Physical Access Control with BACnet
White Paper

Abstract
This document outlines the use of existing definitions of as well as extensions to ANSI/ASHRAE 135-2004 BACnet to enable the implementation of and interfacing to Physical Access Control Systems using the BACnet data model and services. The extensions shall enable inter-domain interoperability and common user interfaces. They also enable the construction of Physical Access Control Systems containing devices of different product vendors and product generations. The extensions include new object types, alarming and logging.

This document represents the ongoing work of the SSPC135 LSS-Working Group, and the basis for proposed changes to the BACnet standard. The contents are subject to change. It is anticipated that some content of the document will become an informative Annex to the BACnet Standard.

Contributors
Bernhard Isler, Senior system architect, Fire Safety and Security Products, Siemens Building Technologies, Zug, Switzerland.
Hans-Joachim Mundt, Head of standards, Siemens Building Technologies, Karlsruhe, Germany
Rob Zivney, Vice President of Marketing, HIRSCH Electronics, Santa Ana, CA, USA
David Ritter, Senior software developer/technical lead for Access Control Products, Delta Controls, Surrey, BC, Canada.
Stephen Treado, Ph.D., P.E., Mechanical engineer, Building and Fire Research Laboratory with the NIST, Gaithersburg, MD, USA
Attendees of LSS-Working Group meetings since January 2003
Reviewers of HJM-002, the conceptual work document of the LSS-Working Group and base for this white paper

1 of 102
# Contents

1. **Introduction** ........................................................................................................................................... 4
   1.1 Purpose .................................................................................................................................................. 4
   1.2 Scope................................................................................................................................................... 4
   1.3 Audience ............................................................................................................................................. 4
   1.4 Related BACnet and Working Group Documents.............................................................................. 5
   1.5 Related Non-BACnet Documents....................................................................................................... 6

2. **Conceptual Overview** ............................................................................................................................ 7

3. **Physical Access Control** ....................................................................................................................... 8

4. **BACnet Application Model Overview** .................................................................................................. 10
   4.1 BACnet Processes .................................................................................................................................. 10
   4.2 BACnet Process Interface .................................................................................................................... 11
   4.3 BACnet Objects .................................................................................................................................... 12
   4.4 BACnet Application Services .............................................................................................................. 12
   4.4.1 BACnet Access Services .................................................................................................................. 12
   4.4.2 BACnet Notification Services ......................................................................................................... 13

5. **PACS Functional Decomposition** ......................................................................................................... 14
   5.1 Credential Reader Process .................................................................................................................... 15
   5.1.1 Reading, Imaging, Card Communication ........................................................................................ 15
   5.1.2 Indicators, Keypad, etc. ................................................................................................................... 16
   5.1.3 Authentication Factor Processing ................................................................................................... 16
   5.1.4 Credential Data Access .................................................................................................................... 17
   5.1.5 Front Plate Control ........................................................................................................................... 17
   5.1.6 Deployment to Physical Structure ................................................................................................... 18
   5.2 Access Door Process ............................................................................................................................. 19
   5.2.1 Input, Output, Signal Conditioning .................................................................................................. 19
   5.2.2 Abstraction, Monitoring, Control .................................................................................................... 20
   5.2.3 Deployment to Physical Structure ................................................................................................... 20
   5.3 Authentication & Authorization Process ................................................................................................ 21
   5.3.1 Authorization ................................................................................................................................... 22
   5.3.2 Authentication .................................................................................................................................. 23
   5.3.3 Validation ......................................................................................................................................... 23
   5.3.4 Door Control.................................................................................................................................. 23
   5.3.5 Notification and Logging ................................................................................................................ 23
   5.3.6 Credential Database ......................................................................................................................... 23
   5.3.7 Replication & Synchronization ........................................................................................................ 24
   5.3.8 Deployment to Physical Structure ................................................................................................... 24

6. **PACS Data Model Overview** .................................................................................................................. 25

7. **Authentication & Authorization Interface** .......................................................................................... 28
   7.1 Geographical Organization .................................................................................................................. 28
   7.1.1 Access Point Object Type ................................................................................................................ 29
   7.1.2 Access Zone Object Type ................................................................................................................ 42
   7.2 Authentication ..................................................................................................................................... 48
   7.2.1 Access Credential Object Type ...................................................................................................... 49
   7.2.2 Access User Object Type ................................................................................................................. 57
   7.3 Authorization ....................................................................................................................................... 60
   7.3.1 Access Rights Object Type ............................................................................................................. 61
   7.3.2 Configuration and Validation of Access Rights ............................................................................. 64
   7.3.3 Time Ranges ................................................................................................................................... 66
   7.3.4 External Conditions ......................................................................................................................... 67
   7.3.5 Two-Person-Rules ............................................................................................................................ 67
1. Introduction

1.1 Purpose

BACnet is extending its scope to include Physical Access Control Systems (PACS) and functionality. This takes BACnet beyond HVAC, Lighting, Energy Consumption Management, Fire, etc..

Physical Access Control Systems (PACS) have requirements to the data model, services, alarming and logging, which are not well covered by BACnet. Although some manufacturers already have implementations based on BACnet or provide BACnet interfaces to such systems by using the current standard and proprietary extensions, a more comprehensive data model and services capability is required to allow:

- Interfacing PACS with systems of other BACnet domains (e.g. HVAC, Fire, Elevators, Lighting, etc.) for inter-domain interoperability,
- Interfacing PACS with systems of non-BACnet domains (e.g., Human Resource Management Systems)
- Unified user interfaces for all systems of a building (e.g. common workstation with common data representation and operation).
- Construction of Physical Access Control Systems containing devices of different product vendors and product generations.
- Harmonization with other industry standards, such as developed by the Security Industry Association (SIA).

This document defines the basic concept of Physical Access Control Systems from a BACnet perspective, and outlines the use of existing definitions and new extensions to ANSI/ASHRAE 135-2004 BACnet to model such systems. This will result in the ability to implement a PACS or a gateway to a PACS by using BACnet as the communication protocol and data model framework.

1.2 Scope

This document covers the extensions to BACnet for PACS and those elements of intrusion detection that are associated with doors. The BACnet data modeling concepts serve as a framework and base for these extensions; and the overall PACS model will use existing definitions as well. However, the existing BACnet definitions are not replicated herein.

Extensions for other security systems such as Closed Circuit TV (CCTV, Digital Video, or video surveillance) are not part of this document.

Application functionality is not required to be exposed through the data model. Such unexposed functionality is addressed as a local matter, according to BACnet convention.

As is becoming industry practice, the term Physical Access Control Systems or PACS is used herein to differentiate from Logical Access Control Systems which provide access to computers, information and networks. However, with “convergence” and one card solutions becoming more common, BACnet has embraced concepts that are expected to work well in a Logical Access implementation.

1.3 Audience

This document is intended for:

- ASHRAE SSPC 135 Life Safety & Security Working Group (LSS-WG)
- ASHRAE SSPC 135
- BACnet users, integrators and manufacturers
- Access Control Industry
1.4 Related BACnet and Working Group Documents

|-------|-----------------------------|----------------------|

Figure 1–1, Document Structure
## 1.5 Related Non-BACnet Documents

| --- | --- | --- |
2. Conceptual Overview

In order to understand what the BACnet standardization of PACS is about and what it covers, required prerequisites are to understand the application functionality of a PACS and to know the basic BACnet application model.

The PACS application functionality is decomposed into elements which can be mapped to the BACnet application model, and the dependencies and interfaces between these elements are identified. The data and service model of these interfaces is defined by using and extending the current BACnet data model (i.e. object types and properties). No new BACnet application services are added.

The BACnet interfaces defined include the new PACS models and reuse existing BACnet models. The interfaces are not specific to any client, and allow BACnet capable clients to easily be extended to support PACS. They support both manual operations through user interface devices and machine-to-machine interaction.

Manual operation covers tasks carried out manually by operators at a workstation or any other type of user interface.

- Browsing
- Operation
- Configuration
- Event Management
- Device Management
- Etc.

Machine-to-Machine Interaction covers tasks carried out by machines autonomously, without operator intervention. This could be devices of a PACS, or devices of other domains.

- Alarm and event logging
- Log archiving
- Automation
- Commanding
- Scheduling
- Trending
- Etc.
3. Physical Access Control

A Physical Access Control System (PACS) manages passage of people or assets through an opening in a secure perimeter based on a set of rules.

Users requesting passage through a secured perimeter are individual persons, assets or even a group of persons and / or assets. The general term used for this is access user. An access user has credentials assigned. An access user can have more than one physical credential if for instance the user visits different sites that implement different vendor technologies resulting in having to carry multiple cards.

Credentials may be physical credentials, e.g. cards carried by a person or bar code stickers at an asset. Physical credentials contain authentication factors, such as simple numbers or structured data. Physical credentials implicitly identify the user. Access user properties may be used as biometric authentication factors, e.g. fingerprint, hand-shape, or iris. Biometric authentication factors are typically processed and condensed into a biometric template, both for authentication and storage. Biometric authentication factors allow an explicit identification of a user. An access user also may know an authentication factor, typically a personal identification number (PIN). Authentication factors known by an access user allow implicit identification of access users only.

A credential reader can read one or more authentication factors and forwards the data to the authentication and authorization function. A read of an authentication factor typically starts the authentication and authorization process to decide on access. Different authentication factors may be required to be read for multi-factor authentication.

The opening in the secure perimeter is referred to as an access door. An access door can be any controlled opening in the secure perimeter including a door, a window, or a roof hatch. An access door in access control is a collection of physical devices. These physical devices typically include: An electromechanical lock, a door monitor switch (alarm contact), a request to exit device (REX or RQE) such as a pushbutton or motion detector. Special access doors may allow passage in one direction only.

The area or space enclosed by the secure perimeter is called a zone. A zone can have one or multiple doors that provide passage into or out of the zone. A door is always associated with two and only two distinct zones, one on each side. Where there are several zones at a site, a user typically moves from one zone to another.

The rules used to manage access through a secure perimeter are based on the concepts of authentication and authorization. Authentication is a process of proving identity based on comparison of the access user’s current authentication factors with those previously enrolled and maintained in the PACS database. Authorization is a process of checking one or more pre-defined validation rules, such that passing ALL validation checks is a pre-requisite to being granted access. A basic example of authorization validation checks would be the right to pass through a specific door at a specific time. It is not unusual to have numerous additional validation checks that might include: Two person rule, expiration date not yet passed, anti-passback, holiday, use count limits not reached, etc. The order that the elements of authentication and authorization are processed is a local matter.

An access point is a logical construct that binds authentication and authorization for passage to a geographical location. From an access zone viewpoint, an ingress access point is the point to enter the access zone, while an egress access point is the point to leave the access zone. An ingress access point is related with the credential readers outside of the access door, behind which the access zone to enter is. An egress access point is related with the credential reader inside the access door.
The access point determines which authentication factors are required for the authentication policy in effect. For instance, a card may be required during the day, but both a card and PIN are required after hours.

Access grants and denials, called transactions, are reported as events along with door forced open alarms (actually a shared Intrusion Detection function), and status such as a door being open and/or locked. A fundamental access control function is to temporarily “mask” (not shunt) a door forced open alarm for a predetermined time interval following an access grant. It is important to note that for an access zone to be “Secured”, the door(s) must be closed, locked and alarms unmasked.
4. **BACnet Application Model Overview**

The BACnet application model is based on processes running in devices. Processes implement and perform application functionality. A process may expose an interface accessible by processes of remote devices. The data model of exposed interfaces is based on BACnet objects. BACnet access services are used by remote processes to access BACnet objects, while the BACnet objects of the interface notify subscribed remote processes about changes of values and events.

Note: The BACnet Application Model is part of the BACnet framework. For further details of this framework, especially the underlying communication protocol stack and networking see clause “Functions and Features Inherent in the BACnet Framework”, or the BACnet standard [STD].

### 4.1 BACnet Processes

BACnet processes implement and perform application functionality. BACnet does not specify what the processes perform, or how, as these are considered a “local matter”. Multiple processes may run in a physical device.

Seen from outside of a device, processes may take a server or client role or both at the same time. In the server role, they expose a BACnet Process Interface to the network (the lollipop). In the client role, they use an exposed interface.

![Figure 4–1, Roles of BACnet Processes](image-url)
4.2 BACnet Process Interface

A BACnet process interface, as exposed to the network by a server role process, is the communication peer for remote client role processes to communicate with over the BACnet network. It provides standardized access to the functionality of a process. Multiple client role processes may communicate with one BACnet process interface. The data exposed in a BACnet process interface is a collection of BACnet objects. BACnet application services are used in the communication between the BACnet objects and a remote client role process.

![Figure 4-2, BACnet Process Interface](image)
4.3 BACnet Objects

BACnet objects are used to structure and identify data of a BACnet process interface. The BACnet standard defines object types and the properties they shall or may contain. The application functionality performed in a device, and through this the set of object instances in a physical device, is defined individually by vendors. The overall set of objects of the exposed interfaces of a device models the externally visible overall functionality of the device. BACnet mandates that one instance of a Device Object must be present in a device, to represent the device itself.

Every object type defines the required and optional properties an object instance of this type may have. Properties are of a defined BACnet Data Type, each composed of a defined set of primitive data types. They represent a property or feature of the object. Properties are used to represent:

- Identification
- Values used or provided by the process
- Parameters of the process
- State of object or the process
- Event states and event notification parameters
- Relations to other objects
- Etc.

Properties can be read and written by client role processes using various BACnet application services. Commanding an object is done through writing values to properties. Command arbitration is done by prioritizing commands, where the highest priority command wins. Objects are the source of notifications sent to client role processes. Notifications report about changes of values (COV) of properties or events and alarms detected.

4.4 BACnet Application Services

BACnet defines a set of application services for remote communication between processes and objects of networked devices. A service basically consists of a request and optionally a response message. Both the service request and the service response have defined parameters, composed of BACnet Data Types.

There are services defined for object access, change of values (COV) reporting, event reporting, and remote device management. Virtual terminal session services allow a device to provide a VT100 terminal style user interface on remote devices. The set of defined services can be classified in BACnet Access Services and BACnet Notification Services.

4.4.1 BACnet Access Services

BACnet Access Services are used to access properties of objects and commanding of objects. They are initiated by client role processes and addressed to objects for execution and response.

Since objects are used to expose the functionality of the server role process, the server role process effectively performs the execution of the service request and may return a response.

If the access is performed internal in a device (i.e. client and server role process in the same device), no service requests and responses are visible on the BACnet network. Such device internal services are not in the scope of BACnet definitions.
4.4.2 BACnet Notification Services

BACnet Notification Services are used to asynchronously notify subscribed client role processes on changes of value or changes of event state of objects. In order to receive notifications, the client role process subscribes to objects of interest using BACnet Access Services. Notification requests are initiated by objects and addressed to subscribed client role processes. There are two sub-classes of BACnet Notification Services:

- Change-Of-Value (COV) notifications when values of properties of an object change.
- Event notifications when the event state of an object changes.

Since objects are used to expose the functionality of the server role process, the server role process is effectively initiating notification service requests. The client role process is executing the service and typically provides a simple response indicating reception of the request.

If notification is performed internal in a device (i.e. client and server role process in the same device), no service requests and responses are visible on the BACnet network. Such device internal services are not in the scope of BACnet definitions.
5. **PACS Functional Decomposition**

The PACS as defined in this document is segmented into functional units to identify the fundamental logical PACS processes, the associated interfaces, and their interrelationship. Note that this is not a physical decomposition, but a functional one. This serves to identify the interfaces to these functional units. The data and service models of these interfaces can then be defined using BACnet objects.

![PACS Functional Decomposition Diagram](image)

**Figure 5–1, PACS Functional Decomposition**

The PACS includes the following logical processes, which are described in detail in the following sections:

- Credential Reader Process
- Access Door Process
- Authentication & Authorization Process

Note that, depending in part on the technology or intelligence being employed in the Credentials and Credential Reader as well as the Physical Door and its Electro-Mechanical Control and Monitoring Equipment, it could be argued that this equipment is or is not part of the PACS. Industry practitioners would consider this equipment as part of the PACS. Such determination has no impact to the BACnet interfaces, since hidden to those by the respective processes.
5.1 Credential Reader Process

The Credential Reader Process performs reading and validation of access credentials, control of indicators and / or keys at the reader front plate, may access other data of a credential etc. The exact functionality and implementation of this process is not part of the BACnet definitions; it is a local matter of the device or subsystem which implements it. Any physical structure or deployment of this functionality behind the BACnet Process Interface provided by this process is a local matter, hidden to the BACnet network. This includes non-BACnet reader device interfaces, such as Wiegand type interfaces, or reader to card communication.

The Credential Reader Process represents its functionality at its BACnet process interface, the Credential Reader Interface. This interface is subject of the BACnet standardization, and modeled in detail later in this document. Within a PACS, it is used by the Authentication & Authorization Process for access decisions. It may also be used by other processes performing other application functions, such as Time & Attendance, Guard Tour Monitoring, Muster Station, etc.

This process does not take any client role. Its operation is independent of other PACS processes.

5.1.1 Reading, Imaging, Card Communication

This part of the Credential Reader Process performs communication with access credentials or sensing of authentication factors. Depending on the technology, various types of one- or two-way communication may take place:

- Magnetic-stripe card reading
- Barcode reading
- Contact or contact-less smartcard communication
- Finger-print scanning
- Hand-shape scanning
- Iris scanning
- Imaging (e.g. for face recognition)
- Etc.

This functionality may be performed in a dedicated physical device, such as a card reader device, fingerprint scanner, camera, etc. The connection of such dedicated devices to the controller device, which contains the remaining parts of
the Credential Reader Process and provides the Credential Reader Interface, is outside the scope of BACnet standardization. Existing and upcoming industry standards are typically used for this connection (e.g. Wiegand).

The data generated by this functionality is considered a raw authentication factor. Some implementations may make this raw authentication factor data available at the Credential Reader Interface, for e.g. diagnostics purposes.

### 5.1.2 Indicators, Keypad, etc.:

This part of the Credential Reader Process manages front plate elements for interaction with the access user. It includes:

- Signaling LED’s
- Display (monochrome, color, text, graphics, etc.)
- Keypad
- Etc.

This functionality may also be performed in a dedicated device, such as a card reader device. The connection of such devices to the controller device, which contains the remaining parts of the Credential Reader Process and provides the Credential Reader Interface, is outside the scope of BACnet standardization. Existing and upcoming industry standards are typically used for this connection (e.g. Wiegand).

### 5.1.3 Authentication Factor Processing

The raw authentication factor data read from a credential, or e.g. produced by biometrics scanning, is processed and validated before made available at the Credential Reader Interface.

Reading data from a credential or imaging biometrics may include transferring such data from a non-BACnet reader device into a controller through any non-BACnet communication. Such communication is considered a local matter of the Credential Reader Process.

Processing and validation may include parity checks and strip-off of parity bits, structuring of data, authentication by certificates, verification of authenticity by hashing algorithms or a PIN, validation of expiry date information read with the factor, minutiae generation of biometrics etc. Failed processing may be indicated at the Credential Reader Interface. Resulting authentication factor data is presented at the Credential Reader Interface for any client role processes using that interface.

Any information used to validate an Authentication Factor itself is not required to be presented at the Credential Reader Interface, since the PACS does not use it for Authentication & Authorization. Such information is used by the Credential Reader Process itself for preprocessing and validation of Authentication Factors.

Examples:

- The credential reader process is able to read Wiegand numbers from a magnetic stripe card, to check parity bits and strip them off before providing the number at the Credential Reader Interface.
- If a PIV card is read, the entire Card Holder Unique Identifier (CHUID) is typically not used in the PACS, but either the FASC-N part or GUID is used in the PACS. The credential reader process is responsible to read the PIV card, to validate its content against expiration date, and may use the signature to further validate the CHUID. Then, it extracts the FASC-N from the CHUID and provides it as an authentication factor at the Credential Reader Interface.
- The raw scan of a fingerprint is analyzed, and a minutia of that scan is generated. The minutiae data is provided at the Credential Reader Interface as an authentication factor.

A Credential Reader Process may be capable of providing different subsets or formats of authentication factors, or different authentication factors. This capability is represented at the Credential Reader Interface through according BACnet objects.
### 5.1.4 Credential Data Access

The Credential Reader Process may make credential data accessible. This is data, available on some credentials, may be for example smart card blocks or credits. Although this is out of scope of PACS, the Credential Reader Process may, at its Credential Reader Interface, provide models for such content and making it accessible for reading and writing it by any client role process.

### 5.1.5 Front Plate Control

A Credential Reader Process controls front plate elements for input from and indication to the access user. Such elements may be:

- Keypads
- LED indicators
- LCD displays
- Etc.

Access to such elements by client role processes may be provided at the Credential Reader Interface.
5.1.6  Deployment to Physical Structure

BACnet basically does not define how functionality is deployed to physical devices. Any physical structure may be possible behind a BACnet process interface. Sample deployments are:

- The entire process is deployed into an intelligent reader device. This would result in a reader device which has a BACnet network connection.

- In case the functionality is distributed over a reader device and a controller, the Credential Reader Interface is provided by the controller, accessible through its BACnet network connection. Communication between the reader device and the controller is a local matter of the process, not defined by BACnet. Such communication may be based on any access control industry common communication protocol.

Figure 5–3, Example Deployment of the Credential Reader Process
5.2 Access Door Process

The Access Door Process performs the control and monitoring of the mechanical entrance equipment, the access door. The exact functionality and implementation of this process is not part of the BACnet definitions; it is a local matter of the device or subsystem which implements it. Any physical structure or deployment of this functionality behind the BACnet process interface provided by this process is a local matter, hidden to the BACnet network. The means how this process communicates with the mechanical door equipment such as drives, locks etc. is a local matter, outside the scope of BACnet.

This process represents its functionality at its BACnet process interface, the Access Door Interface. This interface is subject of the BACnet standardization, and modeled later in this document. Within a PACS, it is used by the Authentication & Authorization Process to control entrance based on access decisions. It may be used by other processes performing other applications, such as Schedulers, Fire Systems, Intrusion Detection Systems, etc.

This process does not take any client role. Its operation is independent of other PACS processes.

5.2.1 Input, Output, Signal Conditioning

Sensors at the door provide input to the process. Such input may be conditioned before further processing. This may include adaptation curves, debouncing etc. Inputs may also be made accessible individually at the Access Door Interface. Sensors may be:

- Lock contacts
- Dead-bolt contacts
- Door closed contacts
- Emergency stop buttons
- Operation continuation buttons or sensors (e.g. inside revolving doors)
- Movement detectors
- Request-to-exit buttons
- Manual open buttons
- Handle switches
- Etc.

Actuators at the door are used to enable control of the door by the process. Such actuators may also be made accessible individually at the Access Door Interface. Actuators may be:

- Dead-bolt coils
- Electric strikes
- Drives (e.g. sliding doors)
- Etc.
5.2.2 Abstraction, Monitoring, Control
The individual elements of a door are abstracted into a uniform model of a door, to simplify and standardize control and monitoring of various door types by external client processes. This includes monitoring of the door state and status based on sensor values, as well as control of individual actuators. Such control may include timing, speed, interlocks etc.

The abstracted door functionality is made accessible at the Access Door Interface.

