine Quittierung (osdp_ACK)	41
Tabelle 46 – Negative Quittierung (osdp_NAK)	41
Tabelle 47 – Fehlercodes	42
Tabelle 48 – Geräteidentifikationsbericht (osdp_PDID)	43
Tabelle 49 – Bericht über Gerätefunktionen (osdp_PDCAP).....	44
Tabelle 50 – Lokaler Statusbericht (osdp_LSTATR).....	44
Tabelle 51 – Eingangsstatusbericht (osdp_ISTATR)	44
Tabelle 52 – Ausgangsstatusbericht (osdp_OSTATR)	45
Tabelle 53 – Bericht über den Sabotagestatus des Lesegeräts (osdp_RSTATR).....	45
Tabelle 54 – Bericht über Kartendaten, Rohbitfeld (osdp_RAW)	46
Tabelle 55 – Bericht über Kartendaten, Zeichenfeld (osdp_FMT)	46
Tabelle 56 – Tastaturredatenbericht (osdp_KEYPAD).....	47
Tabelle 57 – Bericht über die Konfiguration der Kommunikation (osdp_COM)	47
Tabelle 58 – Scannen und Senden biometrischer Daten (osdp_BIOREADR)	48
Tabelle 59 – Scannen und Abgleichen mit biometrischem Template (osdp_BIOMATCHR)	48
Tabelle 60 – Herstellerspezifische Antwort (osdp_MFGREP)	49
Tabelle 61 – Antwort „PD beschäftigt“ (osdp_BUSY)	49
Tabelle 62 – Antwort auf die Anforderung von PIV-Daten (osdp_PIVDATAR).....	50
Tabelle 63 – Reaktion auf die Anforderung zur allgemeinen Authentifikation (osdp_GENAUTHR).....	50
Tabelle 64 – Reaktion auf Challenge (osdp_CRAUTHR)	51
Tabelle 65 – Herstellerspezifische Antwort auf einen Status (osdp_MFGSTATR).....	51
Tabelle 66 – Herstellerspezifische Antwort auf einen Fehler (osdp_MFGERRR)	51
Tabelle 67 – Status der Dateiübertragung (osdp_FTSTAT)	52
Tabelle 68 – Antwort auf die Anforderung des erweiterten Lesemodus	53
Tabelle 69 – Modusspezifische Antwortcodes	53
Tabelle 70 – Fehlerantwort.....	53
Tabelle 71 – Bericht über die Moduseinstellungen	54
Tabelle 72 – Bericht über Karteninformationen.....	54
Tabelle 73 – Modusspezifische Antwortcodes	55
Tabelle 74 – Fehlerantwort.....	55
Tabelle 75 – Antwort mit Benachrichtigung „Karte vorhanden“	55
Tabelle 76 – Antwort mit transparenten Kartendaten.....	56
Tabelle 77 – Antwort mit transparenten Kartendaten.....	56

	Seite
Tabelle A.1 – Befehlscodenummern.....	57
Tabelle A.2 – Antwortcodenummern	58
Tabelle B.1 – Funktionscodes	59
Tabelle D.1 – SEC_BLK_TYPE-Zuordnung	66
Tabelle D.2 – Befehlsstruktur: Header aus 2 Bytes, gefolgt von einem Template variabler Länge.....	70
Tabelle D.3 – Befehlsstruktur: 8 Byte lange Zufallszahl als „Challenge“	70
Tabelle D.4 – Befehlsstruktur: 16 Byte langes Server-Kryptogramm.....	71
Tabelle D.5 – Befehlsstruktur: 32-Byte-Struktur	71
Tabelle D.6 – Befehlsstruktur: 16-Byte-Struktur	71
Tabelle F.1 – Anforderungen an die Schnittstelle des Zutrittspunkts	78
Tabelle F.2 – Anforderungen an Anzeige/Meldung/Hinweise/Signalisierung	79
Tabelle F.3 – Anforderungen an die Erkennung.....	83
Tabelle F.4 – Anforderungen an die Bedrohungssignalisierung	85
Tabelle F.5 – Anforderungen an die Vorrangschaltung.....	85
Tabelle F.6 – Anforderungen an den Selbstschutz der Anlage	85

Einleitung

Dieses Dokument beschreibt das Kommunikationsprotokoll für den Anschluss von einem oder mehreren Peripheriegerät(en) (PD) an eine Zutrittskontrollzentrale (ACU). Dieses Dokument legt die Protokollimplementierung über einen seriellen Mehrpunkt-Kommunikationskanal mit zwei Leitern nach dem RS-485-Standard fest.

Dieses Dokument beruht auf der Arbeit der OSDP-Arbeitsgruppe der Security Industry Association.

1 Anwendungsbereich

In diesem Teil von IEC 60839 wird das Open Supervised Device Protocol (OSDP) für elektronische Zutrittskontrollanlagen festgelegt. Dies umfasst Kommunikationseinstellungen, Befehle und Antworten zwischen der ACU und den Peripheriegeräten. Ebenfalls eingeschlossen ist eine vergleichende Darstellung von verbindlich vorgeschriebenen und optionalen Anforderungen nach IEC 60839-11-1:2013, wie in Anhang F enthalten.

Dieses Dokument gilt nur für die physische Sicherheit. Die physische Sicherheit hindert unbefugte Mitarbeiter sowie Angreifer und versehentliche Eindringlinge daran, physischen Zutritt zu einem Gebäude, einem Raum usw. zu erhalten.

