DD IEC/TS 62351-8:2011

BSI Standards Publication

Power systems management and associated information exchange — Data and communications security

Part 8: Role-based access control

raising standards worldwide™

National foreword

This Draft for Development is the UK implementation of IEC/TS 62351-8:2011.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 67829 5

ICS 33.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 31 October 2011.

Amendments issued since publication

Amd. No.	Date	Text affected

IEC/TS 62351-8

Edition 1.0 2011-09

TECHNICAL SPECIFICATION

colour inside

Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE X

ICS 33.200

ISBN 978-2-88912-723-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 8: Role-based access control

FOREWORD

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

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-8, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/1119/DTS	57/1153/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all the parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

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

INTRODUCTION

This Technical specification covers access control in power systems. The power system environment supported by this specification is enterprise-wide and extends beyond traditional borders to include external providers, suppliers, and other energy partners. Driving factors are the liberalization of the energy sector, the increasingly decentralized generation of energy, and the need to control access to data of precious resources. This specification supports a distributed security environment in which security is also a distributed service.

The power system sector is continually improving the delivery of energy by leveraging technical advances in computer-based applications. Utility operators, energy brokers and end-users are increasingly accessing multiple applications to deliver, transmit and consume energy in a personalized way. These disparate applications are naturally connected to a common network infrastructure that typically supports protection equipment, substation automation protocols, inter-station protocols, remote access and business-to-business services. Consequently, secure access to these distributed and often loosely coupled applications is even more important than access to an application running on a stand-alone object.

Secure access to computer-based applications involves authentication of the user to the application. After authentication, the level at which a user can use the application is determined. The use of local mechanisms for authorization creates a patchwork of approaches which are difficult to uniformly administer across the breadth of a power system enterprise. Each application decides the authorization on its own logic. If applications can use a network, a database can serve as a trusted source of user's group or role affiliation. Thus, the access to a shared user base can be controlled centrally. Each application can then examine the rights listed for a subject and corresponding role and determine their level of authorization.

The role of a user is transported in a container called an access token of that user to the object. Access tokens are created and administered by a (possibly federated) identity management tool. All access tokens have a lifetime and are subject to expiration. Prior to verification of the access token itself, the user transmitting the access token must be authenticated by the object. The object trusts the management tool to issue access tokens with suitable lifetime. This enables local verification of the access token's validity at remote sites without the need to access a centralized repository (e.g. a centralized revocation list).

Three different access token formats are supported as three different profiles. Two of them are X.509 Access tokens and the third is a software token similar to Kerberos. They can be used over TCP/IP and serial communication links.

This specification defines role-based access control (RBAC) for enterprise-wide use in power systems. It supports a distributed or service-oriented architecture where security is a distributed service and applications are consumers of distributed services.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 8: Role-based access control

1 Scope

This technical specification covers the access control of users and automated agents – in the following subjects – to data objects in power systems by means of role-based access control (RBAC). RBAC is not a new concept used by many operating systems to control access to system resources. RBAC is an alternative to the all-or-nothing super-user model. RBAC is in keeping with the security principle of least privilege, which states that no subject should be given more rights than necessary for performing that subject's job. RBAC enables an organization to separate super-user capabilities and package them into special user accounts termed roles for assignment to specific individuals according to their job needs. This enables a variety of security policies, networking, firewall, back-ups, and system operation. A site that prefers a single strong administrator but wants to let more sophisticated users fix portions of their own system can set up an advanced-user role. RBAC is not confined to users however, it applies equally well to automated computer agents, i.e., software parts operating independent of user interactions. The following interactions are covered by the scope of this technical specification:

– local (direct wired) access to the object by a human user;
– local (direct wired) access to the object by a local and automated computer agent, e.g. another object at the substation;
– direct access by a user to the object using the objects' built-in HMI or panel;
– remote (via dial-up or wireless media) access to the object by a human user;
– remote (via dial-up or wireless media) access to the object by a remote automated computer agent, e.g. another object at another substation, or a control centre application.

As in many aspects of security, RBAC is not just a technology; it is a way of running a business. As subject names change more frequently than role names and as role names change more frequently than the rights of a data model (e.g. IEC 61850), it is advisable to store the frequently changing entities (i.e. the subjects names) outside the object. Less frequently changing role names and rights are stored inside the object.

RBAC thus provides a means of reallocating system controls as defined by the organization policy.

The scope of this specification covers everything that is needed for interoperability between systems from different vendors. The purpose of this specification is therefore:

– firstly, to introduce 'subjects-roles-rights' as authorization concept;
– secondly, to promote role-based access control for the entire pyramid in power system management; and
– thirdly, to enable interoperability in the multi-vendor environment of substation automation and beyond.

Out of scope for this specification are all topics which are not directly related to the definition of roles and access tokens for local and remote access, especially administrative or organizational tasks, such as:

– user names and password definitions/policies;

– management of keys and/or key exchange;
– engineering of roles;
– assignment of roles;
– selection of trusted certificate authorities issuing credentials (access tokens);
– defining the tasks of a security officer;
– integrating local policies in RBAC.