5.2.3 Deployment to Physical Structure
BACnet basically does not define how functionality is deployed to physical devices. Any physical structure may be possible behind a BACnet process interface. Sample deployments are:

- The entire process is deployed into an access controller. The door sensors and actors are directly connected to the access controller. The Access Door Interface is accessible through the access controller’s BACnet connection.

- The door has its own door controller device, unaware of whether it is used by a PACS. The door sensors and actors are connected to that door controller. The door controller makes the Access Door Interface accessible through its BACnet connection. An access controller device would use the BACnet connection to interact with the door.

![Figure 5–5, Example Deployment of the Access Door Process](image-url)
5.3 Authentication & Authorization Process

The Authentication & Authorization process performs the effective access control functionality. It uses information read from access credentials (i.e. authentication factors) as provided at the Credential Reader Interface to authenticate the credential, determines access authorization and controls the door through the Access Door Interface. Authentication and authorization functionality may be summarized as answering the following four “W” questions:

Where is access requested?
The geographical organization of access control structures the geography of a site. This includes secured zones and the points of access to such zones, where authentication and authorization for access takes place.

Who or what requests access?
Authentication of the users which request access to secured zones is required. This includes representation of persons, assets, groups thereof, as well as the credentials they use for authentication.

Why should access be granted?
Access rights define the rights which a user has at an access point or for an access zone. Access authorization may also depend on the credential presented, or other internal or external conditions.

When can access be granted?
Access rights may depend on the time of day, day of week or date.
Notification and logging of access transactions and alarms is an essential function of this process. The exact functionality and implementation of this process is not part of the BACnet definitions; it is a local matter of the device or subsystem which implements it. Any physical structure or deployment as well as partial support of this functionality behind the BACnet Process Interface provided by this process is a local matter, hidden to the BACnet network.

This process represents its functionality at its BACnet process interface, the **Authentication & Authorization Interface**. This interface is subject of the BACnet standardization, and modeled later in this document. Within a PACS, it is typically used by other Authentication & Authorization Processes running in other devices, for data replication and synchronization, or to complement it to full access functionality. Another typical usage of this interface is access user and credential enrollment, performed by some external system such as a Credential Management System (CMS) or Identity Management System (IDMS). An access control management system uses this interface for e.g. rights assignment, credential status setting, etc.

This process takes a client role at Credential Reader Interfaces for authentication factor input, as well as a client role at Access Door Interfaces for control of doors, if the corresponding processes are deployed to other physical devices. If they run internally in the same device, interaction with these processes is not subject to BACnet definitions, and considered a local matter.

![Figure 5–6, Authentication & Authorization Process](image)

### 5.3.1 Authorization

Authorization is the basic function of a PACS. It includes authentication of credentials, validation of access rights and other conditions. This is a series of checks required to pass successfully before access is granted. Granting access results in controlling a door.
5.3.2 Authentication
Authentication factors are provided at the Credential Reader Interface at the time a user requests access. These factors are compared with information in the credential database, in order to find a matching credential representation in the database. Matching algorithms are a local matter of the process. Authentication is one of the checks performed for authorization. Without finding any matching credential representation, access is denied.

The results of authentication may be reported to client role processes through the Authentication & Authorization Interface.

5.3.3 Validation
Validation represents a series of checks to pass successfully before access is granted. The sequence of checks is not mandated. Example checks are:

- Validation of credentials based on its status, expiry time etc.
- Evaluation of external conditions
- Sufficient access rights assigned to the credential for the access point
- Etc.

Some validation checks are related to the geographical location where the respective credential has been read. The geographical location is given through which credential reader has read an authentication factor.

The validation checks may be taken in any order, before or after authentication, or run in parallel. A failed check results in finally denying access, while only if there is a sufficient number of successful validation checks, access is granted.

The device’s local Credential Database holds data which is used for some of the validation checks, although in some implementations data is used which is located in external devices, typically access servers. Degraded validation may take place if such external devices are not accessible when validation checks have to be preformed.

Some checks may already be performed by the Credential Reader process, but then the Authentication & Authorization Process does not become active since no valid authentication factor is received from the Credential Reader Interface.

The results of validation may be reported to client role processes through the Authentication & Authorization Interface.

5.3.4 Door Control
Doors are controlled based on the results of authentication and validation. Typically, a door is opened after successful authentication and validation. Access Door Interfaces are used to control respective doors. Which door to control is determined based on which credential reader has read an authentication factor.

5.3.5 Notification and Logging
Notification and logging of access transactions and alarms is an essential function of the Authentication & Authorization Process. Notifications may be directed to other access control devices as well as management systems. Logging of such notifications is typically supported by an implementation, to allow autonomous operation of the device the process is deployed to.

5.3.6 Credential Database
To perform authentication and validation checks, information is required on credentials and access rights. Such data is typically available in the device the process runs, and stored in some form of database. This is not necessarily a
database as known in the IT realm, such as a relational database, but optimized for constrained resources and fast access to essential data.

It typically holds data about:

- Credentials, their authentication factors, and relations with access users
- Access rights and relations with credentials and geographical structure
- Relations among access rights and credentials
- Access user representations and relations

Depending on implementation and supported functionality, more or less of this data may be present.

The storage format of such data within a controller is not necessarily the same as the format visible at the Authentication & Authorization Interface. The Authentication & Authorization Interface enables provisioning of such data into the access control device using BACnet.

### 5.3.7 Replication & Synchronization

Data in the credential database may be required to be synchronized among different devices, or replicated in multiple devices. This is required since for example state and parameters of a specific credential must be the same in all devices which know that credential. Any state change must be synchronized among all credential databases.

The amount of data to be replicated and synchronized depends on the nature of data and its usage in a device. For example, it is not required to have access rights present which are valid for some door which is not controlled by the device.

There may be synchronization and replication between access controllers, or via a central access control server, which holds the master data for all controllers of the PACS, and is responsible for replication and synchronization.

The Authentication & Authorization Interface supports this functionality through an appropriate BACnet data model and BACnet application service support.

### 5.3.8 Deployment to Physical Structure

BACnet basically does not define how functionality is deployed to physical devices. Any physical structure may be possible behind a BACnet process interface. Sample deployments are:

- The entire process and its entire database are deployed into an access controller. Logging is performed by the controller itself, such that fully autonomous operation is possible. Any external functionality such as credential enrollment accesses this controller directly. The Authentication & Authorization Interface is accessible through the access controller’s BACnet connection.

- The process and the database are partially deployed onto access controllers and a central access server. Only the minimum required data is loaded into the controller, while the overall master data is located in a central server. Logging may be centralized in this server, while the controllers only have limited logging capacity to span communication interruptions. The access controller’s Authentication & Authorization Interface is accessible through the controller’s BACnet connection. The central server not necessarily provides such an interface; it may contain client role processes only.
6. PACS Data Model Overview

The overview of the PACS data model reflects the three BACnet process interfaces as identified in the functional decomposition of the PACS.

Figure 6–1, Data Model Overview
An overview of the relationship among these objects in a PACS is shown in the figure following. Note that any client role process may have relationships with the objects shown.

The arrows between two object types show the association or relationship between the two object types while the direction of the arrow indicates the direction of this relationship. When an arrow points from one object type to another it means that an instance of the first object type will hold a reference to an instance of the second object type. In the example given, the Access Rights object will hold references to zero or more Access Point or Access Zone objects.

Figure 6–2, Relationship Overview
A more detailed overview of the relations is given by the following figure. The details are discussed in the following clauses of this document.

Figure 6–3, Relationship Details
7. Authentication & Authorization Interface

The Authentication & Authorization Interface defines a data model that represents the structure and data required to perform authentication and authorization. The data model also enables to control the functionality of the authorization and authentication process. Access transaction and alarm notifications are issued by the objects of this interface.

7.1 Geographical Organization

The point of authentication and access to secured zones is represented by objects of type Access Point. The secured zones may be represented by Access Zone objects. Note that the mechanical entrance equipment is subordinate to this concept, and provided by the Access Door Interface.

![Figure 7–1, Example Geographical Organization](image-url)
7.1.1 Access Point Object Type

The Access Point object represents the authentication & authorization process at a specific geographic access controlled point (i.e., door, gate, turnstile, etc). Access through this point is directional in that it represents access in one direction only. A door in which access is controlled in both directions leads to two separate Access Point objects.

In the most simple access control systems the Access Point controls access through a secured door. In more sophisticated systems the Access Point controls entry into a zone (Ingress Access Point) or exit from a zone (Egress Access Point). In the case of adjacent zones, the Access Point is an Ingress Access Point for one zone and an Egress Access Point for the other zone at the same time.

<table>
<thead>
<tr>
<th>Access Point</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification:</strong> Name, ID, Type, Description, Profile</td>
</tr>
<tr>
<td><strong>General Health:</strong> Status Flags, Event state, Reliability, Out of service</td>
</tr>
<tr>
<td><strong>Authentication Policies:</strong> Select one of a predefined set policies</td>
</tr>
<tr>
<td><strong>Authorization Mode:</strong> Defines Authorization</td>
</tr>
<tr>
<td><strong>Lockdown:</strong> Failed Authentication Attempts and Lockdown</td>
</tr>
<tr>
<td><strong>Threat Level:</strong> Minimum Requirement to Credential’s Threat Authority</td>
</tr>
<tr>
<td><strong>Occupancy Limits:</strong> Enforcement of limits in the Access Zone</td>
</tr>
<tr>
<td><strong>Access Event Reporting:</strong> Alarm and Transaction Events</td>
</tr>
<tr>
<td><strong>Access Doors:</strong> The Access Doors controlled and supervised</td>
</tr>
<tr>
<td><strong>Muster Station Support:</strong> Flag to indicate a Muster Point</td>
</tr>
<tr>
<td><strong>Ingress („Zone To“):</strong> Access Point to enter which Zone</td>
</tr>
<tr>
<td><strong>Egress („Zone From“):</strong> Access Point to leave which Zone</td>
</tr>
</tbody>
</table>

*Figure 7–2, Access Point Object Type*

7.1.1.1 Identification

These are the standard properties of BACnet objects for object identification, type identification, description, etc.

7.1.1.2 General Health and Out of Service

Properties are defined which indicate the general health of the object. Reliability indication and out of service is supported.

The property *Status Flags*, of type *BACnetStatusFlags*, indicates, by a set of individual flags (i.e. bits), the general health of the object. Each flag is related to specific properties, which provide more details.

- The IN_ALARM flag is 1 if the object has an event state other than NORMAL.
- The FAULT flag is 1 if the property Reliability has a value other than NO_FAULT_DETECTED.
- The OVERRIDDEN flag is 1 if the object is overridden by some mechanism local to the BACnet device.
- The OUT_OF_SERVICE flag is 1 if the property Out_Of_Service is TRUE.

The property *Event State*, of type *BACnetEventState*, indicates the event state associated with the object. Since access event reporting is considered state-less, this property has a value of NORMAL, except if Reliability is something else than NO_FAULT_DETECTED. In this case it has a value of FAULT.
The optional property **Reliability**, of type `BACnetReliability`, indicates the detailed reliability of the authentication & authorization process at the access point this object represents. The following enumeration values may be supported:

- **NO_FAULT_DETECTED** The process and the object are reliable.
- **PROCESS_ERROR** The process is unreliable.
- **CONFIGURATION_ERROR** The configuration of the device or object has an error preventing reliable processing.
- **UNRELIABLE_OTHER** An unspecified reason leads to unreliable processing.

If the Reliability property has a value other than **NO_FAULT_DETECTED** then no authentication or authorization is performed. No access events are generated in this case.

The property **Out_Of_Service**, of type `BOOLEAN`, indicates whether the authentication & authorization process at the access controlled point this object represents is out of service or not. If it is **TRUE** neither authentication nor authorization takes place at the access controlled point.

### 7.1.1.3 Authentication Policies

Authentication may utilize multiple authentication factors such as card and PIN. An Authentication Policy determines which authentication factors are used and how they are used to reach an authentication decision. Each Access Point may have its own Authentication Policy and may allow selecting the active policy from a set of policies.

If the Access Point object supports to select the active Authentication Policy, it exposes an enumeration of names of supported Authentication Policies. The explicit definition of each supported Authentication Policy may be exposed optionally, as well as individual maximum times to present the authentication factors. A selector allows selecting the active Authentication Policy. The figure following provides an overview and example Authentication Policy support.

![Figure 7–3, Authentication Policy Overview and Example](image)

The enumeration of the names of the supported Authentication Policies is exposed by the optional property **Authentication_Policy_Names**, of type `Array of CharacterString`. An empty string in an element of the array indicates an undefined policy. This property is required to be present if the Access Point allows selecting the active Authentication Policy.
The optional property *Active Authentication Policy*, of type *Unsigned*, contains the array index of the active Authentication Policy of Authentication_Policy_Names. The size of the Authentication_Policy_Names array specifies the range of values (0..size) that can be written to this property. A value of zero disables the Access Point, because there is no authentication policy in effect, and through this, no authentication and no authorization. In case the active Authentication Policy becomes invalid through modification, the property takes a value of zero, disabling the Access Point. This property is required to be present if the Access Point allows selecting the active Authentication Policy.

For the explicit and network visible definition of Authentication Policies, the following model is supported:

An Authentication Policy is a set of required or optional authentication factors to be presented for successful authentication. The definition of what authentication factor type is to be used is made by a reference to a BACnetAuthenticationFactor value property, where the respective authentication factor is read from. This implicitly defines the type of Authentication Factor.

The following basic elements are known to define an Authentication Policy:

- **Required authentication factor types** of a policy. This defines what authentication factor types are required to be presented at the Access Point for successful authentication.
- **Choice of optional authentication factor types** of a policy. One of these authentication factor types is required to be presented at the Access Point for successful authentication.

An Authentication Policy consists of 0..n required authentication factor types and 0..m choices of optional authentication factor types. At least one of these two elements must be present to form a valid Authentication Policy.

The sequence of presenting the authentication factors is not implied by the sequence order in an Authentication Policy. The authentication factors may be presented in any sequence.

Authentication factors are read at a Credential Reader front plate, preprocessed and presented by the Credential Reader Process at the Credential Reader Interface as a value of type BACnetAuthenticationFactor. The Authentication & Authorization Process reads these BACnetAuthenticationFactor values and determines if the active Authentication Policy is met.

The explicit configuration of defined authentication policies is made visible through the optional property *Authentication Policy List*. This is an Array of BACnetAuthenticationPolicy. Each BACnetAuthenticationPolicy is an array of tuples of type BACnetAuthenticationRule. Authentication_Policy_List shall, if present, contain at least one policy, in order to expose a valid authentication policy. If this property is present, then the Authentication_Policy_Name property shall be present. The i<sup>th</sup> element of this array corresponds to the i<sup>th</sup> element of the Authentication_Policy_Names array. The size of the Authentication_Policy_List array must equal the size of Authentication_Policy_Names array.
Attempts to write malformed policies shall be denied by the Access Point object. Since Authentication_Policy_List is an array of arrays of BACnetAccessAuthenticationRule elements, BACnet services allow reading or writing entire policies only.

One element of an Authentication Policy is of type BACnetAccessAuthenticationRule, which contains two fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication-</td>
<td>This field is a choice of options, and indicates whether the Authentication-</td>
</tr>
<tr>
<td>Factor-Requirement</td>
<td>Factor-Requirement needs to be used for authentication, or may be used</td>
</tr>
<tr>
<td></td>
<td>alternatively.</td>
</tr>
<tr>
<td>REQUIRED</td>
<td>The Authentication Factor is required to be presented as defined in this</td>
</tr>
<tr>
<td></td>
<td>policy. The Authentication-Factor-Input field must be present.</td>
</tr>
<tr>
<td>CHOICE_BEGIN</td>
<td>Opens a group of OPTION entries. One of the authentication factors specified</td>
</tr>
<tr>
<td></td>
<td>by the OPTION entries following this and before the CHOICE_END entry is</td>
</tr>
<tr>
<td></td>
<td>required for successful authentication. Before another CHOICE_BEGIN</td>
</tr>
<tr>
<td></td>
<td>follows, a CHOICE_END shall be present. The Authentication-Factor-Input</td>
</tr>
<tr>
<td></td>
<td>field is not present.</td>
</tr>
<tr>
<td>CHOICE_END</td>
<td>Closes a group of OPTION entries opened with a CHOICE_BEGIN entry. The</td>
</tr>
<tr>
<td></td>
<td>Authentication-Factor-Input field is not present.</td>
</tr>
<tr>
<td>OPTION</td>
<td>The authentication factor specified is an option of a choice of authentication</td>
</tr>
<tr>
<td></td>
<td>factors specified by all OPTION entries within the CHOICE_BEGIN and CHOICE_</td>
</tr>
<tr>
<td></td>
<td>END boundaries. The Authentication-Factor-Input field shall be present.</td>
</tr>
<tr>
<td>Authentication-</td>
<td>This optional field indicates from which object and property to read the</td>
</tr>
<tr>
<td>Factor-Input</td>
<td>Authentication Factor from. It is not present for some of the Authentication-</td>
</tr>
<tr>
<td></td>
<td>Factor-Requirement field’s options.</td>
</tr>
<tr>
<td>&lt;Authentication Factor</td>
<td>This field of type BACnetDeviceObjectPropertyReference contains a reference</td>
</tr>
<tr>
<td>Input Property&gt;</td>
<td>to a property of type BACnetAuthenticationFactor, which is used as the</td>
</tr>
<tr>
<td></td>
<td>Authentication Factor Input. The Authentication &amp; Authorization Process</td>
</tr>
<tr>
<td></td>
<td>expects to read an Authentication Factor from the property specified.</td>
</tr>
</tbody>
</table>

The time in which all Authentication Factors of a policy have to be presented may be exposed. If not all of the Authentication Factors are presented within this time, the process of presenting the Authentication Factors of the active policy has to be restarted.

The timeout for each policy is exposed by the optional property Authentication_Policy_Timeouts, of type Array of Unsigned values indicating the timeout in seconds individually for each policy. If this property is present, then the Authentication_Policy_Name property shall be present. The i\textsuperscript{th} element of this array corresponds to the i\textsuperscript{th} element of the Authentication_Policy_Names array. The size of the array must equal the size of the Authentication_Policy_Names array.
7.1.1.4 Authorization Mode
The Authorization Mode determines how authorization is performed at the Access Point. This is exposed by the optional property named Authorization_Mode of type BACnetAuthorizationMode.

The enumeration BACnetAuthorizationMode has the values:

- AUTHORIZE: The access rights of an active credential are evaluated aside from other authorization checks.
- GRANT_ACTIVE: An active credential is granted access without evaluating the access rights assigned to the credential. Other authorization checks may still lead to denying access.
- DENY_ALL: Any credential, whether active or not, is denied access. Other authorization checks may be performed, but can not lead to granting access.

<Proprietary Enum Values>: A vendor may use other proprietary enumeration values to allow proprietary authorization modes other than those defined by the standard.

Note that locking down a door requires the Access Door to be commanded accordingly.

7.1.1.5 Authentication Attempts and Lockdown
An Access Point may restrict the number of consecutive failed authentication attempts within a given time. Attempts are considered to be failed if a presented Authentication Factor is unknown by the PACS. If the number of failed attempts exceeds the limit within a specific time window, the Access Point is locked down, meaning not to accept any Authentication Factors for authentication, and by this, not authorizing any Access Credential to pass the Access Point.

A maximum failed attempts value specifies how many failed attempts are allowed before the Access Point is locked down. The failed attempts are counted during a defined duration of time, and the Access Point lockdown may be relinquished after a specified timeout.

The optional property Lockdown, of type BOOLEAN, is TRUE if the Access Point object is in a lockdown state. When the Access Point is in a lockdown state any authentication and authorization requests will fail and for each failed attempt the Last_Access_Event will be set to DENIED_LOCKDOWN. An Access Point may be set to a lockdown state due to too many failed access attempts, as defined in the Max_Failed_Attempts property, or by writing TRUE to this property.

When the property Lockdown becomes TRUE due to too many failed authentication attempts, the Access Point object sets Last_Access_Event to LOCKDOWN_MAX_ATTEMPTS. If TRUE is written to this property for any other reason the Access Point object sets Last_Access_Event to LOCKDOWN_OTHER. When the Lockdown property becomes FALSE, the Access Point sets Last_Access_Event to LOCKDOWN_RELINQUISHED.

The optional property Lockdown_Relinquish_Time, of type Unsigned, is used to specify the time, in seconds, to delay, after the Lockdown property has taken on the value TRUE, before automatically relinquishing the lockdown state. The lockdown state is relinquished by writing FALSE to the Lockdown property. A value of zero indicates that the lockdown state will not automatically be relinquished.

The optional property Failed_Attempts, of type Unsigned, represents the actual number of failed attempts within the actual Failed_Attempts_Time period. Writing to this property may be allowed for resetting this counter. Automatic reset of this counter is a local matter.

The optional property Max_Failed_Attempts, of type Unsigned, represents the maximum number of failed attempts that can be done at this Access Point, before Lockdown is set to TRUE. Zero indicates an infinite number of attempts without locking down the Access Point. This property shall be present if the object supports this functionality.
If the Failed_Attempts_Time property is present the Failed_Attempts property shall be present.

The optional property Failed_Attempts_Time, of type Unsigned, represents the time, in seconds, to delay before setting the Failed_Attempts property to zero, after the last failed authentication attempt. If an intervening successful access occurs, the Failed_Attempts property is set to zero.

If the Failed_Attempts_Time property is present the Failed_Attempts property must be present.

7.1.1.6 Threat Level
The Access Point exposes its actual Threat Level by the optional property Threat_Level, of type BACnetAccessThreatLevel. This is an unsigned value in the range 0..100, with 0 the lowest threat level, effectively switching off threat levels. For authorization to pass the Access Point, authenticated Access Credentials are required to have the same or higher threat authority.

The Threat Level, if supported, can be set from other processes, in order to adjust security, locking out Access Credentials with insufficient threat authority.

7.1.1.7 Occupancy Limits Enforcement
The Access Point supports configuration of enforcement of occupancy limits. Access Credentials may be exempted from occupancy limit enforcement.

The optional property Occupancy_Upper_Threshold_Enforced, of type BOOLEAN, indicates whether the upper occupancy threshold of the Access Zone for which the Access Point is an Ingress Access Point is enforced. If the flag is TRUE, passage may be denied if the Access Zone’s Occupancy_Count is greater than or equal to its Occupancy_Upper_Threshold.

The optional property Occupancy_Lower_Threshold_Enforced, of type BOOLEAN, indicates whether the lower occupancy threshold of the Access Zone for which the Access Point is an Egress Access Point is enforced. If the flag is TRUE, passage may be denied if the Access Zone’s Occupancy_Count is less than or equal to its Occupancy_Lower_Threshold.
7.1.1.8 Access Event Reporting

The Access Point object may support intrinsic reporting of access alarm events and access transaction events. The mechanism is based on the new ACCESS_EVENT event algorithm. This algorithm may also be applied on Access Point objects by Event Enrollment objects. For details of the event algorithm and the use of Event Enrollment objects see main clause Event Reporting and Logging below.

The basic value representing access events is an enumeration of possible authentication and authorization decisions and maybe subsequent actions taken by a user. This enumeration is defined by the new data type BACnetAccessEvent.