Dieses Dokument soll die Hersteller in keiner Weise darin einschränken, dem hier festgelegten Protokoll weitere Befehle hinzuzufügen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 60839-11-1:2013, *Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements*

IEC 60839-11-2:2014, *Alarm and electronic security systems – Part 11-2: Electronic access control systems – Application guidelines*

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 60839-11-1, IEC 60839-11-2 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

– IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

– ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1.1

Client

Dienstanforderer

BEISPIEL Nutzerschnittstelle usw.

3.1.2

Server

Dienstleister

BEISPIEL Zutrittskontrollzentrale usw.

3.1.3

Peripheriegerät

E/A-Gerät, das über OSDP mit der Zutrittskontrollzentrale verbunden ist

BEISPIEL Erfassungseinheit für ein Identifikationsmittel, Kartenlesegerät, biometrisches Lesegerät, Client usw.

3.2 Abkürzungen

Für die Anwendung dieses Dokuments gelten die Abkürzungen nach IEC 60839-11-1, IEC 60839-11-2 und die folgenden Abkürzungen.

ACU	Zutrittskontrollzentrale (en: access control unit)
AES	hochentwickelter Verschlüsselungsstandard (en: advanced encryption standard)
APDU	Anwendungsprotokoll-Dateneinheit (en: application protocol data unit)
CBC	Blockchiffrenkettung (en: cypher block chaining)
C-MAC	Befehls-MAC (für Pakete von der ACU an das PD) (en: command MAC)
cUID	eindeutige Kennung des Clients (en: client's unique identifier)
ICV	initialer Kettungsvektor (en: initial chaining vector)
MAC	Nachrichtenauthentifizierungscode (en: message authentication code)
MK	Hauptschlüssel (en: master key)
PD	Peripheriegerät (en: peripheral device)
PGM	Portable Grey Map
R-MAC	Antwort-MAC (für Pakete vom PD an die ACU) (en: reply MAC)
SCBK	Basisschlüssel des sicheren Kanals (en: secure channel base key)
SCS	sichere Kanalsitzung (en: secure channel session)
S-ENC	Sitzungsschlüssel zur Sicherstellung der Vertraulichkeit der Daten (Meldungsverschlüsselung)
S-MAC1	Sitzungsschlüssel für die Nachrichtenauthentifizierung, Schlüssel 1
S-MAC2	Sitzungsschlüssel für die Nachrichtenauthentifizierung, Schlüssel 2
SPE	sichere PIN-Eingabe (en: secure PIN entry)

4 Überblick

Dieses Dokument definiert das Protokoll für den Anschluss einer ACU an Peripheriegeräte, einschließlich Kommunikationseinstellungen, Befehlen und Antworten, wie in Bild 1 gezeigt.

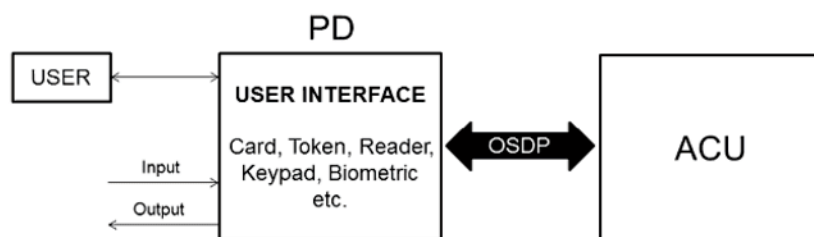


Bild 1 – Schematischer Überblick über eine OSDP-Verbindung

5 Kommunikationseinstellungen

5.1 Physikalische Schnittstelle

Die physikalische Schnittstelle muss ein Halbduplex-Kommunikationsbus nach dem RS-485-Standard mit einer einzigen verdrehten Leitung sein, die abgeschirmt und betriebsgeerdet ist.

5.2 Signalgebung

Der Signalport muss ein asynchroner serieller Halbduplex-Port mit den folgenden Einstellungen sein:

- 8 Datenbits;
- 1 Stoppbit;
- keine Paritätsbits;
- mindestens einer der folgenden Werte: 9 600 Baud, 19 200 Baud, 38 400 Baud, 57 600 Baud, 115 200 Baud, 230 400 Baud.

5.3 Zeichenverschlüsselung

Die Datenverschlüsselung muss UTF-8 entsprechen (ISO/IEC 10646:2017).

5.4 Kanalzugang

Der Kommunikationskanal wird im Modus „Abfrage/Antwort“ verwendet. Nur die ACU darf spontan eine Meldung senden. Jede von der ACU gesendete Meldung wird an nur ein PD adressiert. Für die „Broadcast-Meldung“, wie sie in [Tabelle 1](#) beschrieben ist, wird davon ausgegangen, dass nur ein einziges PD mit der ACU verbunden ist.

Das PD muss innerhalb der in [5.7](#) festgelegten Verzögerung MAX_REPLY_DELAY auf jede an das Gerät adressierte Meldung eine einzelne Antwortmeldung senden.

Sonderfall: Wenn das PD aufgrund temporärer Nichtverfügbarkeit einer Ressource, die zur Verarbeitung des Befehls erforderlich ist, den Befehl nicht zur Verarbeitung annehmen kann, muss das PD die Antwort osdp_BUSY senden, wie in [7.19](#) definiert. Wenn die ACU die osdp_BUSY-Antwort empfängt, darf sie frei wählen, denselben Befehl noch einmal zu senden, wie es bei einer Zeitüberschreitung der Übertragung des Befehls der Fall wäre. Wenn sich die ACU dafür entscheidet, den Befehl, der die osdp_BUSY-Antwort verursacht hat, erneut zu senden, darf sie dies unmittelbar tun oder aber erst anderen PDs einen Dienst erweisen und anschließend den Befehl neu senden. Wenn sich die ACU allerdings dafür entscheidet, den Befehl, der die BUSY-Antwort empfing, zu verwerfen, muss das PD diesen Zustand (neue Sequenznummer) erkennen und den neuen Befehl verarbeiten.