NOTE These issues will be addressed in IEC/TS 62351-9[1].

The IEC 62351 series specifies end-to-end security in power systems so that secure connections are established between applications. RBAC is recognized as a potentially efficient and safe means to control access to data objects.

Existing standards (see [ANSI INCITS 359-2004], [IEC 62443], and [IEEE 802.1X-2004]) in the process control industry and access control ([RFC2904] and [RFC2905]) are not sufficient as none of them specify either the exact role name and associated rights, the format of the access tokens or the detailed mechanism by which access tokens are transferred to and authenticated by the target system – however, all this information is needed though for interoperability.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850 (all parts), *Communication networks and systems in substations*

IEC 61850-7-2, *Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)*

IEC/TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC/TS 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC/TS 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS*

IEC/TS 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

ISO 9594-8/ITU-T Recomendation X.509:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

---

1 Under consideration.

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions of IEC/TS 62351-1 apply, as well as the following.

3.1 Terms and definitions

3.1.1
area of responsibility
range of authority, for instance based on network segregation

3.1.2
automated agent
computer program running on a single machine

NOTE It performs local and/or remote operations independent of user inputs.

3.1.3
access token
evidence or testimonials concerning one's right to credit, confidence, or authority

3.1.4
holder
entity that possesses or owns an access token

3.1.5
issuer
entity that issues an access token

3.1.6
identity provider
entity that creates, maintains and manages identity information; typically used in single sign-on scenarios

3.1.7
object
any system resource subject to access control such as a file, printer, terminal, database record, etc.

3.1.8
operation
executable image of a program which upon invocation executes some function/activity for the subject

3.1.9
privilege
attribute or property assigned to a subject by an authority

3.1.10
privilege management infrastructure
PMI
the infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a public key infrastructure

3.1.11
right
atomic set of accessing privileges assigned to a particular system object

3.1.12
role
job function within the context of an organization with some semantics associated regarding the authority and responsibility conferred on the user assigned to the role

NOTE A role subsumes a set of rights.

Pre-defined role: a role that is defined in this specification.

Default role: a role that is defined by the vendor of the protection equipment (not by its specification) and that is valid generally for all objects of that vendor.

Specific role: a role that is defined by the utility operator for its particular needs.

3.1.13
service
permission in the context of IEC 61850

3.1.14
session
encounter between a user and an application or with the computer in general

NOTE One user session is the time between starting the communication channel (either local or remote) and terminating (either by the user or the system).

3.1.15
static separation of duty
SSD
enforcement constraints on the assignment of users to roles

NOTE Membership in one role may prevent the user from being a member of one or more other roles, depending on the SSD rules enforced.

3.1.16
dynamic separation of duty
DSD
limitation of the availability of rights by placing constraints on the roles that can be activated within or across a user's sessions

NOTE 1 DSD provides the capability to address potential conflict of interest issues at the time a user is assigned to a role.

NOTE 2 DSD allows a user to be authorized for roles that do not cause a conflict of interest when acted in independently, but which produce policy concerns when activated simultaneously. Although this separation of duty could be achieved through the establishment of a static separation of duty relationship, DSD relationships generally provide the enterprise with greater operational flexibility.

3.1.17
out-of-band
communications which occur outside a previously established communication method or channel

3.1.18
service provider
an object that provides services

NOTE It is subject to access control.

3.1.19
subject
user or an automated agent

NOTE A subject is a right holder. It has a name attribute whose value is mandatory. It is this name that is used to enrol a subject in a particular role.

3.1.20
token
physical instance of an access token

3.1.21
user
human being

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

AC	attribute certificate
ACL	access control list
ACRL	attribute certificate revocation list
ACSI	abstract communication system interface
AMI	advanced metering infrastructure
AoR	area of responsibility
CIM	common Information model
CRL	certificate revocation list
DER	distributed energy resource
HMAC	keyed-hash message authentication code
HMI	human machine interface
IED	intelligent electronic device; stands for a field device, a gateway or a PC in the net control centre
ID	identity
IS	international standard
ISA	instrument system and automation society
LDAP	lightweight directory access protocol
LD	logical-device (IEC 61850)
LN	logical node (IEC 61850)
OCSP	online certificate status protocol
OID	object identifier
OSI	open systems interconnection
PKI	public key infrastructure; the complete set of processes required to provide encryption and digital signature services
PMI	privilege management infrastructure; the complete set of processes required to provide an authorization service
RBAC	role-based access control
SCL	substation configuration description language (IEC 61850)
SSL	secure socket layer
SW	software
TCP	transport control protocol
TLS	transport layer security
UID	universal identifier

4 RBAC process model

4.1 General

The purpose of an access control mechanism is to protect system resources, formally called objects. For a system that implements RBAC, system resources can represent information containers (e.g. files, directories in an operating system and/or columns, rows, tables, and views within a database management system) or exhaustible device resources, such as printers, disk space and CPU cycles.

