

	DIN EN 60839-11-32 (VDE 0830-81-11-32)	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 13.320 Alarmanlagen – Teil 11-32: Elektronische Zutrittskontrollanlagen – Überwachung der Zutrittskontrolle basierend auf Web Services (IEC 60839-11-32:2016); Deutsche Fassung EN 60839-11-32:2017 Alarm and electronic security systems – Part 11-32: Electronic access control systems – Access control monitoring based on Web services (IEC 60839-11-32:2016); German version EN 60839-11-32:2017 Systèmes d'alarme et de sécurité électroniques – Partie 11-32: Systèmes de contrôle d'accès électronique – Commande de contrôle d'accès en fonction des services Web (IEC 60839-11-32:2016); Version allemande EN 60839-11-32:2017 Gesamtumfang 81 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2016-12-29 angenommene Europäische Norm als DIN-Norm ist 2017-10-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 60839-11-32 (VDE 0830-81-11-32):2016-07.

Für dieses Dokument ist das nationale Arbeitsgremium UK 713.1 „Gefahrenmelde- und Überwachungsanlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom TC 79 „Alarm and electronic security systems“ erarbeitet.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

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
EN 60839 (alle Teile)	IEC 60839 (alle Teile)	DIN EN 60839 (VDE 0830) (alle Teile)	VDE 0830
EN 60839-11-1	IEC 60839-11-1	DIN EN 60839-11-1 (VDE 0830-8-11-1)	VDE 0830-8-11-1
EN 60839-11-2	IEC 60839-11-2	DIN EN 60839-11-2 (VDE 0830-8-11-2)	VDE 0830-8-11-2
EN 60839-11-31	IEC 60839-11-31	DIN EN 60839-11-31 (VDE 0830-81-11-31)	VDE 0830-81-11-31

Nationaler Anhang NB (informativ)

Literaturhinweise

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

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

DIN EN 60839-11-2 (VDE 0830-8-11-2), *Alarmanlagen – Teil 11-2: Elektronische Zutrittskontrollanlagen – Anwendungsregeln*

DIN EN 60839-11-31 (VDE 0830-81-11-31), *Alarmanlagen – Teil 11-31: Elektronische Zutrittskontrollanlagen – Basis Kommunikationsprotokoll basierend auf Web Services*

**Alarmanlagen –
Teil 11-32: Elektronische Zutrittskontrollanlagen –
Überwachung der Zutrittskontrolle basierend auf Web Services
(IEC 60839-11-32:2016)**

Alarm and electronic security systems –
Part 11-32: Electronic access control systems –
Access control monitoring based on Web services
(IEC 60839-11-32:2016)

Systèmes d'alarme et de sécurité électroniques –
Partie 11-32: Systèmes de contrôle d'accès
électronique –
Commande de contrôle d'accès en fonction des
services Web
(IEC 60839-11-32:2016)

Diese Europäische Norm wurde von CENELEC am 2016-12-29 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, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, 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: Avenue Marnix 17, B-1000 Brüssel

© 2017 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 60839-11-32:2017 D

Europäisches Vorwort

Der Text des Dokuments 79/523/CDV, zukünftige 1. Ausgabe der IEC 60839-11-32, erarbeitet vom IEC/TC 79 „Alarm and electronic security systems“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN 60839-11-32:2017 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): 2017-09-29
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2019-12-29

Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments Patentrechte berühren können. CENELEC [und/oder CEN] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 60839-11-32:2016 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung ist unter „Literaturhinweise“ zu der aufgelisteten Norm die nachstehende Anmerkung einzutragen:

IEC 60839-11-31 ANMERKUNG Harmonisiert als **EN 60839-11-31**.

Inhalt

Seite

Europäisches Vorwort	2
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe und Abkürzungen	8
3.1 Begriffe	8
3.2 Abkürzungen	10
4 Überblick	10
4.1 Interoperabilität	10
4.2 Ereignisbehandlung	11
4.3 Architektur	11
4.4 Externe Autorisierung (Vorrangschaltung)	12
4.5 Sicherheitserwägungen	12
4.6 Türsteuerung (Zutrittspunktsteuerung)	12
4.7 Designerwägungen	12
4.7.1 Fähigkeiten auf der Instanzebene	12
4.7.2 Abruf des Zustandes	13
4.7.3 Abruf der Systemkonfiguration	13
5 Zutrittskontrolle	14
5.1 Allgemeines	14
5.2 Dienstfähigkeiten	14
5.2.1 Allgemeines	14
5.2.2 Datenstrukturen: ServiceCapabilities	14
5.2.3 GetServiceCapabilities-Befehl	14
5.3 Zutrittspunktinformationen (portalseitig)	14
5.3.1 Datenstrukturen	14
5.3.2 GetAccessPointInfoList-Befehl	16
5.3.3 GetAccessPointInfo-Befehl	16
5.4 Bereichsinformationen	17
5.4.1 Datenstrukturen AreaInfo	17
5.4.2 GetAreaInfoList-Befehl	17
5.4.3 GetAreaInfo-Befehl	18
5.5 Zutrittspunktstatus (portalseitig)	19
5.5.1 Allgemeines	19
5.5.2 Datenstrukturen: AccessPointState	19
5.5.3 GetAccessPointState-Befehl	19
5.6 Befehle der Zutrittskontrolle	19

	Seite
5.6.1 Allgemeines	19
5.6.2 Datenstrukturen: Entscheidungsaufzählung	19
5.6.3 EnableAccessPoint-Befehl	20
5.6.4 DisableAccessPoint-Befehl	20
5.6.5 ExternalAuthorization-Befehl	20
5.7 Benachrichtigungsthemen	21
5.7.1 Ereignisübersicht	21
5.7.2 Allgemeiner Aufbau eines Transaktionsereignisses	22
5.7.3 Access granted (Zutritt gewährt)	22
5.7.4 Access taken (Zutritt ist erfolgt)	23
5.7.5 Access not taken (Zutritt nicht erfolgt)	24
5.7.6 Access denied (Zutritt verwehrt)	25
5.7.7 Duress (Bedrohung)	27
5.7.8 External authorization (Override) (Externe Autorisierung) (Vorrangschaltung)	28
5.7.9 Zustandsänderungen	29
5.7.10 Änderungen an der Konfiguration	29
6 Türsteuerung (Zutrittspunktsteuerung)	30
6.1 Allgemeines	30
6.2 Dienstfähigkeiten	30
6.2.1 Allgemeines	30
6.2.2 Datenstrukturen: ServiceCapabilities (Dienstfähigkeiten)	30
6.2.3 GetServiceCapabilities-Befehl	30
6.3 Türinformationen (Zutrittspunktinformationen)	31
6.3.1 Datenstrukturen	31
6.3.2 GetDoorInfoList-Befehl	32
6.3.3 GetDoorInfo-Befehl	33
6.4 Türzustand (Zutrittspunktzustand)	34
6.4.1 Allgemeines	34
6.4.2 Datenstrukturen	34
6.4.3 GetDoorState-Befehl	37
6.5 Türsteuerungsbefehle (Zutrittspunktsteuerungsbefehle)	37
6.5.1 Allgemeines	37
6.5.2 AccessDoor-Befehl	38
6.5.3 LockDoor-Befehl	39
6.5.4 UnlockDoor-Befehl	39
6.5.5 BlockDoor-Befehl	40
6.5.6 LockDownDoor-Befehl	40
6.5.7 LockDownReleaseDoor-Befehl	41
6.5.8 LockOpenDoor-Befehl	42

