

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Video surveillance systems for use in security applications –
Part 2-33: Video transmission protocols – Cloud uplink and remote management
system access**

**Systèmes de vidéosurveillance destinés à être utilisés dans les applications de
sécurité –
Partie 2-33: Protocoles de transmission vidéo – Liaison montante au nuage et
accès au système de gestion à distance**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2022 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Video surveillance systems for use in security applications –
Part 2-33: Video transmission protocols – Cloud uplink and remote management
system access**

**Systèmes de vidéosurveillance destinés à être utilisés dans les applications de
sécurité –
Partie 2-33: Protocoles de transmission vidéo – Liaison montante au nuage et
accès au système de gestion à distance**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 13.320

ISBN 978-2-8322-3973-5

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms and definitions	7
4 Overview	8
4.1 General.....	8
4.2 Remote access	8
4.3 Cloud uplink.....	9
5 Requirements	10
5.1 General.....	10
5.2 Functional requirements.....	10
5.3 Protocol requirements.....	11
6 Resource addressing.....	11
6.1 Token based addressing	11
6.2 Remote tokens.....	12
6.3 Token context	12
7 Resource queries	12
7.1 General.....	12
7.2 Resource event.....	13
7.3 Location filter	13
7.4 Prefix filter	14
7.5 Scope filter	14
7.6 Select filter	14
7.7 Live checks.....	15
7.8 Informative examples	15
7.8.1 Live video.....	15
7.8.2 Forensic.....	15
8 Uplink.....	16
8.1 Protocol.....	16
8.1.1 Connection establishment.....	16
8.1.2 Connection management	16
8.1.3 Authentication	17
8.1.4 HTTP/2 frames	17
8.1.5 HTTP transactions.....	17
8.2 Configuration interface.....	17
8.2.1 Configuration parameters	17
8.2.2 GetUplinks.....	17
8.2.3 SetUplink.....	18
8.2.4 DeleteUplink.....	18
8.2.5 Capabilities	18
Annex A (informative) Addressing scheme.....	19
A.1 Overview	19
A.2 Field definitions	19
A.2.1 Zone code	19
A.2.2 Agency code.....	19

A.2.3	Device type code	20
A.2.4	Serial number	22
A.2.5	Examples	22
Annex B (informative)	APIs with token adaption	24
B.1	General.....	24
B.2	Consuming live video	24
B.3	Controlling PTZ cameras	24
B.4	Retrieving recordings	24
B.5	Forwarding of events	24
Bibliography		25
Figure 1	– Hierarchical system example.....	9
Figure 2	– Standard connection initiated from the client	9
Figure 3	– Connection initiation from the device.....	10
Figure 4	– Connection initiation sequence.....	16
Figure A.1	– Fields of the device ID scheme	19
Table A.1	– The zone code elements	19
Table A.2	– Industry coding	20
Table A.3	– Device type codes.....	21
Table A.4	– Serial number value	22

IECNORM.COM : Click to view the full PDF of IEC 62676-2-33:2022

INTERNATIONAL ELECTROTECHNICAL COMMISSION

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 2-33: Video transmission protocols – Cloud uplink and remote management system access

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62676-2-33 has been prepared by IEC technical committee 79: Alarm and electronic security systems. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
79/658/FDIS	79/666/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

A list of all the parts in the IEC 62676 series, under the general title *Video surveillance systems for use in security applications*, can be found on the IEC website.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

IECNORM.COM : Click to view the full PDF of IEC 62676-2-33:2022

INTRODUCTION

Surveillance systems are important in public safety projects to maintain law and order as well as public safety, and to assist the police to perform forensic analysis. Due to organizational and security reasons, large-scale surveillance systems are split in segments, which can lead to information silos. This document provides a standardized interface for management systems such that authorized entities can easily access remote information using the same mechanism they are using today for accessing local information.

IECNORM.COM : Click to view the full PDF of IEC 62676-2-33:2022

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 2-33: Video transmission protocols - Cloud uplink and remote management system access

1 Scope

This document specifies management systems interfaces and mechanisms for remote operational access to physical security devices such as video surveillance devices and systems. For video surveillance, the use cases focus on accessing live video and retrieving recordings. The mechanisms defined in this document are not restricted to surveillance applications, but also cover remote access to security systems and electronic access control systems. Configuration of devices and management systems is out of the scope of this document.

Clause 4 introduces remote management access. Clause 5 defines a set of requirements that the protocol needs to fulfil. Clause 6 extends the token-based resource-addressing scheme of IEC 60839-11-31. Clause 7 describes how to retrieve information about remote resources. Clause 8 defines how to connect to devices that are not directly reachable because they are for instance located behind firewalls.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60839-11-31, *Alarm and electronic security systems – Part 11-31: Electronic access control systems – Core interoperability protocol based on Web services*

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

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 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1

resource

IEC 62676-2 entity that can be addressed via a token

3.2

uplink

connection established by the local service to the remote client

4 Overview

4.1 General

IEC 62676-2-31 and IEC 62676-2-32 provide a detailed protocol definition for interacting with video surveillance devices such as cameras and digital recorders. Similarly, IEC 60839-11-32 and IEC 60839-11-33 describe how to monitor and configure electronic access control systems. These two parts are based on IEC 60839-11-31, which defines a communication mechanism based on web services. This document extends IEC 60839-11-31 by adding cloud connectivity and remote addressing to the framework. Note that this document does not contain any domain-specific details, since all interfaces defined in the above-mentioned parts are applicable without any modifications. Therefore, this document covers the integration of a wide range of physical security systems into any management system. This document describes how a remote client or management system connects to resources such as cameras. The approach shown here allows scaling over several hierarchies. The examples in 4.2 show the mechanism principle with two layers of video surveillance systems (VSS) called "lower level" and "higher level". In this system, a higher-level VSS can retrieve a resource like device information from a lower-level VSS, to trigger corresponding actions for different devices that are connected to the lower-level VSS.

Access to remote VSS can require strict authentication constraints. The related definitions are outside of the scope of this document.

4.2 Remote access

Figure 1 shows a typical management system topology as deployed for bigger installations. So-called lower-level video surveillance systems incorporate numerous surveillance cameras and other equipment to monitor a region of a premises or city district. Higher-level video management systems allow supervision of large compounds.

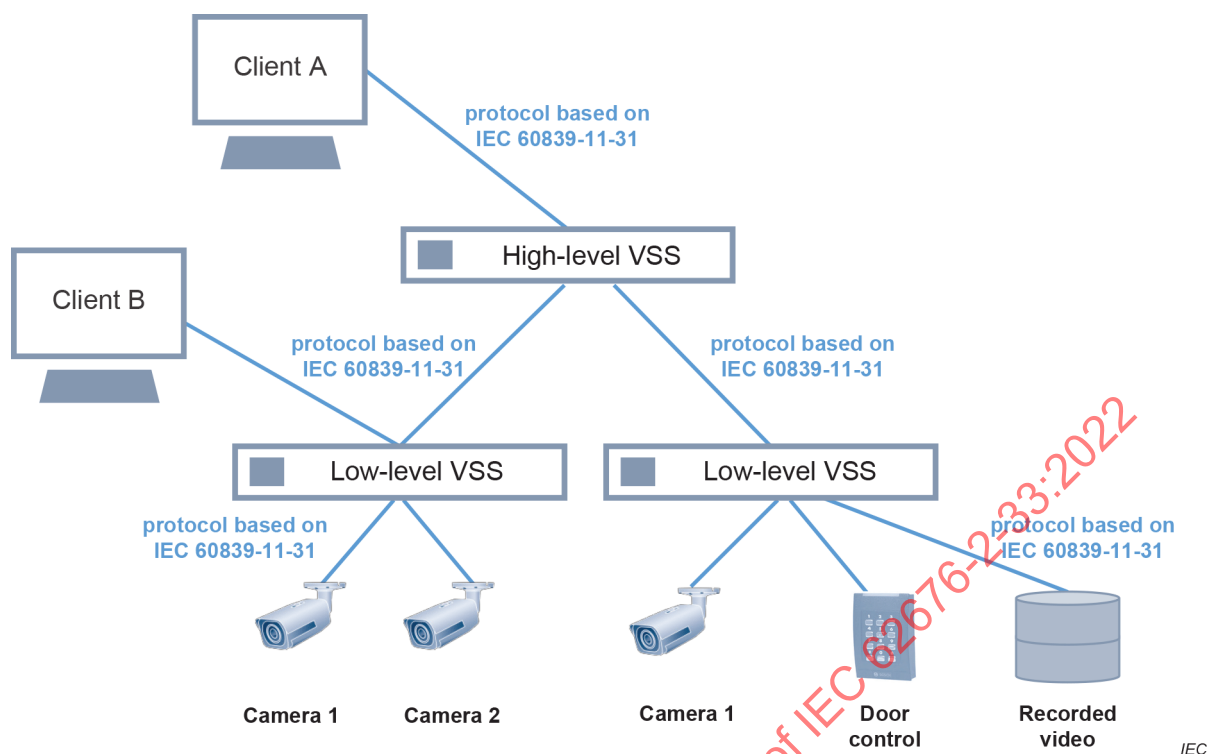


Figure 1 – Hierarchical system example

In a way similar to the cameras shown in Figure 1, the VSSs expose an interface towards the higher layer via which a client can access any resource placed below. Typically, the VSS restricts the access to any of its associated resources depending on the authorization granted to the client.