Role-based access control (RBAC) is a technology that has the potential to reduce the complexity and cost of security administration in networks with large numbers of intelligent devices. Under RBAC, security administration is simplified through the use of roles and constraints to organize subject access levels. RBAC reduces costs within an organization primarily because it accepts that employees change roles and responsibilities more frequently than the rights within roles and responsibilities have to be changed.

Figure 1 is a generic picture for access control. It consists of a subject, an identity provider and an object.

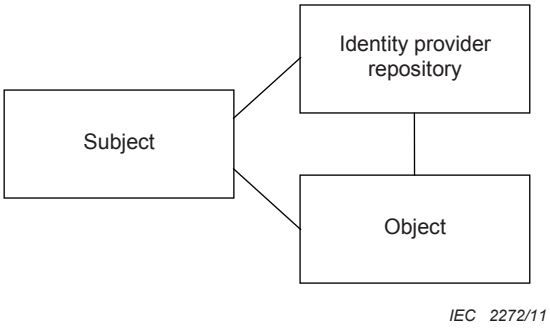


Figure 1 – Generic framework for access control

The subject wants to access the resources of the object by means of an access token provided by the identity provider. There are generally two ways to do this:

– the access token can be fetched by the object from the repository of the identity provider when the subject connects to the object: This case is called “PULL”;
– alternatively, the subject can first fetch the access token from the repository of the identity provider prior to accessing the object: This case is called “PUSH”.

The access token contains the role of the subject. Role-based access control is part of a general authentication, authorisation and accounting infrastructure for access control to data.

The subject provides information about its identity to the repository of the identity provider in order to get authenticated along with a request for an access token to the object (PUSH) or the object can get the required information (access token) from a repository (PULL).

In general, the subject has rights assigned via roles that are pushed to or pulled by the object. In deciding whether to employ a push or pull model, several factors should be considered:

For the PUSH model:

– the access token holding the authorisation information must be sufficiently secure;

– the access token should have a short time to live to prevent replay attacks;
– the access token must be validated;
– the token exchange should be cryptographically protected.

For the PULL model:

– the authentication service at the repository must be accessible;
– a trusted communication path to the authentication service is required;
– there is no computational overhead associated with verification of the token (but there will be a time delay for communications);
– the pulled authentication information is always current.

4.2 Separation of subjects, roles, and rights

4.2.1 General

A model for RBAC including separation of duty (static as well as dynamic) is given in Figure 2.

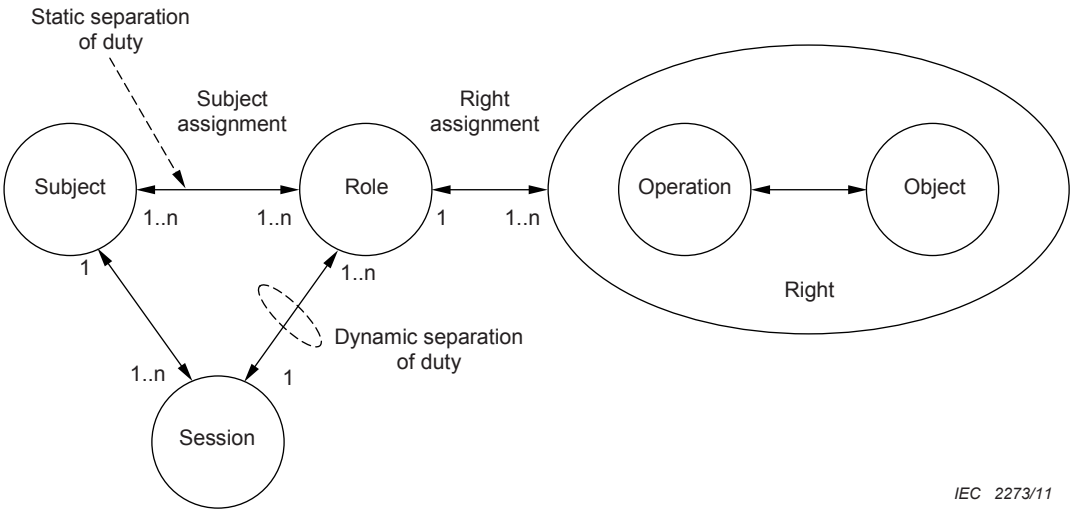


Figure 2 – Diagram of RBAC with static and dynamic separation of duty according to (ANSI INCITS 359-2004)

The arrows in Figure 2 indicate relationships (e.g., a subject can be assigned to one or more roles, and a role can be assigned to one or more subjects). This arrangement provides great flexibility and granularity in assigning rights to roles and subjects to roles. Without these conveniences, there is a danger that a subject may be granted more access to resources than is needed because of limited control over the type of access that can be associated with subjects and resources. Any increase in the flexibility of controlling access to resources also strengthens the application of the principle of least right.

Each session is a mapping of one subject to possibly many roles, i.e., a subject establishes a session during which the subject activates one or a subset out of a set of roles that it is assigned to. Each session is associated with a single subject and each subject is associated with one or more roles.