Befehle, die spezifische Daten vom PD anfordern, müssen auf Daten beschränkt werden, die erwartungsgemäß unmittelbar zur Verfügung stehen. Entsprechend dieser Leitlinie müssen Anwendungen, bei denen die ACU Daten anfordern muss, die einige Zeit brauchen können, bis sie verfügbar sind, den Vorgang in zwei verschiedenen Schritten umsetzen. Die ACU muss einen Befehl ausgeben, mit dem die Daten angefordert werden. Die Annahme dieses Befehls muss durch osdp_ACK angezeigt werden. Um den Vorgang abzuschließen, muss das PD die passende Antwort als Reaktion auf osdp_POLL zurücksenden.

5.5 Datenverschlüsselung mit mehreren Bytes

Meldungen werden anhand eines Zeichenstrommodells aufgebaut, d. h., alle Daten müssen ohne jegliche „Auffüllzeichen zur Ausrichtung“ gepackt werden.

Numerische Datentypen, die mehr als 1 Byte benötigen, werden mit dem niedrigstwertigen Byte an erster Stelle gespeichert („Little-Endian“-Format).

5.6 Begrenzung der Paketgröße

Für die Implementierung des Standardmeldungssatzes müssen alle Geräte in der Lage sein, Pakete bis zu einer Länge von 128 Bytes anzunehmen und an andere Geräte adressierte Meldungen bis zu einer Gesamtlänge von höchstens 1 440 Bytes zu tolerieren.

Wenn das Paket für ein anderes Gerät bestimmt war, sollte mit der Begrenzung kein ungünstiger Zustand im PD erzeugt werden. Wenn das PD ein Paket empfängt, das speziell an dieses Gerät adressiert ist und größer ist als seine gemeldete RX-Puffergröße, würde dies einen Protokollfehler darstellen und mit einem NAK-Code 0x02 antworten.

Dieses Protokoll soll in erster Linie die Kommunikation mit einfachen Geräten auf einem gemeinsamen (Multi-Drop)-Kanal unterstützen. Große Pakete sollten vermieden werden.

5.7 Zeitanforderungen

Das sendende Gerät muss eine Leerlaufzeit entsprechend der Länge zweier UTF-8-Zeichen sicherstellen, bevor es auf den Kommunikationskanal zugreifen darf. Diese Leerleitungsverzögerung ist erforderlich, um Signalwandlern und/oder Multiplexern die Möglichkeit zu geben, zu erkennen, dass die Leitung unbenutzt ist.

Das sendende Gerät muss die Leitung für eine Mindestdauer entsprechend einem UTF-8-Zeichen in einen Markierungszustand versetzen, bevor es das erste Zeichen einer Meldung sendet (dies kann durch Senden eines Zeichens erreicht werden, bei dem alle Bits auf 1 gesetzt sind).

Das sendende Gerät darf die Leitung nach der Übertragung des Stoppbits des letzten Zeichens einer Meldung nicht länger als die einem vollständigen UTF-8-Zeichen entsprechende Dauer in diesem Zustand halten.

Ein Gerät muss die Übertragung seiner Antwort innerhalb der festgelegten Verzögerung `REPLY_DELAY` ab dem letzten Zeichen der Meldung, die die Antwort anfordert, beginnen.

`REPLY_DELAY` darf 200 ms nicht überschreiten. `REPLY_DELAY` wird als die Zeit ab dem Empfang des Prüfsummenzeichens des Befehls bis zur Übertragung des ersten Bytes der Antwort definiert. Der typische Wert für `REPLY_DELAY` sollte weniger als 3 ms betragen. Wenn ein Gerät mit Daten überflutet wird, kann es eine oder mehrere `BUSY`-Meldung(en) senden. (Die längste `REPLY_DELAY`-Verzögerung tritt auf, wenn lokale Daten verarbeitet werden; typischerweise ein seltenes Ereignis.)

Das PD muss seine Kommunikation als „offline“ ansehen, wenn das Intervall zwischen Meldungen, auf die es antwortet, länger als 8 s ist. Beide Seiten müssen den Verbindungszustand auf „offline“ setzen und eine neue Verbindungssequenz initiieren.

Wenn die ACU keine Antwort vor Ablauf von `REPLY_DELAY` empfängt, springt sie zum nächsten Kommunikationszyklus.

5.8 Meldungssynchronisation

Um Meldungssynchronisation zu erreichen, muss ein Peripheriegerät (PD) im Allgemeinen auf eine Zeitüberschreitung zwischen Zeichen warten und dann einen Start-Of-Message-Code (SOM-Code) suchen. Das Gerät sollte anschließend mindestens die Header-Felder empfangen und speichern sowie gleichzeitig die Prüfsumme/CRC für den Rest der Meldung berechnen. Ist die Prüfsumme korrekt, verarbeitet nur das PD die Meldung, das mit dem Adressfeld übereinstimmt. Alle anderen PDs sollten jedoch das Paket überwachen, indem sie die verbleibenden Teile des Pakets zählen, um den Beginn des nächsten Pakets vorhersehen zu können.