6.5.9	LockOpenReleaseDoor-Befehl	43
6.5.10	DoubleLockDoor-Befehl	43
6.6	Benachrichtigungsthemen.....	44
6.6.1	Allgemeines.....	44
6.6.2	Zustandsänderungen	44
6.6.3	Änderungen an der Konfiguration	46
Anhang A (normativ)	XML-Schemata für die Zutrittskontrollschnittstelle	47
A.1	Zutrittskontrolldienst-WSDL	47
A.2	Türsteuerungsdienst-WSDL.....	54
A.3	Allgemeines Schema	65
Anhang B (informativ)	Vergleichende Darstellung der in IEC 60839-11-1 verbindlich vorgeschriebenen Funktionen.....	66
Literaturhinweise		76
Anhang ZA (normativ)	Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	77

Bilder

Bild 1 – Schematische Darstellung einer Tür mit Zutrittskontrolle.....	11
--	----

Tabellen

Tabelle 1 – GetServiceCapabilities-Befehl.....	14
Tabelle 2 – GetAccessPointInfoList-Befehl	16
Tabelle 3 – GetAccessPointInfo-Befehl.....	17
Tabelle 4 – GetAreaInfoList-Befehl	18
Tabelle 5 – GetAreaInfo-Befehl	18
Tabelle 6 – GetAccessPointState-Befehl	19
Tabelle 7 – EnableAccessPoint-Befehl	20
Tabelle 8 – DisableAccessPoint-Befehl	20
Tabelle 9 – ExternalAuthorization-Befehl	21
Tabelle 10 – GetServiceCapabilities-Befehl.....	31
Tabelle 11 – GetDoorInfoList-Befehl	33
Tabelle 12 – GetDoorInfo-Befehl.....	34
Tabelle 13 – GetDoorState-Befehl	37
Tabelle 14 – AccessDoor-Befehl	38
Tabelle 15 – LockDoor-Befehl	39
Tabelle 16 – UnlockDoor-Befehl	40
Tabelle 17 – BlockDoor-Befehl.....	40
Tabelle 18 – LockDownDoor-Befehl.....	41
Tabelle 19 – LockDownReleaseDoor-Befehl	42
Tabelle 20 – LockOpenDoor-Befehl	42
Tabelle 21 – LockOpenReleaseDoor-Befehl.....	43

	Seite
Tabelle 22 – DoubleLockDoor-Befehl.....	44
Tabelle B.1 – Anforderungen an die Zutrittspunkt-Schnittstelle	66
Tabelle B.2 – Anforderungen an Anzeige/Meldung/Hinweise/Signalisierung	67
Tabelle B.3 – Anforderungen an die Erkennung	71
Tabelle B.4 – Anforderungen an die Bedrohungssignalisierung	74
Tabelle B.5 – Anforderungen an die Vorrangschaltung.....	74
Tabelle B.6 – Anforderungen an den Selbstschutz der Anlage.....	75

Einleitung

Das vorliegende Dokument ermöglicht die Einrichtung einer Alarmanlage mit Clients, üblicherweise einem Überwachungsbedienplatz und von unterschiedlichen Herstellern stammenden Geräten – üblicherweise eine Zutrittskontrollzentrale – unter Verwendung gemeinsamer und genau festgelegter Schnittstellen.

In diesem Dokument werden nur die Daten- und Kontroll- bzw. Steuerungsinformationsströme zwischen einem Client und den Diensten ohne Bezugnahme auf irgendein physisches Gerät festgelegt, weil sich die zur Implementierung einer normgerechten elektronischen Zutrittskontrollanlage (EACS) (en: electronic access control system) erforderlichen Dienste nicht notwendigerweise in nur einem Gerät implementieren lassen, d. h. alle Dienste können auf einer Bedientafel laufen, eine Ereignisaggregatoren-Software auf einem PC, usw.

Die interne Kommunikation zwischen einer Zutrittskontrollzentrale und ihren gegebenenfalls in einem einzigen Gerät implementierten Komponenten wird in diesem Dokument nicht festgelegt.

Dieses Dokument basiert auf Arbeitsergebnissen des ONVIF Open Industry Forum. Die Spezifikation zur Zugriffskontrolle (en: ONVIF Access Control specification) und die Spezifikation zur Türkontrolle (en: ONVIF Door Control specification) sind mit diesem Dokument kompatibel.

Diesem Dokument wird von einer Reihe von computerlesbaren Schnittstellendefinitionen beigelegt:

- Zutrittskontrolldienst-WSDL, siehe Abschnitt [A.1](#);
- Türkontrolldienst-WSDL, siehe Abschnitt [A.2](#);
- allgemeines Schema, siehe Abschnitt [A.3](#).

Aufgrund der Unterschiede in den Terminologien von [IEC 60839-11-1](#) und IEC 60839-1-2 und der ONVIF-Spezifikation, auf der der vorliegende Teil von IEC 60839 basiert, sollte der Leser dem Abschnitt „Begriffe“ besondere Aufmerksamkeit widmen.

Zusätzliche Dienste, die für die Konfiguration von EACS benötigt werden, wie z. B. Festlegungen von Ablaufplänen, Handhabung von Zutrittsregeln, Lesern und Zugangsdaten, sind nicht Gegenstand dieses Dokuments. Diese Dienste werden in anderen Teilen der Normenfamilie IEC 60839-11-3x behandelt werden.

1 Anwendungsbereich

Im vorliegenden Teil von IEC 60839 wird die Webservices-Schnittstelle für elektronische Zutrittskontrollanlagen (EACS) festgelegt. Dies schließt die Auflistung der Komponenten von elektronischen Zutrittskontrollanlagen und deren logische Zusammensetzung sowie deren Zustandsüberwachung und -regelung ein. Ebenfalls eingeschlossen ist eine vergleichende Darstellung von verbindlich vorgeschriebenen und optionalen Anforderungen nach IEC 60839-11-1.

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.

Die Nutzung von Webservices und die Funktionalität des Gerätemanagements sind nicht Gegenstand dieses Dokuments. Zu weiteren Informationen siehe IEC 60839-11-31.

