

	DIN EN IEC 62676-2-33 (VDE 0830-71-2-33)	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 „etx Elektrotechnik + Automation“ bekannt gegeben worden.	VDE

ICS 13.310; 33.160.40

Einsprüche bis 2022-02-10

Entwurf

**Videoüberwachungsanlagen für Sicherungsanwendungen –
Teil 2-33: Cloud-Uplink und Fernzugriff von Managementsystemen
(IEC 79/642/CDV:2021);
Deutsche und Englische Fassung prEN IEC 62676-2-33:2021**

Video surveillance systems for use in security applications –
Part 2-33: Cloud uplink and remote management system access
(IEC 79/642/CDV:2021);
German and English version prEN IEC 62676-2-33:2021

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité –
Partie 2-33: Liaison montante au nuage et accès au système de gestion à distance
(IEC 79/642/CDV:2021);
Version allemande et anglaise prEN IEC 62676-2-33:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-12-10 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 51 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments prEN IEC 62676-2-33:2021-03 „Videoüberwachungsanlagen für Sicherungsanwendungen – Teil 2-33: Cloud-Uplink und Fernzugriff von Managementsystemen“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 79/642/CDV:2021-03 „Video surveillance systems for use in security applications – Part 2-33: Cloud uplink and remote management system access“ unverändert in den Entwurf prEN IEC 62676-2-33:2021-03 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom IEC/TC 79 „Alarm and electronic security systems“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und unterliegt dem Copyright der IEC . Das Dokument wurde den nationalen Komitees zur Stellungnahme vorgelegt.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für dieses Dokument ist das nationale Arbeitsgremium DKE/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.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnichtsnummer, 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.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

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.

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

**Videoüberwachungsanlagen für Sicherungsanwendungen –
Teil 2-33: Cloud-Uplink und Fernzugriff von Managementsystemen**

Inhalt

Seite

Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Überblick	6
4.1 Fernzugriff	7
4.2 Cloud-Uplink	8
5 Anforderungen	8
5.1 Funktionale Anforderungen	8
5.2 Protokollanforderungen	9
6 Ressourcenadressierung	10
6.1 Einleitung	10
6.2 Entfernte Token	10
6.3 Token-Kontext	11
7 Abfrage von Ressourcen	11
7.1 Allgemeines	11
7.2 Ressourcenereignis	11
7.3 Ortsfilter	12
7.4 Präfix-Filter	12
7.5 Aufgabenbereichsfilter	12
7.6 Auswahlfilter	13
7.7 Live-Überprüfungen	13
7.8 Beispiele (informativ)	13
7.8.1 Live-Video	13
7.8.2 Kriminaltechnik	14
8 Uplink	14
8.1 Protokoll	14
8.1.1 Verbindungsherstellung	14
8.1.2 Verbindungsverwaltung	15
8.1.3 Authentifizierung	15
8.1.4 HTTP/2-Frames	16
8.1.5 HTTP-Transaktionen	16
8.2 Konfigurationsschnittstelle	16
8.2.1 Konfigurationsparameter	16
8.2.2 GetUplinks	16
8.2.3 SetUplink	16

8.2.4	DeleteUplink	17
8.2.5	Fähigkeiten	17
Anhang A (informativ) Adressierungsschema		18
A.1	Überblick.....	18
A.2	Felddefinitionen	18
A.2.1	Gebietscode	18
A.2.2	Dienststellencode	18
A.2.3	Gerätetypcode	20
A.2.4	Seriennummer	21
A.2.5	Beispiele	22
Anhang B (informativ) APIs mit Tokenanpassung.....		23
B.1	Ansehen von Live-Videos.....	23
B.2	Steuerung von PTZ-Kameras.....	23
B.3	Abruf von Aufzeichnungen	23
B.4	Weiterleitung von Ereignissen.....	23
Literaturhinweise.....		24
Tabellen		
Tabelle A1 – Elemente des Gebietscodes		18
Tabelle A2 – Dienststellencodes		18
Tabelle A3 – Gerätetypcodes		20
Tabelle A4 – Seriennummerwert		21
Bilder		
Bild 1 – Beispiel eines hierarchischen Systems		7
Bild 2 – Vom Client hergestellte Standardverbindung		8
Bild 3 – Verbindungsaufbau seitens des Gerätes		8
Bild 4 – Abfolge der Verbindungsherstellung		15
Bild A1 – Felder des Geräte-ID-Schemas		18

Einleitung

Überwachungssysteme werden in Projekten der öffentlichen Sicherheit benötigt, um gesetzlichen Vorschriften nachzukommen, die öffentliche Sicherheit zu gewährleisten und die Polizei bei der Durchführung kriminaltechnischer Analysen zu unterstützen. Aus organisatorischen und sicherheitstechnischen Gründen werden große Überwachungssysteme in Segmente unterteilt, welche zu Informationssilos werden können. Diese Spezifikation stellt eine standardisierte Schnittstelle für Managementsysteme bereit, über die berechnete Einheiten leicht auf entfernt liegende Informationen zugreifen können, indem sie den gleichen Mechanismus wie für den Zugriff auf lokale Informationen anwenden.

1 Anwendungsbereich

Dieser Teil der Normenreihe IEC 62676 legt eine Schnittstelle für Managementsysteme sowie einen Mechanismus für den operativen Fernzugriff auf physische Sicherheitsgeräte, z. B. Videoüberwachungsgeräte und -systeme, fest. Im Bereich der Videoüberwachung liegt der Schwerpunkt der Anwendungsfälle auf dem Zugriff auf Live-Videos und dem Abrufen von Aufzeichnungen. Der in dieser Spezifikation festgelegte Mechanismus ist nicht auf Überwachungsanwendungen beschränkt, sondern eignet sich auch für den Fernzugriff auf Sicherheitssysteme und elektronische Zutrittskontrollanlagen. Die Konfiguration von Geräten und Managementsystemen liegt außerhalb des Anwendungsbereiches dieser Spezifikation.