Tritt während des Empfangs der Meldung eine Zeitüberschreitung zwischen Zeichen auf, muss das PD die Empfangssequenz abbrechen. Unmittelbar nach dem Abbruch sollte das PD mithilfe des vorstehend beschriebenen Verfahrens eine erneute Synchronisation starten.

Der Nennwert der Zeitüberschreitung zwischen Zeichen muss 20 ms betragen. Dieser Parameter muss für besondere Betrachtungen der Kanalzeitsteuerung möglicherweise angepasst werden.

5.9 Paketformat

Alle Meldungen müssen ungeachtet ihrer Herkunft der in Tabelle 1 definierten Struktur folgen.

Tabelle 1 – Paketformat

Größe (in Byte)	Name	Bedeutung	Wert
1	SOM	Anfang der Meldung (en: start of message) ANMERKUNG 1 Jeder Meldungs-Header beginnt mit dem konstanten Wert 0x53. Dieses Zeichen wird für die Synchronisation verwendet.	0x53
1	ADDR	Physische Adresse des PD ANMERKUNG 2 Die 7 niedrigstwertigen Bits dieses Zeichens repräsentieren die Adresse des PD, an die die Meldung geleitet wird, oder die Adresse des PD, die die Antwort sendet. In einem Befehl wird das höchstwertige Bit auf 0 gesetzt und in einer Antwort wird es auf 1 gesetzt. Die Adresse 0x7F ist als besondere BROADCAST-Adresse reserviert, von der jedes PD Meldungen annimmt und an die jedes PD Antworten sendet, so, als ob sie mit seiner Kommunikationsadresse übereinstimmen würde. In der Antwortmeldung wird 0x7F zuzüglich dem Antwort-Flag (0x7F+0x80=0xFF) im Adressfeld verwendet. Da jedes PD auf 0x7F antworten wird, sollte die Verwendung der Broadcast-Adresse auf kontrollierte Konfigurationen (einzelnes PD) begrenzt werden.	0x00 bis 0x7E 0x7F = Broadcast
1	LEN_LSB	Niedrigstwertiges Byte der Paketlänge ANMERKUNG 3 Der Wert des aus zwei Zeichen bestehenden Längenfelds entspricht der Gesamtanzahl der in der Meldung enthaltenen Zeichen, einschließlich SOM bis hin zu den CKSUM- oder CRC-Zeichen.	Beliebig
1	LEN_MSB	Höchstwertiges Byte der Paketlänge ANMERKUNG 4 Der Wert des aus zwei Zeichen bestehenden Längenfelds entspricht der Gesamtanzahl der in der Meldung enthaltenen Zeichen, einschließlich SOM bis hin zu den CKSUM- oder CRC-Zeichen.	Beliebig
1	CTRL	Meldungssteuerinformationen	Siehe Tabelle 2
1	SEC_BLK_LEN	(optional) Länge des Sicherheitssteuerblocks	Beliebig
1	SEC_BLK_TYPE	(optional) Sicherheitsblocktyp ANMERKUNG 5 Der Sicherheitsblock (SB) ist optional. Sein Vorhandensein wird durch Setzen des CTRL::SBC-Flags angegeben. Der SB soll die Implementierung der Datensicherheit innerhalb des OSDP-Rahmens vereinfachen. Der SB selbst dient nicht dazu, die Art der verwendeten Sicherheitsverfahren zu definieren oder festzulegen. Es unterstützt eher die Verwendung verschiedener Sicherheitsverfahren, wie OSDP-Gerätefunktionen und die Änderung der Sicherheitsanforderungen des Clients. Für weitere Einzelheiten siehe Anhang D .	Siehe Tabelle 3

Größe (in Byte)	Name	Bedeutung	Wert
1	SEC_BLK_DATA	(optional) Sicherheitsblockdaten	Basiert auf dem Typ
1	CMND/REPLY	Befehls- oder Antwortcode ANMERKUNG 6 Befehle und Antworten bilden den eigentlichen Datenblock der Kommunikationspakete. Ein von der ACU erzeugtes Paket wird als Befehl bezeichnet, ein vom PD zurückgesendetes Paket stellt eine Antwort dar. Zweck und Bedeutung eines einzelnen Meldungspakets wird durch seinen Befehls- oder Antwortcode bestimmt. Die eigentlichen Codes und deren zugehörige Datenblöcke (sofern vorhanden) werden in den folgenden Abschnitten ausführlich beschrieben. Siehe Tabelle A.1 für eine schnelle Referenztabelle für die numerischen Befehlswerte.	Siehe A.1 und A.2
1	DATA	(optional) Datenblock	Basiert auf CMD/REPLY
4	MAC	für gesicherte Meldungen vorhanden ANMERKUNG 7 Optionaler 4 Byte langer MAC, falls das SBC-Bit in CTRL gesetzt ist.	
1	CKSUM/CRC_LSB	Prüfsumme oder niedrigstwertiges Byte von CRC-16 ANMERKUNG 8 OSDP unterstützt zwei verschiedene Formen der Fehlererkennung, wie im Absatz „CKSUM/CRC“ unter CTRL erörtert. Wenn das PD das angegebene Prüfsummen-/CRC-Verfahren nicht unterstützt oder wenn es einen Prüfsummen-/CRC-Fehler erhält, muss es eine osdp_NAK-Antwort mit error_code gleich 0x01 senden.	
1	CRC_MSB	(optional) höchstwertiges Byte von CRC-16	