Dieses Dokument soll die Hersteller in keiner Weise darin einschränken, weitere Protokolle hinzuzufügen oder das hierin festgelegte Protokoll zu erweitern. Zu Regeln dazu, wie dies zu erreichen ist, siehe IEC 60839-11-31.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. 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, *Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements*

IEC 60839-11-2, *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 und IEC 60839-11-2 und die folgenden Begriffe.

ISO und IEC unterhalten Terminologiedatenbanken zur Verwendung bei der Normung unter den folgenden Adressen:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>;
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>.

ANMERKUNG In den Fällen, in denen ein in IEC 60839-11-1 und IEC 60839-11-2 definierter IEC-Begriff im vorliegenden Dokument anders definiert ist, wird der betreffende IEC-Begriff in den Abschnittsüberschriften in Klammern angegeben.

3.1.1

Zutrittspunkt

(en: access point)

Portal

(en: portal)

physischer Eingang/Ausgang, an dem der Zutritt durch eine Tür, ein Drehkreuz oder andere gesicherte Absperrungen gesteuert werden kann

Anmerkung 1 zum Begriff: Für die Anwendung dieses Dokuments wird der Zugangspunkt als eine logische Einheit angesehen, die sich aus einer physischen Tür und einem oder mehreren Lesern zusammensetzt und den Zutritt in einer Richtung steuert.

Anmerkung 2 zum Begriff: In diesem Dokument hat die Benennung „Tür“ dieselbe Bedeutung wie „Zutrittspunkt“ oder „Portal“.

3.1.2

Zutrittspunkt-Stellglied

(en: access point actuator)

Portalstellglied

(en: portal actuator)

Teil einer Zutrittskontrollanlage, welches an eine Zutrittskontrollzentrale angekoppelt ist, die den Zutritt gemäß den definierten Regeln freigibt oder sichert

Anmerkung 1 zum Begriff: In diesem Dokument wird die Benennung „Türverriegelungseinrichtung“ (en: door lock) verwendet.

3.1.3

Zustand des Zutrittspunkts (en: access point mode)

logische Betriebsart des Portals, die anzeigt, ob das Portal verriegelt, entriegelt, blockiert, im geschlossenen Zustand verriegelt oder im geöffneten Zustand verriegelt ist usw.

Anmerkung 1 zum Begriff: In diesem Dokument wird die Benennung „Betriebsart der Tür“ (en: door mode) verwendet.

3.1.4

Zutrittspunkt-Rückmelder

(en: access point sensor)

Portalsensor

(en: portal sensor)

elektrische Baugruppe, welche eingesetzt wird, um den Geöffnet- oder Geschlossen-Zustand eines Zutrittspunktes oder den Verriegelt-/Entriegelt-Zustand eines Verschlusses bzw. den Gesichert-/Ungesichert-Zustand eines elektromagnetischen Schlosses/Beschlags zu überwachen

Anmerkung 1 zum Begriff: In diesem Dokument wird die Benennung „Türüberwachung“ (en: door monitor) verwendet.

3.1.5

Vorrangschaltung für die Zutrittspunkt-Betätigung

(en: access point overriding)

Vorrangschaltung für die Portalbetätigung

(en: portal overriding)

manuelle Steuerung, um die vorgegebene Entscheidung (z. B. Freigabe/sichern/abweisen) an einem Zutrittspunkt zu umgehen

Anmerkung 1 zum Begriff: In diesem Dokument sind die Benennungen „momentaner Zutritt“ (en: momentary access) und „nicht verriegelt“ (en: unlocked) Beispiele für Vorrangschaltungen für die Zutrittspunkt-Betätigung.

3.1.6

Alarm

(en: alarm)

<Zutrittskontrollsystem> Zustand, der eine menschliche Bewertung oder einen Eingriff erfordert

Anmerkung 1 zum Begriff: Oft benutzt bei elektronischen Zutrittskontrollanlagen im Sinne von Alarmmeldung (en: alert).

Anmerkung 2 zum Begriff: In diesem Dokument wird die Benennung „Türalarm“ (en: door alarm) verwendet.

3.1.7

Client

(en: client)

Dienstanforderer

BEISPIEL Systemmanagement, Signalisierung, Konfiguration des Überwachungsbedienplatzes.

3.1.8

Gerät

(en: device)

Dienstleister

BEISPIEL Zutrittskontrollzentrale.

3.1.9

Portalseite

(en: portal side)

logische Zusammensetzung einer physischen Tür und eines oder mehrerer Leser, die den Zutritt in einer Richtung steuert

3.2 Abkürzungen

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

ACMS	System für das Management der Zugriffskontrolle (en: Access Control Management System)
BMS	Gebäudemanagementsystem (en: Building Management System)
HTTP	Hypertext-Übertragungsprotokoll (en: Hypertext Transfer Protocol)
PSIM	Verwaltung von Informationen zur physischen Sicherheit (en: Physical Security Information Management)
SOAP	einfaches Objektzugriffsprotokoll (en: Simple Object Access Protocol)
TLS	Transportschichtssicherheit (en: Transport Layer Security)
WSDL	Webservice-Beschreibungssprache (en: Web Services Description Language)

4 Überblick

4.1 Interoperabilität

Dieses Dokument stellt neue Möglichkeiten zur Sicherstellung der Interoperabilität durch Trennung der Konfiguration von Steuerung und Überwachung zur Verfügung. In herkömmlichen Systemen sendet das zentrale Managementsystem beim Start sämtliche Konfigurationsdaten an die betreffenden Geräte und erwartet, dass diese Konfigurationsdaten von anderen Clients nicht geändert werden. Stattdessen müssen Clients davon ausgehen, dass alle Informationen auf Endgeräten gespeichert werden und von anderen geändert werden können.

Eine den Festlegungen des vorliegenden Dokuments entsprechende elektronische Zutrittskontrollanlage baut auf den Grundsätzen der dienstorientierten Architektur auf. Dies ermöglicht Installationen, in denen verschiedene Komponenten unabhängig voneinander ersetzt oder aktualisiert werden können.

4.2 Ereignisbehandlung

Die Ereignisbehandlung ist ein entscheidender Teil von Operationen der Zutrittskontrolle. Zusätzlich zur Ausgabe von Ereignissen in Echtzeit stellt IEC 68839-11-31 das Mittel für den Zugriff auf am Rande gespeicherte Ereignisse zur Verfügung, um diese zu liefern, falls die Verbindung zusammenbricht.