Instead of defining a new interface, this document defines a small set of rules explaining how a VSS has to present resources to a higher-layer entity. Devices implementing IEC 60839-11-31 address resources via tokens for which this document defines a small set of mapping rules. In the example of Figure 1, both the high-level VSS as well as clients A and B can use exactly the same interface to control a camera as the lower-level VSS does today.

4.3 Cloud uplink

The IEC 60839-11-31 defines that the client initiates a connection to a device, as depicted in Figure 2.

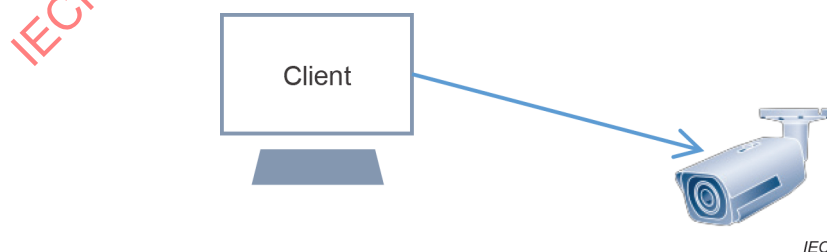


Figure 2 – Standard connection initiated from the client

This connection mechanism works very well within standard networks. However, in cases where the device is located behind a firewall and the client resides in the cloud, the client cannot establish the connection. In these cases, the device needs to establish the connection. Such a connection is called "uplink" and needs to be initiated from the device, as depicted in Figure 3.

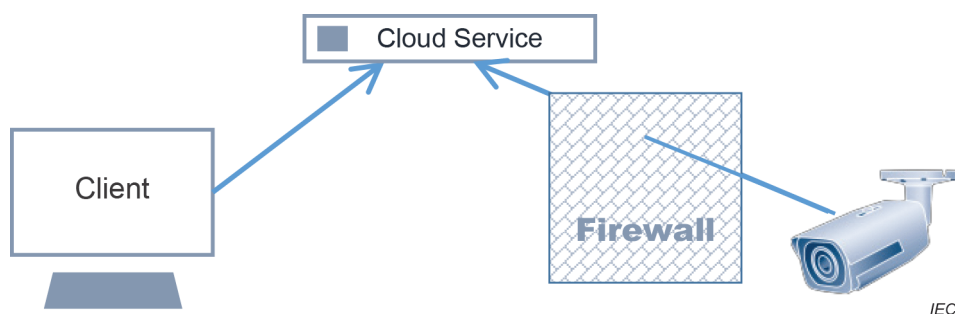


Figure 3 – Connection initiation from the device

This document specifies a solution that allows a camera or management system to use an uplink to facilitate existing web server functionality and RTSP server functionality using the HTTP/2 protocol.

5 Requirements

5.1 General

To achieve the interconnection between High-level VSS (H-VSS) and Low-level VSS (L-VSS), there are some basic requirements for the system.

5.2 Functional requirements

The detailed functional requirements of the interconnection between H-VSS and L-VSS are described in two aspects: resource usage and configuration.

For resource usage acquired from L-VSS to H-VSS, the following requirements are described:

- a) Live streaming control. Live streaming on demand, supporting on-demand image display, zoom, capture and recording, and multi-user support for the same image resources on-demand at the same time.
- b) Historical image retrieval and playback. Retrieve historical image data of the device in the network, according to the specified equipment, channel, time, alarm information, etc., playback and download. Playback supports the following methods: normal playback, fast playback, slow playback, picture pause, image capture and zoom display. The recording information is in the L-VSS.
- c) Remote control. The remote operation of the device can be controlled remotely by manual or automatic operation, e.g. using pan, tilt or zoom (PTZ) functions. Optionally support locking to gain exclusive access.
- d) Output of the decoded image. Real-time image decode, the output could be displayed. Remote control of video wall located in L-VSS.
- e) Storage management. Hierarchical distributed storage management, combining device storage and client storage, to support the storage settings of location, time, backup strategy, finishing strategies, etc.
 - Content transfers from L-VSS and H-VSS.
- f) Client management. L-VSS sends the management information to the H-VSS after receiving the request from the H-VSS.
 - When a new device enters the system, the L-VSS should notify the device information to the H-VSS.
 - Clock synchronization: the H-VSS and L-VSS should have clock synchronization, and the high-level clock source should be the backup of the low-level clock source.
 - Support the transport security between H-VSS and L-VSS.

- Query the equipment manufacturers, equipment model, version, and other basic information from H-VSS to L-VSS.
- g) User management
- Support the function of user registration, authentication, authorization management, access control, transmission and audit of user identifier from L-VSS to H-VSS.
 - Grant access control permissions of the appropriate resources to different users.
- h) Log management: support the logging in L-VSS and query from H-VSS to L-VSS.
- i) Access control: the VSS can support the access control service.

5.3 Protocol requirements

This section lists the requirements for web service protocols between two VSS in different levels:

- The L-VSS shall report its cameras. The L-VSS shall inform the H-VSS on any changes in its associated cameras.
- A L-VSS behind a firewall shall be able to connect to an H-VSS in the Internet.
- Device information query
The protocol should support the hierarchical query to get the device directory information. The device directory information contains the device ID, device name, manufacturer name, device type, device address, device mode, device status, etc. A CameraID can be used to get the device information.
- Authority control
Set different user names and passwords for different administrators, to limit the administrative rights, management scope, login time range and login IP address range of the administrator to achieve more detailed management authorization.
- Live streaming control
As defined in the IEC 62676-2-32 media service document, the GetStreamUri command is used to define how the encoded data is expected to be streamed to the client. This command can be extended to support the hierarchical streaming.

6 Resource addressing

6.1 Token based addressing

Devices implementing IEC 60839-11-31 address resources by so-called tokens. Tokens are character strings of a defined length and are enumerated by the device to ease the devices' resource management. Similarly, this document assumes that a VSS enumerates its attached device resources in such a way that a unique token is assigned to each of its attached devices' resources.

Additionally, this document assumes that a VSS implements resource token mapping by adding a prefix delimited by a colon. Whether a VSS simply adds a prefix to a device token or does a complete remapping is outside of the scope of this document.

The following is an incomplete list of resources that can be handled:

- media profiles and configurations including OSD and masks,
- video and audio sources,
- digital inputs and relay outputs,
- door locks and card readers,
- recordings, recording tracks and recording jobs.

This document uses the property event mechanism defined in IEC 60839-11-31 to model global resources. A client or upper level VSS subscribes to a VSS pull point. In consecutive requests, it then pulls all resources it is interested in in order to get to know all relevant resources of a lower-level VSS. As soon as it receives a resource, it can apply an action on it.

Once all resources have been reported, further pull messages will either timeout when no changes happen or report changes. In this context, changes are added resources, modification of resource properties or removed resources. By applying the property event notification mechanism to resources, a client or upper level VSS has always up-to-date information about the lower level VSS resources it is interested in.

6.2 Remote tokens

IEC 60839-11-31 assumes that the device defines tokens, which are unique within a device and its context. This document extends the scheme to allow building globally unique tokens called remote tokens.

A remote token shall be constructed like a QName with a device-specific prefix and a local token.

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

The overall string length of the remote token is limited to 64 characters. A local token shall not exceed 36 characters and should contain no colon. The length limitation is chosen in such a way that it enables the use of UUIDs as defined in RFC 4122. Note that device implementations typically use compact tokens.

A VSS shall use the same prefix for all tokens of the same device. This allows a client to understand which tokens they can use for any web service API call.

A VSS can choose to simply use device local tokens as LocalToken part or create an internal mapping. A client may not assume that tokens received from a VSS can be used in device calls by stripping the prefix.

The naming conventions for the prefix part are outside of the scope of this document. Depending on the application area, implementers can choose different approaches. Therefore, this document does not require that remote tokens are globally unique between different VSSs. See Annex A for a country-specific definition of globally unique addresses.

See Annex B for a guide to token adaptation.

6.3 Token context

Clients talking to multiple servers at a time, such as VSSs and/or devices, shall address resources to a server only with tokens received from that same server. There is no guarantee that remote tokens received from one server can be used to address the same resource at another server.

7 Resource queries

7.1 General

This document models resources as so-called property events. A resource is a configuration item addressed via a token.

Resources are queried and reported via the event mechanism. This mechanism provides two advantages over a classical query interface. Firstly, the mechanism can cope with very large responses by chopping the response packets into multiple pull cycles. Secondly, the mechanism provides a real-time update facility so that services can inform clients very efficiently about resource changes.