Abschnitt 4 enthält eine Einführung in den Fernzugriff von Managementsystemen. In [Abschnitt 5](#) sind Anforderungen an das Protokoll festgelegt. [Abschnitt 6](#) erweitert das tokenbasierte Ressourcenadressierungsschema der zugrunde liegenden Spezifikation [IEC 60839-11-31](#). In [Abschnitt 7](#) ist beschrieben, wie Informationen über entfernte Ressourcen abgerufen werden können. In [Abschnitt 8](#) ist festgelegt, wie eine Verbindung zu Geräten hergestellt werden kann, die nicht direkt erreichbar sind, weil sie sich beispielsweise hinter einer Firewall befinden.

2 Normative Verweisungen

IANA Media Type Reference

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*

[IEC 60839-11-31](#), *Alarm and electronic security systems – Part 11-31: Electronic access control systems – Core interoperability protocol based on WebServices*

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol, Version 1.2*

IETF RFC 6125, *Representation and Verification of Domain-Based Application Service
Identity within Internet Public Key Infrastructure Using X.509 (PKIX)
Certificates in the Context of Transport Layer Security (TLS)*

IETF RFC 7540, *Hypertext Transfer Protocol Version 2 (HTTP/2)*

3 Begriffe

3.1

Ressource

In diesem Dokument bezieht sich die Bezeichnung auf eine Ressource nach IEC 62676-2, die über ein Token adressiert werden kann

3.2

Uplink

Die vom lokalen Dienst aufgebaute Verbindung zum entfernten Client

3.3

VSS

Videoüberwachungssystem

4 Überblick

Die IEC-Spezifikationen 62676-2-31 und 62676-2-32 enthalten eine ausführliche Protokolldefinition für die Interaktion mit Videoüberwachungssystemen, wie Kameras und digitale Rekorder. Analog dazu ist in [IEC 60839-11-32](#) und [IEC 60839-11-33](#) beschrieben, wie elektronische Zutrittskontrollanlagen überwacht und konfiguriert werden. Alle Spezifikationen basieren auf [IEC 60839-11-31](#), in der ein

Kommunikationsmechanismus auf der Basis von Webservices festgelegt ist. Diese Spezifikation erweitert IEC 60839-11-31 durch die Funktionen Cloud-Konnektivität und Fernadressierung des Frameworks. Es ist zu beachten, dass diese Spezifikation keine domänenspezifischen Einzelheiten enthält, da alle in den oben genannten Spezifikationen definierten Schnittstellen ohne Anpassungen anwendbar sind. Deshalb deckt diese Spezifikation die Integration verschiedenster physischer Sicherheitssysteme in ein beliebiges Managementsystem ab. Dieses Dokument beschreibt, wie sich ein entfernter Client oder ein Managementsystem mit Ressourcen wie Kameras verbinden lässt. Der hier gezeigte Ansatz ermöglicht die Skalierung über mehrere Hierarchien hinweg. In den Beispielen im Abschnitt „Überblick“ wird das Grundprinzip des Mechanismus mithilfe zweier Ebenen dargestellt, der sogenannten „niedrigeren Ebene“ und der „höheren Ebene“. In diesem System kann ein VSS auf höherer Ebene eine Ressource, wie die Geräteinformationen, von einem VSS auf niedrigerer Ebene abrufen, um entsprechende Aktionen für verschiedene Geräte auszulösen, die mit dem VSS auf niedrigerer Ebene verbunden sind.

Der Zugriff auf das entfernte VSS kann strenge Authentifizierungsbeschränkungen erfordern. Einzelheiten zur Server- und Clientauthentifizierung sind in den auf Webservices basierenden Spezifikationen enthalten.

4.1 Fernzugriff

Bild 1 zeigt die typische Topologie eines Managementsystems, wie sie bei größeren Installationen eingesetzt wird. Die Videoüberwachungssysteme auf niedrigerer Ebene schließen zahlreiche Überwachungskameras und andere Ausrüstung zur Überwachung eines Bereiches eines Geländes oder eines Stadtteils ein. Videomanagementsysteme auf höherer Ebene ermöglichen die Überwachung größerer Areale.