Die Ereignisse werden je nach ihrem Ursprung und ihrem Zweck in 3 Gruppen eingeteilt:

- 1) Konfigurationsänderungseignisse. Diese Ereignisse erfolgen, um für Interoperabilität zwischen mehreren Clients zu sorgen, die ein und dasselbe Gerät gleichzeitig steuern.
- 2) Transaktionseignisse. Die Kernfunktionalität von EACS, die die tägliche Überwachung aller Zutrittsereignisse ermöglicht, dazu gehören Ereignisse der Zutrittsgewährung, die so angelegt sind, dass die betreffenden Clients über alle Detailinformationen (wer, wann und wahrscheinlich wo Zutritt erhalten hat) zu jedem spezifischen Ereignis der Zutrittsgewährung benachrichtigt werden, Ereignisse der Zutrittsverwehrung (diese können Informationen zu den Gründen enthalten, dies braucht aber nicht notwendigerweise der Fall zu sein) usw.
- 3) Alarm- und Fehlerereignisse. Diese Ereignisse ermöglichen die Überwachung des „Gesundheitszustandes“ und somit den Operatoren, im Falle eines Hardwarefehlers, eines Eindringens oder anderer verdächtiger Aktivitäten entsprechende Maßnahmen zu ergreifen.

Zu Einzelheiten über die Verfahren der Ereignisausgabe siehe IEC 68839-11-31, und für eine Liste der im vorliegenden Dokument festgelegten Ereignisse siehe 5.7.

4.3 Architektur

Dieses Dokument schreibt keine bestimmte Bauart eines physischen Geräts vor. Das in Bild 1 angegebene Schema ist nicht als Muster gedacht, sondern soll als Bezug für ein besseres Verständnis der gegebenen Spezifikation dienen. Auf der Grundlage der nachstehenden Definitionen sind verschiedene physische Konfigurationen für Türen mit Zutrittskontrolle möglich.

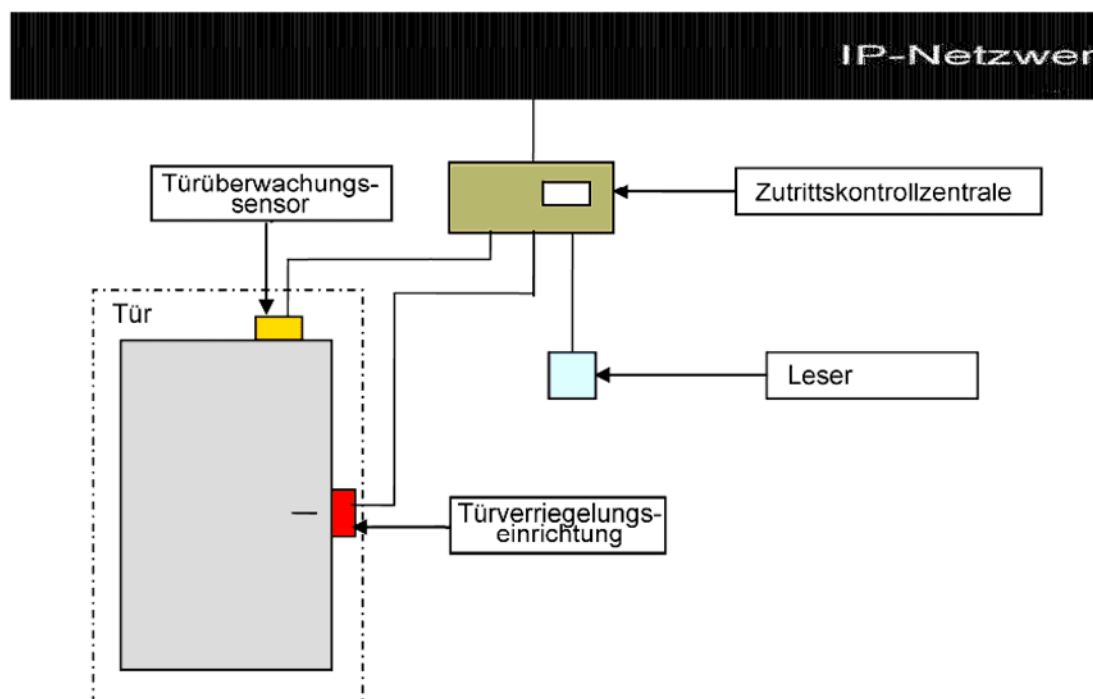


Bild 1 – Schematische Darstellung einer Tür mit Zutrittskontrolle

Türen, die von einer elektronischen Zutrittskontrollanlage gesteuert werden, sind mit den folgenden Geräten ausgerüstet:

- Einer Zutrittskontrollzentrale, die Anschlüsse für den Leser, den Türsensor, die Türverriegelungseinrichtung und zusätzliche Digitalein- und -ausgänge bereitstellt. Diese Bedientafel ermöglicht der Software, mit den physischen Einheiten zu interagieren. In einigen Fällen enthalten diese Bedientafeln auch Module zur Speicherung und für eine lokale Intelligenz, um Offline-Funktionen zur Verfügung zu stellen, so dass die Tür so funktioniert, wie es von ihr erwartet wird, und zwar selbst dann, wenn kein den oben stehenden Angaben entsprechendes Managementsystem zur Verfügung steht.
- Einem Leser, der in der Lage ist, Zugangsdaten zu lesen. In den meisten Fällen wird nur an der äußeren (nicht gesicherten) Seite der Tür ein Leser angebracht. Falls das System auch überwacht, wenn jemand den betreffenden Bereich verlässt, wird an der Tür beidseitig jeweils ein Ausweisleser angebracht.
- Einem Türüberwachungssensor, der der Bedientafel signalisiert, dass die Tür geöffnet oder geschlossen ist.
- Einer Türverriegelungseinrichtung, die von der Zutrittskontrollzentrale auf Freigabe der Tür eingestellt werden kann, z. B. dann, wenn Zugangsdaten mit der entsprechenden Autorisierung erkannt werden.

Die Zutrittskontrollzentrale wird durch das IP-Netzwerk an ein zur Überwachung und Konfiguration geeignetes System, üblicherweise einen Überwachungsbedienplatz, angeschlossen.

4.4 Externe Autorisierung (Vorrangschaltung)

Die externe Autorisierung ist eine Funktion, die dazu dient, Zutrittsentscheidungen für einen Zutrittspunkt außerhalb der Zutrittskontrollzentrale zu treffen. Die externe Autorisierung umfasst u. a. eine Richtlinie innerhalb der Zutrittskontrollzentrale, in der die Zutrittskontrollzentrale die Zutrittsentscheidungen an eine externe Einheit, wie z. B. eine Wache oder ein ACMS, delegiert.

4.5 Sicherheitserwägungen

Dieses Dokument geht davon aus, dass die EACS-Systeme für Gebäude auf der Geräteebe miteinander interagieren können. Dies bedeutet, dass umfassendere Sicherheitserwägungen angestellt werden müssen als bei der üblichen Interaktion von Clients und Servern.