A server supporting resource queries shall signal the supported resource queries via the GetEventProperties interface of the event service. The following resources can be enumerated:

For media configurations:

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

For media profiles: MediaProfile

7.2 Resource event

Each resource maps to the following event definition;

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

The source item Token is mandatory and shall contain a qualified token that is unique within the serving system.

The data items are optional.

The data item scope refers to the discovery scope entry defined in IEC 60839-11-31. It can occur multiple times for each scope entry supported by the device.

An event shall be generated with PropertyOperation set to Initialized whenever a resource is signaled the first time in a subscription or it is newly added to the system. An event with PropertyOperation set to Deleted shall be generated when a resource is removed from the system.

Note that a change from online to offline or vice versa shall only create a PropertyOperation of type Changed if the event contains an Offline state Boolean.

7.3 Location filter

A service supporting resource queries shall support the Location Filter.

```
<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>
```

Devices with unknown location shall correspond to a match if the property includeUnknown is set.

7.4 Prefix filter

A server supporting resource queries shall support the Prefix Filter. The prefix filter allows restricting the search to any events of a device by the prefix assigned by the VMS.

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

7.5 Scope filter

A server supporting resource query shall support the Scope Filter allowing searching for device scope entries.

```
<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>
```

See IEC 60839-11-31 for the scope matching rules.

7.6 Select filter

A server supporting resource query shall support the Select Filter allowing restricting the resulting data items of each event in order to reduce the message sizes of large queries.

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

Each entry defines an XPath expression that matches to one of the event data items.

The following example restricts the content of the result to the resource name and location scope:

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

7.7 Live checks

The mechanism defined in this document makes use of the real-time pull point defined in IEC 60839-11-31. When no events are pending at a pull point, the PullMessages call will timeout after a client defined timeout. The client is in control of the timeout and can ensure a continuous heartbeat from the server. Hence, there is no need for an additional ping or heartbeat interface.

7.8 Informative examples

7.8.1 Live video

This example assumes that a police station client wants to get live feeds related to an incident at a certain geo location.

- 1) The client authenticates itself at the VSS using its client certificate.
- 2) Client subscribes to VSS topic Resource/MediaProfile within 100 m of a lon/lat provided geo location.
- 3) VSS responds to PullMessages enumerating all media profiles in the given area.
- 4) If the client receives multiple profiles for a remote device, it can select the best suited one by querying the profile configurations. For each profile token, the client calls GetProfiles. By supplying parameter Type set to VideoSource and VideoEncoder, it will receive detailed information about the Video resolution and encoder settings.
- 5) The client calls GetStreamUri for each video source on the selected profile.
- 6) The client streams video and displays it on the Police Video Wall.

At first glance, it looks like no new functional interface has been defined. Although this is correct, the VSS shall still implement a number of operations in order to make the above example happen:

- a) enumerate its attached camera profiles as resource events;
- b) implement the Media2 API;
- c) map request media profile token to cameras and their local tokens;
- d) map response profile tokens to global tokens;
- e) support streaming proxy and map camera stream URI to proxy.

Additionally, an intelligent VSS can expose only those media profiles to its client that have a decent data rate so that it is able to proxy those Video streams.

Instead of directly connecting to the remote lower level VSS systems, the police station client can connect to an upper level VSS that in turn combines search results from multiple lower level VSS and forwards commands to individual camera sources via the appropriate lower-level VSS.

7.8.2 Forensic

This example assumes that a police station client wants to retrieve recordings related to an incident at a certain geo location.

- 1) The client authenticates itself at the VSS using its client certificate.
- 2) Client subscribes to VSS topic Resource/VideoSource within 100 m of a lon/lat provided geo location.
- 3) VSS responds to PullMessages enumerating all video sources in the given area.
- 4) The client calls FindEvents passing the interested time range and a list of video sources in the search scope.
- 5) The client calls GetEventSearchResults to get all available recordings at the interested location and in the given period of time.

- 6) The client retrieves the RTSP URIs by calling the GetReplayUri method for the recording.
- 7) The client plays back video of interested cameras by retrieving the RTSP media stream for the URI retrieved by a call to Replay:GetReplayUri.

As an alternative to the above approach, the client might also directly query the recording resource at a geo location. Some replays can fail because the cameras did not record for the selected location at the selected time of day.

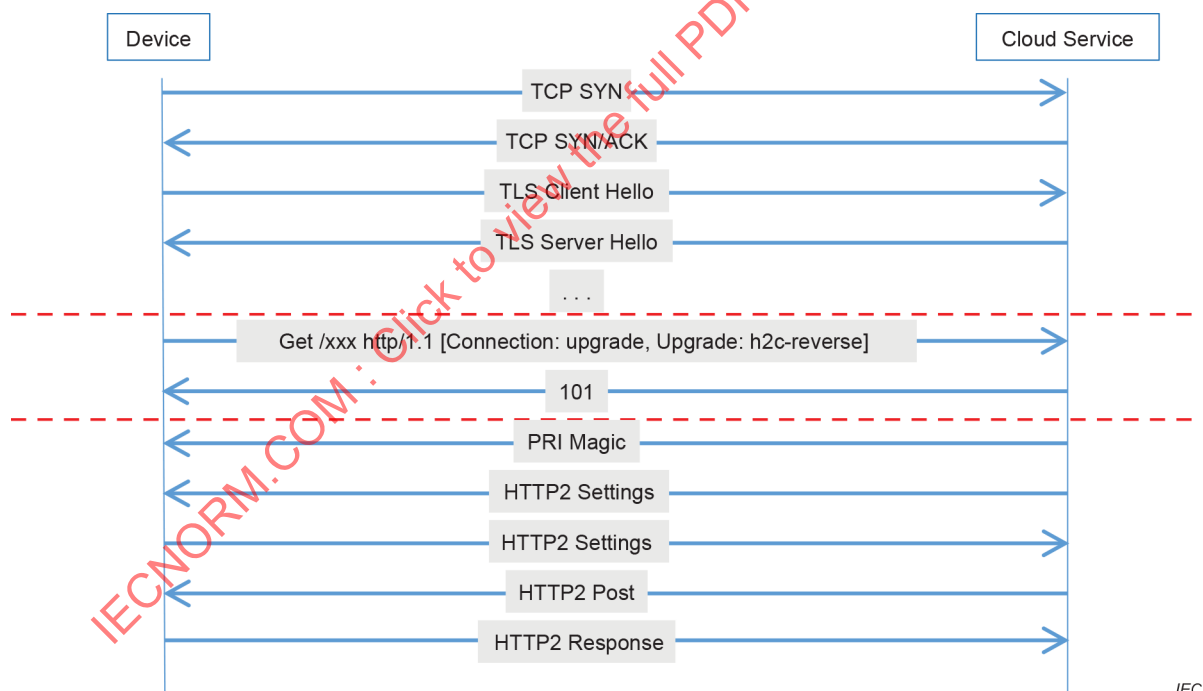
The above example is applicable for both content stored in camera's edge storage and VMS recording server. It is up to the VMS application how the recordings are retrieved.

8 Uplink

8.1 Protocol

8.1.1 Connection establishment

The device initiates the connection to the cloud service. Figure 4 shows the three phases. In the first phase, the device acts as a TLS client that connects to the cloud service. The figure only shows the most relevant packets. Details of the TCP and TLS exchanges are out of the scope of this document. The second phase includes the connection upgrade to HTTP/2, which the cloud service confirms with a 101 HTTP response. The third phase of the connection then fully complies with an HTTP2 connection as if the cloud service were the initiator.



IEC

Figure 4 – Connection initiation sequence

8.1.2 Connection management

A local service that is offered to a remote client for utilization is responsible for maintaining an operational communication channel. Since the connection shall be established from the service to the remote client, this connection is called uplink. The uplink shall be secured via the TLS.

The service shall monitor whether the remote client is able to communicate via the uplink. It can use the HTTP/2 ping mechanism to check whether a link is still operational if no packets have been received for a longer period of time.

A local service shall close and reconnect the uplink whenever no packets have been received from the remote client for more than 30 s. Each camera shall use an individual ascending interval strategy to avoid that all cameras connect at the same time.

The following example shows patterns chosen by two cameras A and B:

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

If the uplink list contains multiple entries the device shall try to establish all connections in parallel.

Note that this document assumes that scenarios with multiple clients are designed such that they do not interfere with each other. The coordination between such multiple clients is outside the scope of the document.

8.1.3 Authentication

Note that for the following discussion the roles of client and server are swapped.

The remote client shall authenticate itself using a valid server certificate. The service shall verify the validity of the remote certificate in accordance with RFC 6125.

The service shall authenticate itself at the remote client using TLS client authentication in accordance with RFC 5246 or subsequent specifications (TLS 1.2 and later).

To uniquely identify local service on remote client, it is recommended to have a unique client certificate installed on each local service. For example, the CN field or Serial number of the installed certificate could be used to uniquely identify the local service.