The main components of RBAC are thus: subject, role, right for operations and objects, and session.

There are two mappings between these components that need be configured by the administrator:

– subject-to-role mapping termed subject assignment; and
– role-to-right mapping termed role assignment.

Figure 3 gives a survey of subjects, roles, rights, and operations in the scope of the IEC 61850 standard.

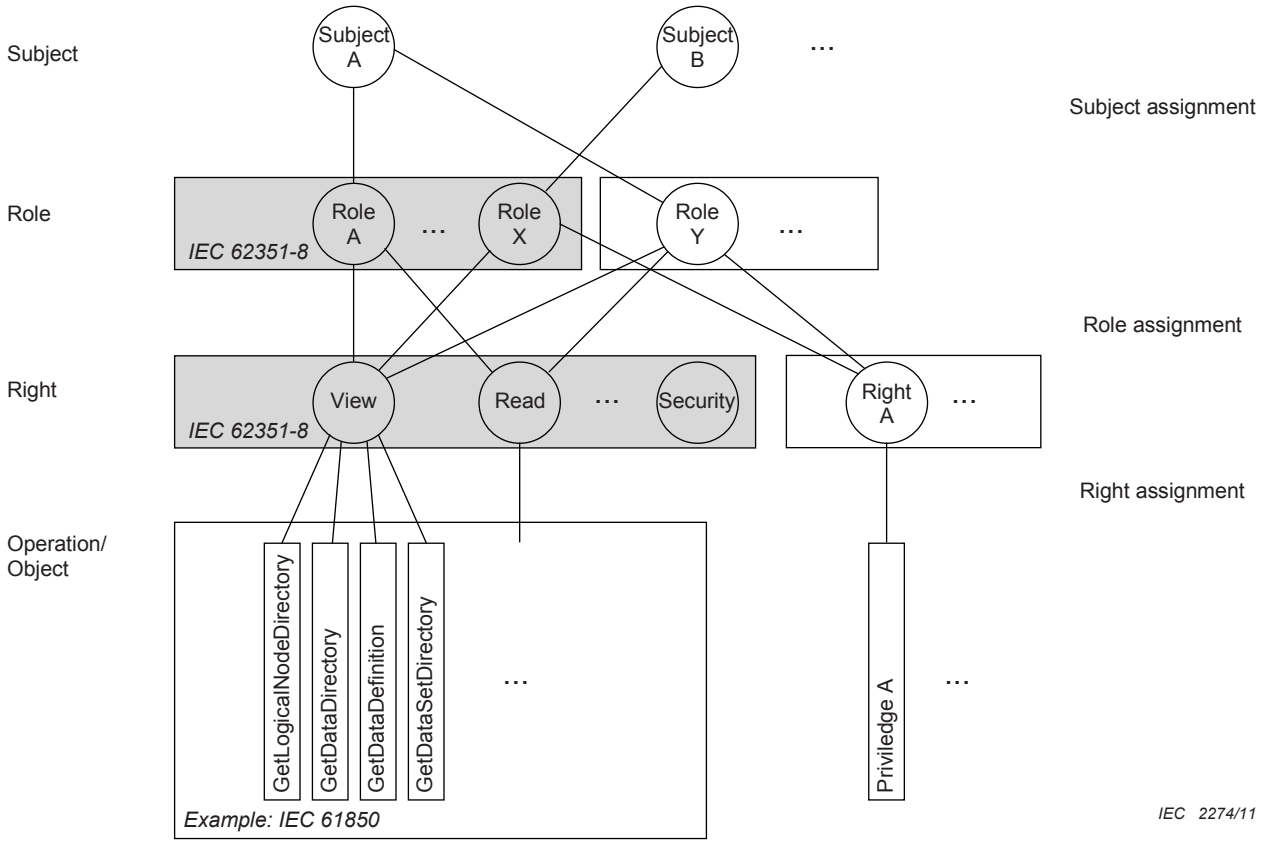


Figure 3 – User, roles, rights and operations

A right subsumes a set of operations which is determined by the data model in use; e.g. a protection system may use the IEC 61850 data model. This specification supports data models for power systems as listed in 5.2.

A set of roles and associated rights must be defined to enable proper operability. These so-called pre-defined roles and pre-defined rights are encircled by grey boxes in Figure 3. They represent the core part of this specification and are defined in 5.2. The pre-defined rights represent an abstraction layer towards the underlying data models.

4.2.2 Subject assignment

The subject assignment or subject-to-role mapping is stored *outside* the system in a repository. The repository may be accessed with an LDAP-enabled service to retrieve the access tokens.

One or more subjects can be assigned to one or more roles.

The time period during which a particular subject-to-role mapping is valid should be kept flexible.

4.2.3 Role assignment

The role assignment or role-to-right mapping is stored inside the object. It represents the configuration of the object and depends on the data model in use.

This mapping is also determined by security/safety regulations and is the main focus of this specification. Pre-defined roles and pre-defined rights are used to implement such policies.