In **IEC 60839-11-31** sind hierfür mehrere Verfahren festgelegt. Dazu gehören unter anderen:

- TLS für die Transportverschlüsselung;
- HTTP-Digest für die Client-Authentifizierung;
- Benutzerverwaltung und Zugriffsrichtlinien für die Autorisierung von Clients;
- IEEE 802.1X-Zertifikatsverwaltung für die Serverauthentifizierung und den Schutz vor Manipulation (en: spoofing).

Zu weiteren Informationen siehe die einschlägigen Weißbücher und Spezifikationen.

4.6 Türsteuerung (Zutrittspunktsteuerung)

Der Türsteuerungsdienst stellt Verfahren für die Steuerung von physischen Türinstanzen und die Überwachung von deren Zustand zur Verfügung.

Im vorliegenden Dokument kann sich die Benennung „Tür“ auf physische Objekte, wie z. B. eine automatische Absperrung oder eine mit einem elektrischen Schloss ausgerüstete Tür, beziehen. Drehkreuze, die den Zutritt in beiden Richtungen beschränken können, können als Türenpaar dargestellt werden.

4.7 Designerwägungen

4.7.1 Fähigkeiten auf der Instanzebene

Ein einzelnes EACS-Gerät kann über mehrere Komponenten desselben Typs verfügen. So kann z. B. eine Steuerung zwei Türen betreiben: eine am Eingang des Gebäudes, die über sichere Verriegelungs-, Über-

wachungs- und Alarmfähigkeiten verfügt, und eine weitere im Gebäudeinneren, die nur verriegelt und entriegelt werden kann.

Entsprechend lassen sich die Fähigkeiten in zwei Gruppen einteilen:

- allgemeine Dienstfähigkeiten;
- Fähigkeiten für eine bestimmte Entität innerhalb des Dienstes. Diese können auch mit der GetEvent-Properties-Funktion zusammenarbeiten, um eine feiner abgestufte Kontrolle über das System zu erhalten.

Zu weiteren Informationen siehe 5.2 und 6.2.

4.7.2 Abruf des Zustandes

Im vorliegenden Dokument werden zwei parallele Verfahren für den Abruf von Zustandsinformationen für die meisten Entitäten festgelegt:

- Get<Entity>State-Funktionen geben eine kumulative Momentaufnahme des aktuellen Zustandes bzw. Status, der Betriebsart und weiterer Laufzeitinformationen aus.
- Der Ereignisdienst gibt aktuelle und gleichbleibende Zustände von Entitäten aus. Jede Entität stellt eine Menge von Ereignissen (üblicherweise eins für jedes Feld im Statustyp) bereit, um einen Client über Zustandsänderungen zu benachrichtigen. Sofern es sich bei diesen Ereignissen um Eigenschaftsereignisse handelt, erhält ein Client jedes Mal, wenn eine neue Subskription initialisiert wird, den aktuellen Status.

4.7.3 Abruf der Systemkonfiguration

In diesem Dokument werden mehrere Get-Funktionen festgelegt, die Daten inkrementell ausgeben können. Diese Funktionen ermöglichen die Verarbeitung einer großen Anzahl von Entitäten auch bei stark eingeschränkten Ressourcen.

Um Daten inkrementell auszugeben, nutzen diese Funktionen einen Parameter, der als StartReference bezeichnet wird. StartReference ist ein geräteinterner Bezeichner, der dazu dient, den Abruf von Daten aus der letzten Position fortzusetzen, und der es einem Client ermöglicht, über einen großen Datensatz in kleineren Blöcken zu iterieren. Das Gerät behandelt eine nachvollziehbare Anzahl von unterschiedlichen StartReferences gleichzeitig, und diese haben eine nachvollziehbare Lebensdauer, was es Clients ermöglicht, vollständige Datensätze abzurufen.

Der Client übergibt immer den aufgrund einer vorangegangenen Anforderung ausgegebenen Wert, um den Abruf der Daten fortzusetzen. Ein Client verwendet dieselbe Referenz niemals mehr als einmal.

So kann die StartReference z. B. die inkrementell ansteigende Startplatznummer oder der zugrundeliegende Datenbanktransaktionsbezeichner sein.

Die ausgegebene NextStartReference wird als der StartReference-Parameter in aufeinanderfolgenden Aufrufen verwendet und kann vom Gerät bei jedem Aufruf geändert werden.

Der folgende Pseudocode zeigt, wie von einem Gerät Informationen über alle Zutrittspunkte erhalten werden können:

```
StartRef = null
do {
    Response = GetAccessPointInfoList(StartReference = StartRef)
    if (Response.AccessPointInfo != null) {
        AllAccessPoints.Append(Response.AccessPointInfo)
    }
    StartRef = Response.NextStartReference
} while (StartRef != null)
```

5 Zutrittskontrolle

5.1 Allgemeines

Dieser Dienst stellt Befehle für den Abruf von Zustandsinformationen und zur Steuerung von Zutrittspunktinstanzen zur Verfügung.

5.2 Dienstfähigkeiten

5.2.1 Allgemeines

Jedes Gerät muss Dienstfähigkeiten auf zwei Arten und Weisen zur Verfügung stellen:

- 1) mit Hilfe der GetServices-Methode des Gerätedienstes, falls IncludeCapability wahr ist. Zu weiteren Einzelheiten siehe IEC 68839-11-31;
- 2) mit Hilfe der GetServiceCapabilities-Methode.

5.2.2 Datenstrukturen: ServiceCapabilities

Die Dienstfähigkeiten spiegeln optionale Funktionalitäten eines Dienstes wider. Diese Information ist statisch und ändert sich im Verlauf des Gerätebetriebs nicht. Die folgenden Fähigkeiten stehen zur Verfügung:

- **MaxLimit**
Die maximale Anzahl der aufgrund einer einzelnen Get<Entity>List- oder Get<Entity>-Anforderung ausgegebenen Einträge. Das Gerät darf in einer einzigen Antwort niemals mehr als diese Anzahl von Entitäten ausgeben.

5.2.3 GetServiceCapabilities-Befehl

Diese Operation gibt die Fähigkeiten des Zutrittskontrolldienstes aus. Dieser Befehl muss von allen Geräten unterstützt werden, wie in Tabelle 1 beschrieben.

Tabelle 1 – GetServiceCapabilities-Befehl

GetServiceCapabilities		Zugriffsklasse: PRE_AUTH
Nachrichtenname	Beschreibung	
GetServiceCapabilitiesRequest	Dies muss eine leere Nachricht sein.	
GetServiceCapabilitiesResponse	Diese Nachricht enthält: – „Capabilities“: Die Fähigkeiten-Antwortnachricht enthält die angeforderten Fähigkeiten des Zutrittskontrolldienstes in einer hierarchisch gegliederten XML-Fähigkeitsstruktur. tac:ServiceCapabilities Capabilities [1][1]	
Fehlercodes	Beschreibung	
	Keine befehlspezifischen Fehler.	