8.1.4 HTTP/2 frames

Once an HTTP/2 connection has been established the communication parameters are negotiated as specified by RFC 7540 so that the uplink can be used to exchange frames between the remote client and the local service.

8.1.5 HTTP transactions

The uplink shall be used in reverse direction for HTTP requests and responses. The remote client shall send requests that are served in a standard HTTP manner by the local service.

8.2 Configuration interface

8.2.1 Configuration parameters

- RemoteAddress Uniform resource locator by which the remote client can be reached.
- CertificateID ID of the certificate to be used for client authentication.
- UserLevel Authorization level that will be assigned to the uplink connection
- Status Current connection status

Field RemoteAddress is used as a key of the list of uplink configurations.

8.2.2 GetUplinks

A device supporting uplinks shall support this command to retrieve the configured uplink configurations. The Status field shall signal whether a connection is Offline, Connecting or Online.

REQUEST

<empty>

RESPONSE

- **Configuration – optional, unbounded [Configuration]**

List of configurations

8.2.3 SetUplink

A device supporting uplinks shall support this command to add or modify an uplink configuration. The Status property of the UplinkConfiguration shall be ignored by the device. A device shall use the field RemoteAddress to decide whether to update an existing entry or create a new entry.

REQUEST

- **Configuration – [UplinkConfiguration]**

Configuration to be added or modified.

RESPONSE

<empty>

8.2.4 DeleteUplink

A device supporting uplinks shall support this command to remove an uplink configuration.

REQUEST

- **RemoteAddress – [xs:anyURI]**

Configuration to be deleted.

RESPONSE

<empty>

8.2.5 Capabilities

- **MaxUplinks** Maximum number of uplink connections that can be configured.

Annex A (informative)

Addressing scheme

A.1 Overview

Annex A defines a globally unique addressing scheme that can be used to address devices like cameras, DVRs and others. The scheme includes information for area and device type.

Figure A.1 shows the order of the four fields in the 20-digit encoding scheme:

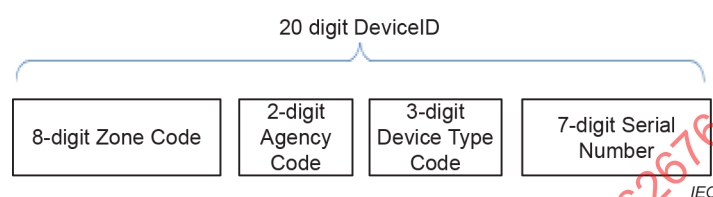


Figure A.1 – Fields of the device ID scheme

The device ID and ID of other resources should finish the initial configuration in the bottom platform.

A.2 Field definitions

A.2.1 Zone code

The eight-digit zone code is split into four two-digit items as shown in Table A.1.

Table A.1 – The zone code elements

2 digits	2 digits	2 digits	2 digits
Province	City	District	Unit

The first six digits are the administrative division code, which depends on the location of the surveillance center and meets the requirement of GB/T 2260-2007, similar to the postcode. For example, the code of city X is 420100.

The unit code is defined by users, such as police stations. It starts from 01, 00 represents the surveillance center.

A.2.2 Agency code

Table A.2 defines the two-digit agency codes.

Table A.2 – Industry coding

Code type	Name	Subject	Notes
00	Urban roadway	Government offices	includes urban roadway, commercial avenue, public areas and key areas, etc.
01	Society community		includes residential districts, buildings, and cybercafés, etc.
02	Social security agency		includes public security buildings and detention rooms
03	Other security agencies		
04	Traffic roadway		includes road arteries, national roadways and highways
05	Traffic checkpoints		includes crossroads, E-police, checkpoint and toll gate, etc.
06	Traffic management agency		includes traffic control office buildings, etc.
07	Agency relates to traffic management		
08	City management		
09	Health and environmental management		
10	Commodity inspection and custom		
11	Education		
12-39			Reserved 1
40	Farming, forestry, animal husbandry and fishery	Enterprise/administrative institution	
41	Mining		
42	Manufacturing		
43	Metallurgy		
44	Electric power		
45	Gas		
46	Construction		
47	Logistics		
48	Postal services		
49	IT		
50	Hotels and catering		
51	Financing		
52	Real estate		
53	Commercial services		
54	Water resources enterprises		
55	Entertainment		
56-79			Reserved 2
80-89		Application area	Reserved 3
90-99		Other entities	Reserved 4

A.2.3 Device type code

Table A.3 defines the three-digit device type codes.

Table A.3 – Device type codes

Code value	Device type	Notes
111	DVR	111-130: Front-end devices
112	Video server	
113	Encoder	
114	Decoder	
115	Video switching matrix	
116	Audio switching matrix	
117	Alarm controller	
118	NVR (network video recorder)	
119	Online information acquisition device	
120	Online information acquisition system	
121	Checkpoints on roadway	
130	HVR (hybrid video recorder)	
121-129	Extended front-end devices	
131	Camera	
132	IPC (IP camera)	
133	Display encoding	
134	Alarm input devices (IR alarm, smoke sensor alarm and access control, etc.)	
135	Alarm output devices (Alarm bell and alarm lamp)	
136	Audio input devices	
137	Audio output devices	
138	Mobile transmission devices	
139	Other peripheral devices	
140-149	Types of extended peripheral devices	
200	Central signaling control server (Signal networking unit)	200-299 indicates platform devices.
201	Web application server	
202	Media distribution server	
203	Proxy server	
204	Security server	
205	Alarm server	
206	Database server	
207	GIS server	
208	Management server	
209	Access gateway	
210	Media storage server	
211		
215	Traffic grouping	
216	Virtual grouping	
212-213 217-299	Extended device type	

Code value	Device type	Notes
300	Central user	300-399 indicates the central user.
301-343	Industrial role user	
344-399	Extended central user type	
400	Terminal user	400-499 indicates terminal user.
401-443	Industrial role user	
444-499	Extended central user type	
500	Signaling server of video/image information application platform	500-599 indicates the external servers of platform.
501	Signaling server of video/image information maintenance platform	
502	Video/image analysis device/system of public security	Newly-added in video/image library
503	Video/image information database of public security	Newly-added in video/image library
504	Video/Image information platform of public security	Newly-added in video/image library
505-599	Extended platform server (external)	
600-699	Extended type	600-699 indicates the extended types.

A.2.4 Serial number

Table A.4 shows the seven-digit serial number. It follows numerical order, which includes the location information, such as Subway – Subway Passage – Ticket Office – Platform – Subway Carriage.

Table A.4 – Serial number value

1 digit	6 digits
Network ID	Serial number of device or user

The Network ID is encoded as follows:

- 0, 1, 2, 3 and 4 refer to a surveillance alarm network;
- 5 refers to a public security network;
- 6 refers to a government network;
- 7 refers to the Internet;
- 8 and 9 are reserved.

A.2.5 Examples

IP Camera No.15 of metro line 1's No.10 ticket-check in city X:

City X	Metro line 1	Agency code	Device type code	Station No.	Ticket check	IPC No.
320100	01	07	132	10	08	015

Server No.02 of metro line 1's surveillance center in city X:

City X	Line 1	Agency code	Device type code	Invalid station No.	Invalid Ticket check	Server No.
320100	01	07	200	00	00	002

IECNORM.COM : Click to view the full PDF of IEC 62676-2-33:2022

Annex B (informative)

APIs with token adaption

B.1 General

Annex B provides guidance to implementers about the expected resource token handling of a VSS. Incoming global token might need to be transformed into device local tokens and tokens received from a device might need to be transformed into global tokens.

B.2 Consuming live video

- Media2:GetProfiles
Both incoming and outgoing profile and configuration tokens might need to be adapted.
- Media2:GetStreamingUri
The incoming profile token might need to be adapted. Additionally, the VSS needs to ensure that the streaming URI can be reached by the client. This may include a streaming proxy service.
- Media2:GetSnapshotUri
The incoming profile token might need to be adapted. Additionally the VSS needs to ensure that the snapshot URI can be reached by the client. This may include a proxy service.

B.3 Controlling PTZ cameras

For all the below listed functions, the incoming profile token shall be adapted.

- PTZ:AbsoluteMove, PTZ:ContinuousMove
- PTZ:Stop
- PTZ:GetPresets, PTZ:GotoPreset
- PTZ:SendAuxiliaryCommand

B.4 Retrieving recordings

- RecordingSearch:GetRecordingInformation
Both incoming and outgoing recording and track tokens might need to be adapted.
- RecordingSearch:FindRecordings
Both incoming and outgoing recording, track and search tokens might need to be adapted.
- RecordingSearch:GetRecordingSearchResults
Both incoming and outgoing recording, track and search tokens might need to be adapted.
- RecordingSearch:EndSearch
The incoming search tokens might need to be adapted.
- Replay:GetReplayUri
The incoming recording token might need to be adapted. Additionally, the VSS needs to ensure that the streaming URI can be reached by the client. This may include a streaming proxy service.