Tabelle 2 – Meldungssteuerinformationen

BIT	MASKE	NAME	Bedeutung
0-1	0x03	SEQN	<p>Die Sequenznummer der Meldung wird für die Bestätigung der Meldungszustellung und für die Wiederherstellung im Fehlerfall verwendet.</p> <p>ANMERKUNG 1 Die Sequenznummer wird durch die ACU von Befehl zu Befehl erhöht, wobei null übersprungen wird: 0->1->2->3->1->... Sequenznummern ungleich null unterstützen die Wiederherstellung im Fehlerfall: die ACU bestätigt die letzte Antwort, indem sie den nächsten Befehl mit der erhöhten Sequenznummer sendet, oder sie wiederholt den Befehl, ohne die Sequenznummer zu ändern, um die Wiederholung der letzten Antwort anzufordern. Mithilfe dieses Verfahrens kann der Empfänger den Befehl ordnungsgemäß handhaben: den Befehl verarbeiten, wenn er ihn beim letzten Mal nicht korrekt empfangen hat (Fehler trat im Befehl auf) oder die bereits erstellte Antwort einfach wiederholen, ohne den Befehl erneut auszuführen (Fehler trat in der Antwort auf).</p> <p>Eine SEQN von null sollte nur für die Initialisierung der Kommunikation beim Systemstart oder nach einem Kommunikationsverlust verwendet werden. Ein Wert von null zwingt das PD dazu, seine letzte Antwort zu verwerfen und den aktuellen Befehl anzunehmen und zu verarbeiten.</p>

BIT	MASKE	NAME	Bedeutung
2	0x04	CKSUM/CRC	<p>Gesetzt – Der 16 bit lange CRC-Wert ist in den letzten 2 Bytes der Meldung enthalten.</p> <p>Frei gelassen – Die 8 bit lange Prüfsumme (CHECKSUM) ist in dem letzten Byte der Meldung enthalten.</p> <p>ANMERKUNG 2 Diese Einstellung legt das Meldungsprüfzeichenverfahren fest, das der Fehlererkennung dient.</p> <p>Der CKSUM-Wert entspricht den 8 niedrigstwertigen Bits des Zweierkomplementwerts der Summe aller vorhergehenden Zeichen der Meldung. Dieser Modus ist für Geräte mit begrenzten Ressourcen vorgesehen; neue Geräte sollten aber das CRC-Verfahren verwenden.</p> <p>Die CRC-Berechnung wird auf alle vorherigen Zeichen der Meldung angewendet. Für die Definition und den Beispielcode für den CRC-Algorithmus wird auf Anhang C verwiesen.</p>
3	0x08	SCB	<p>Gesetzt – Sicherheitssteuerblock ist in der Meldung vorhanden</p> <p>Frei gelassen – kein Sicherheitssteuerblock in der Meldung</p>
4-7	0xF0		Muss auf null gesetzt sein

Tabelle 3 – Sicherheitsblock (SB)

Größe (in Byte)	Name	Bedeutung	Wert
1	SEC_BLK_LEN	<p>Länge des Sicherheitssteuerblocks</p> <p>ANMERKUNG 1 Dieses Feld wird auf die Gesamtbytezahl des SB, einschließlich seiner selbst, festgelegt.</p>	Beliebig
1	SEC_BLK_TYPE	<p>Sicherheitsblocktyp</p> <p>ANMERKUNG 2 Dieses Feld definiert, wie der Sicherheitsblock auf den Rest der Meldung (das optionale Feld SEC_BLK_DATA[], den Befehl/die Antwort, das optionale Feld DATA[] und die Meldungsprüfzeichen) angewendet wird.</p>	In Tabelle D.1 festgelegt
n	SEC_BLK_DATA	<p>Daten variabler Länge (optional)</p> <p>ANMERKUNG 3 Dieser Abschnitt entspricht einem Feld der Größe (sec_blk_length-2). Der Dateninhalt wird für jeden Sicherheitsblocktyp (SEC_BLK_TYPE) einzeln definiert.</p> <p>Ein PD, das einen SB empfängt, aber die Verarbeitung des SB nicht unterstützt, sollte eine osdp_NAK-Antwort mit dem Fehlercode 0x05 zurücksenden.</p> <p>Ein PD, dessen Einstellungen eine verschlüsselte Verbindung erfordern und das einen Befehl ohne die entsprechenden Datensicherheitserweiterung empfängt, muss eine osdp_NAK-Antwort mit dem Fehlercode 0x06 zurücksenden.</p>	Beliebig

5.10 Mehrteilige Meldungen

5.10.1 Allgemeines

Unter bestimmten Umständen ist es erforderlich, Informationen zu senden, die nicht in eine einzige OSDP-Meldung passen. Um diese Funktion zu unterstützen, schließen bestimmte Meldungen, wie in [Abschnitt 6](#) oder [Abschnitt 7](#) definiert, Kontrollfelder zur Unterstützung von Meldungen mit mehreren Teilen ein. Dies ist für die Übermittlung von Datenblöcken vorgesehen, die die größte Menge unterstützter Nutzdaten einer einzigen OSDP-Meldung überschreiten können. Siehe [Tabelle 4](#).