5.3 Zutrittspunktinformationen (portalseitig)

5.3.1 Datenstrukturen

5.3.1.1 AccessPointInfo

Die AccessPointInfo-Struktur enthält grundlegende Informationen über eine Zutrittspunktinstanz (en: access point instance). Ein Zutrittspunkt definiert eine Entität, der Zugangsdaten erteilt werden können oder der der

Zutritt verwehrt werden kann. `AccessPointInfo` stellt grundlegende Informationen darüber zur Verfügung, wie der gerichtete Zutritt durch eine Tür (aus welchem Bereich in welchen Bereich) gesteuert wird.

Dieselbe Tür kann von mehreren Zutrittspunkten gesteuert werden. Ein typischer Fall ist ein Zutrittspunkt für den Eingang und ein weiterer für den Ausgang, die beide auf dieselbe Tür verweisen.

Ein Gerät muss für jede Zutrittspunktinstanz die folgenden Felder bereitstellen:

- **Token**
Einen innerhalb des Dienstes eindeutigen Bezeichner des Zutrittspunktes.
- **Name**
Einen für den Benutzer lesbaren Namen. Dieser muss eine Länge von bis zu 64 Zeichen haben können.
- **Entity**
Verweis auf die für die Zutrittskontrolle verwendete Entität; der Entitätstyp darf mit Hilfe des nachstehend erläuterten optionalen `EntityType`-Feldes festgelegt werden, üblicherweise jedoch handelt es sich um eine Tür.
- **Capabilities**
Die Fähigkeiten des Zutrittspunktes.

Um weitere Informationen zur Verfügung zu stellen, darf das Gerät darüber hinaus die folgenden optionalen Felder enthalten:

- **Description**
Optional eine für den Benutzer lesbare Beschreibung des Zutrittspunktes. Diese muss eine Länge von bis zu 1 024 Zeichen haben können.
- **AreaFrom**
Optional einen Verweis auf den Bereich, von dem ausgehend Zutritt erbeten wird.
- **AreaTo**
Optional einen Verweis auf den Bereich, zu dem Zutritt erbeten wird.
- **EntityType**
Optional den Entitätstyp; ist dieser nicht vorhanden, so sollte von einem Türtyp nach der Festlegung des Türsteuerungsdienstes ausgegangen werden. Dieser kann auch durch den QName-Wert „tdc:Door“ dargestellt werden, falls tdc der Namensraum des Türsteuerungsdienstes ist: <http://www.onvif.org/ver10/doorcontrol/wsd>. Dieses Feld ist für zukünftige Erweiterungen vorgesehen; es ermöglicht die Erweiterung des Zutrittspunktes, um auch andere Entitätstypen als Türen abdecken zu können.

5.3.1.2 AccessPointCapabilities

Die `AccessPoint`-Fähigkeiten spiegeln optionale Funktionalitäten einer bestimmten physischen Entität wider. Verschiedene Zutrittspunktinstanzen dürfen unterschiedliche Mengen von Fähigkeiten haben. Diese Informationen können sich im Verlauf des Gerätebetriebs ändern, z. B. dann, wenn Hardwareeinstellungen geändert werden. Die folgenden Fähigkeiten stehen zur Verfügung:

- **DisableAccessPoint**
Zeigt an, ob die betreffende Zutrittspunktinstanz die Befehle `EnableAccessPoint` und `DisableAccessPoint` unterstützt.
- **Duress**
Zeigt an, ob die betreffende Zutrittspunktinstanz die Generierung von Bedrohungsereignissen unterstützt.
- **AnonymousAccess**
Zeigt an, ob der betreffende Zutrittspunkt über eine REX oder eine andere Eingabe verfügt, die den anonymen Zutritt ermöglicht.
- **AccessTaken**
Zeigt an, ob die betreffende Zutrittspunktinstanz die Generierung von `AccessTaken`- und `AccessNotTa`-Ereignissen unterstützt.

Falls sowohl AnonymousAccess als auch AccessTaken wahr sind, zeigt dies an, dass auch die anonymen Versionen von AccessTaken und AccessNotTaken unterstützt werden.

– **ExternalAuthorization**

Zeigt an, ob die betreffende AccessPoint-Instanz die ExternalAuthorization-Operation und die Generierung von Anforderungsereignissen unterstützt.

Falls sowohl AnonymousAccess als auch ExternalAuthorization wahr sind, zeigt dies an, dass auch die anonyme Version unterstützt wird.

5.3.2 GetAccessPointInfoList-Befehl

Diese Operation dient zur Anforderung einer Liste aller vom Gerät bereitgestellten AccessPointInfo-Elemente. Dieser Befehl muss von allen Geräten unterstützt werden, wie in Tabelle 2 beschrieben.

Wird diese Methode aufgerufen, so muss dies zur Ausgabe einer StartReference führen, falls nicht alle Daten ausgegeben wurden und weitere Daten zur Verfügung stehen. Die Verweisung muss für den Abruf des nächsten Datensatzes gültig sein. Zu weiteren Einzelheiten siehe 4.7.3.

Die ausgegebene Anzahl an Elementen darf nicht größer als der Grenzwertparameter sein.

Tabelle 2 – GetAccessPointInfoList-Befehl

GetAccessPointInfoList		Zugriffsklasse: READ_SYSTEM
Nachrichtenname	Beschreibung	
GetAccessPointInfoListRequest	Diese Nachricht enthält: – "Limit": die höchste Anzahl an auszugebenden Einträgen. Falls "Limit" weggelassen wird oder der damit angegebene Grenzwert den vom Gerät unterstützten Wert überschreitet, muss das Gerät die von ihm unterstützte höchste Anzahl an Einträgen ausgeben. – "StartReference": Beginne mit der Ausgabe von Einträgen ab diesem Startverweis. Falls nicht festgelegt, müssen Einträge mit dem Anfang des Datensatzes beginnen. xs:int Limit [0][1] xs:stringStartReference [0][1]	
GetAccessPointInfoListResponse	Diese Nachricht enthält: – "NextStartReference": StartReference, die bei nächstem Aufruf zum Erhalt der folgenden Elemente zu verwenden ist. Falls diese nicht vorhanden ist, sind keine weiteren Elemente mehr verfügbar. – "AccessPointInfo": eine Liste von AccessPointInfo-Elementen. xs:string NextStartReference [0][1] tac:AccessPointInfoAccessPointInfo [0][unbounded]	
Fehlercodes	Beschreibung	
env:Sender ter:InvalidArgVal ter:InvalidStartReference	StartReference ist ungültig oder das entsprechende Zeitlimit wurde überschritten. Der Client muss mit dem Abruf noch einmal von vorn beginnen.	