B.5 Forwarding of events

Typically the source section contains tokens that might need to be adapted.

Bibliography

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

IEC 60839-11-33, *Alarm and electronic security systems – Part 11-33: Electronic access control systems – Access control configuration based on Web services*

IEC 62676-2-31, *Video surveillance systems for use in security applications – Part 2-31: Live streaming and control based on web services*

IEC 62676-2-32, *Video surveillance systems for use in security applications – Part 2-32: Recording control and replay based on web services*

IECNORM.COM : Click to view the full PDF of IEC 62676-2-33:2022

SOMMAIRE

AVANT-PROPOS	28
INTRODUCTION.....	30
1 Domaine d'application	31
2 Références normatives	31
3 Termes et définitions	31
4 Vue d'ensemble	32
4.1 Généralités	32
4.2 Accès à distance.....	32
4.3 Liaison montante au nuage	33
5 Exigences.....	34
5.1 Généralités	34
5.2 Exigences fonctionnelles.....	34
5.3 Exigences relatives au protocole.....	35
6 Adressage des ressources	36
6.1 Adressage par jetons	36
6.2 Jetons distants.....	36
6.3 Contexte des jetons	37
7 Requêtes sur les ressources	37
7.1 Généralités	37
7.2 Événement de ressource	38
7.3 Filtre d'emplacement.....	38
7.4 Filtre de préfixe.....	38
7.5 Filtre de domaine d'application.....	39
7.6 Filtre de sélection	39
7.7 Vérifications en direct	39
7.8 Exemples informatifs.....	40
7.8.1 Vidéos en direct.....	40
7.8.2 Analyses d'investigation	40
8 Liaison montante	41
8.1 Protocole.....	41
8.1.1 Etablissement de la connexion	41
8.1.2 Gestion de la connexion	41
8.1.3 Authentification.....	42
8.1.4 Trames HTTP/2	42
8.1.5 Transactions HTTP.....	42
8.2 Interface de configuration	42
8.2.1 Paramètres de configuration	42
8.2.2 GetUplinks.....	43
8.2.3 SetUplink.....	43
8.2.4 DeleteUplink	43
8.2.5 Fonctionnalités	43
Annexe A (informative) Schéma d'adressage	44
A.1 Vue d'ensemble	44
A.2 Définition des champs.....	44
A.2.1 Code de zone	44
A.2.2 Code d'agence	44

A.2.3	Codes de type de dispositif.....	45
A.2.4	Numéro de série	47
A.2.5	Exemples	47
Annexe B (informative) API avec adaptation des jetons		49
B.1	Généralités	49
B.2	Consommation des vidéos en direct.....	49
B.3	Contrôle des caméras PTZ	49
B.4	Extraction des enregistrements	49
B.5	Transfert d'événements	49
Bibliographie.....		50
Figure 1 – Exemple de système hiérarchique.....		33
Figure 2 – Connexion normalisée établie par le client		33
Figure 3 – Connexion établie par le dispositif.....		34
Figure 4 – Séquence d'établissement de la connexion		41
Figure A.1 – Champs du schéma d'ID de dispositif		44
Tableau A.1 – Eléments du code de zone		44
Tableau A.2 – Codage des secteurs		45
Tableau A.3 – Codes de type de dispositif		46
Tableau A.4 – Valeur du numéro de série		47

IECNORM.COM : Click to view the full PDF of IEC 62676-2-33:2022

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

SYSTÈMES DE VIDÉOSURVEILLANCE DESTINÉS À ÊTRE UTILISÉS DANS LES APPLICATIONS DE SÉCURITÉ –

Partie 2-33: Protocoles de transmission vidéo – Liaison montante au nuage et accès au système de gestion à distance

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 62676-2-33 a été établie par le comité d'études 79 de l'IEC: Systèmes d'alarme et de sécurité électroniques. Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
79/658/FDIS	79/666/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Une liste de toutes les parties de la série IEC 62676, publiées sous le titre général *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité*, se trouve sur le site web de l'IEC.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de ce document indique qu'il contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Les systèmes de surveillance constituent un élément important des projets de sécurité publique qui visent à maintenir l'ordre et la sécurité publique. Ces systèmes aident également la police dans ses analyses d'investigation. Pour des raisons d'organisation et de sécurité, les systèmes de surveillance à grande échelle sont divisés en segments, ce qui peut créer des silos d'informations. Le présent document fournit une interface normalisée pour les systèmes de gestion afin que les entités autorisées puissent accéder facilement aux informations distantes en utilisant le même mécanisme que celui actuellement utilisé pour l'accès aux informations locales.

IECNORM.COM : Click to view the full PDF of IEC 62676-2-33:2022

SYSTÈMES DE VIDÉOSURVEILLANCE DESTINÉS À ÊTRE UTILISÉS DANS LES APPLICATIONS DE SÉCURITÉ –

Partie 2-33: Protocoles de transmission vidéo – Liaison montante au nuage et accès au système de gestion à distance

1 Domaine d'application

Le présent document spécifie les interfaces et les mécanismes des systèmes de gestion pour un accès opérationnel à distance aux dispositifs de sécurité physiques tels que les dispositifs et les systèmes de vidéosurveillance. Pour la vidéosurveillance, les cas d'utilisation concernent l'accès aux vidéos en direct et l'extraction des enregistrements. Les mécanismes définis dans le présent document ne se limitent pas aux applications de surveillance, mais couvrent également l'accès à distance aux systèmes de sécurité et aux systèmes de contrôle d'accès électronique. La configuration des dispositifs et des systèmes de gestion ne relève pas du domaine d'application du présent document.

L'Article 4 présente l'accès à la gestion à distance. L'Article 5 définit l'ensemble d'exigences dont le respect par le protocole est nécessaire. L'Article 6 étend le schéma d'adressage des ressources par jetons défini dans l'IEC 60839-11-31. L'Article 7 explique comment extraire les informations relatives aux ressources distantes. L'Article 8 définit comment se connecter aux dispositifs qui ne sont pas directement accessibles, par exemple lorsqu'ils sont situés derrière des pare-feu.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60839-11-31, *Systèmes d'alarme et de sécurité électroniques – Partie 11-31: Systèmes de contrôle d'accès électronique – Protocole de base d'interopérabilité en fonction des services Web*

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace* (disponible en anglais seulement)

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol*, Version 1.2 (disponible en anglais seulement)

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)* (disponible en anglais seulement)

IETF RFC 7540, *Hypertext Transfer Protocol Version 2 (HTTP/2)* (disponible en anglais seulement)

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <http://www.iso.org/obp>

3.1

ressource

entité IEC 62676-2 qui peut être adressée par un jeton

3.2

liaison montante

connexion au client distant établie par le service local

4 Vue d'ensemble

4.1 Généralités

L'IEC 62676-2-31 et l'IEC 62676-2-32 établissent une définition de protocole complète pour interagir avec les dispositifs de vidéosurveillance comme les caméras et les enregistreurs numériques. L'IEC 60839-11-32 et l'IEC 60839-11-33 décrivent également comment surveiller et configurer les systèmes de contrôle d'accès électronique. Ces deux parties reposent sur l'IEC 60839-11-31, qui spécifie un mécanisme de communication fondé sur les services web. Le présent document étend l'IEC 60839-11-31 en ajoutant la connectivité au nuage et l'adressage à distance au cadre d'application. Noter que le présent document ne comporte aucune information spécifique au domaine, car toutes les interfaces définies dans les parties mentionnées ci-dessus sont applicables sans aucune modification. Par conséquent, le présent document traite de l'intégration d'une vaste gamme de systèmes de sécurité physique au sein d'un système de gestion. Le présent document décrit notamment comment un client ou un système de gestion distant se connecte aux ressources telles que des caméras. L'approche présentée permet un déploiement selon plusieurs niveaux hiérarchiques. Les exemples en 4.2 représentent le principe de fonctionnement d'un mécanisme à deux couches de systèmes de vidéosurveillance (VSS, *Video Surveillance Systems*), désignées "niveau inférieur" et "niveau supérieur". Dans ce système, un VSS de niveau supérieur peut extraire une ressource telle que des informations de dispositif à partir d'un VSS de niveau inférieur pour permettre aux différents dispositifs connectés au VSS de niveau inférieur de déclencher les actions adéquates.

L'accès au VSS distant peut exiger l'application de contraintes d'authentification rigoureuses. Les définitions associées ne relèvent pas du domaine d'application du présent document.

4.2 Accès à distance

La Figure 1 représente la topologie type d'un système de gestion déployé dans une installation de plus grandes dimensions. Les systèmes de vidéosurveillance dits de niveau inférieur comprennent plusieurs caméras de surveillance et d'autres équipements qui couvrent une zone dans des locaux ou un quartier d'une ville. Des systèmes de gestion vidéo de niveau supérieur permettent la supervision de vastes complexes.