Tabelle 4 – Struktur einer mehrteiligen Meldung

Größe (in Byte)	Code	Name	Bedeutung
2	0x00 bis 0xFF	MpSizeTotal (LSB)	Gesamtgröße aller Fragmente, die zusammen die Daten der mehrteiligen Meldung bilden
	0x00 bis 0xFF	MpSizeTotal (MSB)	
2	0x00 bis 0xFF	MpOffset (LSB)	Byte-Offset der Daten in diesem Fragment
	0x00 bis 0xFF	MpOffset (MSB)	
2	0x00 bis 0xFF	MpFragmentSize (LSB)	Anzahl der Datenbytes in diesem Fragment
	0x00 bis 0xFF	MpFragmentSize (MSB)	

5.10.2 Regeln für die Verwendung mehrteiliger Meldungen

Auch wenn die Meldungsstruktur mehrteilige Meldungen unterstützt, müssen die folgenden Regeln beachtet werden:

- die Datenfelder müssen in sequenzieller Reihenfolge lückenlos übertragen werden;
- bei der ersten Meldung einer mehrteiligen Meldung muss MpOffset immer auf null festgelegt sein;
- die Übertragung einer mehrteiligen Meldung darf vom Sender schon frühzeitig begrenzt werden, indem MpOffset auf denselben oder einen größeren Wert von MpSizeTotal und MpFragmentSize auf null festgelegt werden. Im Umkehrschluss muss das empfangende Gerät diesen Zustand als frühzeitige Begrenzung der mehrteiligen Übertragung erkennen;
- die Übertragungssequenz mehrteiliger Meldungen darf nicht unterbrochen werden, um andere Meldungen zwischendurch zu senden;
 - bei mehrteiligen Befehlen gilt eine einfache Regel: Sobald die ACU die Übertragung einer mehrteiligen Meldung beginnt, darf sie solange keine anderen Befehle an das PD senden, bis die gesamte Übertragung abgeschlossen ist. (Es besteht die Möglichkeit, das „abort“-Paket zu senden, um den Vorgang frühzeitig zu beenden);
 - natürlich darf die ACU bei einer mehrteiligen Übertragungssequenz an ein PD Meldungen an andere PDs zwischendurch senden, die keine Auswirkungen auf die mehrteilige Übertragung haben;
 - das PD kann einen mehrteiligen Befehl durch Senden einer NAK-Antwort mit dem Antwortcode 0x09 zurückweisen. Diese Antwort muss zum Abbruch der mehrteiligen Sequenz durch die ACU führen;
- wenn das PD den aktuellen Frame eines mehrteiligen Befehls aufgrund eines vorübergehenden Belegzustands nicht verarbeiten kann, muss es die Antwort osdp_BUSY nach 5.4 und 7.19 verwenden;
- die ACU steuert den Empfang von Antworten von einem PD, deshalb müssen keine besonderen Vorkehrungen getroffen werden, um Antworten mit mehreren Paketen zu drosseln.

5.11 Handhabung von Smartcards

Das OSDP schließt einen Satz von Meldungen ein, der für die direkte Kommunikation mit Smartcards verwendet werden kann. Dies wird als „transparenter Modus“ bezeichnet. Ein PD, das Smartcards unterstützt (siehe PDCAP-Eintrag bezüglich Smartcard-Unterstützung), stellt mehrere „Verhaltensmodi“ bereit. Diese sind in Tabelle 5 beschrieben.

Tabelle 5 – Verhaltensmodi

XRW_MODE	Beschreibung des Verhaltensmodus
0x00	Default – Es ist kein bestimmter Verhaltensmodus in Kraft. osdp_XWR-Befehle unterstützen das Zurücklesen und das Festlegen des Verhaltensmodus des PD.
0x01	Unterstützung der transparenten Smartcard-Schnittstelle. Dieser Verhaltensmodus unterstützt transparente Vorgänge zwischen dem ACU und einer Smartcard.
0x02-0xFF	reserviert für zukünftige Nutzung.

Die Kombination aus **XRW_MODE** und **XWR_PCMND** ist erforderlich, um den Befehl eindeutig zu identifizieren, und die Kombination aus **XRW_MODE** und **XRD_REPLY** dient der eindeutigen Identifizierung der Antwort. Aus Gründen der Klarheit sollten sie deshalb als Paare behandelt und zitiert werden.

Diese Spezifikation erlaubt die Unterstützung mehrerer Modi durch das PD und sogar die gleichzeitige Unterstützung dieser Modi. Die Vorgabe bezüglich mehrerer Modi ist die, dass das PD alle modusspezifischen Prozesse verarbeiten muss, die es verarbeiten kann. Rufen diese Befehle einen Konflikt hervor, muss das PD als Reaktion einen Fehlercode zurücksenden.

Bestimmte Verhaltensmodi dürfen Hintergrundvorgänge aktivieren, die Daten als osdp_XRD-Antwort auf einen osdp_POLL-Befehl zurücksenden. Befehle des Modus 0 sind in allen Modi verfügbar. Modusspezifische Befehle sollten erst nach dem erfolgreichen Umschalten in den entsprechenden Modus ausgeführt werden.

6 Befehle

6.1 Allgemeines

Die folgenden Befehle können von der ACU an das PD gesendet werden. Der im nachstehenden Abschnitt aufgeführte Wert wird in das CMND-Feld der Meldung eingetragen. Die Werte 0x40 bis 0x7F sind für zentrale Befehle reserviert. Werte außerhalb dieses Bereichs können für anwendungsspezifische und/oder proprietäre Implementierungen verwendet werden. Meldungen mit Werten von 0x40 bis 0x7F müssen die im Protokoll festgelegte Struktur für Befehle aufweisen.