A right belongs to at least one role.

NOTE Role definition and role assignment can have different life-cycles. To assure consistency, they are equipped with a revision number which must be checked in the object (see also 11.1). Otherwise, a role can be presented to an object with a different right assignment than the one stored in the object.

4.2.4 Right assignment

The mapping between rights, operations and objects is given by the data model in use. Refer to 5.2.

4.3 Criteria for defining roles

4.3.1 Policies

A minimum set of roles is defined by policies and standards (such as NERC CIP-001 – CIP-009). These roles are mandatory and are called pre-defined roles. These pre-defined roles are defined in this technical specification.

Vendors of power system equipment may deploy their equipment with a set of additional roles. These roles are called default roles and may serve vendors specific configuration procedures and/or vendor specific handling of the equipment.

Finally, roles may be defined by the utility operator and/or the substation management to meet their specific needs (e.g. local implementation requirements). These roles are termed specific roles.

4.3.2 User, roles, and rights

Subject names change more frequently than role names and role names change more frequently than the rights of a data model (e.g. IEC 61850).

It is thus advisable to have the frequently changing entities centrally stored and administered whereas the entities with a long lifetime are stored decentralized in the object.

– The subject-to-role mapping is stored out-side the object at the identity provider (repository).
– Thus, the role-to-right mapping is stored inside the object.

4.3.3 Introducing roles reduces complexity

Without roles, the complexity of the subject-to-right assignment amounts to

$$O(|s| \times |ri|) \tag{1}$$

where $|s|$ is the number of subjects and $|ri|$ is the number of rights.

The introduction of roles results in two mappings: one mapping of subjects to roles and a second one of roles to rights. The complexity of these two mappings yields

$$O(|s| \times |ro|) + O(|ro| \times |ri|) \quad (2)$$

where $|ro|$ is the number of roles.

Equation (2) can be smaller than Equation (1). In fact, this is always the case if the number of roles is smaller than the half of the minimum of the number of subjects and rights. Thus, the concept of roles is recognized as a possibly efficient means to control access rights.

5 Definition of roles

5.1 Role-to-right assignment inside the object in general

5.1.1 General

Roles shall be assigned a set of rights.

Remark: The rights are defined by the data model in use, see 5.2.

5.1.2 Number of supported rights

The minimum number of supported rights shall be at least one.

5.1.3 Number of supported roles

The minimum number of supported roles shall be at least one.

5.1.4 Flexibility of role-to-right mapping

The mandatory minimal role-to-right assignments are defined in 5.2.

Additional role-to-right assignments shall be allowed.

Security audit functions (with the exceptions of view and read) shall not be implemented in the same role as security administration functions.

5.2 Role-to-right assignment with respect to power systems

5.2.1 Mandatory roles and rights for logical-device access control

5.2.1.1 General

This subclause specifies the minimum set of mandatory roles and rights that shall be available in each logical-device.

5.2.1.2 Mandatory pre-defined role-to-right mapping

Table 1 reflects the minimum set of roles to be supported.

Table 1 – List of pre-defined role-to-right assignment

Value	Role \ Right	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTINGGROUP	SECURITY
<0>	VIEWER	X			X							
<1>	OPERATOR	X	X		X				X			
<2>	ENGINEER	X	X	X	X		X	X		X		
<3>	INSTALLER	X	X		X		X			X		
<4>	SECADM	X	X	X			X	X	X	X	X	X
<5>	SECAUD	X	X		X	X						
<6>	RBACMNT	X	X					X		X	X	
<7…32767>	Reserved	For future use of IEC defined roles.										
<-32768 .. -1>	Private	Defined by external agreement. Not guaranteed to be interoperable.										

Remark: RBACMNT is a sub-role of SECADM.

5.2.1.3 Mandatory pre-defined rights

The list of the pre-defined rights for a particular role shall be represented by the following PACKED LIST (see Table 2):

Table 2 – List of mandatory pre-defined rights

Predefined rights			
AttributeName	**AttributeType**	**Comments**	**M/O** **M: mandatory but conditional, depending on the object model.** **Examples:** – **An IED without a controllable object shall not support the right CONTROL;** – **An IED without a file system shall not support the right FILE.** **O: optional**
View	BOOLEAN		M
Read	BOOLEAN		M
DataSet	BOOLEAN		M
Reporting	BOOLEAN		M
FileRead	BOOLEAN		M
FileWrite	BOOLEAN		M
Control	BOOLEAN		M
Config	BOOLEAN		M
SettingGroup	BOOLEAN		M
FileMgt	BOOLEAN		M
Security	BOOLEAN		M

– VIEW right: Allows the subject/role to discover what objects are present within a Logical-Device by presenting the type ID of those objects. If this right is not granted to a subject/role, the Logical-Device for which the View right has not been granted shall not appear;

– READ right: Allows the subject/role to obtain all or some of the values in addition to the type and ID of objects that are present within a Logical-Device;

– DATASET right: Allows the subject/role to have full management rights for both permanent and non-permanent DataSets;

– REPORTING right: Allows a subject/role to use buffered reporting as well as un-buffered reporting;

– FILEREAD right: Allows the subject/role to have read rights for file objects;

– FILEWRITE right: Allows the subject/role to have write rights for file objects. This right includes the FILEREAD right;

– CONTROL right: Allows a subject to perform control operations;

– CONFIG right: Allows a subject to locally or remotely configure certain aspects of the server;

– SETTINGGROUP right: Allows a subject to remotely configure Settings Groups;

– FILEMNGT right: Allows the role to transfer files to the Logical-Device, as well as delete existing files on the Logical-Device;

– SECURITY right: Allows a subject/role to perform security functions at both a Server/Service Access Point and Logical-Device basis.