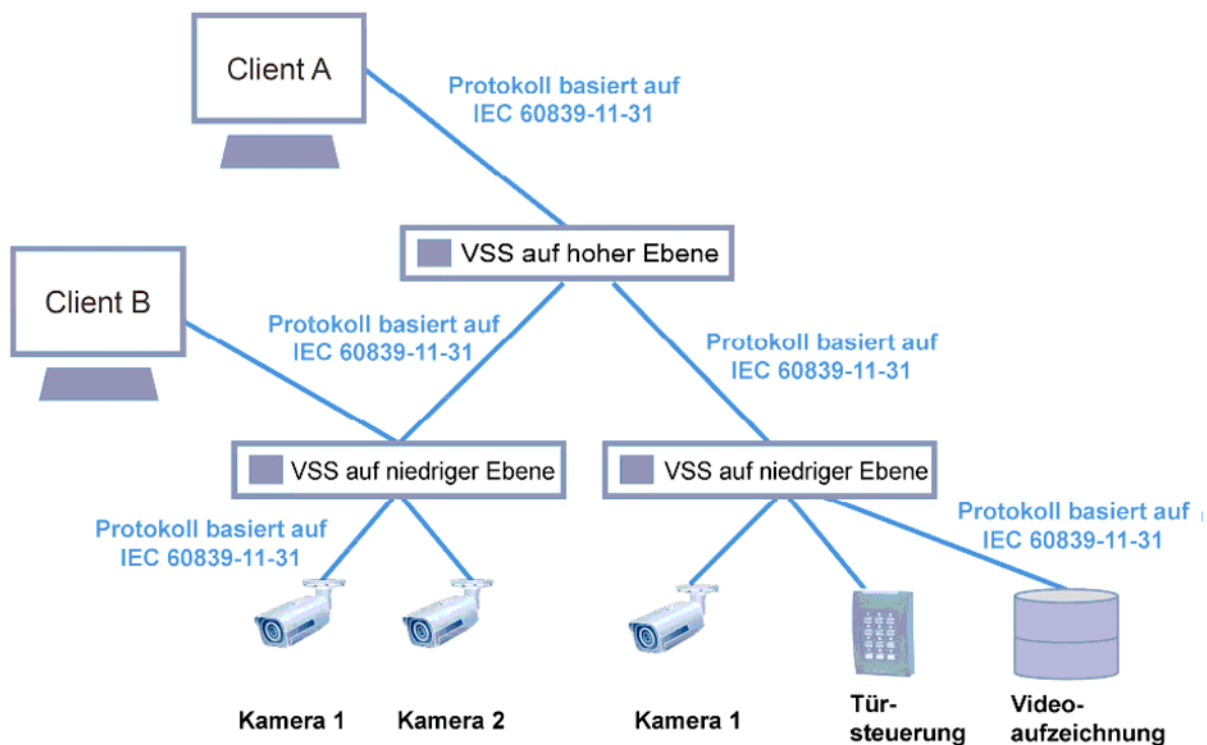


Bild 1 – Beispiel eines hierarchischen Systems

Ähnlich wie die in Bild 1 dargestellten Kameras stellt das VSS eine Schnittstelle zur höheren Ebene bereit, über die ein Client auf eine Ressource unterhalb zugreifen kann. In Abhängigkeit von der Autorisierung, die dem Client gewährt wurde, beschränkt das VSS den Zugriff in der Regel auf seine zugehörigen Ressourcen.

Anstelle einer neuen Schnittstelle legt diese Spezifikation einen kleinen Satz von Regeln dafür fest, wie ein VSS Ressourcen gegenüber einer Einheit auf höherer Ebene darzustellen hat. Alle auf IEC 60839-11-31 aufbauenden Spezifikationen adressieren Ressourcen über Token, für die in dieser Spezifikation ein kleiner Satz von Mapping-Regeln definiert ist. In dem Beispiel in Bild 1 können sowohl das VSS auf höherer Ebene

als auch die Clients A und B genau die gleiche Schnittstelle nutzen, um eine Kamera auf die gleiche Weise wie das VSS auf niedrigerer Ebene zu steuern.

4.2 Cloud-Uplink

In der Spezifikation IEC 60839-11-31 ist festgelegt, dass der Client eine Verbindung zu einem Gerät herstellt, wie in Bild 2 dargestellt.

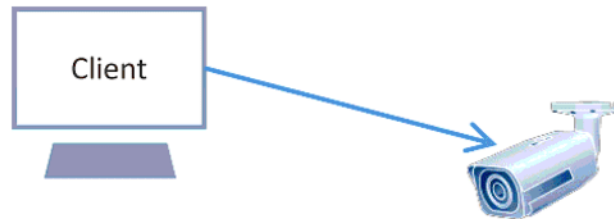


Bild 2 – Vom Client hergestellte Standardverbindung

Dieser Verbindungsmechanismus funktioniert besonders in Standardnetzwerken sehr gut. Wenn sich das Gerät allerdings hinter einer Firewall befindet und der Client in der Cloud lokalisiert ist, kann er keine Verbindung aufbauen. In diesen Fällen muss das Gerät die Verbindung herstellen. Eine derartige Verbindung wird als „Uplink“ bezeichnet und muss vom Gerät wie in Bild 3 dargestellt initiiert werden.

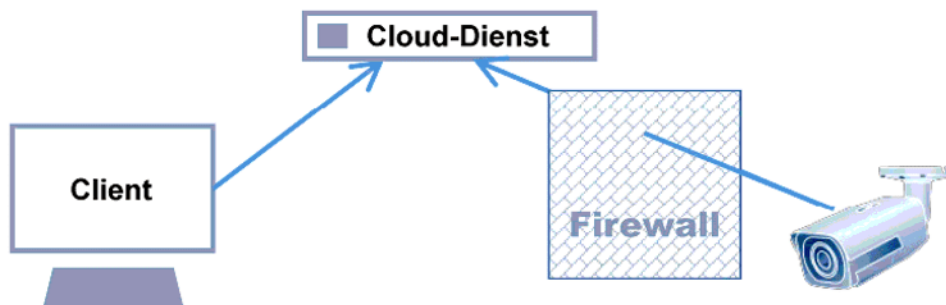


Bild 3 – Verbindungsaufbau seitens des Gerätes

In diesem Dokument wird eine Lösung präsentiert, mit der eine Kamera oder ein Managementsystem einen Uplink verwenden kann, um bestehende Webserver- und RTSP-Server-Funktionen unter Anwendung des HTTP/2-Protokolls zu vereinfachen.

5 Anforderungen

Um eine Verbindung zwischen dem VSS auf höherer Ebene (H-VSS, en: High-Level VSS) und dem VSS auf niedrigerer Ebene (L-VSS, en: Low-Level VSS) zu erzielen, müssen einige grundlegende Anforderungen an das System erfüllt werden.

5.1 Funktionale Anforderungen

Die ausführlichen funktionalen Anforderungen an die Verbindung zwischen H-VSS und L-VSS sind hinsichtlich zwei Aspekten formuliert: Ressourcennutzung und Konfiguration.