<table>
<thead>
<tr>
<th>Enumerations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONE</td>
<td>The Access Point did not yet determine any access event. This is not a reported event. It is required to enable algorithmic ACCESS_EVENT reporting.</td>
</tr>
<tr>
<td>MUSTER</td>
<td>The Access Point acting as a muster point has recognized an Access Credential.</td>
</tr>
<tr>
<td>PASSBACK_DETECTED</td>
<td>Passback of an Access Credential for subsequent entry into the zone has been detected.</td>
</tr>
<tr>
<td>DURERESS</td>
<td>Duress was detected. It is a local matter how a duress event is determined.</td>
</tr>
<tr>
<td>TRACE</td>
<td>The Access Credential recognized has its Trace_Flag set.</td>
</tr>
<tr>
<td>LOCKDOWN_MAX_ATTEMPTS</td>
<td>The Access Point is locked down due to maximum failed authentication attempts.</td>
</tr>
<tr>
<td>LOCKDOWN_OTHER</td>
<td>The Access Point is locked down due to any reason other than maximum attempts.</td>
</tr>
<tr>
<td>LOCKDOWN_RELINQUISHED</td>
<td>The Access Point has relinquished lockdown.</td>
</tr>
<tr>
<td>LOCKED_BY_HIGHER_PRIORITY</td>
<td>The commanded Access Door is locked by a higher priority.</td>
</tr>
<tr>
<td>GRANTED</td>
<td>Access granted. Events related to door activities such as door unlocked or door opened are to be generated by the respective Access Door.</td>
</tr>
<tr>
<td>DENIED</td>
<td>Access is denied. No specific condition or reason.</td>
</tr>
<tr>
<td>DENIED_DENY_ALL</td>
<td>Access denied since Access Point is in authorization mode DENY_ALL.</td>
</tr>
<tr>
<td>DENIED_UNKNOWN_CREDENTIAL</td>
<td>Access denied due to unknown credential</td>
</tr>
<tr>
<td>DENIED_MISSING_AUTHENTICATION_FACTOR</td>
<td>Access denied due to missing authentication factor for multi-factor authentication.</td>
</tr>
<tr>
<td>DENIED_ZONE_NO_RIGHT</td>
<td>Access denied due to no right for Access Zone.</td>
</tr>
<tr>
<td>DENIED_POINT_NO_RIGHT</td>
<td>Access denied due to no right found for the Access Point.</td>
</tr>
<tr>
<td>DENIED_OUT_OF_TIME_RANGE</td>
<td>Access denied due to no active time range.</td>
</tr>
<tr>
<td>DENIED_THREAT_LEVEL</td>
<td>Access denied due to insufficient threat authority.</td>
</tr>
<tr>
<td>DENIED_PASSBACK</td>
<td>Access denied due to passback of an Access Credential for subsequent entry into the zone detected.</td>
</tr>
<tr>
<td>DENIED_UNEXPECTED_LOCATION_USAGE</td>
<td>Access denied due to Access Credential used at a location which is not expected.</td>
</tr>
<tr>
<td>DENIED_MAX_ATTEMPTS</td>
<td>Access denied due to too many retries.</td>
</tr>
<tr>
<td>DENIED_LOW_OCCUPANCY_THRESHOLD</td>
<td>Exit from zone for which this Access Point is an Egress Access Point denied due to zone occupancy below or at lower threshold.</td>
</tr>
<tr>
<td>DENIED_HIGH_OCCUPANCY_THRESHOLD</td>
<td>Access to zone for which this Access Point is an Ingress Access Point denied due to zone occupancy above or at</td>
</tr>
</tbody>
</table>
DENIED_CREDENTIAL_UNASSIGNED
Access denied due to Access Credential presented is not yet assigned to an Access User.

DENIED_CREDENTIAL_INVALID
Access denied due to invalidated Access Credential.

DENIED_CREDENTIAL_NOT_YET_ACTIVE
Access denied due to not yet active Access Credential used.

DENIED_CREDENTIAL_EXPIRED
Access denied due to expired Access Credential used.

DENIED_CREDENTIAL_MANUALLY_DISABLED
Access denied due to manually disabled Access Credential used.

DENIED_CREDENTIAL_LOCKEDOUT
Access denied due to locked Access Credential used.

DENIED_CREDENTIAL_EXCEEDED_USE
Access denied due to exceeding use of the Access Credential.

DENIED_CREDENTIAL_INACTIVITY
Access denied due to inactive Access Credential used.

DENIED_CREDENTIAL_MISSING
Access denied due to missing Access Credential used.

DENIED_CREDENTIAL_DAMAGED
Access denied due to damaged Access Credential used.

DENIED_CREDENTIAL_DESTROYED
Access denied due to Access Credential used which is marked as to be destroyed.

DENIED_CREDENTIAL_DISABLED
Access denied due to the credential being disabled due to unknown or unspecified reasons.

DENIED_CREDENTIAL_TIMEOUT
Did not enter credential within given time (such as PIN)

DENIED_INCORRECT_CREDENTIAL
Credential entered is not correct or not the credential expected.

DENIED_NO_ACCOMPANIMENT
There was no accompanying Access Credential authenticated.

DENIED_INCORRECT_ACCOMPANIMENT
The accompanying Access Credential is incorrect.

DENIED_LOCKDOWN
The Access Point is in lock down state.

DENIED_OTHER
Access is denied, but none of the other “denied” access events are applicable.

<Proprietary Enum Values>
A vendor may use other proprietary enumeration values to indicate Access Events other than those defined by the standard.

To support algorithmic event reporting as well as object and property-level COV reporting, the Access Point has the optional property Last_Access_Event, of type BACnetAccessEvent, to expose the last access event. This property is required if the Access Point object supports intrinsic reporting. It is also required if the Access Point object supports COV reporting.

For COV reporting and remote event enrollment using COV subscription, COV Notifications are issued whenever the value of this property is updated on an access transaction, even if the new value is the same as the old value. To support this using standard BACnet mechanisms and services, the time of last update of Last_Access_Event is part of the COV algorithm of this object.

The optional property Update_Time, of type BACnetTimeStamp indicates the most recent update time of the Last_Access_Event property. This property changes its value on each update of Last_Access_Event. This property is required to be present if the Last_Access_Event property is present.
To provide the further event notification parameter values for reporting, the following optional properties may be present in an Access Point object:

The optional property **Last_Access_Credential**, of type `BACnetObjectIdentifier`, holds the Access Credential object identifier if the Last_Authentication_Factor could be found, otherwise the instance part is 4194303. This property is required to be present if Last_Access_Event is present.

The optional property **Last_Authentication_Factor**, of type `BACnetAuthenticationFactor` holds the last Authentication Factor used. If there was no Authentication Factor read up to now, the BACnetAuthenticationFactor type indicated is UNDEFINED, with no content, i.e. a NULL value or empty string of any type. For the definition of BACnetAuthenticationFactor see the Credential Reader Interface section.

The Access Point supports the intrinsic reporting of two different levels of Access Events:

- **Access Alarm Events**: These are events requiring immediate operator attention and handling.
- **Access Transaction Events**: These are events which are to be logged, not requiring immediate operator attention.

To support these two levels, the Access Point applies the ACCESS_EVENT algorithm twice in its intrinsic reporting. A specific Access Event may be reported as an Access Alarm Event and as an Access Transaction Event at the same time. To parameterize these two algorithms, the Access Point has distinct properties if required, other properties are shared among both algorithms. Sharing is possible since either the same value is used, or the value is irrelevant or ignored for one of the two levels.
The Access Point properties required to be present and used as follows:

<table>
<thead>
<tr>
<th>Access Point Properties</th>
<th>Access Alarm Events</th>
<th>Access Transaction Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event_State</td>
<td>Shared, NORMAL always(^1)</td>
<td>Shared, NORMAL always(^1)</td>
</tr>
<tr>
<td>Last Access Event</td>
<td>Monitored Value</td>
<td>Monitored Value</td>
</tr>
<tr>
<td>Update_Time</td>
<td>Time of update</td>
<td>Time of update</td>
</tr>
<tr>
<td>Access_Alarm_Events</td>
<td>List of Access Events to be reported as Access Alarm Events. Acts as List Of Access Events for algorithm.</td>
<td>-</td>
</tr>
<tr>
<td>Access_Transaction_Events</td>
<td>-</td>
<td>List of Access Events to be reported as Access Transaction Events. Acts as List Of Access Events for algorithm.</td>
</tr>
</tbody>
</table>

**Notification Class**

- Notification Class Properties: Priority[TO-NORMAL]\(^2\), Ack_Required(to-normal) flag and Recipient List for Recipients of Access Alarm Event notifications.

**Transaction Notification Class**

- Notification Class Properties: Priority[TO-NORMAL]\(^2\) and Recipient List for Recipients of Access Transaction Event notifications. Ack_Required(to-normal) flag is not used, always FALSE in notification.

**Event_Enable**

- TO-NORMAL bit applies to enable Access Alarm Event notifications
- TO-NORMAL bit applies to enable Access Transaction Event notifications

**Notify_Type**

- Used for notification.
- Not used, always EVENT in event notification.

**Acked_Transitions**

- Indicates acknowledgement of Access Alarm Events
- Not affected

**Event_Time_Stamps**

- Time stamp [TO-NORMAL]\(^2\) holds time of last Access Alarm Event
- Not affected

\(^1\) For Access Events, the Event State always transitions from NORMAL to NORMAL, since all access events are stateless. The BACnet framework requires conveying From State and To State in event notifications, as well as having the Event State property.

\(^2\) Array element [TO-NORMAL] is the array’s element with index 3.
The Notification Class Properties are used as follows. Note that for Access Alarm Events the standard Notification Class is used as referenced by the Access Point’s Notification_Class property, while for Access Transaction Events the Notification Class referenced by the Access Point’s Transaction_Notification_Class property is used. If the Transaction_Notification_Class property is not present, then the Notification Class referenced by the Notification_Class property is used.

<table>
<thead>
<tr>
<th>Notification Class Properties</th>
<th>Access Alarm Events</th>
<th>Access Transaction Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification Class Instance</td>
<td>(referenced by Access Point’s Notification_Class)</td>
<td>(referenced by Access Point’s Transaction_Notification_Class if present, otherwise referenced by Notification_Class)</td>
</tr>
<tr>
<td>Priority</td>
<td>Used in event notification</td>
<td>Used in event notification</td>
</tr>
<tr>
<td>Ack_Required</td>
<td>Used in event notification and Access Point’s Aced_Transitions regular handling.</td>
<td>Not used, always FALSE in notification. Access Point’s Aced_Transitions are not affected.</td>
</tr>
</tbody>
</table>

Event notification parameters differ for Access Alarm Events and Access Transaction Events.

<table>
<thead>
<tr>
<th>Event Notification Parameters</th>
<th>Access Alarm Events</th>
<th>Access Transaction Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeStamp</td>
<td>Current time. Is also stored in Access Point’s Event_Time_Stamps [TO-NORMAL]</td>
<td>Current time. Access Point’s Event_Time_Stamps [TO-NORMAL] is not affected!</td>
</tr>
<tr>
<td>notificationClass</td>
<td>Notification Class referenced by Access Point’s Notification_Class property</td>
<td>Notification Class referenced by Access Point’s Transaction_Notification_Class property if present, otherwise referenced by Notification_Class property</td>
</tr>
<tr>
<td>priority</td>
<td>Notification Class Priority</td>
<td>Notification Class Priority</td>
</tr>
<tr>
<td>eventType</td>
<td>ACCESS_EVENT</td>
<td>ACCESS_EVENT</td>
</tr>
<tr>
<td>messageText (OPTIONAL)</td>
<td>&lt;any&gt;</td>
<td>&lt;any&gt;</td>
</tr>
<tr>
<td>notifyType</td>
<td>Access Point’s Notify_Type</td>
<td>EVENT</td>
</tr>
<tr>
<td>ackRequired</td>
<td>Notification Class’ Ack_Required</td>
<td>FALSE</td>
</tr>
<tr>
<td>fromState</td>
<td>NORMAL</td>
<td>NORMAL</td>
</tr>
<tr>
<td>toState</td>
<td>NORMAL</td>
<td>NORMAL</td>
</tr>
<tr>
<td>eventValues</td>
<td>CHOICE = ACCESS_EVENT</td>
<td>CHOICE = ACCESS_EVENT</td>
</tr>
<tr>
<td>Access_Event</td>
<td>Access Point’s new</td>
<td>Access Point’s new</td>
</tr>
<tr>
<td></td>
<td>Last_Access_Event value</td>
<td>Last_Access_Event value</td>
</tr>
<tr>
<td>Status_Flags</td>
<td>Access Point’s Status_Flags value</td>
<td>Access Point’s Status_Flags value</td>
</tr>
<tr>
<td>Update_Time</td>
<td>Access Point’s new Update_Time value</td>
<td>Access Point’s new Update_Time value</td>
</tr>
<tr>
<td>Access_Credential</td>
<td>Access Point’s</td>
<td>Access Point’s</td>
</tr>
<tr>
<td></td>
<td>Last_Access_Credential value</td>
<td>Last_Access_Credential value</td>
</tr>
<tr>
<td>Authentication_Factor</td>
<td>Access Point’s</td>
<td>Access Point’s</td>
</tr>
<tr>
<td>(OPTIONAL)</td>
<td>Last_Authentication_Factor value if present</td>
<td>Last_Authentication_Factor value if present</td>
</tr>
</tbody>
</table>

The optional property Notification_Class, of type Unsigned, refers to the notification class for Access Alarm Events at the Access Point. This property is required to be present if the Access Point object supports intrinsic reporting.
The optional property `Transaction_Notification_Class`, of type `Unsigned`, refers to the notification class for Access Transaction Events at the Access Point. If this property is not present, the Access Transaction Events are distributed through the standard Notification Class, but still ignoring Ack_Required of the Notification Class.

The optional property `Access_Alarm_Events`, of type `List of BACnetAccessEvent`, holds the Access Events to be reported as Access Alarm Events. This property is required to be present if the Access Point object supports intrinsic reporting.

The optional property `Access_Transaction_Events`, of type `List of BACnetAccessEvent`, holds the Access Events to be reported as Access Transaction Events. This property is required to be present if the Access Point object supports intrinsic reporting.

The optional property `Event_Enable`, of type `BACnetEventTransitionBits`, allows specifying which event state transitions are reported. Since the Access Point supports TO-NORMAL transitions of Event_State only, deactivating the TO-NORMAL bit of this property effectively switches off reporting of any access event. This property is required to be present if the Access Point object supports intrinsic reporting.

The optional property `Acked_Transitions`, of type `BACnetEventTransitionBits`, indicates acknowledgement of access alarm events. Access Transaction Events do not affect this property. This property is required to be present if the Access Point object supports intrinsic reporting.

The optional property `Notify_Type`, of type `BACnetNotifyType`, specifies whether the Access Alarm Events are notified as ALARM or EVENT. Access Transaction Events are always reported as EVENT, ignoring the value of this property. The notify type is a classification of notifications typically used in client role processes. It has no effect on the server role process behavior. This property is required to be present if the Access Point object supports intrinsic reporting.

The optional property `Event_Time_Stamps`, an `Array of BACnetTimeStamp`, holds the time stamp as conveyed in the most recent notifications for the individual event state transitions. The array element associated with the TO-NORMAL transition (i.e. array element 3) holds the time stamp of the most recent Access Alarm Event. Access Transaction Events do not modify this property. This property is required to be present if the Access Point object supports intrinsic reporting.

### 7.1.1.9 Access Door Relationship

The Access Point exposes which Access Door objects are controlled by the Authentication & Authorization Process for the Access Point. Control of the Access Door objects referred to takes place after successful authorization at this Access Point.

The Access Doors related to the Access Point object are exposed in the required property `Access_Doors`, as an `Array of BACnetDeviceObjectReference` object references to Access Door objects.

For controlling the Access Doors, a single command priority is specified which is used when commanding the Access Doors.

The command priority to be used when commanding the Access Doors is exposed in the required property `Priority_For_Writing`, of type `Unsigned` in the range 1..16.

### 7.1.1.10 Muster Station Support

An Access Point object can act as a muster point for muster applications. If it acts as a muster point, every Access Credential recognized is reported by a MUSTER access event.

The optional property `Master_Point`, of type `BOOLEAN`, indicates whether the Access Point generates MUSTER access events.
7.1.1.11 Access Zone Relationship

Access Points are the entry or exit points of Access Zones. Access Point objects may therefore expose such relationships. The use of Access Zones is optional, the relationship may not exist.

7.1.1.11.1 Ingress (“Zone To”)

The Access Point may refer to the Access Zone for which the Access Point acts as an ingress point. The Access Point allows entering the Access Zone referred to.

The Access Zone this Access Point allows entry to is exposed by the optional property Zone_To, of type BACnetDeviceObjectReference, to an Access Zone object. This property shall not reference the same Access Zone object as the Zone_From property. If the Access Point is not an ingress point of an Access Zone then this property shall contain 4194303 in the instance part of the object identifier.

7.1.1.11.2 Egress (“Zone From”)

The Access Point may refer to an Access Zone for which the Access Point acts as an egress point. The Access Point allows leaving the Access Zone referred to.

The Access Zone this Access Point allows exit from is exposed by the optional property Zone_From, of type BACnetDeviceObjectReference, to an Access Zone object. This property shall not reference the same Access Zone object as the Zone_To property. If the Access Point is not an egress point of an Access Zone then this property shall contain 4194303 in the instance part of the object identifier.
7.1.2 Access Zone Object Type

A secured zone is represented by an Access Zone object. Simple systems may model the Authorization & Authentication Interface without using this object, if the functionality this object represents is not exposed at the interface.

The Access Zone object type provides the following features:

<table>
<thead>
<tr>
<th>Access Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification:</td>
</tr>
<tr>
<td>Name, ID, Type, Description, Profile</td>
</tr>
<tr>
<td>General Health:</td>
</tr>
<tr>
<td>Status Flags, Reliability, Out of service</td>
</tr>
<tr>
<td>Occupancy State:</td>
</tr>
<tr>
<td>Indication and Reporting</td>
</tr>
<tr>
<td>Occupancy Counting:</td>
</tr>
<tr>
<td>Actual Occupancy, Thresholds</td>
</tr>
<tr>
<td>Who's in Reporting:</td>
</tr>
<tr>
<td>Access Credentials in the zone</td>
</tr>
<tr>
<td>Pass-Back Detection Support:</td>
</tr>
<tr>
<td>Passback Mode and Passback Timeout</td>
</tr>
<tr>
<td>Access Point Relationships:</td>
</tr>
<tr>
<td>Ingress Access Points, Egress Access Points</td>
</tr>
</tbody>
</table>

Figure 7-4, Access Zone Object Type

The concept of commanding an Access Zone was considered not to be appropriate, since securing a zone requires much more than what is in the scope of the Access Zone object, e.g. arming intrusion detectors, switching lighting, etc. The Access Zone does not support any commanding. The existing Command Object type may be used for this purpose.

The Access Zone’s Occupancy_State property indicates the current occupancy state. Intrinsic alarming is on Occupancy_State using the existing CHANGE_OF_STATE algorithm. Event Enrollment objects may be configured to watch Access Zone properties.

Object-level COV reporting is not foreseen. But property-level COV may be supported at a vendor’s discretion.

7.1.2.1 Identification

Control of a secured zone may be shared by multiple controller devices; each involved device will have a representation of this secured zone in the form of an Access Zone object. In this case all Access Zone objects within these devices representing the same secured zone shall have the same identification (i.e. Object_Identifier property value) and property content where applicable. The identification is then not within the scope of the device, but in the scope of the entire system (inter-network-wide).

The synchronization of content is a local matter, but the model supports this requirement through the use of standard BACnet services. How the synchronization between devices occurs is considered a local matter. However, this may be done through COV notifications.
7.1.2.2 General Health

Properties are defined which indicate the general health of the object. Reliability indication and out of service is supported.

The property Status_Flags, of type BACnetStatusFlags, indicates, by a set of individual flags (i.e. bits), the general health of the object. Each flag is related to specific properties, which may provide more details.

- The IN_ALARM flag is 1 if the property Event_State has a value other than NORMAL.
- The FAULT flag is 1 if the property Reliability has a value other than NO_FAULT_DETECTED.
- The OUT_OF_SERVICE flag is 1 if the property Out_Of_Service is TRUE.
- All other flags are always 0.

The property Event_State, of type BACnetEventState, indicates the event state associated with the object. The following event states are supported:

- NORMAL: Occupancy is considered in allowed range.
- OFFNORMAL: Occupancy is outside allowed range.
- FAULT: Processing or the object is unreliable.

The optional property Reliability, of type BACnetReliability, indicates the detailed reliability of the Authentication & Authorization Process at the access point this object represents. The following enumeration values may be supported:

- NO_FAULT_DETECTED: The process and the object are reliable.
- CONFIGURATION_ERROR: The configuration of the device or object has an error preventing reliable processing.
- UNRELIABLE_OTHER: An unspecified reason leads to unreliable processing.

If the Reliability property is present and has any value other than NO_FAULT_DETECTED, then the Event_State property has a value of FAULT.

The property Out_Of_Service, of type BOOLEAN, indicates whether the Occupancy_Count property is decoupled from the processing of occupancy counting. In addition, the Reliability property and the corresponding state of the FAULT flag of the Status_Flags property is decoupled when Out_Of_Service is TRUE. While the Out_Of_Service property is TRUE, writing to the Adjust_Value property does not modify the Occupancy_Count, the Occupancy_Count and Reliability properties may be changed to any value as a means of simulating specific fixed conditions or for testing purposes. Other functions that depend on the state of the Occupancy_State or Reliability properties respond to changes made to these properties while Out_Of_Service is TRUE.
7.1.2.3 Occupancy State and Reporting

The Access Zone supports indication and reporting of the occupancy state.

The property **Occupancy_State**, of type BACnet, of type `BACnetAccessZoneOccupancyState`, reflects the occupancy state of the Access Zone. It uses Occupancy_Count and the occupancy threshold properties to evaluate its state. Proprietary evaluations and states are possible.

BACnetAccessZoneOccupancyState is an enumeration of possible occupancy states:

- **NORMAL**: This is the default occupancy state when no other standard or proprietary states are applicable or occupancy counting is disabled.
- **BELOW_LOWER_THRESHOLD**: If Occupancy_Lower_Threshold property is present and the Occupancy_Count property is lower than this.
- **AT_LOWER_THRESHOLD**: If Occupancy_Lower_Threshold property is present and the Occupancy_Count property is equal to this value.
- **AT_UPPER_THRESHOLD**: If Occupancy_Upper_Threshold property is present and the Occupancy_Count property is equal to this value.
- **ABOVE_UPPER_THRESHOLD**: If Occupancy_Upper_Threshold property is present and the Occupancy_Count property is greater than this.

<Proprietary Enum Values>: A vendor may use other proprietary enumeration values to indicate proprietary occupancy states.

For intrinsic reporting of occupancy state events, the existing Change-Of-State algorithm is used. This requires the presence of the following properties.

The optional property **Alarm_Values**, a List of `BACnetAccessZoneOccupancyState`, defines which occupancy states of the Occupancy_State property are reported as alarms. This property is required if intrinsic reporting is supported by this object.