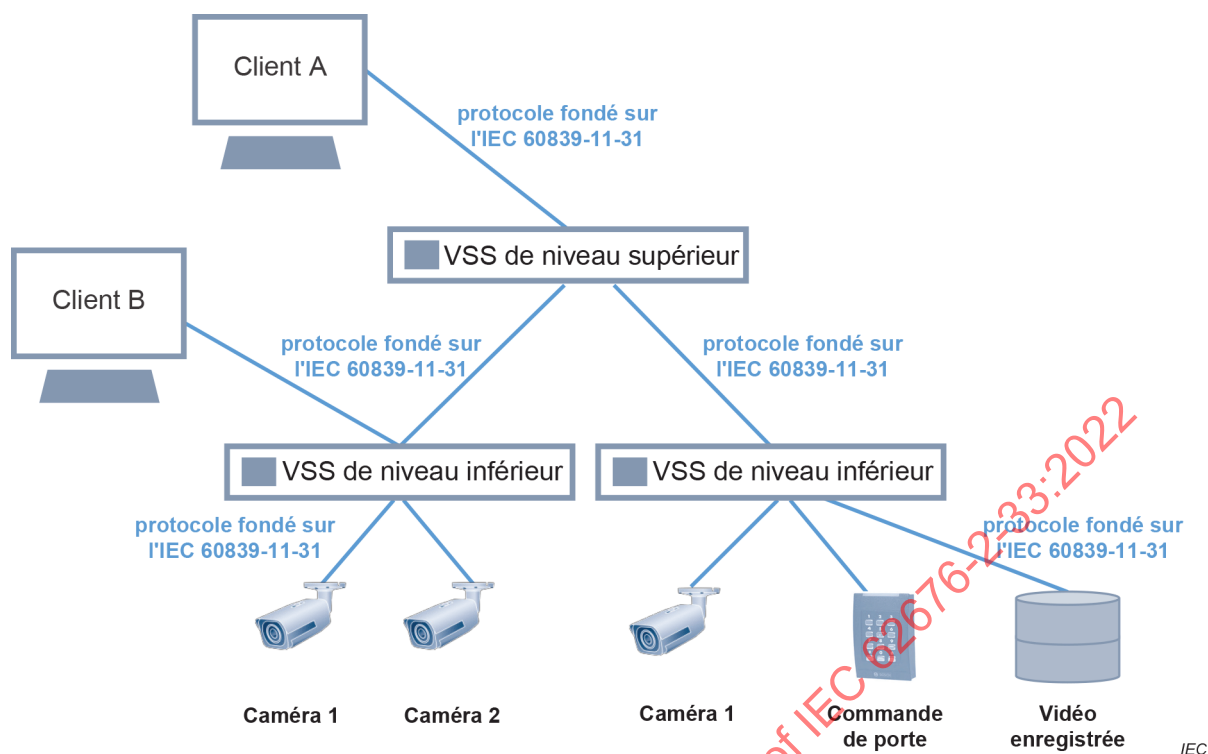


Figure 1 – Exemple de système hiérarchique

D'une manière similaire aux caméras représentées sur la Figure 1, les VSS comportent une interface vers la couche supérieure qu'un client peut utiliser afin d'accéder aux ressources inférieures. Généralement, le VSS restreint l'accès à certaines de ses ressources selon l'autorisation accordée au client.

Le présent document ne définit pas une nouvelle interface, mais établit un ensemble limité de règles qui expliquent comment un VSS doit présenter les ressources à une entité de la couche supérieure. Les dispositifs qui mettent en œuvre l'IEC 60839-11-31 gèrent l'adressage des ressources au moyen de jetons pour lesquels le présent document définit un ensemble limité de règles de mise en correspondance. Dans l'exemple de la Figure 1, le système de vidéosurveillance de niveau supérieur et les clients A et B peuvent utiliser exactement la même interface que celle actuellement utilisée par le système de vidéosurveillance de niveau inférieur afin de contrôler une caméra.

4.3 Liaison montante au nuage

Selon l'IEC 60839-11-31, le client établit une connexion avec un dispositif de la manière représentée sur la Figure 2.

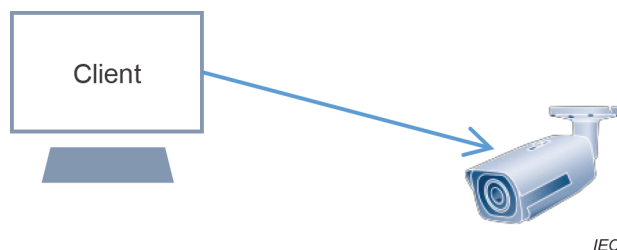


Figure 2 – Connexion normalisée établie par le client

Ce mécanisme de connexion fonctionne très bien dans les réseaux normalisés. Toutefois, lorsque le dispositif est situé derrière un pare-feu et que le client réside dans le nuage, le client ne peut pas établir la connexion. Dans ce cas, il est nécessaire que le dispositif établisse la connexion. Ce type de connexion est appelé "liaison montante"; elle nécessite d'être établie par le dispositif de la manière représentée sur la Figure 3.

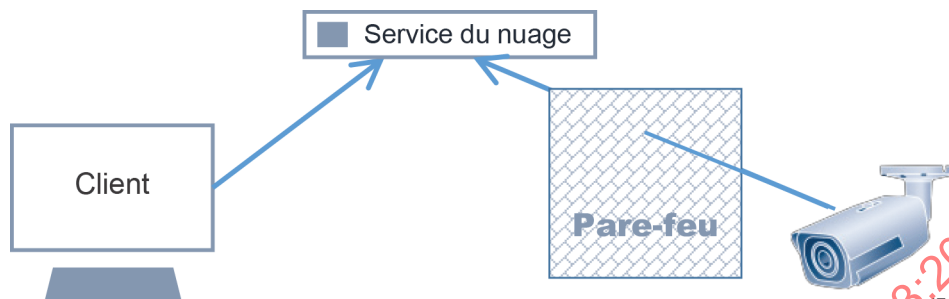


Figure 3 – Connexion établie par le dispositif

Le présent document spécifie une solution qui permet à une caméra ou à un système de gestion d'utiliser une liaison montante pour mettre en œuvre les fonctionnalités de serveur web et de serveur RTSP existantes selon le protocole HTTP/2.

5 Exigences

5.1 Généralités

Pour interconnecter le système de vidéosurveillance de niveau supérieur (H-VSS, *High-level VSS*) et le système de vidéosurveillance de niveau inférieur (L-VSS, *Low-level VSS*), le système est soumis à quelques exigences de base.

5.2 Exigences fonctionnelles

Les exigences fonctionnelles complètes pour l'interconnexion du H-VSS et du L-VSS sont décrites selon deux axes: utilisation des ressources et configuration des ressources.

Pour l'utilisation des ressources acquises par le H-VSS auprès du L-VSS, les exigences suivantes sont décrites.

- a) contrôle de la diffusion directe en continu: diffusion directe en continu à la demande, prise en charge de l'affichage, l'agrandissement, la capture et l'enregistrement d'images à la demande, prise en charge de l'accès multiutilisateur à la demande et en simultané aux mêmes ressources d'image;
- b) extraction et lecture d'images d'archive: extraction, lecture et téléchargement des données d'images d'archive du dispositif stockées sur le réseau, en fonction des éléments spécifiés tels que l'équipement, le canal, l'heure, les informations d'alarme, etc. La lecture comprend les fonctions et modes suivants: lecture normale, lecture accélérée, ralenti, arrêt sur image, capture d'image et agrandissement. Les informations d'enregistrement résident dans le L-VSS;
- c) commande à distance: le dispositif peut être commandé à distance de manière manuelle ou automatique, par exemple au moyen d'une caméra PTZ (Pan, Tilt, Zoom). Prise en charge facultative du verrouillage pour bénéficier d'un accès exclusif;
- d) sortie de l'image décodée: décodage des images en temps réel; le résultat peut être affiché. Commande à distance du mur d'images du L-VSS;

- e) gestion du stockage: gestion hiérarchique du stockage distribué, qui combine le stockage sur le dispositif et le stockage chez le client, afin de prendre en charge les différents paramètres de stockage (site, heure, stratégie de sauvegarde, stratégies de rendu final, etc.):
- transfert du contenu entre le L-VSS et le H-VSS.
- f) gestion des clients: le L-VSS envoie les informations de gestion au H-VSS lorsque celui-ci en fait la demande:
- lorsqu'un nouveau dispositif est ajouté au système, il convient que le L-VSS transmette les informations relatives à ce dispositif au H-VSS;
 - synchronisation des horloges: il convient que les horloges du H-VSS et du L-VSS soient synchronisées et que la source d'horloge de niveau supérieur constitue la sauvegarde de la source d'horloge de niveau inférieur;
 - prise en charge de la sécurité du transport entre le H-VSS et le L-VSS;
 - gestion des demandes d'informations du H-VSS concernant le L-VSS (fabricant, modèle et version de l'équipement, et autres informations de base).
- g) gestion des utilisateurs:
- prise en charge des fonctions suivantes: enregistrement d'utilisateurs, authentification, gestion des autorisations, contrôle d'accès, transmission et audit de l'identifiant utilisateur entre le L-VSS et le H-VSS;
 - octroi des autorisations de contrôle d'accès sur les ressources adéquates aux différents utilisateurs;
- h) gestion des journaux: prise en charge de la journalisation dans le L-VSS et des requêtes envoyées par le H-VSS au L-VSS;
- i) contrôle d'accès: le VSS peut prendre en charge le service de contrôle d'accès.