Für die Nutzung der Ressourcen des H-VSS durch das L-VSS sind die folgenden Anforderungen festgelegt:

- Steuerung des Live-Streaming; Live-Streaming auf Abruf, Unterstützung der Bildwiedergabe auf Abruf, Zoom, Bildaufnahme und Aufzeichnung, Unterstützung mehrerer Benutzer bei gleichzeitigem Zugriff auf dieselben Bildressourcen auf Abruf.
- Abruf und Wiedergabe historischer Bilder. Abruf historischer Bilddaten auf dem Gerät im Netzwerk entsprechend den Angaben zu Ausrüstung, Kanal, Zeit, Alarminformationen usw. sowie Wiedergabe und

Download dieser Daten. Bei der Wiedergabe werden die folgenden Methoden unterstützt: normale Wiedergabe, schnelle Wiedergabe, langsame Wiedergabe, Anhalten, Bildaufnahme und Zoom. Die aufzeichnenden Informationen befinden sich im L-VSS.

- c) Fernsteuerung. Der Betrieb des Gerätes kann aus der Ferne manuell oder automatisch gesteuert werden, z. B. PTZ. Optional wird die Arretierung unterstützt.
- d) Ausgabe des dekodierten Bildes. Dekodierung von Echtzeitbildern; die Ausgabe könnte durch Fernsteuerung durch das L-VSS auf der Videowand angezeigt werden.
- e) Speicherverwaltung. Verteilte hierarchische Speicherverwaltung, bei der der Gerätespeicher und der Clientspeicher kombiniert werden, um die Speichereinstellungen zu Ort, Zeit, Backup-Strategie, Bearbeitungsstrategien usw. zu unterstützen.
 - Übertragung von Inhalten vom L-VSS und H-VSS.
- f) Client-Verwaltung. Das L-VSS sendet die Managementinformationen an das H-VSS, nachdem es die entsprechende Anfrage vom H-VSS empfangen hat.
 - Wenn ein neues Gerät dem System beitrifft, sollte das L-VSS die Geräteinformationen an das H-VSS melden.
 - Taktsynchronisierung: Das H-VSS und das L-VSS sollten die Taktsynchronisierung unterstützen, und der Taktgeber auf hoher Ebene sollte die Sicherung des Taktgebers auf niedriger Ebene sein.
 - Es ist die Transportsicherheit zwischen dem H-VSS und dem L-VSS zu unterstützen;
 - Abfrage von Informationen zu Herstellern der Ausrüstung, Ausrüstungsmodell, Version und anderen grundlegenden Parametern beim H-VSS durch das L-VSS.
- g) Benutzerverwaltung
 - Es sind die folgenden Funktionen zu unterstützen: Benutzerregistrierung, Authentifizierung, Autorisierungsverwaltung, Zugriffssteuerung, Übertragung und Prüfung der Benutzererkennung vom L-VSS an das H-VSS.
 - Gewähren von Zugriffsberechtigungen auf bestimmte Ressourcen gegenüber verschiedenen Benutzern; das VSS auf niedrigerer Ebene (z. B. Zweigstelle) sollte dem VSS auf höherer Ebene (z. B. Zentrale) die Zugriffsberechtigung auf seine Ressourcen erteilen.
- h) Protokollverwaltung. Es ist die Protokollierung im L-VSS sowie die Abfrage vom H-VSS durch das L-VSS zu unterstützen.
- i) Zutrittskontrolle. Das VSS kann den Zutrittskontrolldienst unterstützen.

5.2 Protokollanforderungen

Die folgenden Anforderungen an Webservice-Protokolle sollten an der Schnittstelle zwischen zwei VSS auf unterschiedlichen Ebenen berücksichtigt werden:

- Das L-VSS muss seine Kameras melden. Das L-VSS muss das H-VSS über alle Änderungen an seinen zugehörigen Kameras informieren.
- Ein L-VSS hinter einer Firewall muss sich mit einem H-VSS im Internet verbinden können.
- Abfrage von Geräteinformationen.
- Das Protokoll sollte die hierarchische Abfrage unterstützen, um die Geräteverzeichnisinformationen erhalten zu können. Die Geräteverzeichnisinformationen umfassen die Geräte-ID, den Gerätenamen, den Herstellernamen, den Gerätetyp, die Geräteadresse, den Gerätemodus, den Gerätestatus usw. Um die Geräteinformationen zu erhalten, kann der Parameter „CameraID“ verwendet werden.
- Autoritätskontrolle.
- Für verschiedene Administratoren sind unterschiedliche Namen und Kennwörter zu vergeben, um die administrativen Rechte, den Verwaltungsbereich, den Anmeldezeitraum und den Anmelde-IP-Adressbereich zu beschränken und somit eine spezifischere Verwaltungsautorisierung zu erreichen. Für die Autoritätskontrolle zwischen zwei VSS können neue Befehle erforderlich sein.
- Steuerung des Live-Streaming.

- Wie in der Mediaservice-Spezifikation [IEC 62676-2-32](#) definiert, wird der Befehl „GetStreamUri“ verwendet, um festzulegen, wie die kodierten Daten an den Client gestreamt werden sollen. Dieser Befehl kann erweitert werden, sodass er das hierarchische Streaming unterstützt.

6 Ressourcenadressierung

6.1 Einleitung

In den auf [IEC 60839-11-31](#) aufbauenden Spezifikationen werden Ressourcen über sogenannte Token adressiert. Token sind Zeichenfolgen von definierter Länge, die vom Gerät aufgezählt werden, um die Verwaltung der Geräteressourcen zu vereinfachen. Ebenso wird in dieser Spezifikation angenommen, dass ein VSS seine zugehörigen Geräteressourcen derart aufzählt, dass jeder Ressource ein eindeutiges Token zugewiesen wird.

Darüber hinaus geht diese Spezifikation davon aus, dass ein VSS das Ressourcentoken-Mapping implementiert, indem jedem Token ein Präfix vorangestellt wird, das durch einen Doppelpunkt getrennt ist. Ob ein VSS einem Gerätetoken ein Präfix voranstellt oder ob es ein vollständiges Re-Mapping durchführt, liegt außerhalb des Anwendungsbereiches dieser Spezifikation.