The optional property **Time_Delay**, of type `Unsigned`, specifies the minimum period of time in seconds that the Occupancy_State property value must remain equal to any one of the values in the Alarm_Values property before a TO-OFFNORMAL event is generated; or not equal to any of the values in the Alarm_Values property before a TO-NORMAL event is generated. This property is required if intrinsic reporting is supported by this object.

The optional property **Notification_Class**, of type `Unsigned`, specifies the notification class to be used when handling and generating event notifications for this object. This property is required if intrinsic reporting is supported by this object.

The optional property **Event_Enable**, of type `BACnetEventTransitionBits`, has three flags that separately enable and disable reporting of TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. This property is required if intrinsic reporting is supported by this object.

The optional property **Acked_Transitions**, of type `BACnetEventTransitionBits`, has three flags that separately indicate the receipt of acknowledgments for TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. This property is required if intrinsic reporting is supported by this object.

The optional property **Notify_Type**, of type `BACnetNotifyType`, indicates whether the notifications generated by the object should be EVENTS or ALARMS. This classification is typically used by client role processes receiving notifications. It has no impact on the behavior of the authentication and authorization process. This property is required if intrinsic reporting is supported by this object.
The optional property *Event_Time_Stamps*, an *Array of BACnetTimeStamp*, holds the times of the last event notifications for TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events, respectively. This property is required if intrinsic reporting is supported by this object.

### 7.1.2.4 Occupancy Counting and Thresholds

The Access Zone may support counting occupancy if appropriate entry and exit hardware is present. The precision of counting depends on the entry and exit hardware used. The actual occupancy count is incremented if access takes place at an Ingress Access Point, and decremented if exit takes place at an Egress Access Point. Incrementing or decrementing may be accomplished through other means, which are a local matter.

The actual occupancy count is exposed by the property *Occupancy_Count* of type *Unsigned*. If *Occupancy_Count_Enable* is FALSE, this property has a value of zero. The value of the *Occupancy_Count* property may be adjusted by writing to the *Adjust_Value* property. The *Occupancy_Count* property is writable when *Out_Of_Service* is TRUE. When *Out_Of_Service* becomes FALSE it is a local matter as to what the value the occupancy count is set to.

The property *Occupancy_Count_Enable*, of type *BOOLEAN*, indicates whether occupancy counting is in effect (TRUE) or not (FALSE).

The optional property *Adjust_Value*, of type *INTEGER*, when written, adjusts the *Occupancy_Count* property. The following series of operations are performed atomically when this property is written and the value of the *Occupancy_Count_Enable* property is TRUE:

1. The value written to *Adjust_Value* is stored in the *Adjust_Value* property.
2. If the value written is non-zero then this value is added to the value of the *Occupancy_Count* property. If the value written is zero then the value of the *Occupancy_Count* property is set to zero. If the resulting value of the *Occupancy_Count* property would be less than zero the *Occupancy_Count* property is set to zero.
3. The *Adjust_Value* property is set to zero.

When this property is written and the value of the *Occupancy_Count_Enable* property is FALSE, then the *Adjust_Value* property is set to zero. If *Adjust_Value* has never been written, it has a value of zero.

The optional property *Occupancy_Upper_Threshold* of type *Unsigned*, specifies the occupancy upper threshold of the zone. If this property has a value of zero then there is no upper threshold. If this value is not zero, it shall be greater than the value of the *Occupancy_Lower_Threshold*, if present.

The optional property *Occupancy_Lower_Threshold* of type *Unsigned*, specifies the occupancy lower threshold of the zone. If this property has a value of zero then there is no lower threshold.

If thresholds are present, an Ingress Access Point of the Access Zone may generate corresponding access events if a threshold is reached or exceeded. Whether or not events are generated is defined by adding the corresponding events to the respective access event lists of the Access Point where the current access transaction takes place.

Whether the occupancy thresholds are enforced or not may be enabled or disabled individually at each Access Point of an Access Zone. Enforcement means to deny access if the threshold would become exceeded if access takes place. Access Credentials may be exempted from occupancy enforcement checks.
7.1.2.5 “Who Is In” Reporting

The Access Zone may support live view reporting of who is currently in the Access Zone if appropriate entry and exit hardware is present. This information is used by passback detection, or for “Who-Is-In” live-view reporting. If a live-view needs to display persons and person related data instead of Access Credentials, the Access Credential information allows retrieving which Access Users are in the Access Zone.

The list of present Access Credentials is exposed by the optional property Credentials_In_Zone, of type List of BACnetObjectIdentifier referring to Access Credential objects.

For synchronization purposes among the Access Zone objects present in different access control devices and representing the same secured zone, the Access Zone may be required to expose which Access Credential is added to Credentials_In_Zone, and which one is removed. The reason for adding or removing is not relevant, and may be, among others:

- Regular access
- Regular exit
- Manual removal
- Timed removal
- Etc.

The availability of this information as properties is required if standard BACnet application services are to be used for synchronization among access control devices participating in controlling the same secured zone. Most typically, a property-level COV is applied on the following properties, to keep Credentials_In_Zone synchronized in all access control devices controlling the same secured zone.

The optional property Last_Credential_Added, of type BACnetObjectIdentifier, holds the reference to the Access Credential object which has last been added to the Credentials_In_Zone property. When no Access Credential has been added yet, the instance part of the object identifier holds a value of 4194303. If property level COV subscriptions are in place on this property, any update, even with the same value, is reported by a COV notification.

The optional property Last_Credential_Removed, of type BACnetObjectIdentifier, holds the reference to the Access Credential object which has last been removed from the Credentials_In_Zone property. When no Access Credential has been removed yet, the instance part of the object identifier holds a value of 4194303. If property level COV subscriptions are in place on this property, any update, even with the same value, is reported by a COV notification.

7.1.2.6 Passback Violation Detection

A Passback violation occurs when two successive entry transactions into the Access Zone occur using the same Access Credential without an intermediate exit transaction or the passback check timeout for the Access Credential did not yet expire.

The validation of passback is part of the authorization. The validation uses Credentials_In_Zone information to verify if the Access Credential is not already in the zone. If it is already listed in the Credentials_In_Zone list, and its timeout has not yet expired, a passback violation is detected.

The Access Zone exposes the actual passback validation mode for all Ingress Access Points of this zone in the optional property Passback_Mode, of type BACnetAccessPassbackMode.

The enumeration BACnetAccessPassbackMode has the values:
PASSBACK_OFF  Passback violations are not checked.
HARD_PASSBACK  Passback violations are checked and enforced (i.e. deny access) and violations are reported by the Ingress Access Points.
SOFT_PASSBACK  Passback violations are checked but not enforced. Violations are reported by the Ingress Access Points.

The optional property *Pass_Back_Timeout*, of type *Unsigned*, specifies the passback timeout in minutes. The timeout is evaluated individually for every credential used to enter the zone. The timeout period for a particular credential begins at the time of successful access to the zone. After the timeout has expired for a particular credential a passback violation of this credential will no longer be detected. A value of zero or absence of this property indicates passback violations will never time out.

### 7.1.2.6.1 Shared control of a secured zone

In case not all Access Points of a secured zone are controlled by the same access control device, shared control of a secured zone is in place. If passback violation detection is to be achieved for the secured zone, some requirements arise:

1. Each access control device involved in securing a certain zone needs to have an Access Zone object for representing the same secured zone.
2. All Access Zone objects representing the same secured zone, but residing in different devices, shall have the same object identifier.
3. The information in the different representations of the same secured zone, i.e. in the Access Zone objects in the different access control devices, needs to be synchronized.

### 7.1.2.7 Access Point Relationship

The Access Zone object refers to all Access Points to enter or exit the Access Zone. These are the Ingress and Egress Access Points respectively.

The Access Zone exposes these Ingress and Egress Access Point relations by the two properties *Ingress_Points* and *Egress_Points*, both of type *List of BACnetDeviceObjectReference* to Access Point objects.

The Egress Access Point for one Access Zone is typically the Ingress Access Point of a neighboring Access Zone.
7.2 Authentication

Authentication is the process of validating an Access Credential and is considered as a validation check required for authorization. If an authentication fails due to any reason, access is denied.

The data model for authentication consists of two basic representations:

- **Access Credential**
  An Access Credential represents a container of Authentication Factors. This supports multi-factor cards as well as multi-factor authentication. For multi-factor authentication, all Authentication Factors required at an Access Point need to be contained in a single Access Credential. Access rights are assigned to an Access Credential.

- **Access User**
  An Access User represents an individual person, an asset or a group. A group is any combination of persons and assets. An Access User owns one or multiple Access Credentials, of which the Authentication Factors are used to authenticate the Access User. The model allows operating PACS without Access User objects. This may be due to resource constraints, security reasons or any other design considerations.

An Authentication Factor read is processed and validated by the Credential Reader Process and formatted into a BACnetAuthenticationFactor before made available at the Credential Reader Interface.

The Authentication & Authorization Process of the PACS gets this formatted Authentication Factor at the Credential Reader Interface. It scans through its internal credential database (i.e. Access Credentials representation) to see whether the Authentication Factor is known, i.e. listed as one of the Authentication Factors of an Access Credential.

If the matching Access Credential (contains the Authentication Factor!) representation is found, and single factor authentication is in place, this Access Credential is authenticated.

If the Authentication Policy indicates multi-factor authentication, then only when all Authentication Factors are read as required by the active authentication policy of the Access Point, and match with those of a specific Access Credential object, the Access Credential is authenticated.

If the authenticated Access Credential is assigned to an Access User, this Access User is authenticated too, but implicitly.
7.2.1 Access Credential Object Type

There are many types of Access Credentials today, and various new types may come up in the future. Some are a single Authentication Factor; others are typically physical containers of multiple Authentication Factors.

- Media Conveyed Authentication Factors:
  o Numbers from magnetic stripes
  o Structure elements of magnetic stripes
  o Numbers from contact and contact-less cards
  o Structure elements of contact and contact-less cards
  o Bar codes of various shape and type
  o Codes stored in smart cards
  o Others

- Biometric Authentication Factors
  o Finger print
  o Iris image or pattern
  o Hand shape or pattern
  o Face geometry
  o Face image
  o Others

- Remembered Authentication Factors
  o PIN
  o Daily-Code
  o Others

To achieve interoperability among different Access Control devices, and because of the lack of a general standard covering any type of such Authentication Factors, the data model defines well known Authentication Factors while allowing for vendor or organization specific definitions. For details see the Credential Reader Interface section below.

The Access Credential object type holds a single or multiple Authentication Factors.
The Access Credential object represents a container of related Authentication Factors such as card, PIN, biometric, etc. Authentication Factors are grouped in a single container when each factor has the identical access rights and when one or more authentication factors are used in multi-factor authentication (i.e., card and biometric). The authentication factors in a credential may physically exist on the same media, such as a smart card (including FIPS-201 card), or may exist as physically separate entities, such as a card and PIN. Access Rights are assigned to an Access Credential object. The Access Credential object may be assigned to an Access User.

<table>
<thead>
<tr>
<th>Access Credential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification:</td>
</tr>
<tr>
<td>Name, ID, Type, Description, Profile</td>
</tr>
<tr>
<td>Status:</td>
</tr>
<tr>
<td>Access Credential Status</td>
</tr>
<tr>
<td>Authentication:</td>
</tr>
<tr>
<td>Authentication Factors</td>
</tr>
<tr>
<td>Validity:</td>
</tr>
<tr>
<td>Time Window</td>
</tr>
<tr>
<td>Disabling:</td>
</tr>
<tr>
<td>Disabling of the Access Credential</td>
</tr>
<tr>
<td>Use Counting:</td>
</tr>
<tr>
<td>Absolute, remaining Uses</td>
</tr>
<tr>
<td>Relationship:</td>
</tr>
<tr>
<td>Access User Relationship</td>
</tr>
<tr>
<td>Access Rights:</td>
</tr>
<tr>
<td>Assigning and enabling Access Rights</td>
</tr>
<tr>
<td>Threat Handling:</td>
</tr>
<tr>
<td>Threat Authority</td>
</tr>
<tr>
<td>Trace &amp; Search:</td>
</tr>
<tr>
<td>Tracing and Searching Support</td>
</tr>
<tr>
<td>Credential Special Support:</td>
</tr>
<tr>
<td>Extended Door Unlock Time, Exemptions</td>
</tr>
</tbody>
</table>

Figure 7–5, Access Credential Object Type

7.2.1.1 System-wide Identification
Since the same Access Credentials have to be represented in multiple devices, it is recommended that all Access Credential objects representing the same Access Credential have the same identification (i.e. Object_Identifier property value) and relevant content. Some content may not be required in all devices, e.g. a fingerprint Authentication Factor is not required when no fingerprint reader is present at the device.

The identification is not within the scope of the device, but in the scope of the entire system (inter-network-wide). The synchronization of content is a local matter, but the model supports this requirement through the use of standard BACnet services.
7.2.1.2 Access Credential Status

The Access Credential status indicates the validity of the Access Credential object for authentication, and provides reasons for the Access Credential being inactive.

The property **Credential_Status**, of type **BACnetBinaryPV**, indicates whether the Access Credential is active or inactive. Only the value ACTIVE enables the Access Credential to be used for authentication. While the list in property **Reason_For_Disable** is nonempty the status of the Access Credential is INACTIVE, otherwise it is ACTIVE.

The property **Reason_For_Disable**, of type List of **BACnetAccessCredentialDisableReason**, contains a list of reasons why the credential has been disabled. The Access Credential can be disabled for multiple reasons at the same time. While the Credential_Status property has a value INACTIVE this list shall not be empty. When an entry is removed from this list which results in the list becoming empty the Credential_Status is set to ACTIVE.

The enumeration **BACnetAccessCredentialDisableReason** of reasons for which the credential can be disabled is as follows:

- **DISABLED** The credential is disabled for unspecified reasons.
- **DISABLED_NEEDS_PROVISIONING** The credential needs further provisioning which can include vendor proprietary data.
- **DISABLED_UNASSIGNED** The credential is not currently assigned to any access user. This status is assigned only if the property **Belongs_To** is present and contains instance 4194303 in the object identifier.
- **DISABLED_NOT_YET_ACTIVE** The credential is not yet valid at this time. The current time is before the Activation_Time.
- **DISABLED_EXPIRED** The credential is not valid any more at this time. The current time is after the Expiry_Time.
- **DISABLED_LOCKED_OUT** Too many retries in multi-factor authentications have been performed.
- **DISABLED_USE_COUNT** The maximum number of uses has been reached.
- **DISABLED_INACTIVITY** The credential has exceeded the allowed period of inactivity.
- **DISABLED_MANUAL** The credential is commanded to be disabled by a human operator.
- **DISABLED_MISSING** The physical credential is missing; it can be stolen or lost.
- **DISABLED_DAMAGED** The physical credential is damaged.
- **DISABLED_DESTROYED** The physical credential is destroyed.
- <Proprietary Enum Values> A vendor may use other proprietary enumeration values to indicate disable reasons other than those defined by the standard. For proprietary extensions of this enumeration see clause 23.1 of this standard.

A PACS is not required to support all these reasons for disable.

There is no intrinsic alarming foreseen in the Access Credential object. The Access Credential object does not support object-level COV reporting.

7.2.1.3 Authentication Factors

Authentication Factors are values of type **BACnetAuthenticationFactor** which are used to identify the Access Credential. The Authentication & Authorization Process uses these values to compare with a **BACnetAuthenticationFactor** value read from the Credential Reader Interface, in order to find the according Access Credential object. Note that this is not the BACnet object identifier. For details about the **BACnetAuthenticationFactor** data type see the Credential Reader Interface section.
The Access Credential object exposes these values in the property **Authentication_Factors**, of type `Array of BACnetAuthenticationFactor` elements.

For multi-factor authentication, all Authentication Factors required need to be in the same Access Credential object. If a particular factor of a multi-factor authentication can also be used independently of the other factors and has access rights which differ from the rest of the factors, then this factor must also be instantiated in a separate Access Credential object.

For the definition of BACnetAuthenticationFactor see the Authentication Factor Input object type definition in the Credential Reader Interface section.

### 7.2.1.4 Validity Time Window

An Access Credential may optionally be valid only during a predefined time window. The time window for which the credential is valid is bounded by the activation time, which defines the start of the validity period, and the expiry time, which defines the end of the validity period.

The optional property **Activation_Time**, of type `BACnetDateTime`, indicates the date and time at or after which the Access Credential may be valid. If the current time is before the activation time, the Access Credential is disabled and the value DISABLED_NOT_YET_ACTIVE is added to the Reason_For_Disable list. The value DISABLED_NOT_YET_ACTIVE is removed from the Reason_For_Disable list when this condition no longer applies. If any of the fields of the BACnetDateTime contain "wildcard" values, or this property is not present, then the credential can be used from ‘start of time’.

The optional property **Expiry_Time**, of type `BACnetDateTime`, indicates the date and time from when the Access Credential is expired. This defines the end of the validity period of the Access Credential. If the current time is after the expiry time, the Access Credential is disabled and the value DISABLED_EXPIRED is added to the Reason_For_Disable list. The value DISABLED_EXPIRED is removed from the list when this condition no longer applies. If any of the fields of the BACnetDateTime contain "wildcard" values, or this property is not present, then the credential can be used until ‘end of time’.

### 7.2.1.5 Disabling an Access Credential

An Access Credential object can be disabled by an operator or by any process. If disabled, the Reason_For_Disable contains a corresponding reason, and Credential_Status becomes INACTIVE. If no disable is set (NONE), the status of the Access Credential is determined according other properties of the object.

The property **Credential_Disable**, of type `BACnetAccessCredentialDisable`, allows an operator or external process to disable the Access Credential. When this property takes on any value other than NONE the Access Credential is disabled and the corresponding disable reason is added to the Reason_For_Disable list. When this property is changed any value previously added to the Reason_For_Disable list, as a result of changing this property, is removed from that list.
The following disable enumeration values are known and defined in the new BACnet enumeration `BACnetAccessCredentialDisable`:

- **NONE**: The credential has not been disabled by an operator or external process.
- **DISABLE**: The credential has been disabled for unspecified reasons. The value DISABLED is added to the `Reason_For_Disable` property.
- **DISABLE_MANUAL**: The credential has been disabled by a human operator. The value DISABLED_MANUAL is added to the `Reason_For_Disable` property.
- **DISABLE_MISSING**: The credential is disabled because it has been reported to be stolen or lost. The value DISABLED_MISSING is added to the `Reason_For_Disable` property.
- **DISABLE_DAMAGED**: The credential is disabled because it has been damaged. The value DISABLED_DAMAGED is added to the `Reason_For_Disable` property.
- **DISABLE_DESTROYED**: The credential is disabled because it has been destroyed. The value DISABLED_DESTROYED is added to the `Reason_For_Disable` property.
- **DISABLE_LOCKOUT**: The credential is disabled because it has been locked out by an external process. The value DISABLED_LOCKOUT is added to the `Reason_For_Disable` property.

<Proprietary Enum Values> A vendor may use other proprietary enumeration values for disabling a credential other than those defined by the standard. A disable reason has to be added to the `Reason_For_Disable` property. It is a local matter which disable reason is added. For proprietary extensions of this enumeration see clause 23.1 of this standard.

### 7.2.1.6 Use Counting

Access Credentials may be limited in the number of their use for authentication. The uses may be counted based on different criteria.

#### 7.2.1.6.1 Number of days used

An Access Credential can be limited in the number of days it may be used. The days do not need to be contiguous days.

The optional property `Days_Remaining`, of type `Unsigned`, indicates the number of remaining days for which the credential can be used. If this property is present and has a value of zero, authentication is no longer possible using this credential. If this property becomes zero, the Access Credential is disabled and the value DISABLED_USE_COUNT is added to the `Reason_For_Disable` list. The value DISABLED_USE_COUNT is removed from the list when this condition no longer applies.

#### 7.2.1.6.2 Number of uses

An Access Credential can be limited in the number of uses for access. Access granted at an Access Point counts as one use. Ingress or Egress is both counted as one use of the Access Credential.
The optional property *Uses.Remaining*, of type *Unsigned*, indicates the number of remaining uses which the credential can be used for authentication. Access granted at an access controlled point counts as a single use. If this property is present and has a value of zero, the Access Credential is disabled and the value *DISABLED_USE_COUNT* is added to the Reason_For_Disable list. The value *DISABLED_USE_COUNT* is removed from the list when this condition no longer applies.

### 7.2.1.6.3 Number of days not used (Inactivity Counter)

An Access Credential may become invalid after a number of days of not being used. This is independent of the Expiry_Time, and is reset each time the Access Credential is used for access.

The optional property *Absentee_Limit*, of type *Unsigned*, specifies the maximum number of consecutive days for which the credential can remain inactive (i.e. unused) before it becomes disabled. The calculation of inactivity duration is based on the time of last use as indicated by the property Last.Use.Time. If Last.Use.Time does not have a valid time and date then the absentee limit is considered not being exceeded. When the absentee limit is exceeded the Access Credential is disabled and the value *DISABLED_INACTIVITY* is added to the Reason_For_Disable list. The value *DISABLED_INACTIVITY* is removed from the list when this condition no longer applies.

### 7.2.1.7 Access User Relationship

The Access Credential may be assigned to an Access User. This is used to provide the reference to the owning Access User.

The optional property *Belongs.To*, of type BACnetDeviceObjectReference, references an Access User object which represents the owning access user (i.e. person, group, or asset). If this property is present and the credential is not assigned to an access user, this property contains an instance number of 4194303 in the object identifier. The determination of whether the credential is valid for authentication, based on the value of this property, is a local matter. If the credential has not been assigned to an access user and the policy of the site requires that it be assigned, then the credential is disabled and the value *DISABLED_UNASSIGNED* is added to the Reason_For_Disable list. The value *DISABLED_UNASSIGNED* is removed from the list when this condition no longer applies.

Note that there is a single reference to an Access User. This is by intent, enforcing the use of Access User objects to represent groups owning the same Access Credential.

### 7.2.1.8 Assigned Access Rights

An Access Credential object refers to the Access Rights assigned. Once the Access Credential is authenticated, the Authentication & Authorization Process uses this information to find the Access Rights assigned to the Access Credential.

The required property *Assigned_Access_Rights*, of type Array of BACnetObjectIdentifier, refers to Access Rights objects which define the access rights assigned to this credential. Each object referenced in the Assigned_Access_Rights property shall be an Access Rights object. Any entry with an instance number of 4194303 or a reference to a non-existent Access Rights object shall be ignored.

The required property *Access_Rights_Enable* is an Array of BOOLEAN, which allows enabling and disabling assigned Access Rights individually for this Access Credential. Setting an element of this array enables (TRUE) or disables (FALSE), for this Access Credential, the Access Rights referenced by the corresponding Assigned_Access_Rights array element. The i\textsuperscript{th} element applies to the i\textsuperscript{th} element of Assigned_Access_Rights. The size of this array must match the size of the Assigned_Access_Rights array.
7.2.1.9 Tracing and Searching Support

The Access Credential object may refer to the last Access Point where this Access Credential has been recognized. An Access Credential is recognized when one of its Authentication Factors matches the Authentication Factor read from the Credential Reader Interface.