5.3.3 GetAccessPointInfo-Befehl

Diese Operation dient zur Anforderung einer Liste von AccessPointInfo-Elementen, die zu den angegebenen Token passen. Dieser Befehl muss von allen Geräten unterstützt werden, wie in Tabelle 3 beschrieben.

Das Gerät muss Token, die es nicht auflösen kann, ignorieren und eine leere Liste ausgeben, wenn keine Elemente vorliegen, die zu festgelegten Token passen. Das Gerät darf in diesem Fall keinen Fehler ausgeben.

Falls die Anzahl der angeforderten Elemente den als MaxLimit angegebenen Wert überschreitet, muss ein TooManyItems-Fehler ausgegeben werden.

Tabelle 3 – GetAccessPointInfo-Befehl

GetAccessPointInfo		Zugriffsklasse: READ_SYSTEM
Nachrichtenname	Beschreibung	
GetAccessPointInfoRequest	Diese Nachricht enthält: – "Token": Token von abrufbaren AccessPointInfo-Elementen. pt:ReferenceTokenToken [1][unbounded]	
GetAccessPointInfoResponse	Diese Nachricht enthält: – "AccessPointInfo": eine Liste von AccessPointInfo-Elementen. tac:AccessPointInfoAccessPointInfo [0][unbounded]	
Fehlercodes	Beschreibung	
env:Sender ter:InvalidArgs ter:TooManyItems	Es wurden zu viele Elemente angefordert, siehe die MaxLimit-Fähigkeit.	

5.4 Bereichsinformationen

5.4.1 Datenstrukturen ArealInfo

Die ArealInfo-Struktur enthält grundlegende Informationen über einen Bereich. Das Gerät muss die folgenden Felder für jeden Bereich zur Verfügung stellen:

- **Token**
Einen innerhalb des Dienstes eindeutigen Bezeichner des Bereiches.
- **Name**
Einen für den Benutzer lesbaren Namen. Dieser muss eine Länge von bis zu 64 Zeichen haben können.
Um weitere Informationen zur Verfügung zu stellen, darf das Gerät darüber hinaus die folgenden optionalen Felder enthalten:
- **Description**
Eine für den Benutzer lesbare Beschreibung des Bereichs. Diese muss eine Länge von bis zu 1 024 Zeichen haben können.

5.4.2 GetArealInfoList-Befehl

Diese Operation dient zur Anforderung einer Liste aller vom Gerät bereitgestellten ArealInfo-Elemente. Dieser Befehl muss von allen Geräten unterstützt werden, wie in [Tabelle 4](#) beschrieben.

Wird diese Methode aufgerufen, so muss dies zur Ausgabe einer StartReference führen, falls nicht alle Daten ausgegeben wurden und weitere Daten zur Verfügung stehen. Die Verweisung muss für den Abruf des nächsten Datensatzes gültig sein. Zu weiteren Einzelheiten siehe [4.7.3](#).

Die ausgegebene Anzahl an Elementen darf nicht größer als der Grenzwertparameter sein.

Tabelle 4 – GetAreaInfoList-Befehl

GetAreaInfoList		Zugriffsklasse: READ_SYSTEM
Nachrichtenname	Beschreibung	
GetAreaInfoListRequest	Diese Nachricht enthält: – "Limit": die höchste Anzahl an auszugebenden Einträgen. Falls "Limit" weggelassen wird oder der damit angegebene Grenzwert den vom Gerät unterstützten Wert überschreitet, muss das Gerät die von ihm unterstützte höchste Anzahl an Einträgen ausgeben. – "StartReference": Beginne mit der Ausgabe von Einträgen ab diesem Startverweis. Falls nicht festgelegt, müssen Einträge mit dem Anfang des Datensatzes beginnen. xs:int Limit [0][1] xs:string StartReference [0][1]	
GetAreaInfoListResponse	Diese Nachricht enthält: – "NextStartReference": StartReference, die bei nächstem Aufruf zum Erhalt der folgenden Elemente zu verwenden ist. Falls diese nicht vorhanden ist, sind keine weiteren Elemente mehr verfügbar. – "AreaInfo": Liste von AreaInfo-Elementen. xs:string NextStartReference [0][1] tac:AreaInfoAreaInfo [0][unbounded]	
Fehlercodes	Beschreibung	
env:Sender ter:InvalidArgVal ter:InvalidStartReference	StartReference ist ungültig oder das entsprechende Zeitlimit wurde überschritten. Der Client muss mit dem Abruf noch einmal von vorn beginnen.	

5.4.3 GetAreaInfo-Befehl

Diese Operation dient zur Anforderung einer Liste von AreaInfo-Elementen, die zu den angegebenen Token passen. Dieser Befehl muss von allen Geräten unterstützt werden, wie in Tabelle 5 beschrieben.

Das Gerät muss Token, die es nicht auflösen kann, ignorieren und darf eine leere Liste ausgeben, wenn keine Elemente vorliegen, die zu festgelegten Token passen.

Falls die Anzahl der angeforderten Elemente den als MaxLimit angegebenen Wert überschreitet, muss ein TooManyItems-Fehler ausgegeben werden.

Tabelle 5 – GetAreaInfo-Befehl

GetAreaInfo		Zugriffsklasse: READ_SYSTEM
Nachrichtenname	Beschreibung	
GetAreaInfoRequest	Diese Nachricht enthält: – "Token": Token von abrufbaren AreaInfo-Elementen. pt:ReferenceTokenToken [1][unbounded]	
GetAreaInfoResponse	Diese Nachricht enthält: – "AreaInfo": Liste von AreaInfo-Elementen. tac:AreaInfoAreaInfo [0][unbounded]	
Fehlercodes	Beschreibung	
env:Sender ter:InvalidArgs ter:TooManyItems	Es wurden zu viele Elemente angefordert, siehe die MaxLimit-Fähigkeit.	

5.5 Zutrittspunktstatus (portalseitig)

5.5.1 Allgemeines

Der Zustand des Zutrittspunkts wird von einer Reihe von Operationen bestimmt, die an ihm in Abhängigkeit von seinen Fähigkeiten ausgeführt werden können; siehe die Zutrittspunktfähigkeiten in 5.3.1.2.

5.5.2 Datenstrukturen: AccessPointSize

Der AccessPointSize enthält Informationen zum Zustand bzw. Status eines Zutrittspunktes. Das Gerät muss für jede Zutrittspunktinstanz die folgenden Felder bereitstellen:

- **Enabled**
Zeigt an, dass der Zutrittspunkt aktiviert ist. Standardmäßig muss dieser Feldwert wahr sein, falls die DisableAccessPoint-Fähigkeit nicht unterstützt wird.