5.2.1.4 Mandatory pre-defined roles (see Table 3)

Table 3 lists the pre-defined roles in the context of this specification.

Table 3 – Pre-defined roles

Predefined roles			
AttributeName	**Value**	**Comments**	**M/O**
VIEWER	<0>		M
OPERATOR	<1>		M
ENGINEER	<2>		M
INSTALLER	<3>		M
SECADM	<4>		M
SECAUD	<5>		M
RBACMNT	<6>		M

– VIEWER: can view what objects are present within a Logical-Device by presenting the type ID of those objects.

– OPERATOR: An operator can view what objects and values are present within a Logical-Device by presenting the type ID of those objects as well as perform control actions.

– ENGINEER: An engineer can view what objects and values are present within a Logical-Device by presenting the type ID of those objects. Moreover, an engineer has full access to DateSets and Files and can configure the server locally or remotely.

– INSTALLER: An installer can view what objects and values are present within a Logical-Device by presenting the type ID of those objects. Moreover, an installer can write files and can configure the server locally or remotely.

– SECADM: Security administrator can change subject-to-role assignments (outside the device) and role-to-right assignment (inside the device) and validity periods; change security setting such as certificates for subject authentication and access token verification.

– SECAUD: Security auditor can view audit logs.

– RBACMNT: RBAC management can change role-to-right assignment.

5.2.2 Power utility automation – IEC 61850

The access control for IEC 61850 data objects is implemented by all virtual access view or services. Operations are called services in IEC 61850.

A subject shall be identified by the authentication parameters passed to the server (e.g. applying his certificate and the corresponding private key in a challenge response fashion).

A session shall then be established along with the role of the subject and assigned to the subject at the client side.

A subject shall then be permitted access to an IEC 61850 data object simply if the required access right (of that data object) is associated with at least one of the roles used in the current session; see server class and application association model in IEC 61850-7-2.

There are two areas in which access control shall be applied:

– Service-access-point: Access control will be used to ALLOW or DENY remote access to a ACSI server (in context of IEC 61850) and/or its children over an access point; a connecting client can then access a logical-device and/or a file; and

– Data objects: Access control shall be applied to each instance of the hierarchy logical-device, logical-node, and data-object. Access to the Logical-Device shall be granted or restricted based upon access rights.

5.2.2.1 Service access control

5.2.2.1.1 Mandatory pre-defined role-to-right mapping (see Table 4)

Table 4 lists the pre-defined role-to-right mapping in the context of this specification.

Table 4 – Mandatory role-to-right mapping for service access control

Role \ Right	ALLOW	DENY
Role configured in the device (see 5.2.1 and others)	X	
Any other role		X

Additionally, a maximum number of simultaneous active associations shall be able to be configured for a specific subject. The default value for any configured subject/role shall be unlimited (e.g. bounded by the maximum number of associations supported by the server).

5.2.2.1.2 Mandatory pre-defined rights-to-operations/services assignments

5.2.2.1.2.1 ALLOW right (see Table 5)

Table 5 defines the ALLOW right.

Table 5 – The ALLOW right

ACSI service name	Comments
Associate	Must be defined as part of access control
Release	
Abort	

5.2.2.1.2.2 DENY right (see Table 6)

Table 6 defines the DENY right.

Table 6 – The DENY right

ACSI service name	Comments
Associate	Must be defined as part of access control
Release	
Abort	

5.2.2.2 Definition of mandatory rights other than security rights

The operations assignment of these roles is relegated to IEC 61850.

Informative example: VIEW right.

This right allows the subject/role to discover what objects are present within a logical-device. If this right is not granted to a subject/role, the logical-device for which the VIEW right has not

been granted shall not appear within the response to the ACSI `GetLogicalDeviceDirectory`.

If the VIEW right is granted to a role, then the role shall have access to objects in the logical-device, through the following ACSI services (see Table 7):

Table 7 – VIEW right and associated ACSI services

ACSI service	Comment
GetLogicalNodeDirectory	Retrieve ObjectReference of a specific ACSI class contained in a logical-node
GetDataDirectory	
GetDataDefinition	
GetDataSetDirectory	

5.2.2.3 Logging

Upon a successful authentication and association, the server shall log the subject and allowed roles to a log named SECAUD. The implementation of this log is defined in the specific communication service mapping (SCSM) of IEC 61850-7-2.