The optional property **Last_Access_Point** of type **BACnetDeviceObjectReference** refers to the last Access Point object where at least one of the Authentication Factors of the Access Credential has been recognized. A COV subscription to this property enables monitoring applications to trace and search this Access Credential. These applications, when subscribed, will receive all information required conveyed in the COV notifications. If property level COV is in effect for this property, any update of this property causes a COV notification to be issued, regardless of whether the value of this property changes. If the Access Credential is not yet used, this property contains an instance number of 4194303 in the object identifier.

To trace on access events created by the Access Credential, the optional property **Last_Access_Event**, of type **BACnetAccessEvent**, indicates the last access event created on use of the Access Credential. If multiple access events are generated by the use it is a local matter which access event is the Last_Access_Event. If no access event is created yet, this property has a value of NONE.

The optional property **Last_Use_Time**, of type **BACnetDateTime**, indicates the date and time of the last use of the Access Credential at an Access Point. If the Access Credential is not yet used, this property contains X’FF’ in all fields.

To instruct an Access Point to send out a corresponding TRACE access event notifications if the Access Credential is recognized, the optional property **Trace_Flag**, of type **BOOLEAN**, is set to TRUE.

7.2.1.10 Threat Authority

The Access Credential may be valid for authorization depending on the threat level of an Access Point. If the threat level of the Access Point is higher than the Access Credential’s threat authority, the Access Credential will be denied access at the Access Point.

The optional property **Threat_Authority**, of type **BACnetAccessThreatLevel**, indicates the maximum threat level for which this credential is valid. If this value is less than the Threat_Level of the Access Point where the Access Credential is used, access is denied. If this property is not present it is assumed that the threat authority of the Access Credential is zero.

7.2.1.11 Credential Special Support

The Access User using this Access Credential may need special support of the PACS to have more time to pass an Access Door. If this is the case, EXTENDED_PULSE_UNLOCK is used to command an Access Door, delaying the activation of a DOOR_OPEN_TOO_LONG alarm for longer time according the Access Door configuration.

The need for special support is exposed by the optional property **Extended_Time_Enable** of type **BOOLEAN**. If Extended_Time_Enable is TRUE, EXTENDED_PULSE_UNLOCK is used to command the Access Door, otherwise PULSE_UNLOCK.

It is required that Access Credentials can be excluded from passback detection.

The exclusion from passback detection is indicated by the optional property **Passback_Exemption** of type **BOOLEAN**. If this property is TRUE, the Access Credential is excluded from passback enforcement. The Access Credential is not denied access due to passback violations.
It is required that Access Credentials can be excluded from occupancy enforcements.

The exclusion from occupancy enforcement is indicated by the optional property *Occupancy_Count_Exemption* of type *BOOLEAN*. If this property is TRUE, the Access Credential is excluded from occupancy enforcement. The occupancy count in the Access Zone object is updated as normal however, the Access Credential is not denied access due to occupancy threshold enforcement.
7.2.2 Access User Object Type

The object type Access User is used to represent a single person, an organizational entity or an asset. Relationships among Access Users are supported, to model hierarchical organizations comprising e.g. companies, departments, or groups of any kind, or to model ownership of assets.

The Access User object is not directly involved in Authentication & Authorization. It is used for informational purpose and may hold references to other systems. PACS implementations are not generally required to support this object type, although for some applications it may become useful.

<table>
<thead>
<tr>
<th>Access User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification:</strong> Name, ID, Type, Description, Profile</td>
</tr>
<tr>
<td><strong>Type Indication:</strong> Represented Type</td>
</tr>
<tr>
<td><strong>Name:</strong> User Name</td>
</tr>
<tr>
<td><strong>User Reference:</strong> User Reference Number</td>
</tr>
<tr>
<td><strong>User Information:</strong> User Information Reference</td>
</tr>
<tr>
<td><strong>Hierarchy:</strong> Hierarchical Structures</td>
</tr>
<tr>
<td><strong>Ownership:</strong> Credential Ownership</td>
</tr>
</tbody>
</table>

Figure 7–6, Access User Object Type

7.2.2.1 Identification

Since the same Access Users have to be represented in multiple devices, it is recommended that all Access User objects representing the same Access User have the same identification (i.e. Object_Identifier property value) and relevant content. Some content may not be required in all devices.

The identification is then not within the scope of the device, but in the scope of the entire system (inter-network-wide). The synchronization of content is a local matter, but the model supports this requirement through the use of standard BACnet services.
7.2.2.2  Type Indication
The Access User object exposes an enumeration value which indicates what the object represents. The following values are known and defined in the BACnetAccessUserType enumeration:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| ASSET | The Access User object represents a physical item which may enter and leave a secured zone. Examples are:  
  | Trucks  
  | Cars  
  | Containers  
  | Computers  
  | Baggage  
  | Etc. |
| GROUP | The Access User object represents a group of Access Users. Various types of groupings of assets or persons are possible. This covers:  
  | Organization  
  | Department  
  | Etc. |
| PERSON | The Access User object represents an individual person. |

<Proprietary Enum Values> A vendor may use other proprietary enumeration values to indicate proprietary user types.

The represented type is exposed in the property User_Type of type BACnetAccessUserType, which indicates what the Access User object represents.

7.2.2.3  User Name
The Access User object exposes the clear text name of the person, group or asset it represents. Note that this information is not restricted by uniqueness or other constraints. Content is not restricted, and may even contain multiple lines of printable characters.

The optional property User_Name of type CharacterString, which is the clear text name of the person the object represents.

7.2.2.4  User External Identifier
This indicates an external identifier such as a reference number for the person the Access User object represents. This identifier is not explicitly pointing to any further information. Example uses are:

- FIPS-201 mandated person reference number  
- Social Security Number  
- Employee Number  
- Etc.

The user external identifier is exposed by the optional property User_External_Identifier, of type CharacterString. While the content is typically unique, interpretation of the content is a local matter.

7.2.2.5  User Information Reference
The Access User object may indicate a user information reference in the form of a Character String. This is a reference such as an URL to information located in other systems, such as an HRMS, CMS or IDMS.

The optional property User_Information_Reference, of type CharacterString, holds this reference. Interpretation of the content is a local matter.
7.2.2.6 Hierarchical Structures
The Access User objects may be hierarchically structured, to adapt to organizational structures and assign assets to persons or groups.


An Access User object exposes to what Access User it belongs to by an optional property `Member_Of` of type `List of BACnetDeviceObjectReference`, referring to Access User objects.

7.2.2.7 Credential Ownership
To represent ownership of Access Credentials, the Access User object may have Access Credentials assigned. This information is typically used for operation purposes (e.g. disabling all Access Credentials of a Person).

The credential ownership is exposed by a property `Credentials`, of type `List of BACnetDeviceObjectReference`, referring to Access Credential objects.
7.3 Authorization

Authorization is a series of validation steps before access is granted. The sequence of steps is not mandated. Example validation steps are:

- Authentication and validation of Access Credentials
- Evaluation of external conditions
- Sufficient Access Rights assigned to the Access Credential
- Others

The validation steps may be taken in any order, or run in parallel. A single failed validation step finally denies access, while only if there is a sufficient number of a successful validation steps, access is granted. The process of authorization is to pass all authorization checks without finding a denial reason.

The validation steps are typically performed by the Authentication & Authorization Process.

Some steps may already be performed by the Credential Reader process, but then the Authentication & Authorization Process does not become active since no Authentication Factor is received from the Credential Reader Interface.

For clarity of the model, the step of authenticating an Access Credential is detailed in section Authentication above. Other validation steps are detailed in the following sections, although proprietary validations may take place and are a local matter of the Authentication & Authorization Process.
7.3.1 Access Rights Object Type

The Access Rights object defines a set of access rules. Each access rule specifies when or why access is possible at a geographical location. If an access rule is found which is enabled and matches location and current time of the request to access, then the validation step of checking access rights is successful.

An Access Rights object is referenced from Access Credential objects, which is an assignment of access rights to this Access Credential. Multiple Access Credential objects may refer to the same Access Rights object. Access Rights objects facilitate to model the access rights of “roles”, which Access Users may take within an organization. Access Rights for roles can be inherited to be added to more specific Access Rights.

Access Rights objects may also be used as profiles, e.g. Office Area at office times, Server Room at nightshift, etc.

<table>
<thead>
<tr>
<th>Access Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification:</strong> Name, ID, Type, Description, Profile</td>
</tr>
<tr>
<td><strong>Enabling:</strong> Overall Enable</td>
</tr>
<tr>
<td><strong>Enabling:</strong> Individual Enabling of Access Rules</td>
</tr>
<tr>
<td><strong>Access Rules:</strong> List of Access Rules</td>
</tr>
<tr>
<td><strong>Accompaniment:</strong> Accompaniment Specification</td>
</tr>
<tr>
<td><strong>Inheritance:</strong> Inherited Access Rights</td>
</tr>
</tbody>
</table>

Figure 7–7, Access Rights Object Type

7.3.1.1 Identification

Since the same Access Rights have to be represented in multiple devices, and it is recommended that all Access Rights objects representing the same access rights have the same identification and content, the Access Rights objects representing the same set of access rights shall have the same identification (i.e. Object_Identifier property value) and relevant content. Some content may not be required in all devices, e.g. Access Rights for Access Zones and Access Points not controlled by a particular device.

The identification is then not within the scope of the device, but in the scope of the entire system (inter-network-wide). The synchronization of content is a local matter, but the model supports this requirement through the use of standard BACnet services.

7.3.1.2 Overall Enable

The Access Rights object supports the enabling and disabling of all the access rules it contains or inherits.

The property *Enable*, of type *BOOLEAN*, indicates whether the access rules at all specified by the object, including the inherited ones, are valid (TRUE) or not (FALSE). Even if Enable is TRUE, individual access rules may be disabled individually by their corresponding Access_Rules_Enable entries.
7.3.1.3 Access Rules

The access rules specify access rights (i.e. pass right or “positive” right).

A single access rule contains the following elements:

- The Time Range reference is used to validate the access rule against current time or other external BOOLEAN condition.
- The Location reference is used to validate the access rule against the location of authentication, i.e. the Access Point or Access Zone.

<table>
<thead>
<tr>
<th>Element</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time_Range</td>
<td>BACnetObjectPropertyReference</td>
<td>This field, of type BACnetObjectPropertyReference, references a property that can be evaluated to TRUE or FALSE which defines if the rule is valid (TRUE) or not (FALSE).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the value of the referenced property is of type Unsigned, a value of zero shall evaluate to FALSE, while any other value shall evaluate to TRUE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the value of the referenced property is of type INTEGER, a value of less than or equal to zero shall evaluate to FALSE, while any value greater than zero shall evaluate to TRUE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the value of the referenced property is of type BACnetBinaryPV then INACTIVE shall evaluate to FALSE while ACTIVE evaluates to TRUE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the referenced property does not exist or its value cannot be retrieved, or the value is of type NULL, the Time-Range evaluates to FALSE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the reference property is of any other type, then the evaluation is a local matter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If Time-Range contains an undefined reference (i.e. 4194303 in the instance part), Time-Range evaluates to TRUE.</td>
</tr>
<tr>
<td>Location</td>
<td>BACnetObjectIdentifier</td>
<td>This field, of type BACnetObjectIdentifier refers to the Access Point or Access Zone this access rule is valid for.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When Location refers to an Access Point object, this access controlled point is required to be the location where the credential used to request access has been authenticated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When Location refers to an Access Zone object, the access controlled point where the credential used to request access has been authenticated is required to be an ingress point to this zone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If Location contains an undefined reference (i.e. 4194303 in the instance part), this access rule is considered as valid for any location.</td>
</tr>
</tbody>
</table>

Note: This field can reference a Schedule object Present_Value property for the specification of time ranges.
The structure of an access rule is defined by the type `BACnetAccessRule`, containing a sequence with the two elements as defined above.

The access rules are exposed by the required property `Access_Rules`, of type `Array of BACnetAccessRule`.

If an element of the array can be found where Time_Range evaluates to TRUE and Location matches the location of authentication, and the corresponding element of the Access_Rules_Enable property is TRUE, the evaluation of access rules is considered successful. The size of this array shall equal the size of the Access_Rules_Enable array. The i\(^{th}\) element of this array corresponds to the i\(^{th}\) element of the Access_Rules_Enable property.

### 7.3.1.4 Individual Enabling of Access Rules

The Access Rights object supports the enabling and disabling of individual access rules it contains.

The property `Access_Rules_Enable` of type `Array of BOOLEAN`, allows enabling access rules individually within the Access Rights object. Setting an element of this array enables (TRUE) or disables (FALSE) the corresponding Access_Rules array element. The i\(^{th}\) element applies to the i\(^{th}\) element of Access_Rules. The size of this array must equal the size of Access_Rules. If this property is not present, all access rules are considered as enabled unless overall disabled by the Enable property.

### 7.3.1.5 Accompaniment Specification

An Access Rights object may be valid only if the Access Credential in question is accompanied by another Access Credential. This is configurable by a reference to either another Access Rights object, to an Access Credential object or to an Access User object.

(a) If this property refers to an Access Rights object then the accompanying Access Credential is required to refer to or inherit from that Access Rights object.

(b) If this property refers to an Access Credential object then this object represents the accompanying Access Credential.

(c) If this property refers to an Access User object then this object is required to represent the Access User which owns the accompanying Access Credential.

The optional property `Accompanied`, of type `BACnetObjectIdentifier`, refers to the object the accompanying Access Credential needs to be related to as outlined above.

If the property is present and the instance is 4194303, or the property is absent, the Access Rules of this Access Rights object are further considered without any accompanying Access Credential.

### 7.3.1.6 Inherited Access Rights

The inherited access rights are exposed by the optional property `Inherited_Access_Rights`, of type `List of BACnetObjectIdentifier`, referring to Access Rights objects whose access rules are to be evaluated as well.

This recursively includes access rules inherited by the referenced Access Rights objects. If an inherited Access Rights object is disabled, then its access rules and those which it inherits are not inherited.

Only enabled access rules are inherited from Access Rights objects.

Accompaniment requirements are also inherited from inherited Access Rights objects. The local accompaniment requirement supersedes an inherited accompaniment requirement.
7.3.2 Configuration and Validation of Access Rights

The validation of Access Rights is one of the validation steps in authorization. Access Rights allow specifying, for an Access Credential:

- Where is access possible
- When (or under what condition) is access possible
- Does this credential need to be accompanied

The evaluation of access rules is performed by the Authentication & Authorization Process. Although this is a local matter, the interface’s data model reflects some behavior and allows configuring Access Rights.

The data model for Access Rights facilitates configurations according the Role Based Access Control (RBAC) model introduced by NIST (see [RBAC]) and used widely by the IT industry.

For the sake of simplicity, no dedicated role representation is introduced. The new Access Rights object may represent roles in the sense of RBAC, and privileges are assigned to the role by specifying Access Rules in these Access Rights objects.

Inheritance of access rules is enabled by referencing the Access Rights objects from which to inherit access rules. Inheriting from multiple Access Rights objects is possible.

7.3.2.1 Access Rights Configuration Overview

![Access Rights Configuration Data Structure Overview and Example](image-url)
• An Access User object refers to the Access Credential objects it owns (Property Credentials).
• An Access Credential object refers to Access Rights objects (Property Assigned_Access_Rights).
• Access Rights objects refer to other Access Rights objects from which they inherit access rules (Property Inherit_Form).
• Access Rights objects contain a list of access rules where each defines a time range and a location (Property Access_Rules).
• Access Rights objects may refer to other Access Rights objects from which to inherit access rules (Property Inherit_From).
• Access Rights objects may specify an accompaniment requirement (Property Accompanied).

For details of the Access Rights object see the Access Rights Object Type definition above.

7.3.2.2 Access Rights Validation

The validation of Access Rights starts with the Access Credential(s) authenticated at an Access Point. The Access Credential refers to the Access Rights objects assigned, specifying the access rules. The validation of accompaniment, if specified, requires that the Authentication & Authorization Process collects other Authentication Factors to authenticate the accompanying Access User's Access Credential.

The validation is done by iterating through the Access_Rules properties of the Access Rights objects assigned to the Access Credential, as well as those referred to be inherited. Each access rule is validated and accompaniment requirement is evaluated. The first successful validation results in a successful validation of Access Rights. But access may still be denied due to other reasons (e.g. passback violation, exhausted use count, occupancy thresholds etc.). If there is no successful validation of Access Rights at all, access is finally denied.

A successful validation results if all the following conditions apply:

Access Credential Object:

• The Access_Rights_Enable flag corresponding to the Access Rights object assignment is TRUE in the Access Credential.

Access Rights Object:

• The Access Rights object is enabled.
• The Access_Rules_Enable flag corresponding to the Access_Rules element evaluated is TRUE.
• Time Range of the evaluated Access_Rules element refers to a property which evaluates to TRUE, or contains an undefined reference.
• Location of the evaluated Access_Rules element refers the Access Point of authentication, or refers an Access Zone of which the Access Point of authentication is an Ingress Access Point, or Location is undefined (i.e. valid for any location).
• Either the Access Rights object Accompanied property contains 4194303 as instance in the object identifier
• Or the Accompanied property references an object and one of the following is true:
  o If the Accompanied property refers to an Access Rights object and the accompanying Access Credential refers to or inherits from that Access Rights object.
  o If the Accompanied property refers to an Access Credential object and this object represents the accompanying Access Credential.
  o If the Accompanied property refers to an Access User object and this object represents the Access User which owns the accompanying Access Credential.
7.3.3 Time Ranges

Access rules of the Access_Rules property of Access Rights objects may refer to a time range specification, specifying when in time the rule is valid. The standard BACnet object types Schedule and Calendar are reused for this functionality. The Time Range field of an access rule in the Access_Rules property refers to a Schedule object’s Present_Value, which indicates TRUE (i.e. valid) or FALSE (i.e. invalid). If the Schedule object did not set the Present_Value by a scheduled action, the Present_Value contains NULL, which evaluates to FALSE as well.

Schedules and Calendar objects allow defining sophisticated time ranges consisting of

- Weekly schedules
- Exception schedules
- Effective periods
- Calendar for exception schedules

The Schedule object writes the BOOLEAN values FALSE or TRUE into its own Present_Value. No property references are required in the Schedule object. The Schedule object does not perform write operations to Time Range elements of the Access_Rules property of Access Rights objects.

For an access rule in the Access_Rules property, a Schedule object’s Present_Value of TRUE indicates the access rule is further considered, a value of FALSE (or NULL) invalidates the access rule.

For Time Ranges not related to time of day, but for entire special days of a year, the Time_Range element of an access rule may point to a Calendar object’s Present_Value directly.
7.3.4 External Conditions
Access rules of the Access_Rules property of Access Rights objects may refer to an external condition, specifying if the access rule is valid. The Time_Range field of an access rule refers to a numeric value property of a defined subset of primitive data types. If the referenced property evaluates to TRUE, the access rule is further considered, if it evaluates to FALSE the access rule is invalid.

7.3.5 Two-Person-Rules
“Two-Person-Rule” as a term covers a number of special authorizations which involve multiple Access Users, or Access Credentials. Supported rules are:

Minimum Occupancy: This is supported by the Access Zone object. The Authentication & Authorization Process may read and evaluate further Authentication Factors before granting access.

Accompanied persons: The Access Rights object specifies what other Access Credential or Access User must be authenticated before access is granted. See the Accompanied property of the Access Rights object above.

Group rules: Since Access Rights may be shared among different Access Credentials, and by this forming some kind of group, the Accompanied property of the Access Rights object may point to shared Access Rights, indicating what other group member is required.

Other rules may be supported by the model as defined, but its application by the Authentication & Authorization Process is a local matter.

More sophisticated rules are considered a local matter of the Authentication & Authorization Process and proprietary extensions of the data model. If such rules turn out to be common, the standard model may be extended.
8. Credential Reader Interface

This interface provides access to authentication factors read, validated and processed. It enables control over indication hardware at the credential reader’s front plate. It may provide access to data stored in credentials, such as smart card blocks.

The data model and services provided by this interface are BACnet based. The interface is provided and maintained by the Credential Reader Process.

The Credential Reader Interface provides the following:

- Authentication Factors read, processed and validated by the Credential Reader Process
- False reading indications
- Access to Credential contents, such as files or blocks on smart card
- Access to Credential Reader front plate elements, such as LEDs, beepers etc.
- Credential Reader States

The Credential Reader Interface is modeled using existing and new BACnet objects. This creates the freedom to model simple single factor credential readers up to very sophisticated multi-factor readers with sophisticated front plate elements. The new Authentication Factor Input object type is defined to represent input of Authentication Factors. This object basically provides processed and validated Authentication Factors to any interested client role process.

The Authentication & Authorization Process of the PACS uses this interface to get processed and validated authentication factors presented by the access user at the reader’s front plate, and to control the indication elements of the reader’s front plate. Other processes may also use this interface, e.g. Time & Attendance applications to get timestamps.

8.1 Authentication Factors

The Credential Reader Interface enables access to Authentication Factors read at the Credential Reader front plate and preprocessed by the Credential Reader Process.

The provisioning or enrollment of authentication factors of Access Credential objects into a PACS device is required to know what authentication factor types are supported by the Credential Reader Process and can be read at the Credential Reader Interface.

8.1.1 Structured Authentication Factors

Some authentication factors are structured, of which single elements or the entire structure may be used as Authentication Factors. Examples for such structures are magnetic stripe codes containing a site code and a number, or the US government Personal Identity Verification (PIV) initiative based Card Holder Unique Identifier (CHUID) structure, which contains the Federal Agency Smart Card Number (FASC-N) data structure.

To use such structured information in any way, the Credential Reader Process is required to know about such structures, to be able to extract elements and to provide them as a structured authentication factor at the Credential Reader Interface. Any subset is considered a unique format.

If different subsets or formats of an authentication factor are supported, parallel access to the different formats is supported at the Credential Reader Interface.
8.1.2 Authentication Factor Data Model

The data model used for Authentication Factors is based on structured data of type \textit{BACnetAuthenticationFactor}. Any kind of Authentication Factor is represented as a BACnetAuthenticationFactor structure. This includes, for example, Wiegand numbers, FASC-N numbers, Hash Codes from biometric data etc. The model needs to support the extremely broad range of different Authentication Factors today and increasing variety in the future. Vendors may define proprietary formats.

Up to now there is no standard available which would define how any Authentication Factors looks like in bits & bytes, useful for BACnet. But for interoperability, it is essential that the content of Authentication Factors is defined. Since no standard is available, BACnet defines the structure of well known Authentication Factors, while allowing vendor or organization proprietary definitions. The concept of site specific Format Class identifiers is added for differentiation of authentication factors conveyed by different Access Credential types, where equal authentication factors may be possible, but need to be differentiated in authentication and authorization.

Note: The same data type for Authentication Factors (BACnetAuthenticationFactor) is used to hold known Authentication Factors in the Access Credential object, introduced for the Authentication & Authorization Interface.