Die folgende Liste ist eine unvollständige Aufzählung von möglichen Ressourcen:

- Medienprofile und -konfigurationen, einschließlich Bildschirmanzeige und Masken;
- Video- und Audioquellen;
- Digitaleingänge und Relaisausgänge;
- Türverriegelungen und Kartenlesegeräte;
- Aufzeichnungen, Aufzeichnungsspuren und Aufzeichnungsjobs.

Diese Spezifikation verwendet den in [IEC 60839-11-31](#) definierten Eigenschaftsereignismechanismus, um globale Ressourcen zu modellieren. Ein Client oder ein VSS auf höherer Ebene abonniert einen VSS-Pull-Point. In den darauffolgenden Anfragen werden dann alle interessierenden Ressourcen abgerufen, um alle relevanten Ressourcen eines VSS auf niedrigerer Ebene in Erfahrung zu bringen. Sobald eine Ressource empfangen wurde, kann für sie eine Aktion ausgeführt werden.

Sobald alle Ressourcen gemeldet wurden, führen weitere Pull-Nachrichten zur Überschreitung des Zeitlimits, sofern keine Änderungen aufgetreten sind, oder zur Meldung der entsprechenden Änderungen. In diesem Zusammenhang werden unter Änderungen hinzugefügte Ressourcen, die modifizierte Ressourceneigenschaften oder entfernte Ressourcen verstanden. Durch Anwendung des Mechanismus zur Eigenschaftsereignisbenachrichtigung auf Ressourcen verfügt ein Client oder ein VSS auf höherer Ebene immer über aktuelle Informationen über die interessierenden Ressourcen des VSS auf niedrigerer Ebene.

6.2 Entfernte Token

Auf Webservices basierende Spezifikationen gehen allgemein davon aus, dass das Gerät Token definiert, die innerhalb des Gerätes und seines Kontextes eindeutig sind. Diese Spezifikation erweitert das Schema, um die Erstellung global eindeutiger Token, sogenannter entfernter Token, zu ermöglichen.

Ein entferntes Token muss als QName mit einem gerätespezifischen Präfix und einem lokalen Token erstellt werden.

$\text{RemoteToken} = \text{Präfix} + ':' + \text{LocalToken}$

Die gesamte Stringlänge des entfernten Tokens ist auf 64 Zeichen beschränkt. Ein lokales Token darf nicht länger als 36 Zeichen sein und sollte keinen Doppelpunkt enthalten. Die Längenbeschränkung wird so gewählt, dass die Verwendung von UUIDs nach der Definition in RFC 4122 möglich ist. Es ist zu beachten, dass Geräteimplementationen in der Regel kompakte Token verwenden, die aus wenigen Zeichen zusammengesetzt sind.

Ein VSS muss für alle Token desselben Gerätes das gleiche Präfix verwenden. Dadurch weiß ein Client, welche Token er für einen beliebigen Webservice-API-Aufruf verwenden kann.

Ein VSS kann für den „LocalToken“-Teil entweder geräteleokale Token verwenden oder ein internes Mapping erstellen. Ein Client darf nicht annehmen, dass bei der Nutzung von Token, die von einem VSS direkt in Geräteaufrufen empfangen werden, Präfix weggelassen werden kann.

Die Namenskonventionen für den Präfix-Teil liegen außerhalb des Anwendungsbereiches dieser Spezifikation. Je nach Anwendungsbereich können Implementierer zwischen verschiedenen Ansätzen wählen. Aus diesem Grund gibt diese Spezifikation nicht vor, dass entfernte Token zwischen verschiedenen VSS global eindeutig sein müssen. Siehe [Anhang A](#) für eine länderspezifische Definition global eindeutiger Adressen.

6.3 Token-Kontext

Clients, die gleichzeitig mit mehreren Servern wie VSS und/oder Geräten kommunizieren, dürfen Ressourcen eines Servers nur mithilfe von Token adressieren, die von dem gleichen Server empfangen wurden. Es kann nicht sichergestellt werden, dass von einem bestimmten Server empfangene entfernte Token zur Adressierung der gleichen Ressource auf einem anderen Server verwendet werden können.

7 Abfrage von Ressourcen

7.1 Allgemeines

In dieser Spezifikation werden Ressourcen als sogenannte Eigenschaftsereignisse modelliert. Eine Ressource ist ein Konfigurationselement, das über ein Token adressiert wird.

Ressourcen werden abgefragt und über den Ereignismechanismus gemeldet. Dieser Mechanismus hat gegenüber einer klassischen Abfrageoberfläche zwei Vorteile. Erstens: Der Mechanismus kann sehr große Antworten handhaben, indem er die Antwortpakete auf mehrere Pull-Zyklen aufteilt. Zweitens: Der Mechanismus stellt eine Echtzeit-Aktualisierungsfunktion bereit, sodass Clients durch Dienste sehr effektiv über Änderungen an den Ressourcen informiert werden können.

Ein Server, der die Abfrage von Ressourcen unterstützt, muss die unterstützten Ressourcenabfragen auf der GetEventProperties-Oberfläche des Ereignisdienstes anzeigen. Folgende Ressourcen können aufgezählt werden:

Für Medienkonfigurationen:

VideoSourceConfiguration, AudioSourceConfiguration, VideoEncoderConfiguration,
AudioEncoderConfiguration, AudioOutputConfiguration, AudioDecoderConfiguration,
MetadataConfiguration, AnalyticsConfiguration, PTZConfiguration, OSDConfiguration,
MaskConfiguration

Für Medienprofile: MediaProfile

7.2 Ressourcenereignis

Auf jede Ressource wird die folgende Ereignisdefinition abgebildet:

```
Topic: tns1:Resource/<resource name>
<tt:MessageDescription IsProperty="true">
  <tt:Source>
    <tt:SimpleItemDescription Name="Token" Type="tt:ReferenceToken"/>
  </tt:Source>
  <tt>Data>
    <tt:SimpleItemDescription Name="Name" Type="xs:string"/>
    <tt:ElementItemDescription Name="Location" Type="tt:GeoLocation"/>
    <tt:SimpleItemDescription Name="Scope" Type="xs:string"/>
  </tt>Data>
</tt:MessageDescription>
```

```
<tt:SimpleItemDescription Name="Offline" Type="xs:boolean"/> </tt:Data>
</tt:MessageDescription>
```

Das Quellelement „Token“ ist obligatorisch und muss ein geeignetes Token enthalten, das innerhalb des Systems eindeutig ist.