Einige Befehle sind so ausgelegt, dass sie mehrere Einträge aufnehmen können. Die Auswirkungen von „n“ Einträgen innerhalb eines Befehls entsprechen denen von „n“ Befehlen in der Reihenfolge der Einträge, außer in Bezug auf die Zeitsteuerung. Die Anzahl der in diesen Befehlen enthaltenen Einträge muss durch Division der Länge des DATA-Blocks durch die Größe des Befehlseintrags, der für den jeweiligen CMND-Code in der Meldung definiert ist, berechnet werden.

Befehle mit mehreren Einträgen dürfen nicht die Rücksendung einer spezifischen Datenmeldung anfordern. Das PD muss eine osdp_ACK-Antwort zurücksenden, wenn jeder Befehlseintrag vom PD angenommen wurde; andernfalls muss das PD eine osdp_NAK-Antwort mit dem Fehlercode 0x09 „fehlerhafte(r) Befehlseintrag/-einträge“ zurücksenden, der ein Feld mit 1-Byte-Abschlusscodes mit jeweils einem Eintrag je empfangenem Befehlseintrag folgen darf.

Ergibt diese Division einen Restbetrag ungleich null, liegt ein Fehler des Befehlsformats vor. In einem solchen Fall muss das PD annehmen, dass die ACU nicht die Templategröße für diesen Befehl verwendet, die das PD verarbeiten kann; deshalb muss es die Verarbeitung aller Teile des Befehls abbrechen und eine osdp_NAK-Antwort mit dem Fehlercode 0x09 „Befehlseintrag kann nicht verarbeitet werden“ zurücksenden. In einem solchen Fall schließt das PD kein Feld mit Abschlusscodes für einzelne Befehlseinträge ein, weil es nicht versucht hat, einzelne Einträge zu verarbeiten.

Wenn alle Befehlseinträge annehmbar scheinen, muss das PD beginnen, die Befehlseinträge in der gegebenen Reihenfolge zu verarbeiten. Sind alle Befehlseinträge annehmbar, muss das PD eine osdp_ACK-Antwort zurücksenden. Andernfalls muss das PD eine osdp_NAK-Antwort mit dem Fehlercode 0x09

„Befehlseintrag kann nicht verarbeitet werden“ gefolgt von einem Feld mit Abschlusscodes für die einzelnen verarbeiteten Befehlseinträge zurücksenden. Der Wert null zeigt an, dass kein Fehler vorliegt, während der Wert 0x01 einen generischen Fehler anzeigt. Die verbleibenden Werte sind für die zukünftige Definition reserviert.

Siehe [Anhang A](#) für eine schnelle Referenztabelle für die numerischen Befehlswerte.

6.2 Abfrageanforderung (osdp_POLL)

Dieser Befehl dient der allgemeinen Abfrage. Das PD darf jede beliebige Antwort zurücksenden, die als mögliche „Abfrageantwort“ markiert ist. In der Regel wird das PD nicht eingetragene Eingabedaten oder Zustandsänderungsinformationen als Abfrageantwort zurücksenden. Siehe Tabelle 6.

Tabelle 6 – Abfrageanforderung

Feld für Paketformat	Code	Name
CMND	0x60	osdp_POLL
DATA	ausgelassen	

6.3 Anforderung des ID-Berichts (osdp_ID)

Mit diesem Befehl wird die Rücksendung des ID-Berichts des PD angefordert. Mit dem Code-Parameter der ID-Anforderung darf die erweiterte Form des ID-Blocks des PD angefordert werden. Siehe Tabelle 7.

Tabelle 7 – Anforderung des ID-Berichts

Feld für Paketformat	Code	Name
CMND	0x61	osdp_ID
DATA	0x00	Standard-ID-Block des PD senden

Die Antwort wird, wie in [7.4](#) beschrieben, formatiert.

6.4 Anforderung der Funktionen des Peripheriegeräts (osdp_CAP)

Dieser Befehl fordert die Rücksendung einer Liste der funktionalen Fähigkeiten des PD an, wie Art und Anzahl von Eingangs- und Ausgangspunkten, Ports von Lesegeräten usw. Siehe Tabelle 8.

Tabelle 8 – Anforderung der Funktionen des Peripheriegeräts

Feld für Paketformat	Code	Name
CMND	0x62	osdp_CAP
DATA	0x00	Standard-Antwort senden

Die Antwort wird, wie in [7.5](#) beschrieben, formatiert.

6.5 Anforderung des lokalen Statusberichts (osdp_LSTAT)

Dieser Befehl weist das PD an, mit einem lokalen Statusbericht zu antworten. Siehe [Tabelle 9](#).

Tabelle 9 – Anforderung des lokalen Statusberichts

Feld für Paketformat	Code	Name
CMND	0x64	osdp_LSTAT
DATA	ausgelassen	

Die Antwort wird, wie in 7.6 beschrieben, formatiert.

6.6 Anforderung des Eingangsstatusberichts (osdp_ISTAT)

Dieser Befehl weist das PD an, mit einem Eingangsstatusbericht zu antworten. Siehe Tabelle 10.

Tabelle 10 – Anforderung des Eingangsstatusberichts

Feld für Paketformat	Code	Name
CMND	0x65	osdp_ISTAT
DATA	ausgelassen	

Die Antwort wird, wie in 7.7 beschrieben, formatiert.

6.7 Anforderung des Ausgangsstatusberichts (osdp_OSTAT)

Dieser Befehl weist das PD an, mit einem Ausgangsstatusbericht zu antworten. Siehe Tabelle 11.