BACnetAuthenticationFactor is a sequence with the following fields:

\begin{verbatim}
BACnetAuthenticationFactor ::= SEQUENCE {
    formatClass         [0] Unsigned
    value               [1] CHOICE {
        undefined             [0] CHOICE {
            null                  [0] NULL,
            errorUnsigned         [1] Unsigned,
            errorOctetString      [2] OCTET STRING,
            errorBitString        [3] BITSTRING,
        },
    }
}
\end{verbatim}

The definition of \textit{BACnetAuthenticationFactor} is as follows. Note that some of the elements are or may be unsigned numbers beyond 32 bits!
simpleNumber          [1] Unsigned,
simpleAlphaNumeric    [2] CharacterString,
facilityAndCardNumber [3] SEQUENCE {
    facility            Unsigned,
    card                Unsigned
  },
fascn                 [4] SEQUENCE {
    agencyCode          Unsigned (0..9999),
    systemSiteCode      Unsigned (0..9999),
    credentialNumber    Unsigned (0..999999)
  },
  -- FIPS 201 FASC-N structure
fascnFull             [5] SEQUENCE {
    agencyCode          Unsigned (0..9999),
    systemSiteCode      Unsigned (0..9999),
    credentialNumber    Unsigned (0..999999),
    seriesCode          Unsigned (0..9),
    individualCredentialIssue Unsigned (1..9),
    personIdentifier.........Unsigned (0..9999999999),
    organizationalCategory Unsigned (0..9),
    organizationalIdentifier Unsigned (0..9999),
    associationCategory   Unsigned (0..9)
  },
  -- FIPS 201 FASC-N full structure
gsa75                 [6] SEQUENCE {
    agencyCode           Unsigned (0..16383),
    systemSiteCode       Unsigned (0..16383),
    credentialNumber     Unsigned (0..1048575),
    expirationDate       Date
  },
  -- GSA 75 format
gsa75hmac             [7] SEQUENCE {
    agencyCode           Unsigned (0..16383),
    systemSiteCode       Unsigned (0..16383),
    credentialNumber     Unsigned (0..1048575),
    expirationDdate      Date,
    hmac32               OCTET STRING (SIZE(4))
  },
  -- GSA 75 format with 32 bit HMAC code
cbeffA                [8] OCTET STRING,
  -- NIST CBEFF Patron Format A (CBEFF) content formatted
  -- according CBEFF definitions
cbeffB                [9] OCTET STRING,
  -- NIST CBEFF Patron Format B (BioAPI) content formatted
  -- according CBEFF definitions
cbeffC [10] OCTET STRING,
-- NIST CBEFF Patron Format C (ANSI Standard X9.84) content formatted
-- according CBEFF definitions

userPassword [11] SEQUENCE {
    username CharacterString,
    password CharacterString
},

-- Context tag 254 is used for proprietary formats as follows:

proprietary [254] SEQUENCE {
    vendorID [0] Unsigned,
    typeID [1] Unsigned,
    value [2] ABSTRACT-SYNTAX.&Type
}
-- This format is to be used for proprietary formats not
-- fitting into any standard format. The exact format definition
-- of the value and the associated type ID is vendor specific.

For indication purposes, the enumeration BACnetAuthenticationFactorType is defined. Its assigned values correspond
with the top-level context tag numbers of BACnetAuthenticationFactor's value field.

BACnetAuthenticationFactorType ::= ENUMERATED {
    undefined (0),
    simple-number (1),
    simple-alpha-numeric (2),
    facility-and-card-number (3),
    fasc-n (4),
    fasc-n-full (5),
    gsa75 (6),
    gsa75hmac (7),
    cbeff-A (8),
    cbeff-B (9),
    cbeff-C (10),
    user-password (11),
    reserved (253),
    proprietary (254)
}
-- This enumeration is not extensible by vendors.
8.1.3 Authentication Factor Input Object Type

The Authentication Factor Input object type is introduced to model the input of Authentication Factors, as the key model of the Credential Reader Interface.

<table>
<thead>
<tr>
<th>Authentication Factor Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification: Name, ID, Type, Description, Profile</td>
</tr>
<tr>
<td>Present_Value: Last authentication factor provided</td>
</tr>
<tr>
<td>Format Type: Format Type Specification</td>
</tr>
<tr>
<td>General Health: Overall Status and Reliability</td>
</tr>
<tr>
<td>Update &amp; Status: Update information and Read Status</td>
</tr>
<tr>
<td>Maintenance: Out of service support for simulation</td>
</tr>
</tbody>
</table>

Figure 8–1, Authentication Factor Input Object Type

8.1.3.1 Identification

The common properties for object identification are used as mandated and optional by the BACnet standard [STD]. This includes a numeric identifier, object name, textual description and a profile reference.

8.1.3.2 Present Value

The key value of the Authentication Factor Input object type provides the authentication factors read at the Credential Reader front plate and preprocessed, as a value of type BACnetAuthenticationFactor. This value contains a site specific format class identifier (Format-Class) and the authentication factor value (Value).

The last BACnetAuthenticationFactor provided is exposed by the Present_Value property of type BACnetAuthenticationFactor. If no authentication factor was provided yet, the Value field of BACnetAuthenticationFactor uses option "undefined", with a NULL value.

The Format-Class field always contains the value as set in the Format_Class_Supported property.

The Value field, in case of correct authentication factor readings, uses the option that matches the value of the Format_Type property. The data provided is the preprocessed authentication.

In case of false readings, the Value filed uses the option “undefined”, and it may contain the raw authentication factor data or any other error information. The data types allowed for this are octet string, bit string or character string. The determination of the value is a local matter of the Credential Reader Process.

COV subscriptions on this object will result in notifications sent out each time the Present_Value is updated. This is also the case if the same Authentication Factor is provided again.

The Present_Value is writable when Out_Of_Service is TRUE. When writing, the Format-Class field must match the value of Format_Type_Supported property, and the Value field must be of option "undefined" or the option that matches the value of the Format_Type property.

8.1.3.3 Format Type Specification

The Authentication Input object type exposes what format of Authentication Factors it provides. The identification is based on four elements:
- Format Type, which corresponds with the context tag number of the supported option of BACnetAuthenticationFactor.
- Format Class, which is used as a site specific identifier of Authentication Factor formats. On a site, authentication factors may be used which result in the same format type, but are required to be differentiated. In this case, the Format Class allows differentiation of equal authentication factor format types conveyed in different Access Credentials.
- Vendor Identifier, used only if a proprietary format is provided. Note that this may not be the same as the vendor identifier of the manufacturer of the device. This identifier is maintained by ASHRAE.
- Vendor's Format Identifier, used only if a proprietary format is provided. The value is determined by the vendor as indicated by Vendor Identifier.

The required property **Format_Type**, of type BACnetAuthenticationFactorType, holds the same value as the context tag number of the BACnetAuthenticationFactor value option provided by the object. If a proprietary format is provided, this property has the value 254.

The optional, if present writable, property **Format_Class_Supported**, of type Unsigned, indicates the Format Class conveyed by authentication factors provided by Present_Value. This property is writable for site specific setups. A value of zero is used as default for sites where no differentiation of equal authentication factors from different Access Credentials is used. If this property is not present, the Format-Class filed of authentication factors provided by Present_Value has a value of zero.

The optional property **Vendor_Identifier**, of type Unsigned16, holds the vendor identifier of the vendor defining the proprietary format. This property must be present if a proprietary format is supported. This value may differ from the Vendor_Identifier property value in the Device object, which indicates the device manufacturer.

The optional property **Vendor_Format_Identifier**, of type Unsigned, holds the vendor's proprietary format identifier. This property must be present if a proprietary format is supported.

If a Credential Reader Process supports multiple authentication factor formats or supports differentiation of Access Credential types, it is expected that for each format type and format class an individual Authentication Factor Input object is present. This enables the setup of Authentication Policies. See also Access Point object type.
8.1.3.4 General Health

Properties are defined which indicate the general health of the object. Reliability indication and out of service is supported.

The property **Status_Flags**, of type `BACnetStatusFlags`, indicates, by a set of individual flags (i.e. bits), the general health of the object. Each flag is related to specific properties, which provide more details.

- The **FAULT** flag is 1 if the property **Reliability** has a value other than **NO_FAULT_DETECTED**.
- The **OUT_OF_SERVICE** flag is 1 if the property **Out_Of_Service** is **TRUE**.
- All other flags are always 0.

The property **Reliability**, of type `BACnetReliability`, indicates the detailed reliability of the credential reader processing this object represents. The following enumeration values may be supported:

<table>
<thead>
<tr>
<th>Enumeration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO_FAULT_DETECTED</td>
<td>The process and the object are reliable.</td>
</tr>
<tr>
<td>CONFIGURATION_ERROR</td>
<td>The configuration of the device or object has an error preventing</td>
</tr>
<tr>
<td></td>
<td>reliable processing.</td>
</tr>
<tr>
<td>UNRELIABLE_OTHER</td>
<td>An unspecific reason leads to unreliable processing.</td>
</tr>
</tbody>
</table>

8.1.3.5 Update Information and Read Status

Any consumer of Authentication Factors is required to get any new Authentication Factor preprocessed by the Credential Reader Process. Since COV reporting in BACnet was not designed for streaming, but no new BACnet services shall be introduced for PACS, some additional information is required in properties of the Authentication Factor Input object type, as well as a specific use of COV reporting.

In COV reporting as defined by BACnet, a notification is sent out on subscription or on re-subscription without a change of the **Present_Value**. On the other hand, COV notifications are sent on change of a value. If the value is updated by the same value, no COV notification is issued to the subscribers. This is insufficient for authentication factor input, since the same credential may subsequently be used to request access.

The required behavior is as follows:

- The subscriber needs to distinguish whether it received a COV notification due to an update of **Present_Value**, or (re-)subscription.
- The subscriber needs to receive a COV notification whenever **Present_Value** is updated, regardless whether the new value is different from the last value.
- The subscriber needs to be able to distinguish between valid readings and false readings reported.

To achieve this behavior, an additional property is introduced, which is a **BACnetTimeStamp**, indicating the last update of **Present_Value**. This property is considered as the criterion to generate COV notifications, and will always have a change when **Present_Value** is updated. The value of this property is conveyed in the COV notification, aside **Present_Value**. It allows a client to verify if it got an update of **Present_Value**, or the COV notification was sent due to (re-)subscription.

The required property **Update_Time**, of type `BACnetTimeStamp`, holds the time stamp of the last update of **Present_Value**. This property serves as the criterion to generate COV notifications, and is conveyed in COV notifications from this object. To overcome COV startup issues, this property changes its value on each update of the **Present_Value** property.

The client's behavior can be sketched as follows:

(Re-)Subscription:

1: Read and cache **Update_Time** from the object in question.
2: Subscribe for COV notifications from the object
Operation:

3: Receive COV notifications. If the COV notification conveys the same last update time stamp as read from the object or cached from last notification, a COV notification caused by the subscription was received.
4: If the COV notification conveys another last update time stamp, the COV notification was caused by a real update of Present Value. Act on it and cache the last update time stamp.
5: Continue at step 3

The current read status, associated with the current value in the Present Value, supports a client role process to interpret the value provided in Present Value. The read status is defined as **BACnetAuthenticationFactorReadStatus**, which is an enumeration defined as follows:

- **NOT_INITIALIZED**: The Present_Value does not yet contain a valid or erroneous reading. It has a value of option UNDEFINED, with a NULL value or zero length string of any type.
- **VALID**: The Present_Value contains a valid authentication factor.
- **ERROR**: The Present_Value contains an erroneous reading. It has a value of option UNDEFINED. The value may contain the erroneous raw authentication factor.

The required property **Read_Status**, of type **BACnetAuthenticationFactorReadStatus**, indicates the status of the value of the Present_Value property. This property is conveyed in COV notifications of this object.

### 8.1.3.6 Simulation and Out of Service

The Authentication Factor Input object supports Out-Of-Service for simulation purposes. In Out-Of-Service, the Credential Reader Process does not feed authentication factor readings. Writing authentication factors to Present_Value allows simulating reactions of the PACS on simulated authentication factor readings.

The required property **Out_Of_Service**, of type **BOOLEAN**, is an indication whether (TRUE) or not (FALSE) the Present_Value is prevented from being modified by the Credential Reader Process local to the BACnet device in which the object resides. When Out_Of_Service is TRUE, the Present_Value property may be written to.

### 8.2 Credential Content Access

The Credential Reader Interface may make Credential content accessible. This is data other than Authentication Factors which are available on an Access Credential. Although this is out of scope of PACS, the Credential Reader Interface allows modeling such content and making it accessible to any process through BACnet. The use of smart cards as one of the examples below does not exclude any other type of sophisticated credential which may hold other data as Authentication Factors.

Some design ideas using existing and upcoming BACnet object types are:

- Use File Objects to model smart card blocks
- Use Octet String Value objects to model smart card blocks
- Use BOOLEAN Value objects to model flags present in a smart card
- Use Value objects to model credits
- Etc.

### 8.3 Credential Reader Front Plate Elements Access

A Credential Reader process may expose front plate elements at the Credential Reader Interface. For modeling such elements, BACnet provides a rich set of object types. There are various sets of elements present, and every vendor has some unique features. A certain model is therefore always related to a specific product. The following are just examples of possible model elements.
There are some new object types in discussion within the SSPC-135, to make any value of primitive data type available as an object. This includes Character String Value, Integer Value, Bit String Value etc.

- LED Indicators may be made controllable from external processes through Binary Output objects.
- LCD display lines may be made visible through Character String Value objects*.
- Graphical Display control may be made accessible through a collection of objects.
- Raw magnetic stripe reader head data may be made visible through specific Authentication Factor Input objects.
- Etc.

The following table gives some example modeling possibilities:

<table>
<thead>
<tr>
<th>Element</th>
<th>Data Type</th>
<th>May be modeled as</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED indicators</td>
<td>Binary value</td>
<td>• Binary Output object</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Binary Value object</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multistate Value object if different ON modes, such as blinking in various frequencies or multiple colors.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Property of a proprietary object</td>
</tr>
<tr>
<td>Text Display Line</td>
<td>Character String</td>
<td>• Character String Value object*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Property of a proprietary object</td>
</tr>
<tr>
<td>Graphical Display &amp; Graphical Display Elements</td>
<td>&lt;any&gt;</td>
<td>• Character String Value objects*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Binary Value Objects for binary indicators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unsigned Value objects* for icons</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Proprietary objects and properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Etc.</td>
</tr>
<tr>
<td>Raw Magnetic Stripe data</td>
<td>Authentication Factor Input</td>
<td>• Authentication Factor Input object using UNDEFINED option</td>
</tr>
<tr>
<td>Raw Key Input</td>
<td>Unsigned Character String</td>
<td>• Authentication Factor Input object using a vendor specific option</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Character String Value object*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Property of a proprietary object</td>
</tr>
<tr>
<td>Etc.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* There are some new object types in discussion within the SSPC-135, to make any value of primitive data type available as an object. This includes Character String Value, Integer Value, Bit String Value, etc. The Character String Value object is not yet a standard object type.

8.4 Credential Reader States

Credential Reader states may be provided at the Credential Reader Interface in several ways. Base for this are either BACnet objects used for other purposes, or objects specifically instantiated to indicate status.

- Binary Output objects for LED indicators could indicate fault of LED indicator
- Binary Input object may represent tamper contacts, and going into alarm if activated
- Tamper contacts may be made visible and issuing tamper alarms through Binary Input or Life Safety Point objects.
- Etc.

The following table gives some overview over modeling possibilities:

<table>
<thead>
<tr>
<th>Element</th>
<th>Data Type</th>
<th>May be modeled as</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED indicators</td>
<td>Binary value</td>
<td>• Binary Output object</td>
</tr>
<tr>
<td>Text Display Line</td>
<td>Character String</td>
<td>• Character String Value object*</td>
</tr>
<tr>
<td>Graphical Display</td>
<td>&lt;any&gt;</td>
<td>• Character String Value objects*</td>
</tr>
<tr>
<td>Raw Magnetic Stripe data</td>
<td>Authentication Factor Input</td>
<td>• Authentication Factor Input object using UNDEFINED option</td>
</tr>
<tr>
<td>Raw Key Input</td>
<td>Unsigned Character String</td>
<td>• Character String Value object*</td>
</tr>
<tr>
<td>Etc.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Element | Data Type | May be modeled as
--- | --- | ---
LED Fault | Reliability | • Reliability of Binary Output object  
• Reliability of Binary Value object  
• Any Reliability property of a proprietary object
Tamper contact fault | Reliability | • Reliability of Binary Input object  
• Reliability of Binary Value object  
• Any Reliability property of a proprietary object
Tamper Contact | BACnetLifeSafetyState | • Life Safety Point object
Tamper Contact | Binary Value | • Binary Input object

### 8.5 Example Credential Reader Models

Some sample models of credential readers are outlined. Such models are realized by the Credential Reader Process and exposed at the Credential Reader Interface.

In the object examples, the core values are mentioned only. The full-fledged objects will be according the object definitions as given by the BACnet standard [STD] or Addendum [ADJ]. For properties and values, as well as value notation, refer to the BACnet standard [STD], clause 12 and annex D.

#### 8.5.1 Simple Reader

This example simple credential reader has the following features:

- 26 Bit Wiegand Authentication Factor from magnetic stripe or contact-less (proxy).
- Red and green bicolor LED. Red is always on, but switched to green when access is granted.

This type of reader may be modeled as outlined in the following subsections.

##### 8.5.1.1 Authentication Factor

The sample property values shown (in bold) reflect the situation after reading a Wiegand card.

<table>
<thead>
<tr>
<th>Authentication Factor Input, Instance 1</th>
<th>Object_Name</th>
<th>Allows to identify the object by name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“Door5/AuthenticationFactor”</td>
<td></td>
</tr>
<tr>
<td>Present_Value</td>
<td>Provides the Wiegand value as a BACnetAuthenticationFactor value according the definition for structured Wiegand-26 factors. No Format Class defined:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(0, (137, 27762))</td>
<td></td>
</tr>
<tr>
<td>Format_Identifier</td>
<td>3 (i.e. Facility and Card Number)</td>
<td></td>
</tr>
</tbody>
</table>

##### 8.5.1.2 LED switching to green

The sample property values shown (in bold) reflect the situation when the LED is switched to green.

<table>
<thead>
<tr>
<th>Binary Value, Instance 1</th>
<th>Object_Name</th>
<th>Allows to identify the object by name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“Door5/ReaderSignal”</td>
<td></td>
</tr>
<tr>
<td>Present_Value</td>
<td>Indicates whether the LED is switched to green (ACTIVE) or not:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACTIVE</td>
<td></td>
</tr>
</tbody>
</table>
8.5.2 Multi-Factor Reader

This example multi-factor reader has the following features:

- PIV Card and PIN Authentication Factors
- A red and a green LED as indicators
- A buzzer
- A tamper switch, which may initiate reader tamper alarm.

This type of reader may be modeled as outlined in the following subsections.

8.5.2.1 Authentication Factors

The sample property values shown (in bold) reflect the situation after reading a PIV card.

<table>
<thead>
<tr>
<th>Authentication Factor Input, Instance 5</th>
<th>Object_Name</th>
<th>Allows to identify the object by name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>“NIST-Gate-3-Left-Reader-PIV-FASC-N”</td>
</tr>
<tr>
<td>Present_Value</td>
<td></td>
<td>Provides the FASC-N value as a BACnetAuthenticationFactor value. No Format-Class defined:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(0, (1234, 5678, 101066))</td>
</tr>
<tr>
<td>Format_Identifier</td>
<td>4 (i.e. FASC-N number)</td>
<td></td>
</tr>
</tbody>
</table>

The sample property values shown (in bold) reflect the situation after reading a PIN.

<table>
<thead>
<tr>
<th>Authentication Factor Input, Instance 6</th>
<th>Object_Name</th>
<th>Allows to identify the object by name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>“NIST-Gate-3-Left-Reader-PIN”</td>
</tr>
<tr>
<td>Present_Value</td>
<td></td>
<td>Provides the PIN value as a BACnetAuthenticationFactor value. Format Class is 100:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(100, (“123456”))</td>
</tr>
<tr>
<td>Format_Identifier</td>
<td>2 (i.e. PIN)</td>
<td></td>
</tr>
</tbody>
</table>

8.5.2.2 LEDs

The sample property values shown (in bold) reflect the situation when the red LED is switched on.

<table>
<thead>
<tr>
<th>Binary Output, Instance 1</th>
<th>Object_Name</th>
<th>Allows to identify the object by name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>“NIST-Gate-3-Left-Reader-LED-Red”</td>
</tr>
<tr>
<td>Present_Value</td>
<td>Indicates whether the red LED is switched on (ACTIVE) or not (INACTIVE):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACTIVE</td>
<td></td>
</tr>
</tbody>
</table>
The sample property values shown (in bold) reflect the situation when the green LED is switched off.

<table>
<thead>
<tr>
<th>Binary Output, Instance 2</th>
<th>Object_Name</th>
<th>Allows to identify the object by name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“NIST-Gate-3-Left-Reader-LED-Green”</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Present_Value</th>
<th>Indicates whether the green LED is switched on (ACTIVE) or not (INACTIVE):</th>
</tr>
</thead>
<tbody>
<tr>
<td>INACTIVE</td>
<td></td>
</tr>
</tbody>
</table>

8.5.2.3 Buzzer
The sample property values shown (in bold) reflect the situation when the buzzer is off.

<table>
<thead>
<tr>
<th>Binary Output, Instance 3</th>
<th>Object_Name</th>
<th>Allows to identify the object by name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“NIST-Gate-3-Left-Reader-Buzzer”</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Present_Value</th>
<th>Indicates whether the buzzer is switched on (ACTIVE) or not (INACTIVE):</th>
</tr>
</thead>
<tbody>
<tr>
<td>INACTIVE</td>
<td></td>
</tr>
</tbody>
</table>

8.5.2.4 Tamper Switch
The sample property values shown (in bold) reflect the situation when the tamper is off, not indicating tamper. The object notifies an alarm if Present_Value goes to active. Other properties required for intrinsic reporting are not shown.

<table>
<thead>
<tr>
<th>Binary Input, Instance 1</th>
<th>Object_Name</th>
<th>Allows to identify the object by name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“NIST-Gate-3-Left-Reader-Tamper”</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Present_Value</th>
<th>Indicates whether the tamper switch is active or not:</th>
</tr>
</thead>
<tbody>
<tr>
<td>INACTIVE</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event_State</th>
<th>Indicates the current event state of the tamper switch:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORMAL</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm_Value</th>
<th>Indicates what Present_Value is interpreted as OFF-NORMAL, causing an OFF-NORMAL (i.e. tamper alarm) event state taken:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTIVE</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event_Enable</th>
<th>Indicates which event state transitions are notified. Here, the transitions TO-OFFNORMAL and TO-NORMAL are notified:</th>
</tr>
</thead>
<tbody>
<tr>
<td>{TRUE,FALSE,TRUE}</td>
<td></td>
</tr>
</tbody>
</table>
8.5.3 Smart Card Reader supporting two way communication

This example is not completely worked out. Only the additional features are shown as a sample model. The basic reader functionality may be as outlined above for the multi-factor reader. Of course, the smart card is required to be in the reader to communicate information from and to the smart card.

Additional features supported by the reader device are:

- Reader firmware download
- Accessing smart card content
- Sophisticated indicators and display
- PKI
- Hash code support

These features may be modeled as outlined in the following subsections.

8.5.3.1 Reader Firmware Download

The Credential Reader Process enables the download of firmware into the reader device by exposing a File Object at the Credential Reader Interface. New firmware is downloaded into the reader by writing the firmware code into the File Object, using the Atomic-Write-File service. Upload of firmware may be supported by using Atomic-Read-File service.