5.3 Exigences relatives au protocole

Le présent paragraphe répertorie les exigences applicables aux protocoles de services web entre deux VSS de niveaux différents:

- le L-VSS doit signaler ses caméras. Le L-VSS doit informer le H-VSS de toute modification concernant ses caméras associées;
- un L-VSS situé derrière un pare-feu doit être en mesure de se connecter à un H-VSS par Internet;
- requête d'informations sur le dispositif:
il convient que le protocole prenne en charge les requêtes hiérarchiques afin de collecter les informations d'annuaire des dispositifs. Les informations d'annuaire d'un dispositif comprennent le nom du fabricant, l'ID, le nom, le type, l'adresse, le mode et l'état du dispositif, etc. Un élément CameraID peut être utilisé pour regrouper les informations de dispositif;
- contrôle de l'autorité:
attribution de noms d'utilisateur et mots de passe spécifiques aux différents administrateurs afin de limiter les droits d'administration, le périmètre de gestion, les horaires de connexion et la plage d'adresses IP de connexion des administrateurs pour assurer une autorisation de gestion plus complète;
- contrôle de la diffusion directe en continu:
comme cela est défini dans le document IEC 62676-2-32 relatif aux services multimédias, la commande GetStreamUri définit comment il est prévu que les données codées soient transmises au client. Cette commande peut être étendue afin de prendre en charge la diffusion en continu hiérarchique.

6 Adressage des ressources

6.1 Adressage par jetons

Les dispositifs qui mettent en œuvre l'IEC 60839-11-31 gèrent l'adressage des ressources au moyen de jetons. Les jetons sont des chaînes de caractères d'une longueur définie et sont énumérés par le dispositif afin de faciliter la gestion des ressources de dispositifs. De manière similaire, le présent document admet par hypothèse qu'un VSS énumère ses ressources de dispositifs en affectant un jeton unique à chacune de ses ressources de dispositifs connectées.

En outre, le présent document admet par hypothèse qu'un VSS met en œuvre la mise en correspondance des jetons de ressources en ajoutant un préfixe délimité par un deux-points. Le comportement du VSS (ajout d'un préfixe à un jeton de dispositif ou nouvelle mise en correspondance complète) ne relève pas du domaine d'application du présent document.

La liste suivante répertorie quelques-unes des ressources qui peuvent être gérées:

- profils et configurations de supports, y compris affichages à l'écran (OSD, *On-Screen Display*) et masques;
- sources vidéo et audio;
- entrées numériques et sorties de relais;
- verrous de portes et lecteurs de cartes;
- enregistrements, pistes d'enregistrement et travaux d'enregistrement.

Le présent document utilise le mécanisme d'événement de propriété défini dans l'IEC 60839-11-31 pour modéliser les ressources globales. Un client ou un système de vidéosurveillance de niveau supérieur s'abonne au point d'extraction d'un système de vidéosurveillance. Lors des demandes consécutives, il procède à l'extraction de toutes les ressources qui l'intéressent afin d'identifier l'ensemble des ressources pertinentes d'un système de vidéosurveillance de niveau inférieur. Dès qu'il reçoit une ressource, il peut lui appliquer une action.

Lorsque toutes les ressources ont été déclarées, les messages d'extraction supplémentaires signalent les modifications ou expirent en l'absence de modification. Dans ce contexte, les modifications sont des ressources ajoutées, une modification des propriétés des ressources ou des ressources supprimées. En appliquant le mécanisme de notification d'événement de propriété aux ressources, un client ou un système de vidéosurveillance de niveau supérieur dispose toujours des dernières informations à jour concernant les ressources des systèmes de vidéosurveillance de niveau inférieur qui l'intéressent.

6.2 Jetons distants

L'IEC 60839-11-31 prend pour hypothèse que les jetons définis par le dispositif sont uniques dans un dispositif et son contexte. Le présent document étend le schéma pour permettre la création de jetons globalement uniques, appelés "jetons distants".

Un jeton distant doit être construit comme un QName avec un préfixe spécifique au dispositif et un jeton local.

RemoteToken = préfixe + ':' + LocalToken

La longueur de chaîne totale du jeton distant est limitée à 64 caractères. Un jeton local ne doit pas dépasser 36 caractères; il convient également qu'il ne comporte pas de deux-points. La longueur limite est choisie de manière à permettre l'utilisation des identificateurs uniques universels (UUID, *Universally Unique Identifier*) définis dans la RFC 4122. Noter que les mises en œuvre de dispositifs utilisent généralement des jetons compacts.

Un VSS doit utiliser le même préfixe pour l'ensemble des jetons du même dispositif. Cela permet à un client de comprendre quels jetons il peut utiliser pour les appels d'API de services web.

Un VSS peut choisir d'utiliser simplement des jetons locaux de dispositifs au sein d'une partie LocalToken ou alors d'effectuer une mise en correspondance interne. Un client peut ne pas prendre pour hypothèse que les jetons transmis par un VSS peuvent être utilisés dans les appels de dispositifs en supprimant le préfixe.

Les conventions de dénomination de la partie préfixe ne relèvent pas du domaine d'application du présent document. Selon la zone d'application, les personnes en charge de la mise en œuvre peuvent choisir différentes approches. Par conséquent, le présent document n'exige pas que les jetons distants soient globalement uniques entre les différents systèmes de vidéosurveillance. L'Annexe A fournit une définition par pays des adresses globalement uniques.

L'Annexe B fournit un guide relatif à l'adaptation des jetons.

6.3 Contexte des jetons

Les clients qui communiquent simultanément avec plusieurs serveurs, comme des VSS et/ou des dispositifs, doivent adresser les ressources stockées sur un serveur en utilisant uniquement les jetons transmis par ce serveur. Il n'est pas assuré que les jetons distants transmis par un serveur puissent être utilisés pour adresser la même ressource stockée sur un autre serveur.

7 Requêtes sur les ressources

7.1 Généralités

Le présent document modélise les ressources sous forme d'événements de propriété. Une ressource est un élément de configuration adressé par un jeton.

Les ressources sont interrogées et signalées par le mécanisme d'événement. Ce mécanisme offre deux avantages par rapport à une interface de requête classique. Premièrement, il peut traiter des réponses très volumineuses en découpant les paquets de réponse en plusieurs cycles d'extraction. Deuxièmement, il comporte une fonction de mise à jour en temps réel afin que les services puissent informer très efficacement les clients des modifications concernant les ressources.

Un serveur qui prend en charge les requêtes sur les ressources doit signaler celles qui sont prises en charge par le biais de l'interface `GetEventProperties` du service d'événements. Les ressources suivantes peuvent être énumérées:

pour les configurations de supports:

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

pour les profils de supports: `MediaProfile`.

7.2 Événement de ressource

Chaque ressource est mise en correspondance avec la définition d'événement suivante:

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

L'élément source Token est obligatoire et doit contenir un jeton qualifié unique au sein du système serveur.

Les éléments de données sont facultatifs.

Le domaine d'application de l'élément de données fait référence à l'entrée du domaine d'application de découverte définie dans l'IEC 60839-11-31. Il peut apparaître plusieurs fois pour chaque entrée de domaine d'application prise en charge par le dispositif.

Un événement doit être généré avec l'élément PropertyOperation défini sur "Initialized" chaque fois qu'une ressource est signalée pour la première fois dans un abonnement ou lorsqu'une ressource est nouvellement ajoutée au système. Un événement dont l'élément PropertyOperation est défini sur "Deleted" doit être généré lorsqu'une ressource est supprimée du système.

Une modification de "online" vers "offline" ou inversement ne doit créer un élément PropertyOperation de type "Changed" que si l'événement contient un élément booléen d'état "Offline".

7.3 Filtre d'emplacement

Un service qui prend en charge les requêtes sur les ressources doit prendre en charge le filtre d'emplacement (élément LocationFilter).

```
<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>
```

Les dispositifs dont l'emplacement est inconnu doivent avoir une correspondance si la propriété includeUnknown est définie.

7.4 Filtre de préfixe

Un serveur qui prend en charge les requêtes sur les ressources doit prendre en charge le filtre de préfixe (élément PrefixFilter). Le filtre de préfixe permet de limiter la recherche aux événements d'un dispositif en fonction du préfixe attribué par le système de gestion vidéo (VMS, *Video Management System*).