Die Datenelemente sind optional.

Der Aufgabenbereich des Datenelements bezieht sich auf den in [IEC 60839-11-31](#) festgelegten Aufgabenbereichseintrag 1 der Geräteauffindung (en: Device Discovery). Er darf für jeden vom Gerät unterstützten Aufgabenbereichseintrag mehrfach vorkommen.

Sobald eine Ressource in einer Subskription zum ersten Mal gemeldet oder dem System neu hinzugefügt wurde, kann ein Ereignis mithilfe von PropertyOperation, festgelegt auf „Initialized“ (de: initialisiert), generiert werden. Wenn eine Ressource aus dem System entfernt wird, muss ein Ereignis mit PropertyOperation des Typs „Deleted“ (de: gelöscht) generiert werden.

Es ist zu beachten, dass bei einem Wechsel von Online- in Offline-Betrieb oder umgekehrt nur dann eine PropertyOperation des Typs „Changed“ (de: geändert) erstellt werden darf, wenn das Ereignis einen booleschen Offline-Zustand enthält.

7.3 Ortsfilter

Ein Server, der Abfragen von Ressourcen unterstützt, muss den Ortsfilter unterstützen.

```
<xs:complexType name="LocationFilter">
  <xs:sequence>
    <xs:element name="lon" type="xs:double"/>
    <xs:element name="lat" type="xs:double"/>
    <xs:element name="height" type="xs:float" minOccurs="0"/>
    <xs:element name="radius" type="xs:float"/>
    <xs:element name="includeUnknown" type="xs:boolean" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
```

Geräte mit unbekanntem Ort müssen eine Übereinstimmung aufweisen, wenn die Eigenschaft „includeUnkown“ festgelegt ist.

7.4 Präfix-Filter

Ein Server, der Abfragen von Ressourcen unterstützt, muss den Präfix-Filter unterstützen. Mit dem Präfix-Filter kann die Suche mithilfe des vom VMS zugewiesenen Präfixes auf bestimmte Ereignisse eines Gerätes beschränkt werden.

```
<xs:complexType name="PrefixFilter">
  <xs:sequence>
    <xs:element name="Prefix" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
```

7.5 Aufgabenbereichsfilter

Ein Server, der Abfragen von Ressourcen unterstützt, muss den Aufgabenbereichsfilter unterstützen, mit dem nach Aufgabenbereichseinträgen von Geräten gesucht werden kann.

```
<xs:complexType name="ScopeFilter">
  <xs:sequence>
    <xs:element name="Scope" maxOccurs="unbounded">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="xs:string">
```

```
<xs:attribute name="Match"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
</xs:sequence>
```

Für Aufgabenbereichsvergleichsregeln siehe [IEC 60839-11-31](#).

7.6 Auswahlfilter

Ein Server, der Abfragen von Ressourcen unterstützt, muss den Auswahlfilter unterstützen, um die resultierenden Datenelemente eines jeden Ereignisses zu beschränken und somit die Nachrichtengröße großer Abfragen zu minimieren.

```
<xs:complexType name="SelectFilter">
  <xs:sequence>
    <xs:element name="Path" type="xs:string" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
```

Jeder Eintrag legt einen XPath-Ausdruck fest, der mit einem der Ereignisdatenelemente übereinstimmt.

In dem folgenden Beispiel ist der Inhalt des Ergebnisses auf den Ressourcennamen und den Ortsbereich beschränkt:

```
<SelectFilter>
  <Path>/Name</Path>
  <Path>/Scope/Location</Path>
</SelectFilter>
```

7.7 Live-Überprüfungen

Der in dieser Spezifikation festgelegte Mechanismus verwendet den in [IEC 60839-11-31](#) definierten Echtzeit-Pull-Point. Wenn an einem Pull-Point keine Ereignisse anstehen, wird der PullMessages-Aufruf das Zeitlimit nach der vom Client festgelegten Zeitdauer überschreiten. Durch die Steuerung des Zeitlimits kann der Client einen kontinuierlichen Herzschlag vom Server sicherstellen. Deshalb braucht es keine zusätzliche Ping- oder Herzschlagoberfläche.

7.8 Beispiele (informativ)

7.8.1 Live-Video

In diesem Beispiel wird angenommen, dass eine Polizeistation die Live-Übertragung zu einem Vorfall an einem bestimmten geographischen Ort empfangen möchte.

1. Der Client authentifiziert sich am VSS mithilfe seines Client-Zertifikats.
2. Der Client abonniert das VSS-Topic „Resource/MediaProfile“ für eine Entfernung von 100 Metern von einem geographischen Ort, der mithilfe seiner Koordinaten (Lon/Lat) angegeben wurde.
3. Das VSS antwortet auf PullMessages, indem es alle Medienprofile im gefragten Bereich aufzählt.
4. Empfängt der Client mehrere Profile für ein entferntes Gerät, kann er das am besten geeignete auswählen, indem er die Profilkonfigurationen abfragt. Für jedes Profil-Token ruft der Client GetProfiles auf. Durch Senden des Parameters „Type“ mit dem Wert „VideoSource“ und „VideoEncoder“ empfängt er detaillierte Informationen über die Videoauflösung und die Einstellungen des Kodierers.
5. Der Client ruft für jede Videoquelle in dem ausgewählten Profil GetStreamUri auf.
6. Der Client streamt das Video und zeigt es auf der Videowand der Polizeistation an.