The sample property values shown reflect the situation after firmware has been downloaded, or reflects the actual firmware present in the reader device.

<table>
<thead>
<tr>
<th>File, Instance 1</th>
<th>Object_Name</th>
<th>Allows to identify the object by name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“NIST-Gate-3-Left-Reader-Firmware”</td>
<td></td>
</tr>
<tr>
<td>File_Type</td>
<td>Indicates what type of file this object represents:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“Firmware”</td>
<td></td>
</tr>
<tr>
<td>File_Size</td>
<td>Indicates the size of the file / firmware in octets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>148765</td>
<td></td>
</tr>
<tr>
<td>Modification_Date</td>
<td>Indicates when file content has last been modified (i.e. downloaded):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(5-APR-2006, 08:30:49.0)</td>
<td></td>
</tr>
<tr>
<td>File_Access_Method</td>
<td>Indicates what file access method is possible on this file:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STREAM_ACCESS</td>
<td></td>
</tr>
</tbody>
</table>
### 8.5.3.2 Smart Card Content Access

The model outlined assumes the smart card content is organized as blocks of memory, or files. Each block can be modeled as a File Object. Only one example File Object is shown.

Using the File Object allows both reading and writing to the block. The exact content of the block is not specifically modeled, although descriptive properties of the object may indicate what is contained in the block.

Note that communicating with the card itself is a local matter of the Credential Reader Process, and not exposed at the Credential Reader Interface. The File Object creates some façade to hide this from the client role process.

The sample property values reflect a PKI Certificate residing in block 5 of the smart card.

<table>
<thead>
<tr>
<th>File, Instance 105</th>
<th>Object Name</th>
<th>Allows to identify the object by name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“NIST-Gate-3-Left-Reader-Smartcard-Block-5”</td>
<td></td>
</tr>
<tr>
<td>File_Type</td>
<td>Indicates what type of file this object represents:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“PKI Certificate”</td>
<td></td>
</tr>
<tr>
<td>File_Size</td>
<td>Indicates the size of the file in octets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5567</td>
<td></td>
</tr>
<tr>
<td>Modification_Date</td>
<td>Indicates when file content has last been modified (i.e. downloaded):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(5-APR-2006, 08:30:49.0)</td>
<td></td>
</tr>
<tr>
<td>File_Access_Method</td>
<td>Indicates what file access method is possible on this file:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STREAM_ACCESS</td>
<td></td>
</tr>
</tbody>
</table>

### 8.5.3.3 Sophisticated Indicators and Display

Simple indicator model examples have been given in other model examples above.

Modeling hints for more sophisticated indicators and displays are given in section Credential Reader Front Plate Elements Access section above.

For readability of the document, detailed object examples are not outlined here.

### 8.5.3.4 PKI

The use of Public Key Infrastructure (PKI) for authentication factor validation is expected to be performed by the Credential Reader Process while preprocessing and validating authentication factors.

PKI information such as certificates and keys can be made accessible at the Credential Reader Interface using File Objects etc. See the example object given for Smart Card Content Access above.

### 8.5.3.5 Hash Code Support

The verification of hash codes and the application of hashing algorithms for authentication factor validation is expected to be performed by the Credential Reader Process while preprocessing and validating Authentication Factors.

Hash codes may be made accessible at the Credential Reader Interface by using various BACnet objects. They may be used for any purpose, but such codes are typically not relevant with Authentication Factors used by client role processes using the Credential Reader Interface.
9. **Access Door Interface**

The Access Door Interface is provided by the Access Door Process, which is in charge to coordinate and control the individual and specific pieces of a door.

For control, the process knows about how to unlock the door or how to lock it. For events, the door contact can determine whether the door is open or closed but it can’t determine whether the door has been forced open or whether the door has been open too long. Likewise, the door lock can determine if it is unlocked but it can’t know whether it is unlocked due to a valid card swipe or due to a schedule turning on. While the action is the same, the reporting of the event will be different.

The Access Door Interface provides to client processes a uniform way to control and monitor doors, and may provide detailed information about the physical components of doors. The data model and services provided by this interface are BACnet based.

The Access Door Interface includes:

- An abstract door model suitable for any type of door, as a uniform interface for processes to control and monitor a door. From the PACS perspective, the Authentication & Authorization process is the primary user of this model to control and monitor a door.
- A door equipment elements model, to provide access to single elements comprised in a door, such as locks, deadbolts, contacts, motion detectors, etc.

![Figure 9–1, The Access Door Interface as a collection of standard BACnet objects](image)

### 9.1 Abstract Door Model

The abstract door model represents any type of door in a uniform way. This enables client processes to control and monitor any door in a generic way. The abstract door model allows both commanding and parameterizing a door for control; and retrieving status information for monitoring.
• Commanding: Allows a door to lock, to unlock, to temporarily unlock, or to temporarily unlock with extended time for disabled people’s access.
• Parameterizing: Setting various timeouts, and event reporting parameters
• Monitoring: Provides status of the door leaf, the lock, and an overall secured status of the door, reports events of the door on an abstract level.

Additionally, it may indicate what specific physical door hardware elements belong to the door.

The abstract door model is realized by the Access Door object type.

### 9.1.1 Access Door Object Type

A BACnet object of type Access Door represents the combined physical characteristics of a physical access-controlled door in an abstract way.

It has a relationship to all the physical door hardware and devices that are commonly associated with a door such as a door contact, door lock, Request-To-Exit, etc. Standard BACnet objects may be used to represent the individual components of the physical door hardware, and these objects themselves may be exposed to the outside world. Alternatively, a vendor may wish to not expose, for example, which binary output controls the lock. In fact, the vendor may wish to hide that binary output object completely from the outside world. The Access Door object allows the vendor to do this by having a central point of control for the physical door hardware, and not exposing the relationship to the hardware elements.

<table>
<thead>
<tr>
<th>Access Door</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification:</strong> Name, ID, Type, Description, Profile</td>
</tr>
<tr>
<td><strong>Commanding:</strong> Lock, Unlock, Pulsed Unlock, Extended Pulsed Unlock</td>
</tr>
<tr>
<td><strong>Locking Parameters:</strong> Delays, Durations</td>
</tr>
<tr>
<td><strong>General Health:</strong> Event Status and Event Flags</td>
</tr>
<tr>
<td><strong>Alarms:</strong> Intrinsic Alarming and Alarm Masking</td>
</tr>
<tr>
<td><strong>Detail Status:</strong> Lock, Door, Secured</td>
</tr>
<tr>
<td><strong>Maintenance:</strong> Maintenance Status</td>
</tr>
<tr>
<td><strong>Door Equipment:</strong> Refers to Lock, Contact, etc.</td>
</tr>
</tbody>
</table>

*Figure 9–2, Access Door Object Type*

### 9.1.1.1 Commanding

As an Access Door object could be controlled from multiple sources, such as from the Authentication & Authorization Process when a person uses a valid credential, a schedule to allow free access during the day, a schedule to lock-down the door after hours, the manual operator or through other algorithmic control, the Access Door object is required to have a priority array. The priority array is used to arbitrate conflicting commands coming from different sources.
Figure 9–3, Example Access Door Priority Array

In this example, competing commanding entities have been assigned available priorities based on the specific application. Note that priority assignment is site dependent and therefore is not specified in the BACnet standard.
Because this object represents a physical door it has a Present Value that allows locking or unlocking the door, which is the basic control function in physical access control. In addition to commanding the door to unlock or lock for an indefinite period of time, this object has the ability to “pulse unlock” the door for a specified period of time.

The following commands are known, and defined in the new enumeration \textit{BACnetDoorValue}. Proprietary extensions are not foreseen.

- **LOCK**: The door is commanded to the locked state.
- **UNLOCK**: The door is commanded to the unlocked state.
- **PULSE_UNLOCK**: The door will be commanded to the unlocked state for a maximum of Door\_Pulse\_Time time, after which the value will be automatically relinquished from the priority array at the commanded priority. It is permissible for the Access Door Process to relinquish the value from the priority array before the Door\_Pulse\_Time has expired. The conditions when this may occur are considered a local matter.
  
  If a value of PULSE-UNLOCK is written at a given priority and the Present\_Value is currently being commanded, at any value, at a higher priority then the lower priority value will be relinquished immediately.

- **EXTENDED_PULSE_UNLOCK**: The door will be commanded to the unlocked state for a maximum of Door\_Extended\_Pulse\_Time time, after which the value will be automatically relinquished from the priority array at the commanded priority. It is permissible for the Access Door Process to relinquish the value from the priority array before the Door\_Extended\_Pulse\_Time has expired. The conditions when this may occur are considered a local matter.
  
  If a value of EXTENDED-PULSE-UNLOCK is written at a given priority and the Present\_Value is currently being commanded, at any value, at a higher priority then the lower priority value will be relinquished immediately.

The PULSE_UNLOCK is essentially a temporal version of the UNLOCK value, as it will be automatically relinquished, at the commanded priority, after the pulse unlock time has expired. The PULSE_UNLOCK (and EXTENDED_PULSE_UNLOCK) values are typically used by the Authentication & Authorization Process when a valid credential is presented to gain access to the door for a limited period of time.

The PULSE_UNLOCK (and EXTENDED_PULSE_UNLOCK) self-relinquishing behavior, although unusual, is necessary because there exist situations where the commanding process cannot relinquish an UNLOCK command. For example, the pulse time for certain applications may be too short or too precise for accurate control from a remote device. Also, the Access Door may be commanded at the same priority by more than one process. When this is the case, the commanding process cannot know whether another process has subsequently commanded the door to unlock. Finally, some situations require that the door relocks immediately after the door has been opened rather than relock when the pulse time expires. An object commanding the door may not have this information.

The commanding is done through writing the property \textit{Present\_Value}, which is of type \textit{BACnetDoorValue}. Command prioritization requires having the properties \textit{Relinquish\_Default} of type \textit{BACnetDoorValue} and \textit{Priority\_Array} of type \textit{BACnetPriorityArray}. Their use is according the BACnet standard [STD] clause 19.2.

Note that the Present\_Value represents the commanded state of the door, which does not necessarily correspond to the physical state of the door or door lock.
The Present Value of the Access Door object is defined for a standard access controlled door, where the control operation is to lock or unlock. However, this does not exclude motorized devices such as sliding doors, parking gates, etc where the operation is to open or close. In these cases, LOCK shall be equivalent to closing the door and UNLOCK shall be equivalent to opening the door.

9.1.1.2 Locking Parameters

The Access Door object contains parameters used for locking and unlocking.

The maximum duration of time for how long a door is unlocked for a PULSE_UNLOCK command. This duration is exposed by the optional property Door_Pulse_Time, of type Unsigned, which holds the number of tenths of seconds.

The maximum duration of time for how long a door is unlocked for an EXTENDED_PULSE_UNLOCK command. This duration is exposed by the optional property Door_Extended_Pulse_Time, of type Unsigned, which holds the number of tenths of seconds.

The duration of time the physical door lock will delay unlocking when the Present_Value changes to a value of PULSE_UNLOCK or EXTENDED_PULSE_UNLOCK. This duration is exposed by the optional property Door_Unlock_Delay_Time, of type Unsigned, which holds the number of tenths of seconds to delay unlocking.

9.1.1.3 General Health

The property Status_Flags, of type BACnetStatusFlags, represents four Boolean flags that indicate the general "health" of the physical door. Three of the flags are associated with the values of other properties of this object. A more detailed status could be determined by reading the properties that are linked to these flags. The relationship between individual flags is not defined by the protocol. The four flags are:

- The IN_ALARM flag is logically FALSE (0) if the Event_State property has a value of NORMAL, otherwise logical TRUE (1).
- The FAULT flag is logically TRUE (1) if the Reliability property does not have a value of NOFAULTDETECTED, otherwise logical FALSE (0).
- The OVERRIDDEN flag is logically TRUE (1) if the object has been overridden by some mechanism local to the BACnet Device. In this context “overridden” is taken to mean that the physical door is no longer tracking changes to the Present_Value property and the Reliability property is no longer a reflection of the reliability of the physical inputs(s) and output(s). Otherwise, the value is logical FALSE (0).
- The OUT_OF_SERVICE flag is logically TRUE (1) if the Out_Of_Service property has a value of TRUE, otherwise logical FALSE (0).

The property Event_State, of type BACnetEventState, indicates the event state associated with the object. The following event states are supported:

<table>
<thead>
<tr>
<th>Event State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORMAL</td>
<td>The door has no active alarm or fault state. Door_Alarm_State has a value which is neither in Alarm_Values nor in Fault_Values.</td>
</tr>
<tr>
<td>OFFNORMAL</td>
<td>Door_Alarm_State has a value which is listed in Alarm_Values.</td>
</tr>
<tr>
<td>FAULT</td>
<td>Door_Alarm_State has a value which is listed in Fault_Values or Reliability is not NOFAULTDETECTED.</td>
</tr>
</tbody>
</table>
The property **Reliability**, of type `BACnetReliability`, provides an indication of whether the Present_Value, Door_Alarm_State or the operation of the physical inputs or outputs which comprise this door are "reliable" as far as the BACnet device can determine and, if not, why. This property is writable when Out_Of_Service is TRUE. The Reliability property for this object may have any of the following values:

- **NO_FAULT_DETECTED** The process and the object are reliable.
- **MULTI_STATE_FAULT** Door_Alarm_State has a value which is listed in the Fault_Values property.
- **CONFIGURATION_ERROR** The configuration of the device or object has an error preventing reliable processing.
- **UNRELIABLE_OTHER** An unspecific reason leads to unreliable processing.

The property **Out_Of_Service**, of type `BOOLEAN`, is an indication whether (TRUE) or not (FALSE) the logical door which this object represents is not in service. This means that the Present_Value property is decoupled from the physical door and will not track changes to the physical door when the value of Out_Of_Service is TRUE. In addition, the Reliability property and the corresponding state of the FAULT flag of the Status_Flags property shall be decoupled from the physical door when Out_Of_Service is TRUE. While the Out_Of_Service property is TRUE, the Present_Value and Reliability properties, and if present, the Door_Status, Lock_Status and Door_Alarm_State properties, may be changed to any value as a means of simulating specific fixed conditions or for testing purposes. Other functions that depend on the state of the Present_Value or Reliability properties, and if present the Door_Status, Lock_Status and Door_Alarm_State properties, shall respond to changes made to these properties while Out_Of_Service is TRUE, as if those changes had occurred to the physical door.

### 9.1.1.4 Intrinsic Alarming

The Access Door object uses the CHANGE_OF_STATE alarm algorithm and standard BACnet alarming properties for intrinsic event reporting. The Access Door provides overall alarming on an abstract level. Specific door equipment may provide specific alarming if such equipment is exposed by specific BACnet objects.

However, alarm generation for the Access Door object is different than other BACnet objects, as the alarm is not generated by monitoring the Present_Value property but rather a dedicated alarm state property Door_Alarm_State. The sole purpose of this property is to be a trigger for generating alarms. How the value of this property is set is considered a local matter of the Access Door Process.
A new *BACnetDoorAlarmState* enumeration is defined for door specific alarms such as Door-Open-Too-Long, Forced-Open, Tamper conditions, etc.

<table>
<thead>
<tr>
<th>Enumeration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORMAL</td>
<td>The door is in normal condition.</td>
</tr>
<tr>
<td>ALARM</td>
<td>An unspecific alarm has been detected.</td>
</tr>
<tr>
<td>DOOR_OPEN_TOO_LONG</td>
<td>The door was left open for too long time. This condition occurs when the Present_Value has a value of LOCK and one of the following conditions exist:</td>
</tr>
<tr>
<td></td>
<td>• The Present_Value had a previous value of PULSE_UNLOCK and the door has been in a continual open state for Door_Open_Too_Long_Time tenths of seconds after the Door_Pulse_Time has expired.</td>
</tr>
<tr>
<td></td>
<td>• The Present_Value had a previous value of EXTENDED_PULSE_UNLOCK and the door has been in a continual open state for Door_Extended_Open_Too_Long_Time in tenths of seconds after the Door_Extended_Pulse_Time has expired.</td>
</tr>
<tr>
<td></td>
<td>• The Present_Value had a previous value of UNLOCK and the door has been in a continual open state for Door_Open_Too_Long_Time tenths of seconds</td>
</tr>
<tr>
<td>FORCED_OPEN</td>
<td>The door was forced open.</td>
</tr>
<tr>
<td>TAMPER</td>
<td>Any door equipment was tampered with.</td>
</tr>
<tr>
<td>DOOR_FAULT</td>
<td>Any fault was detected.</td>
</tr>
<tr>
<td>LOCK_DOWN</td>
<td>The door is locked down.</td>
</tr>
<tr>
<td>FREE_ACCESS</td>
<td>The door allows free access.</td>
</tr>
<tr>
<td>EGRESS_OPEN</td>
<td>The door was opened due to egress.</td>
</tr>
<tr>
<td><em>&lt;Proprietary Enum Values&gt;</em></td>
<td>A vendor may use other proprietary enumeration values to indicate alarm states other than those defined by the standard.</td>
</tr>
</tbody>
</table>

The optional property *Door_Alarm_State*, of type *BACnetDoorAlarmState*, holds the current alarm state of the Access Door. This property is required to be present when intrinsic reporting is supported by the object. This property, when present, is writable when Out_Of_Service is TRUE.

The optional property *Alarm_Values*, a list of *BACnetDoorAlarmState* values, holds the alarm states which cause a TO_OFFNORMAL transition.

The optional property *Fault_Values*, also a List of *BACnetDoorAlarmState* values, holds the alarm states which cause a TO_FAULT transition.

For the DOOR_OPEN_TOO_LONG state, a delay parameter property may be exposed by the Access Door object. This is the time to delay before setting the Door_Alarm_State to DOOR_OPEN_TOO_LONG after it is determined that a door was open for a too long time.

The delay time is exposed by the property *Door_Open_Too_Long_Time*, of type *Unsigned*, which holds the number of tenths of seconds to delay the DOOR_OPEN_TOO_LONG alarm state.
If intrinsic reporting is supported, the Access Door object has a set of standard properties related to event notification and acknowledgment:

The optional property **Time_Delay**, of type *Unsigned*, either specifies the minimum period of time in seconds that the Door Alarm State must remain equal to any one of the values in the Alarm_Values property before a TO-OFFNORMAL event is generated or remain not equal to any of the values in the Alarm_Values property before a TO-NORMAL event is generated.

The optional property **Notification_Class**, of type *Unsigned*, specifies the notification class to be used when handling and generating event notifications for this object. The Notification_Class property implicitly refers to a Notification Class object that has a Notification_Class property with the same value.

The optional property **Event_Enable**, of type *BACnetEventTransitionBits*, allows specifying which event state transitions are reported.

The optional property **Acked_Transitions**, of type *BACnetEventTransitionBits*, indicates acknowledgement of reported event state transitions.

The optional property **Notify_Type**, of type *BACnetNotifyType*, specifies whether the events are notified as ALARM or EVENT. The notify type is a classification of notifications typically used in client role processes. It has no effect on the server role process behavior.

The optional property **Event_Time_Stamps**, an *Array of BACnetTimeStamp*, holds the time stamp as conveyed in the most recent notifications for the individual event state transitions.

### 9.1.1.5 Alarm Masking

The standard PACS concept of “alarm masking”, which is used to temporarily prevent specific types of alarms from being generated while some external condition exists, is introduced to BACnet in the Access Door object.

When a specific alarm state is masked, the access door object is prevented from taking an alarm state while that state is in the optional property **Masked_Alarm_Values** list. This optional property is a list of *BACnetDoorAlarmState* values.

To understand how alarm masking is typically used in the access control industry, consider the following example:

Many access-controlled doors have a card reader or other authentication device to restrict access when going through the door in one direction but allow free egress when going through the door in the opposite direction. To be able to detect and report a FORCED_OPEN condition, the access control system needs to be able to determine when the door can legitimately be in the OPEN state. When going through the door in the direction where access is checked this determination is obvious since a person must present a valid credential for the door to be unlocked and then be opened. If going through the door in the opposite direction is achieved by manual egress, such as turning the door handle, then the door is not unlocked but yet the door is opened. To distinguish between this situation and a FORCED_OPEN condition a motion detector or other occupancy detector is used to determine that the door was opened from the secure side of the door and therefore was legitimately opened. In this case, the motion detector will prevent (mask) from taking the FORCED_OPEN state, so the Access Door object will not generate this alarm.

The alarm masking functionality also allows specific types of states to be masked based on a recurring basis for specific time intervals without having to modify the original Alarm_Values list. For example, it is common practice in sites to mask DOOR_OPEN_TOO_LONG alarms for certain doors during regular office hours or mask FORCED_OPEN alarms when the associated security zone is disarmed to prevent nuisance alarms.

Functionally, alarm masking could be achieved in the Access Door object without making it externally visible since the determination of when to generate an alarm can be done internally by the local controller. However, it was decided to include this feature because this is a standard mechanism within the physical access control industry.

In addition, the alarm masking concept is required for the standardized definition for the Secured_Status property, which gives an indication of whether the physical door is in a secured state.
9.1.1.6  **Detail Status**

The Access Door object may expose detail status of key elements of a door:

- Door Status
- Lock Status
- Secured Status

There is no intrinsic event reporting of such detailed states foreseen. Event Enrollments using CHANGE_OF_STATE algorithm may be applied for this.

The Door Status indicates the actual state of the door leaf. It is exposed by an optional property *Door_Status*, which holds a value of the new enumeration *BACnetDoorStatus*. This property, when present, is writable when *Out_Of_Service* is TRUE. The enumeration is defined as follows:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLOSED</td>
<td>The door leaf is closed.</td>
</tr>
<tr>
<td>OPENED</td>
<td>The door leaf is opened.</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>The status of the door leaf is unknown.</td>
</tr>
</tbody>
</table>

The Lock Status indicates the monitored (as opposed to the commanded) status of the lock of the door. It is exposed by an optional property *Lock_Status*, which holds a value of the new enumeration *BACnetLockStatus*. This property, when present, is writable when *Out_Of_Service* is TRUE. The enumeration is defined as follows:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCKED</td>
<td>The lock is locked.</td>
</tr>
<tr>
<td>UNLOCKED</td>
<td>The lock is unlocked.</td>
</tr>
<tr>
<td>FAULT</td>
<td>The lock status input associated with the door lock is unreliable.</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>There is no lock status input associated with the door therefore the status of the physical lock is unknown.</td>
</tr>
</tbody>
</table>

The Secured Status indicates the overall secured status of the door. It is exposed by an optional property *Secured_Status*, which holds a value of the new enumeration *BACnetDoorSecuredStatus*. If this property is present then the *Door_Status* property must be present. This enumeration is defined as follows:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURED</td>
<td>This state is taken, and only if all of the following conditions are met:</td>
</tr>
<tr>
<td></td>
<td>• the IN_ALARM flag of the Status_Flags property is FALSE, and</td>
</tr>
<tr>
<td></td>
<td>• the Masked_Alarm_Values list, if it exists, is empty, and</td>
</tr>
<tr>
<td></td>
<td>• the Door_Status property has a value of CLOSED, and</td>
</tr>
<tr>
<td></td>
<td>• the Present_Value property has a value of LOCK, and</td>
</tr>
<tr>
<td></td>
<td>• the Lock_Status property, if it exists, has a value of LOCKED or UNKNOWN.</td>
</tr>
<tr>
<td>UNSECURED</td>
<td>The door is not in a secured state. One or more of the conditions for SECURED are not met.</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>The secured status is unknown.</td>
</tr>
</tbody>
</table>

9.1.1.7  **Maintenance Status**

The Access Door may expose a maintenance status. This indicates whether the door has detected the need for maintenance.