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

7.5 Filtre de domaine d'application

Un serveur qui prend en charge une requête sur les ressources doit prendre en charge le filtre de domaine d'application (élément ScopeFilter) qui permet de rechercher des entrées de domaine d'application de dispositifs.

```
<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>
```

Pour connaître les règles de mise en correspondance du domaine d'application, se reporter à l'IEC 60839-11-31.

7.6 Filtre de sélection

Un serveur qui prend en charge une requête sur les ressources doit prendre en charge le filtre de sélection (élément SelectFilter) qui permet de limiter les éléments de données résultants de chaque événement afin de réduire la taille des messages des requêtes volumineuses.

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

Chaque entrée définit une expression XPath qui correspond à l'un des éléments de données d'événement.

L'exemple suivant limite le contenu du résultat au nom de la ressource et au domaine d'application de l'emplacement:

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

7.7 Vérifications en direct

Le mécanisme défini dans le présent document utilise le point d'extraction en temps réel défini dans l'IEC 60839-11-31. Lorsqu'aucun événement n'est en attente à un point d'extraction donné, l'appel PullMessages expire après le délai défini par le client. Le client contrôle le délai d'expiration et peut assurer une surveillance continue du bon fonctionnement du serveur. Par conséquent, aucune interface de ping ni de surveillance de bon fonctionnement n'est nécessaire.

7.8 Exemples informatifs

7.8.1 Vidéos en direct

Dans cet exemple, un poste de police (client) souhaite obtenir les flux en direct relatifs à un incident survenu dans un lieu géographique donné.

- 1) Le client s'authentifie auprès du VSS à l'aide de son certificat client.
- 2) Le client s'abonne à la rubrique Resource/MediaProfile du VSS situé à moins de 100 m du lieu géographique donné par une longitude et une latitude.
- 3) Le VSS répond à PullMessages en énumérant l'ensemble des profils de supports disponibles dans la zone donnée.
- 4) Si le client reçoit plusieurs profils pour un dispositif distant, il peut choisir le plus adapté en interrogeant les configurations de profils. Pour chaque jeton de profil, le client appelle GetProfiles. En définissant le paramètre Type sur VideoSource et VideoEncoder, le client reçoit des informations complètes sur la résolution de la vidéo et les paramètres de l'encodeur.
- 5) Le client appelle GetStreamUri pour chaque source vidéo du profil choisi.
- 6) Le client diffuse la vidéo et l'affiche sur le mur d'images de la police.

A première vue, il semble qu'aucune nouvelle interface fonctionnelle n'ait été définie. Même si cela est exact, le VSS doit encore mettre en œuvre un certain nombre d'opérations pour reproduire l'exemple ci-dessus:

- a) énumérer les profils des caméras associées sous forme d'événements de ressources;
- b) mettre en œuvre l'API Media2;
- c) mettre en correspondance le jeton de profil de support de demande avec les caméras et leurs jetons locaux;
- d) mettre en correspondance les jetons de profil de réponse avec les jetons globaux;
- e) prendre en charge le proxy de diffusion en continu et mettre en correspondance l'URI du flux de la caméra avec le proxy.

En outre, un système de vidéosurveillance intelligent peut exposer à son client uniquement les profils de supports qui ont un débit de données suffisant pour pouvoir transmettre ces flux vidéo par le proxy.

Au lieu de se connecter directement aux systèmes de vidéosurveillance de niveau inférieur distants, le poste de police client peut se connecter à un système de vidéosurveillance de niveau supérieur qui regroupe à son tour les résultats de recherche de plusieurs systèmes de vidéosurveillance de niveau inférieur et transmet des commandes aux différentes sources de caméras par le biais du système de vidéosurveillance de niveau inférieur adéquat.

7.8.2 Analyses d'investigation

Dans cet exemple, un poste de police (client) souhaite extraire les enregistrements relatifs à un incident survenu dans un lieu géographique donné.

- 1) Le client s'authentifie auprès du VSS à l'aide de son certificat client.
- 2) Le client s'abonne à la rubrique Resource/VideoSource du VSS situé à une distance maximale de 100 m du lieu géographique donné par une longitude et une latitude.
- 3) Le VSS répond à PullMessages en énumérant l'ensemble des sources vidéo disponibles dans la zone donnée.
- 4) Le client appelle FindEvents en précisant la plage horaire concernée, ainsi qu'une liste de sources vidéo dans la zone de recherche.
- 5) Le client appelle GetEventSearchResults pour obtenir l'ensemble des enregistrements disponibles pour le lieu concerné et la période donnée.

- 6) Le client extrait les URI RTSP en appelant la méthode GetReplayUri pour l'enregistrement.
- 7) Le client lit les fichiers vidéo des caméras concernées en procédant à l'extraction du flux des supports RTSP pour l'URI extrait à l'aide d'un appel à Replay:GetReplayUri.

A défaut de l'approche décrite ci-dessus, le client peut aussi interroger directement la ressource d'enregistrement d'un lieu géographique. Certaines lectures peuvent échouer, notamment si les caméras n'ont pas réalisé d'enregistrement pour le lieu choisi à l'heure choisie.

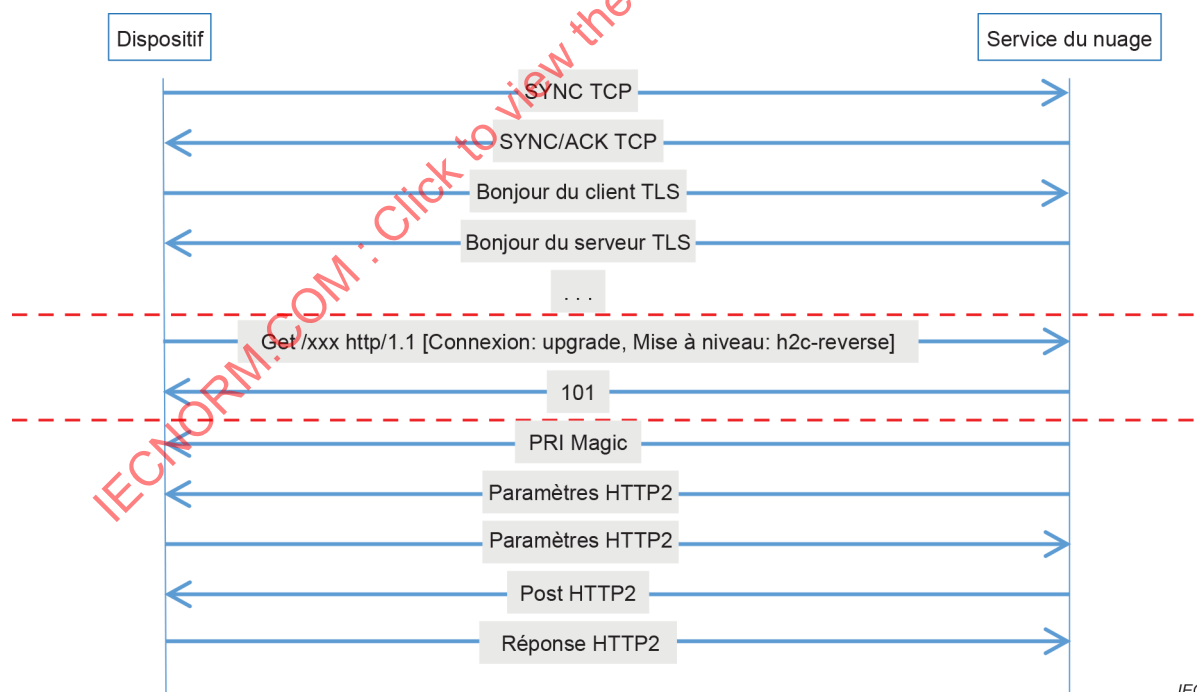
L'exemple ci-dessus s'applique au contenu stocké à la fois dans la caméra et sur le serveur d'enregistrement du VSS. L'application du système de gestion vidéo définit comment sont extraits les enregistrements.

8 Liaison montante

8.1 Protocole

8.1.1 Etablissement de la connexion

Le dispositif établit la connexion avec le service du nuage. La Figure 4 représente les trois phases du processus. Dans la première phase, le dispositif se comporte comme un client TLS (Transport Layer Security) qui se connecte au service du nuage. La figure représente les paquets les plus pertinents uniquement. Les informations relatives aux échanges TCP (Transmission Control Protocol) et TLS ne relèvent pas du domaine d'application du présent document. La deuxième phase comprend la mise à niveau de la connexion vers HTTP/2, que le service du nuage confirme en envoyant une réponse HTTP 101. La troisième phase consiste à vérifier que la connexion est totalement conforme HTTP/2 comme si le service du nuage en était l'initiateur.



IEC

Figure 4 – Séquence d'établissement de la connexion

8.1.2 Gestion de la connexion

Le client distant dispose d'un service local qui permet de maintenir un canal de communication opérationnel. Cette connexion est appelée "liaison montante", car la connexion doit être établie entre le service et le client distant. La liaison montante doit être sécurisée par TLS.