Auf den ersten Blick sieht es so aus, als ob keine neue funktionale Schnittstelle definiert wurde. Auch wenn das stimmt, muss das VSS eine Reihe von Operationen implementieren, um das obige Beispiel umsetzen zu können:

- a. Aufzählen der zugehörigen Kameraprofile als Ressourcenereignisse;
- b. Implementieren der Media2-API;
- c. Zuordnen der Medienprofil-Token der Anfrage zu den Kameras und deren lokalen Token;
- d. Zuordnen der Profil-Token der Antwort zu den globalen Token;
- e. Unterstützen des Streaming-Proxy und Zuordnen des URI des Kamera-Streams zum Proxy.

Darüber hinaus zeigt ein intelligentes VSS seinem Client möglicherweise nur diejenigen Medienprofile an, die eine vertretbare Datenrate aufweisen, damit dieser in der Lage ist, diese Video-Streams zu vertreten.

Statt sich direkt mit den entfernten VSS-Systemen auf niedrigerer Ebene zu verbinden, kann der Client der Polizeistation eine Verbindung zu einem VSS auf höherer Ebene aufbauen, das die Suchergebnisse für mehrere VSS auf niedrigerer Ebene zusammenfasst und über das entsprechende VSS auf niedrigerer Ebene Befehle an die einzelnen Kameraquellen weiterleitet.

7.8.2 Kriminaltechnik

In diesem Beispiel wird angenommen, dass eine Polizeistation Aufzeichnungen zu einem Vorfall an einem bestimmten geographischen Ort abrufen möchte.

1. Der Client authentifiziert sich am VSS mithilfe seines Client-Zertifikats.
2. Der Client abonniert das VSS-Topic „Resource/VideoSource“ für eine Entfernung von 100 Metern von einem geographischen Ort, der mithilfe seiner Koordinaten (Lon/Lat) angegeben wurde.
3. Das VSS antwortet auf PullMessages, indem es alle Videoquellen im gefragten Bereich aufzählt.
4. Der Client ruft FindEvents auf und gibt den gewünschten Zeitraum sowie eine Liste von Videoquellen als Suche aus.
5. Der Client ruft GetEventSearchResults auf, um alle verfügbaren Aufzeichnungen an dem bestimmten Ort im gefragten Zeitraum zu erhalten.
6. Der Client empfängt die RTSP-URIs, indem er die Wiedergabemethode „GetReplayUri“ für die Aufzeichnung aufruft.
7. Der Client spielt die Videos der interessierenden Kameras ab, indem er den RTSP-Medien-Stream für den URI abruft, den er durch den Aufruf „Replay:GetReplayUri“ abgerufen hat.

Alternativ zum oben genannten Ansatz könnte der Client auch direkt die Aufzeichnungsressource für einen geographischen Ort abfragen. Einige Wiedergaben schlagen möglicherweise fehl, wenn die Kameras an dem ausgewählten Ort zu der ausgewählten Tageszeit keine Aufzeichnungen vorgenommen haben.

Das oben beschriebene Beispiel ist sowohl auf Inhalte, die im Kameraspeicher gespeichert sind, als auch auf Inhalte auf dem VMS-Aufzeichnungsserver anwendbar. Die VMS-Anwendung entscheidet, wie die Aufzeichnungen abgerufen werden.

8 Uplink

8.1 Protokoll

8.1.1 Verbindungsherstellung

Das Gerät stellt die Verbindung mit dem Cloud-Dienst her. In [Bild 4](#) sind die drei Phasen dargestellt. In der ersten Phase agiert das Gerät als TLS-Client, der sich mit dem Cloud-Dienst verbindet. Es ist zu beachten, dass im Bild nur die relevantesten Pakete gezeigt werden. Einzelheiten zum TCP- und TLS-Austausch liegen außerhalb des Anwendungsbereiches dieser Spezifikation. In der zweiten Phase wird die Verbindung auf

HTTP/2 aufgerüstet und mit einer HTTP-Antwort mit dem Code 101 vom Cloud-Dienst bestätigt. Die dritte Phase der Verbindung entspricht vollständig einer HTTP/2-Verbindung, so als ob der Cloud-Dienst der Initiator gewesen wäre.