Changes in the role-to-right mapping and thus changes to the revision number in the credential shall be logged by the server to enable a chain of custody for this assignment.

5.2.2.4 Configuration of devices

The configuration shall be performed in out-of-band manner (e.g., manually).

The configuration of role-to-rights assignment shall be defined via an SCL file in the object model.

The configuration of the role-to-right assignment shall have a revision number.

5.2.3 CIM – IEC 61968

At the time of issuing this specification, there were no specific mandatory roles requested for CIM. The mechanism to define own roles offered by this specification may be used to define use case specific roles whenever needed. Additional roles to be defined in the context of IEC/TS 62351-8 may also be part of an amendment or a new edition.

5.2.4 AMI

At the time of issuing this specification, there were no specific mandatory roles requested for AMI. The mechanism to define own roles offered by this specification may be used to define use case specific roles whenever needed. Additional roles to be defined in the context of IEC/TS 62351-8 may also be part of an amendment or a new edition.

5.2.5 DER

At the time of issuing this specification, there were no specific mandatory roles requested for DER. The mechanism to define own roles offered by this specification may be used to define use case specific roles whenever needed. Additional roles to be defined in the context of IEC/TS 62351-8 may also be part of an amendment or a new edition.

5.2.6 Markets

At the time of issuing this specification, there were no specific mandatory roles requested for markets. The mechanism to define own roles offered by this specification may be used to define use case specific roles whenever needed. Additional roles to be defined in the context of IEC/TS 62351-8 may also be part of an amendment or a new edition.

5.3 Role-to-right assignment with respect to other non-power system domains (e.g. industrial process control)

At the time of issuing this specification, there were no specific mandatory roles requested for non-power system domain. The mechanism to define own roles offered by this specification may be used to define use case specific roles whenever needed. Additional roles to be defined in the context of IEC/TS 62351-8 may also be part of an amendment or a new edition.

6 General architecture for the PUSH model

6.1 General

Figure 4 shows the authorization process when a subject wants to access from system A an object (e.g. an application) on system B.

We assume that the systems are properly configured, i.e. the role-to-right assignment has been loaded into system B and subject-to-role assignment with corresponding revision number is stored in the repository.

The small letters define the access control mechanism, i.e.:

a) first, the subject authenticates itself from system A towards a repository for retrieval of its access tokens and roles via an LDAP-enabled service;

b) the repository provides the subject with the access token containing role(s);

NOTE Steps a) and b) may be optional if the subject is already in possession of the access token.

c) the subject submits the access token containing the role(s) from system A to the system B; this can be done online or offline; the mapping is a one-to-many, i.e. the access token is valid for many systems B; restrictions are optional;

d) system B verifies the access tokens of the subject and gives the subject authorized access to the object according to the right(s) associated with the role inside the access token.

   Optionally, system B may verify whether the access token has not been revoked by accessing the repository.

   The configuration of the role-to-right assignment is a prerequisite to enforce RBAC and must be undertaken in the engineering process of the system;

e) acknowledgement of system B to system A.

The process outlined from item a) to item e) is similar to Kerberos. The repository takes the function of a ticketing server. It issues an access token with limited lifetime for a subject used by system A to authenticate towards target system B.

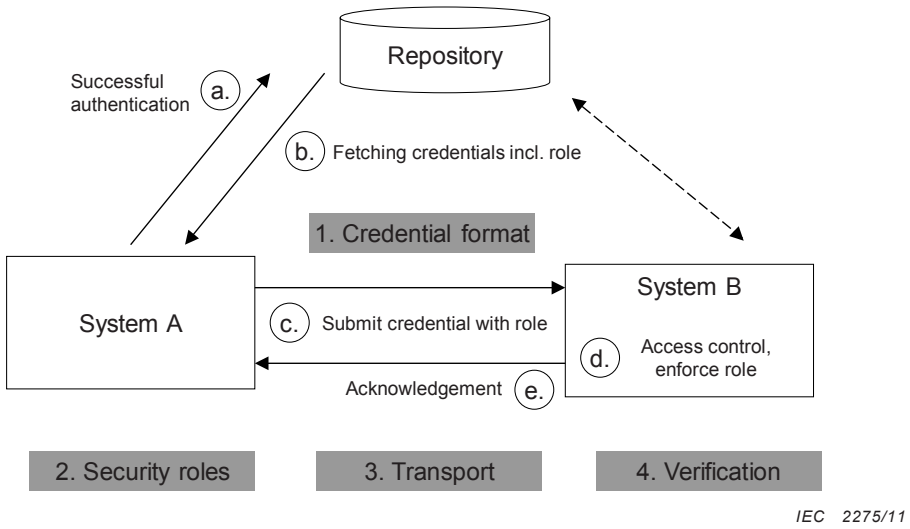


Figure 4 – Schematic view of authorization mechanism based on RBAC

This specification focuses on the numbered parts in Figure 4 that are:

1) formats of access tokens containing roles (see Clause 8);
2) security roles and associated rights (see 5.2);
3) methods to transport the authorization information securely to the target system B using existing protocols (see Clause 10); and
4) verification of access tokens by the target system B. The access token can be bound to a single message or an application layer session (see Clause 11).