5.5.3 GetAccessPointSize-Befehl

Diese Operation dient zur Abfrage des AccessPointSize für die durch den Token angegebene Zutrittspunktinstanz. Dieser Befehl muss von allen Geräten unterstützt werden, wie in Tabelle 6 beschrieben.

Tabelle 6 – GetAccessPointSize-Befehl

GetAccessPointSize		Zugriffsklasse: READ_SYSTEM_SENSITIVE
Nachrichtenname	Beschreibung	
GetAccessPointSizeRequest	Diese Nachricht enthält: – "Token": Token der Zutrittspunktinstanz, für die der AccessPointSize abzufragen ist. pt:ReferenceToken Token [1][1]	
GetAccessPointSizeResponse	Diese Nachricht enthält: – "AccessPointSize": AccessPointSize-Element. tac:AccessPointSizeAccessPointSize [1][1]	
Fehlercodes	Beschreibung	
env:Sender ter:InvalidArgVal ter:NotFound	Dieser Zutrittspunkt wurde nicht gefunden.	

5.6 Befehle der Zutrittskontrolle

5.6.1 Allgemeines

Die Dienststeuerungsbefehle enthalten Operationen, die die Änderung von Zutrittspunktzuständen und die Steuerung von Zutrittspunkten ermöglichen.

5.6.2 Datenstrukturen: Entscheidungsaufzählung

Die Entscheidungsaufzählung stellt die Möglichkeit der Wahl zwischen zwei verfügbaren Optionen für eine Bitte um Gewährung des Zutritts (en: access request) dar:

- **Granted**
Die Entscheidung lautet, Zutritt zu gewähren.
- **Denied**
Die Entscheidung lautet, den Zutritt zu verwehren.

5.6.3 EnableAccessPoint-Befehl

Diese Operation ermöglicht die Aktivierung eines Zutrittspunkts.

Ein Gerät, das signalisiert, dass es die DisableAccessPoint-Fähigkeit für eine bestimmte Zutrittspunktinstanz unterstützt, muss auch diesen Befehl unterstützen, wie in Tabelle 7 beschrieben.

Tabelle 7 – EnableAccessPoint-Befehl

EnableAccessPoint		Zugriffsklasse: ACTUATE
Nachrichtenname	Beschreibung	
EnableAccessPointRequest	<i>Diese Nachricht enthält:</i> – "Token": den Token der zu aktivierenden Zutrittspunktinstanz. pt:ReferenceToken Token [1][1]	
EnableAccessPointResponse	Dies muss eine leere Nachricht sein.	
Fehlercodes	Beschreibung	
env:Sender ter:InvalidArgVal ter:NotFound	Der angegebene Token wurde nicht gefunden.	
env:Receiver ter:ActionNotSupported ter:NotSupported	Diese Operation wird nicht unterstützt.	

5.6.4 DisableAccessPoint-Befehl

Diese Operation ermöglicht die Deaktivierung eines Zutrittspunkts.

Jedes Gerät, das signalisiert, dass es die DisableAccessPoint-Fähigkeit für eine bestimmte Zutrittspunktinstanz unterstützt, muss auch diesen Befehl unterstützen, wie in Tabelle 8 beschrieben.

Tabelle 8 – DisableAccessPoint-Befehl

DisableAccessPoint		Zugriffsklasse: ACTUATE
Nachrichtenname	Beschreibung	
DisableAccessPointRequest	<i>Diese Nachricht enthält:</i> – "Token": den Token der zu deaktivierenden Zutrittspunktinstanz. pt:ReferenceToken Token [1][1]	
DisableAccessPointResponse	Dies muss eine leere Nachricht sein.	
Fehlercodes	Beschreibung	
env:Sender ter:InvalidArgVal ter:NotFound	Der angegebene Token wurde nicht gefunden.	
env:Receiver ter:ActionNotSupported ter:NotSupported	Diese Operation wird nicht unterstützt.	

5.6.5 ExternalAuthorization-Befehl

Diese Operation ermöglicht es, die Entscheidung über die Gewährung oder Verwehrung des Zutritts an einer Zutrittspunktinstanz zu treffen.

Ein Gerät, das signalisiert, dass es die ExternalAuthorization-Fähigkeit für eine bestimmte Zutrittspunktinstanz unterstützt, muss auch diese Methode unterstützen, wie in Tabelle 9 beschrieben.

Tabelle 9 – ExternalAuthorization-Befehl

ExternalAuthorization		Zugriffsklasse: ACTUATE
Nachrichtenname	Beschreibung	
ExternalAuthorizationRequest	Diese Nachricht enthält: – "AccessPointToken": den Token einer Zugriffspunktinstanz; – "CredentialToken": optional den Token der einbezogenen Zugangsdaten; – "Reason": optional den Entscheidungsgrund; – "Decision": die Entscheidung – Zutritt gewährt oder verwehrt. pt:ReferenceToken AccessPointToken [1][1] pt:ReferenceToken CredentialToken [0][1] xs:string Reason [0][1] tac:Decision Decision [1][1]	
ExternalAuthorizationResponse	Dies muss eine leere Nachricht sein.	
Fehlercodes	Beschreibung	
env:Sender ter:InvalidArgVal ter:NotFound	Der Zutrittspunkt wurde nicht gefunden.	
env:Receiver ter:ActionNotSupported ter:NotSupported	Diese Operation wird nicht unterstützt.	

5.7 Benachrichtigungsthemen

5.7.1 Ereignisübersicht

Der AccessControl-Dienst legt die für Zutrittstransaktionen zu verwendenden Ereignisse fest, so wird z. B. eine Bitte um Gewährung des Zutritts gestellt und der Zutritt gewährt oder verwehrt, wenn eine Bedrohung festgestellt wird und eine wichtige Konfiguration geändert wurde.

Die Hauptthemen für Zutrittstransaktionsereignisse sind:

- tns1:AccessControl/AccessGranted/ – wenn der Zutritt gewährt wird.
- tns1:AccessControl/AccessTaken/ – wenn der Zutritt nach Gewährung erfolgte.
- tns1:AccessControl/AccessNotTaken/ – wenn der Zutritt nach Gewährung nicht erfolgte.
- tns1:AccessControl/Denied/ – wenn der Zutritt verwehrt wird.
- tns1:AccessControl/Duress – wenn eine Bedrohung festgestellt wird.
- tns1:AccessControl/Request/ – wenn eine externe Autorisierung angefordert wird oder die dafür geltende Zeitbeschränkung überschritten wurde.

Das Hauptthema für Statusaktualisierungen ist:

- tns1:AccessPoint/State/ – für Statusaktualisierungen.

Die Hauptthemen für Benachrichtigungen über Konfigurationsänderungen sind:

- tns1:Configuration/AccessPoint – wenn die Zutrittspunktconfiguration geändert wurde.
- tns1:Configuration/Area – wenn die Bereichskonfiguration geändert wurde.