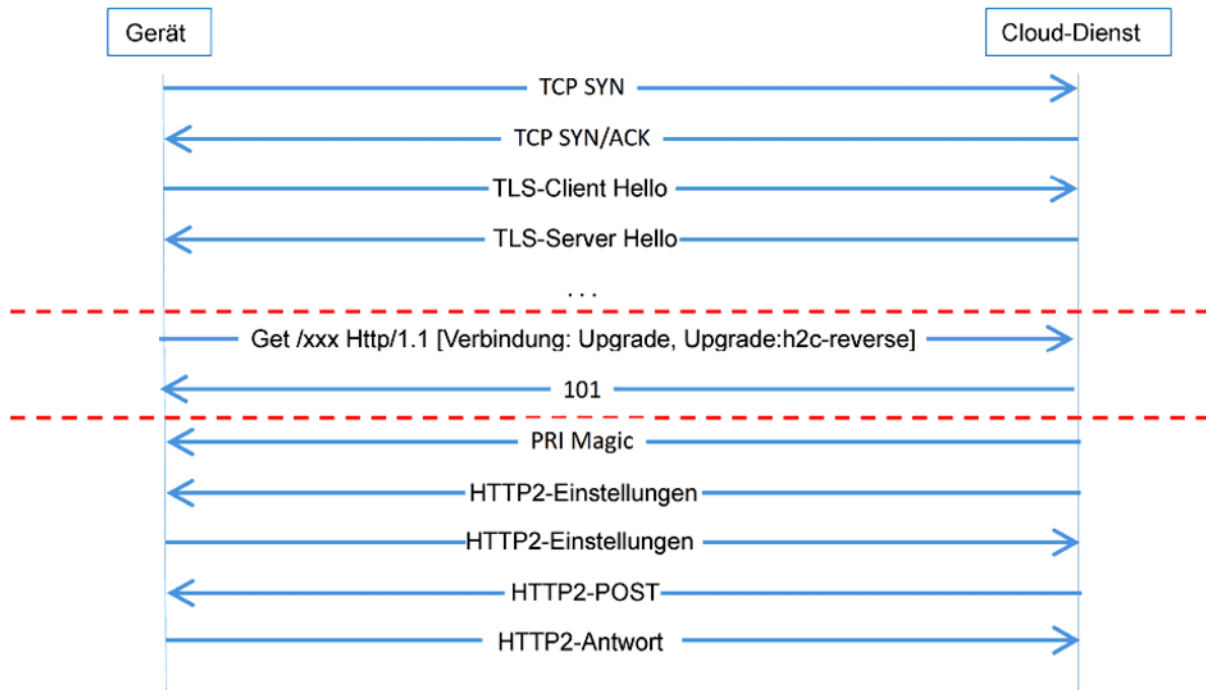


Bild 4 – Abfolge der Verbindungsherstellung

8.1.2 Verbindungsverwaltung

Ein lokaler Dienst, der einem entfernten Client zur Nutzung angeboten wird, muss einen betriebsbereiten Kommunikationskanal aufrechterhalten. Da die Verbindung zum entfernten Client seitens des Dienstes aufgebaut werden muss, spricht man hier von „Uplink“. Der Uplink muss über TLS abgesichert werden.

Der Dienst muss überwachen, ob der entfernte Client über den Uplink kommunizieren kann. Er kann den HTTP/2-Ping-Mechanismus verwenden, um zu überprüfen, ob eine Verbindung noch betriebsbereit ist, falls für eine längere Zeit keine Pakete empfangen wurden.

Ein lokaler Dienst muss den Uplink immer dann schließen und neu herstellen, wenn länger als 30 Sekunden keine Pakete vom entfernten Client empfangen wurden. Jede Kamera muss eine eigene Strategie aufsteigender Intervalle verwenden, um zu verhindern, dass sich alle Kameras zur gleichen Zeit neu verbinden.

Im Folgenden werden beispielhaft Muster gezeigt, die von zwei Kameras A und B gewählt werden:

- Kamera A: 3s, 6s, 12s, 24s, 30s, 30s, 30s ...
- Kamera B: 2s, 4s, 8s, 16s, 30s, 30s, 30s ...

Enthält die Uplink-Liste mehrere Einträge, muss das Gerät versuchen, alle Verbindungen parallel aufzubauen.

Es ist zu beachten, dass in dieser Spezifikation davon ausgegangen wird, dass im Fall von mehreren Clients diese so angelegt sind, dass sie sich gegenseitig nicht stören. Die Koordinierung zwischen mehreren Clients liegt außerhalb des Anwendungsbereiches dieser Spezifikation.

8.1.3 Authentifizierung

Es ist zu beachten, dass für die folgende Betrachtung die Rollen von Client und Server getauscht sind.

Der entfernte Client muss sich mithilfe eines gültigen Serverzertifikats authentifizieren. Der Dienst muss die Gültigkeit des entfernten Zertifikats nach RFC 6125 überprüfen.

Der Dienst muss sich am entfernten Client mithilfe der TLS-Client-Authentifizierung nach RFC 5246 oder den nachfolgenden Spezifikationen authentifizieren.

Um den lokalen Dienst am entfernten Client eindeutig identifizieren zu können, wird empfohlen, für jeden lokalen Dienst ein eindeutiges Client-Zertifikat zu besitzen. Für die eindeutige Identifikation des lokalen Dienstes könnte beispielsweise das CN-Feld oder die Seriennummer des installierten Zertifikats verwendet werden.

8.1.4 HTTP/2-Frames

Sobald eine HTTP/2-Verbindung hergestellt wurde, werden die Kommunikationsparameter wie in RFC 7540 festgelegt verhandelt, damit der Uplink für den Austausch von Frames zwischen entferntem Client und lokalem Dienst genutzt werden kann.

8.1.5 HTTP-Transaktionen

Der Uplink muss in umgekehrter Richtung für HTTP-Anfragen und -Antworten verwendet werden. Der entfernte Client muss Anfragen senden, die dem lokalen Dienst in standardmäßiger HTTP-Form bereitgestellt werden.

8.2 Konfigurationsschnittstelle

8.2.1 Konfigurationsparameter

- RemoteAddress Einheitlicher Ressourcenlokalisator, über den der entfernte Client erreicht werden kann.
- CertificateID ID des für die Client-Authentifizierung zu verwendenden Zertifikats.
- UserLevel Autorisierungsebene, die der Uplink-Verbindung zugewiesen wird.
- Status Aktueller Verbindungsstatus.

Das Feld „RemoteAddress“ wird als Schlüssel der Liste von Uplink-Konfigurationen verwendet.

8.2.2 GetUplinks

Ein Gerät, das Uplinks unterstützt, muss diesen Befehl unterstützen, um die konfigurierten Uplink-Konfigurationen abzurufen. Im Feld „Status“ muss angegeben sein, ob die Verbindung „Offline“, „Connecting“ (de: Verbindung wird hergestellt) oder „Online“ ist.

ANFRAGE

<leer>

ANTWORT

- **Configuration – optional, unbegrenzt [tt:PTZConfiguration]**
Liste von Konfigurationen

8.2.3 SetUplink

Ein Gerät, das Uplinks unterstützt, muss diesen Befehl unterstützen, um eine Uplink-Konfiguration hinzuzufügen oder zu ändern. Das Gerät muss die Eigenschaft „Status“ der UplinkConfiguration außer Acht lassen. Ein Gerät muss das Feld „RemoteAddress“ verwenden, um zu entscheiden, ob ein vorhandener Eintrag aktualisiert oder ein neuer Eintrag erstellt wird.