The maintenance status is exposed by the optional property *Maintenance_Required*, which is of type *BACnetMaintenance*. This enumeration and property is already defined, and is reused from the Life Safety Point object.
9.1.1.8 Door Equipment Elements

The Access Door object may expose its relationship to BACnet objects representing specific door equipment such as I/O devices, authentication devices, schedules, programs, or other objects that are associated with the physical door.

The relationship is exposed by the optional property `Door_Members`, of type `List of BACnetDeviceObjectReference` to BACnet objects associated with the door.

It is a local matter as to how this array is used and which objects are referenced in this array. The array may be empty or not present if the vendor does not wish to expose the individual objects that make up this physical door.

9.2 Door Equipment Elements Model

The door equipment details model is used to model single elements comprised in a door, such as locks, deadbolts, contacts, motion detectors, etc.

The concrete model varies among type of the door, sophistication of the door, vendor’s discretion, etc. There is no standardized model for this.

For any element it is expected that the existing set of BACnet object types is sufficient for modeling such elements. Some possible representations are:

<table>
<thead>
<tr>
<th>Element</th>
<th>Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Control</td>
<td>Binary Output</td>
</tr>
<tr>
<td>Lock State</td>
<td>Binary or Multi-State Input</td>
</tr>
<tr>
<td>Door Contact</td>
<td>Binary or Multistate Input</td>
</tr>
<tr>
<td>Motion Detector</td>
<td>Binary or Multistate Input</td>
</tr>
<tr>
<td>REX Button</td>
<td>Binary or Multistate Input</td>
</tr>
<tr>
<td>Drive</td>
<td>Analog Output</td>
</tr>
</tbody>
</table>

An Access Door object may refer to such objects in its `Door_Members` property.
10. Event Reporting and Logging

Event reporting and logging are key features of a PACS. The PACS reports events from the equipment it controls, and what it decides when authenticating and authorizing users for access.

10.1 Event Reporting

The PACS reports various events to clients. Clients may be PACS server devices performing overall logging, workstations or other operator UIs. Possible events are:

- Access transactions and alarms, such as access denied or grant decisions
- Occupancy state of access zones
- Door alarms and faults
- Credential Reader alarms and faults

There are classes of events which may be reported, and maybe handled differently:

- Authentication and authorization alarms requiring operator attention
- Authentication and authorization transactions to be logged
- Occupancy states requiring operator attention or being logged
- Equipment alarms requiring operator attention, such as door alarms or credential reader tampers
- Equipment faults requiring operator attention
- Etc.

PACS event reporting is entirely based on the standard BACnet event reporting, logging and acknowledgement mechanisms. All objects used for modeling a PACS define their own intrinsic event reporting by using standard BACnet event reporting mechanisms. Event Enrollment objects may be supported for more sophisticated event reporting.

With exception of the ACCESS_EVENT algorithm used by the Access Point object for intrinsic reporting, existing BACnet event algorithms are applied. Event reporting may either follow BACnet’s intrinsic event reporting or algorithmic event reporting using Event Enrollment objects. Event subscription by client role processes is done at standard Notification Class objects provided by the interfaces. The setup and configuration of event reporting is done using the respective properties of the event generating objects and Notification Class objects.

10.1.1 New Event Algorithm ACCESS_EVENT

A new event algorithm ACCESS_EVENT is introduced for the stateless event reporting of the Access Point object. Stateless means that the Access Point or Event Enrollment object does not stay in a respective event state until a condition disappears. Events of an Access Point are related to a certain user action and Authentication & Authorization Process decision. They are instantaneous, and after the event the Access Point is again in normal condition. For the sake of consistency, the Event_State property in the Access Point or Event Enrollment object is present and remains in NORMAL Event State.

When different event detection and reporting setups on a single Access Point are needed, the Event Enrollment object is used. The new ACCESS_EVENT algorithm is defined to enable Event Enrollment objects to report access events.

The event algorithm is described from the viewpoint of the Event Enrollment object. But the same algorithm is applied by the Access Point object for intrinsic reporting.
An ACCESS_EVENT event occurs when the value of the referenced property (typically the Last_Access_Event property of the Access Point) changes and becomes equal or is updated to one of the values contained in the List_Of_Access_Events. Since the events are stateless, no Time_Delay is involved in the conditions to determine an event.

The value of the referenced property at the time an ACCESS_EVENT occurs shall be used in carrying out the algorithm until the next ACCESS_EVENT. For the purposes of event notification, ACCESS_EVENT generates TO-NORMAL transitions.

There is no clearing condition defined, since NORMAL event state is never left, and the events are stateless.

![Figure 10–1, ACCESS_EVENT Algorithm](image)

Event Enrollment objects supporting ACCESS_EVENT enrollments use the Access Point’s Last_Access_Event and Update_Time property as the monitored (referenced) value, and need the following event parameters.

<table>
<thead>
<tr>
<th>Event_Type</th>
<th>Event_States</th>
<th>Event_Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS_EVENT</td>
<td>NORMAL</td>
<td>List_Of_Access_Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update_Time_Property_Reference</td>
</tr>
</tbody>
</table>

List_Of_Access_Events contains all Access Event values which, when taken by the monitored value, cause a TO_NORMAL transition, notified by an ACCESS_EVENT event notification. Whenever the referenced Update_Time property changes, the monitored value is evaluated again to determine if an event notification has to be issued.

Event parameters are those event related values stored by the Event Enrollment object itself. For details see also the Event Enrollment object definition in the BACnet standard [STD] clause 12.

Note that there is a single List_Of_Access_Events only. The ACCESS_EVENT algorithm is not intended to differentiate between Access Alarm Events or Access Transaction Events, as the Access Point does with intrinsic reporting. Supporting both levels of Access Events is achieved by setting up distinct Event Enrollment objects. The differentiation between Access Alarm Events and Access Transaction Events is achieved by appropriate setup of the Event Enrollment objects and associated Notification Classes.
The notification parameters conveyed in an ACCESS_EVENT event notification are:

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Notification Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS_EVENT</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access_Event</td>
<td>The new value of the referenced property</td>
</tr>
<tr>
<td></td>
<td>Status_Flags</td>
<td>The Status_Flags of the referenced object</td>
</tr>
<tr>
<td></td>
<td>Update_Time</td>
<td>The time of update of the referenced property, as indicated by the referenced Update_Time property.</td>
</tr>
<tr>
<td></td>
<td>Access_Credential</td>
<td>The Last_Access_Credential of the referenced object</td>
</tr>
<tr>
<td></td>
<td>Authentication_Factor if present</td>
<td>The Last_Authentication_Factor of the referenced object</td>
</tr>
</tbody>
</table>

10.2 Logging

The PACS data model exclusively uses BACnet event reporting mechanisms. All events are notified using either UnconfirmedEventNotification or ConfirmedEventNotification.

Event logging is done in a standard way by using the Event Log object as defined by the BACnet standard addendum b to 135-2004. There are no extensions to this object needed, since it is capable of logging any kind of UnconfirmedEventNotification or ConfirmedEventNotification.

Event Log objects may be instantiated locally in a PACS controller, or remotely in any other device such as a PACS server device.

The Event Log object stores event notifications issued by any BACnet object. The association of Event Log objects to event sources is not exposed by the Event Log object, and is considered a local matter. Remote Event Log objects implicitly require subscribing at the remote Notification Class objects of the remote event source objects of interest, while local Event Log objects may obtain event notifications through some internal mechanism, not exposed in BACnet.

The Event Log object has mechanisms to manage its log buffer, including high-water mark events (BUFFER_READY), ReadRange service support to retrieve logged entries from its log buffer, and commands to clear a log buffer.
11. Functions and Features Inherent in the BACnet Framework

The following are summarized in this section as they are not Access Control specific, but are the framework upon which the PACS extensions are constructed. This framework will be required in whole or in part to implement a PACS, or an interface to a PACS.

11.1 BACnet Data Types

BACnet application service parameters and properties of objects build on the same data type definitions. A set of defined primitive data types are used, or constructions of complex types based on the primitive types. The formal definition of these data types, as well as their encoding using the BACnet encoding scheme, is done using ASN.1.

11.1.1 Primitive Data Types

BACnet defines 13 primitive data types. These are used as data types of properties or application service parameters. They also serve as the base for constructed data types. This set of primitive data types is not extended for new applications such as PACS.

The defined primitive data types are:

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NULL</td>
<td>&quot;No Value&quot;</td>
</tr>
<tr>
<td>BOOLEAN</td>
<td>TRUE or FALSE</td>
</tr>
<tr>
<td>Unsigned</td>
<td>Unsigned number. Basically unlimited in size. Limited size subtypes are:</td>
</tr>
<tr>
<td></td>
<td>Unsigned8: Range 0..255</td>
</tr>
<tr>
<td></td>
<td>Unsigned16: Range 0..65535</td>
</tr>
<tr>
<td></td>
<td>Unsigned32: Range 0..4294967295</td>
</tr>
<tr>
<td>INTEGER</td>
<td>Signed number</td>
</tr>
<tr>
<td>REAL</td>
<td>ANSI/IEEE-754 single precision floating point number</td>
</tr>
<tr>
<td>Double</td>
<td>ANSI/IEEE-754 double precision floating point number</td>
</tr>
<tr>
<td>OCTET STRING</td>
<td>Block of octets. Basically unlimited in size.</td>
</tr>
<tr>
<td>CharacterString</td>
<td>Character Strings. Supported character sets:</td>
</tr>
<tr>
<td></td>
<td>ANSI X3.4 (ASCII)</td>
</tr>
<tr>
<td></td>
<td>IBM™/Microsoft™ DBCS (Double Byte Character Sets)</td>
</tr>
<tr>
<td></td>
<td>JIS C 6226 (Japanese)</td>
</tr>
<tr>
<td></td>
<td>Unicode ISO 10646 (UCS-4 encoding)</td>
</tr>
<tr>
<td></td>
<td>Unicode ISO 10646 (UCS-2 encoding)</td>
</tr>
<tr>
<td></td>
<td>ISO 8859-1 ISO Latin 1</td>
</tr>
<tr>
<td></td>
<td>Unicode ISO 10646 (UTF-8 encoding, with upcoming Addendum h to BACnet 2004</td>
</tr>
<tr>
<td>BIT STRING</td>
<td>String of bits, or bit set. Basically unlimited in number of bits</td>
</tr>
<tr>
<td>ENUMERATED</td>
<td>Value of a defined enumeration.</td>
</tr>
<tr>
<td>Date</td>
<td>Date. Constructed: Year, Month, Day of Month, Day of Week</td>
</tr>
<tr>
<td>Time</td>
<td>Time of day. Constructed: Hour, Minutes, Seconds, Hundredths of Seconds</td>
</tr>
<tr>
<td>BACnetObjectIdentifier</td>
<td>32 Bit BACnet Object Identifier. Constructed:</td>
</tr>
<tr>
<td></td>
<td>10 most significant bits for Object Type</td>
</tr>
<tr>
<td></td>
<td>22 least significant bits for Object Instance of Object Type</td>
</tr>
</tbody>
</table>
11.1.2 Constructed Data Types

SEQUENCE: Structured data types are a sequence of fields of various types. Each field may be of a primitive data type or constructed data type.

CHOICE: Choices may be defined. One of the defined options is used in a property or application service parameter. Each of the available options may again be of primitive data type or constructed data type.

SEQUENCE OF: Sequences of elements of the same BACnet Data Type may appear as properties (arrays or lists), and in application service parameters. Each element may be of primitive data type or constructed data type. Each element must comply with the same data type definition.

ABSTRACT-SYNTAX.&Type: BACnet allows for proprietary data types. Or an undefined set of possible data types may be used as a structure field or choice option. This is then defined as data type ABSTRACT-SYNTAX.&Type. This indicates that any primitive or constructed data type may be used. The construction must be based on BACnet's primitive data types. The encoding must follow the BACnet encoding rules.

11.1.3 Array and List Properties

Properties may be an Array or a List of elements of the same BACnet Data Type.

11.1.3.1 Array Of

These are properties which contain a sequence of size N of elements (SEQUENCE OF) of the same type. There are no restrictions on element values. Multiple elements may have the same value.

Each element is addressable by an index. Index zero provides the number of elements in the array. Index 1 provides the first element. Index N provides the last element.

In the BACnet Standard, such properties are specified as a $\text{BACnetArray}[N]$ of Data Type, where N may be specified by the standard, or left to the application as a local matter.

If the Data Type of the array elements is again an array or list (i.e. SEQUENE OF), then the content of such elements can be accessed as a whole only using read and write application services. In some cases list manipulation services may be used to access individual elements within an element. The required property definition for this would be $\text{BACnetARRAY}[N]$ of List of Data Type. The current BACnet standard is not very explicit on this.

11.1.3.2 List Of

These are properties which contain a sequence of undefined size of elements (SEQUENCE OF) of the same data type. There are no two elements which contain the same value. It could also be seen as a set of values.

Elements are addressed by value. Specific application services (i.e. list manipulation services) are available to add or remove an element of a list, identified by its value. The content of the list may be read by reading the entire list, or may be modified by writing the entire list.

In the BACnet Standard, such properties are specified as a List of Data Type. The maximum size is a local matter, and typically limited by the resources available in a device.

11.2 Protocol Stack

The BACnet protocol stack is used to transfer application services between physical devices. Several networking options are defined, but these are transparent to the processes performing application functionality and communicating with other processes.
11.2.1 BACnet Application Layer

The application layer supports two types of transmission of application services. The application services of BACnet use either one:

- **Confirmed Services** include a request and a response message being transferred. Both the request or response messages may be segmented to convey large amounts of data. Confirmed services are addressed to a single device only (i.e. Unicast).

- **Unconfirmed Services** consist of a request message only. No response is expected. Segmentation is not supported for such messages. Unconfirmed services may be addressed to a single device (i.e. Unicast), to a group of devices (i.e. Multicast), or to all devices of an inter-network (i.e. Global Broadcast).

The BACnet application layer also includes a fixed data encoding definition, which defines how data is encoded for transmission. This encoding is closely related to the BACnet Data Type definitions in ASN.1.

11.2.2 BACnet Network Layer

The Network Layer supports routing of messages through the inter-network, and connection control of temporary PTP based links. The basis for routing is Network Numbers associated to each BACnet network. A BACnet network is built of a single data link type, each having its own MAC address space. The sum of all networks of a system form an inter-network. It provides a uniform interface to the application layer, hiding specifics of data links which are used in a network.
11.2.3 Data Link Layers

BACnet defines some data link layers, and defines the use of standardized data links. Proprietary data link layers may be used, but are required to support features expected by the BACnet Network Layer. Virtual data link layers allow running multiple BACnet devices in a single physical device.

BACnet defined data link layers

- MS/TP: Master-Slave/Token-Passing using EIA-485 physical layer
- PTP: Point-To-Point using EIA-232 or Modem physical layers
- BVLL: Intermediate layer above UDP, to provide data link features expected by the BACnet Network Layer, but not sufficiently supported by UDP and IP.

Used standard data link layers:

- ISO 8802-2 link layer control, using either Ethernet (IEEE 802-3) or ARCnet
- LONTalk by using explicit messages, on any physical layer supported by LONTalk
11.3 Standards
BACnet is an ANSI standard (ANSI/ASHRAE 135-2004) as well as an ISO standard (ISO 16484-5). Further, BACnet normatively references other standards wherever appropriate and useful. Some of the standards referenced by BACnet which are relevant to Access Control are listed below.

Networking:
- Transport protocols such as Ethernet (IEEE 802-3) and IP
- EIA 232 and EIA 485 for serial connections and networks

Data Definition and Encoding
- ASN.1 (ISO 8825) for data definition and encoding specification (Encoding itself is BACnet specific!)

Network Security:
- AES for encryption
- SHA-256 for message authentication

Character Sets:
- ANSI X3T4 (a.k.a. ASCII)
- Unicode character sets and character encodings
- ISO 8859 character sets

11.4 Extensibility
BACnet supports extensions of data models and services for proprietary purposes. See clause 23 of the BACnet standard [STD]. Possible proprietary extensions include:

- Object types
- Properties of objects
- Enumerations
- Services on any protocol layer

Further, BACnet is designed for standard extensions and continuously maintained for extensions and improvements. ASHRAE is the maintenance organization of the standard and ASHRAE’s Standing Standard Project Committee SSPC-135 is the responsible body.

11.5 Scalability
BACnet supports scalability on various levels:

- System size: BACnet allows addressing 4,194,303 single addressable devices in a system, where each device may contain up to 4,194,303 object instances of each BACnet object type.
- Device performance: BACnet can be implemented on small 8 bit platforms up to high performance computers such as 64 bit GHz-range machines.
- Network performance: BACnet supports networking technologies from 2400 baud serial links up to 10 Gigabit Ethernet LAN and beyond.
- Network topology: BACnet allows creating systems with global span. Various networking technologies support local and wide area networks of almost any topology.
11.6 System Security
In BACnet, two levels of system security are contemplated.

- Network Security: A completely revised definition of network security within BACnet is currently in public review at ASHRAE. This includes features such as encryption, data integrity, device authentication and user authentication. These features are based on well known standards such as AES, HMAC, MD5 and SHA-256. For details see Addendum g to the 2004 version of the BACnet standard [STD], as available from ASHRAE web site (www.ashrae.org) or, when approved, at the BACnet web site (www.bacnet.org).
- Logical Access: The Network Security Working Group (NS-WG) within ASHRAE SSPC-135 is creating standard definitions for logical access control for data and services within a BACnet system. At present this functionality is addressed in a vendor proprietary matter.

11.7 IT Systems Connectivity
BACnet is currently in the process of adding a Web Services (SOAP) definition to allow using SOAP to access BACnet based systems. For details see Addendum c to the 2004 version of the BACnet standard [STD], as available from ASHRAE web site (www.ashrae.org) or the BACnet web site (www.bacnet.org). It is expected that the conversion of BACnet accessible data into SOAP accessible data can be achieved in a generic way such that the SOAP implementation is transparent with regard to PACS.

BACnet supports the implementation of generic IT oriented machine or user interfaces, such as OPC servers, Web Pages Servers, REST servers etc. Such interfaces typically are transparent to extensions made to the data model and services.

With the use of IP networks as BACnet data link, BACnet may run over IP based IT infrastructure. Through this, IT departments may manage the BACnet network infrastructure.

11.8 Functionality Deployment
BACnet provides complete freedom of functionality deployment. A device may contain just simple functional elements, or be very sophisticated containing a huge set of functions of various application domains. The physical structure of the system is completely independent of the functional / logical structure of the system.

11.9 Networking Technology Independence
BACnet supports various networking technologies:

- Networking as defined by the BACnet standard: MS/TP (Master-Slave/Token-Passing on EIA-485), PTP (Point-To-Point on EIA-232 or Modem)
- Networking technologies used: Ethernet, ARCnet, LON
- Networking technologies supporting IP
- Proprietary and virtual networking technologies are permitted as a local matter, but transparent to other BACnet devices.

11.10 Device Implementation Technology Independence
BACnet does not prescribe, require or imply hardware and software technologies devices are to be implemented with. A manufacturer has complete freedom to choose CPU families, operating systems, programming languages and environments etc.
## 12. Terms & Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN.1</td>
<td>Abstract Syntax Notation One. ISO standard 8824 defined language for the definition of syntaxes and data types. Mainly used to define protocol data models.</td>
</tr>
<tr>
<td>CBEFF</td>
<td>Common Biometric Exchange File Format. NISTIR 6529. Describes a set of data elements necessary to support biometric technologies in a common way</td>
</tr>
<tr>
<td>CHUID</td>
<td>Card Holder Unique Identifier. Data format used in PIV smart cards.</td>
</tr>
<tr>
<td>COV</td>
<td>Change-Of-Value. A reporting mechanism of BACnet. A subscriber process subscribes for change of value notifications from an object (Object-Level COV), or a property of an object (Property-Level COV).</td>
</tr>
<tr>
<td>ETS</td>
<td>Electronic Ticketing System</td>
</tr>
<tr>
<td>FASC-N</td>
<td>U.S. government Federal Agency Smart Card Number</td>
</tr>
<tr>
<td>FIPS-201</td>
<td>U.S. Federal Information Processing Standard 201 [FIPS-201]</td>
</tr>
<tr>
<td>GUID</td>
<td>Globally Unique Identifier</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hashed Message Authentication Code</td>
</tr>
<tr>
<td>HRMS</td>
<td>Human resources management system</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation &amp; Air Conditioning</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol. Up to now, BACnet supports IPv4, but there are activities to extend it to be capable to run over IPv6.</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control. A sub-layer of the OSI data link layer, managing access to a shared medium.</td>
</tr>
<tr>
<td>NIST</td>
<td>United States Government’s National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OPC</td>
<td>OLE (Object Linking and Embedding) for Process Control. See <a href="http://www.opcfoundation.org">www.opcfoundation.org</a></td>
</tr>
<tr>
<td>OSI</td>
<td>Open System Interconnection. ISO standard 7498 defining a model of seven protocol layers.</td>
</tr>
<tr>
<td>OSIPS</td>
<td>Open Systems Integration And Performance Standards. SIA initiative to develop integration and performance standards for security products.</td>
</tr>
<tr>
<td>PACS</td>
<td>Physical Access Control System</td>
</tr>
<tr>
<td>Passback</td>
<td>This term is used in the Access Control industry for the act of passing back an Access Credential to a further user to allow this user to request access.</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identity Verification. This is the Personal Identity Verification standard as defined by NIST in FIPS-201, in the course of US government initiatives related to HSPD-12, the US Homeland Security Presidential Directive Number 12: Policy for a Common Identification Standard for Federal Employees and Contractors</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure. Authentication and cryptography methods using asymmetric public and private key pairs.</td>
</tr>
<tr>
<td>RBAC</td>
<td>The Role Based Access Control (RBAC) model for access rights and owner structuring is introduced by NIST and used widely by the IT industry. See also ANSI/INCITS 359-2004.</td>
</tr>
<tr>
<td>REQ</td>
<td>See REX</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer. Roy Fielding: &quot;Representational State Transfer is intended to evoke an image of how a well-designed Web application behaves: a network of web pages (a virtual state-machine), where the user progresses through an application by selecting links (state transitions), resulting in the next page (representing the next state of the application) being transferred to the user and rendered for their use.&quot; See various resources on the world-wide web.</td>
</tr>
<tr>
<td>REX</td>
<td>Request-to-Exit button</td>
</tr>
<tr>
<td>SIA</td>
<td>Security Industry Association (<a href="http://www.siaonline.org">www.siaonline.org</a>)</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol. XML based protocol to access information over HTTP transport protocol.</td>
</tr>
<tr>
<td>T/A</td>
<td>Time and Attendance</td>
</tr>
</tbody>
</table>
13. Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 3, 2006</td>
<td>Renamed to BAC-10-06. Minor corrections and updates. Added contributors list on front page. Added this revision history.</td>
</tr>
</tbody>
</table>