Tabelle 11 – Anforderung des Ausgangsstatusberichts

Feld für Paketformat	Code	Name
CMND	0x66	osdp_OSTAT
DATA	ausgelassen	

Die Antwort wird, wie in 7.8 beschrieben, formatiert.

6.8 Anforderung des Statusberichts des Lesegeräts (osdp_RSTAT)

Dieser Befehl weist das PD an, mit einem Statusbericht des Lesegeräts zu antworten. Siehe Tabelle 12.

Tabelle 12 – Anforderung des Statusberichts des Lesegeräts

Feld für Paketformat	Code	Name
CMND	0x67	osdp_RSTAT
DATA	ausgelassen	

Die Antwort wird, wie in 7.9 beschrieben, formatiert.

6.9 Befehl zur Ausgangssteuerung (osdp_OUT)

Mit diesem Befehl kann der permanente Zustand des Ausgangs verändert oder ein zeitlich abgestimmter Impulsausgang angefordert werden. Der permanente Befehl ist flüchtig (bleibt nicht über Einschaltzyklen hinaus bestehen).

Das Meldungspaket des Befehls zur Ausgangssteuerung darf mehrere 4-Byte lange Einträge enthalten. Das PD sollte anhand der Länge der gesamten Meldung die Anzahl der vorhandenen Einträge bestimmen. Die Anzahl an 4 Byte langen Einträgen sollte die Anzahl der Ausgänge nicht überschreiten, wie in Funktionscode 2 ([Anhang B](#)) angegeben. Einträge mit einer ungültigen Ausgangsnummer oder einem ungültigen Steuercode führen zu einer Antwort mit dem Fehlercode 0x09. Siehe Tabelle 13.

Tabelle 13 – Befehl zur Ausgangssteuerung

Feld für Paketformat	Code	Name	Bedeutung
CMND	0x68	osdp_OUT	
DATA 4 Bytes einmal oder mehrmals wiederholt	0x00 = erster Ausgang 0x01 = zweiter Ausgang usw.	Ausgangsnum mer	
	Siehe Tabelle 14	Steuercode	angeforderter Ausgangszustand
	Siehe 6.9	LSB des Timers	16 bit langer Timer-Wert, in Einheiten von 100 ms
		MSB des Timers	
Die Antwort kann eine der folgenden sein:			
— osdp_ACK, wie in 7.2 beschrieben			
— osdp_NAK, wie in 7.3 beschrieben			
— osdp_OSTATR, wie in 7.8 beschrieben			

Das PD darf mit einer osdp_OSTATR-Antwort antworten, um eine Zustandsänderung des Ausgangs bzw. der Ausgänge anzuzeigen, oder es kann zunächst eine osdp_ACK-Antwort zurücksenden und den Ausgangsänderungsbericht osdp_OSTATR später senden.

Tabelle 14 – Werte des Steuercodes

Steuercodewert	Bedeutung
0x00	NOP – diesen Ausgang nicht verändern
0x01	permanenten Zustand auf OFF setzen, zeitlich abgestimmten Vorgang abbrechen (sofern vorhanden)
0x02	permanenten Zustand auf ON setzen, zeitlich abgestimmten Vorgang abbrechen (sofern vorhanden)
0x03	permanenten Zustand auf OFF setzen, zeitlich abgestimmten Vorgang beenden lassen
0x04	permanenten Zustand auf ON setzen, zeitlich abgestimmten Vorgang beenden lassen
0x05	temporären Zustand auf ON setzen, bei Zeitüberschreitung permanenten Zustand wiederherstellen
0x06	temporären Zustand auf OFF setzen, bei Zeitüberschreitung permanenten Zustand wiederherstellen

6.10 Befehl zur Steuerung der Lesegerät-LEDs (osdp_LED)

Mit diesem Befehl werden die LEDs eines oder mehrerer Lesegeräte(s) gesteuert.

Sobald der Timer des temporären Befehls abläuft, kehrt die LED in den zuletzt festgelegten permanenten Zustand zurück.

Der permanente Befehl ist flüchtig (bleibt nicht über Einschaltzyklen hinaus bestehen).

Die LED blinkt mit der durch die entsprechenden Timer vorgegebenen Geschwindigkeit abwechselnd in den für ON und OFF festgelegten Farben. Wird für die beiden Farbcodes derselbe Wert festgelegt, leuchtet die LED durchgängig (blinkt nicht).

Der 16 bit lange Timer gilt nur für die temporären LED-Befehle.

Das Meldungspaket des Befehls zur LED-Steuerung darf mehrere 14 Byte lange Einträge enthalten. Das PD sollte anhand der Länge der gesamten Meldung die Anzahl der vorhandenen Einträge bestimmen. Die Anzahl der Einträge sollte die Anzahl der LEDs nicht überschreiten, wie in Funktionscode 4 ([Anhang B](#)) angegeben; der obere Grenzwert sollte jedoch nicht die Empfangspuffergröße des PD überschreiten, wie in Funktionscode 10 ([Anhang B](#)) angegeben.

Einträge mit einer ungültigen Lesegerät-/LED-Nummer führen zu einer Antwort mit dem Fehlercode 0x09.

Wenn die ACU eine temporäre Einstellung festlegt und danach versucht, eine andere temporäre Einstellung festzusetzen, sollte der aktuell aktive temporäre Befehl durch einen neuen temporären Befehl aufgehoben werden.

Die Werte von ON-Zeit und OFF-Zeit können nicht beide auf null festgelegt sein. Siehe [Tabelle 15](#).