6.2 Secure access to the LDAP-enabled service

This subclause targets the access to an LDAP enabled repository, holding the access token information.

LDAP v3 with SSL/TLS should be used.

Each subject authenticating to the LDAP server should have the following entries:

– unique user identifier (user ID);
– authentication information; and
– access token.

7 General architecture for the PULL model

7.1 General

To support use cases, in which devices are used that do not feature an appropriate interface to provide the access token locally (e.g., IEDs with simple HMI in terms of display and key pad), a mechanism is needed to provide the role information for the accessing user. The user may logon using a user ID and a password. The “PULL” model described in this clause supports such a user ID, password based logon, but may also be used in conjunction with certificate based logon.

It is important to allow logon to a system in situations where connectivity to the LDAP repository fails. To handle such situations, LDAP supplies a robust and well tested replication mechanism.

Figure 5 shows a generic authorization scenario where a subject wants to access from system A an object (e.g. an application) on system B. Note that for the use case accessing an IED via the HMI described above, systems A and B would coexist and would thus not establish a separate communication connection.

It is assumed that the systems are properly configured, i.e. the role-to-right assignment has been loaded into system B and subject-to-role assignment with corresponding revision number is stored in the repository.

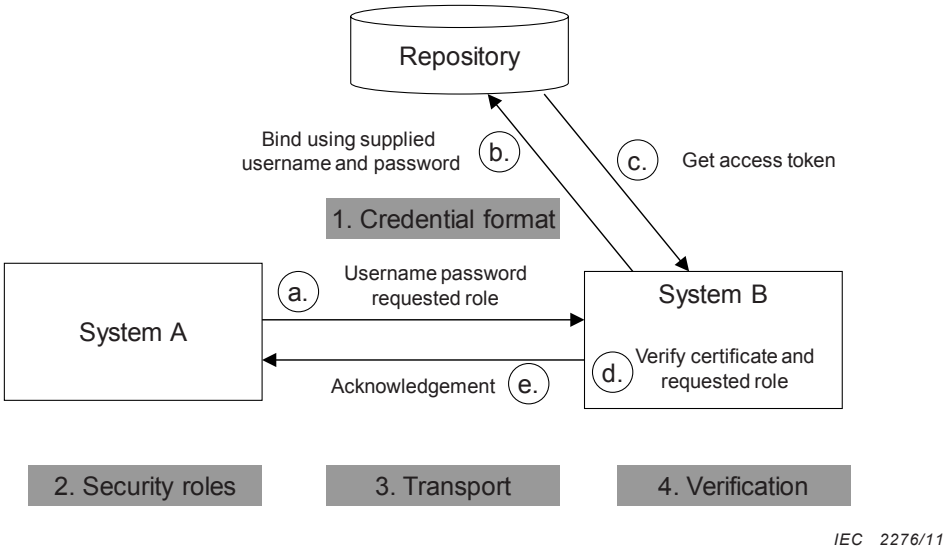
The small letters define the access control mechanism, i.e.:

a) First the system A opens a TLS protected communication channel to system B. System A must use TLS mechanisms to verify the identity of the object being accessed. After successfully verifying the identity of system B, system A transmits authentication credentials to system B (e.g., user ID, password and requested role).
b) System B uses the LDAP bind method and the supplied authentication credentials to verify the authentication information. System B should use TLS to verify the identity of the repository and to protect the bind exchange.
c) System B uses an LDAP query to retrieve the user specific access token from the repository.

NOTE 1 Steps b) and c) may be optional if data from the repository was replicated to System B.

NOTE 2 Step a) may be optional if System A and B collapse in case of a local HMI.

d) System B verifies the access token received from the repository to ensure the user is allowed to act in the specific role.
e) System B acknowledges or rejects authentication and access towards system A.



IEC 2276/11

Figure 5 – Schematic view of authorization mechanism based on RBAC PULL model

This specification focuses on the numbered parts in Figure 5 that are:

1) formats of access tokens containing roles (see Clause 8);

2) security roles and associated rights (see 5.2);
3) methods to transport the authorization information securely to the target system B using existing protocols (see Clause 10); and
4) verification of access tokens by the target system B. The access token can be bound to a single message or an application layer session (see Clause 11).

7.2 Secure access to the LDAP-enabled service

This subclause targets the access to an LDAP enabled repository, holding the access token information.

LDAP v3 with SSL/TLS should be used.

Each subject authenticating to the LDAP server should have the following entries:

- unique user identifier (user ID);
- authentication information; and
- access token.

7.3 LDAP directory organization

In order to facilitate interoperability, this specification provides some recommendations on how to organize data in the LDAP directory:

- Each LDAP object used for RBAC must have a UID attribute (see RFC4524). The value of the UID attribute should be unique. The user ID supplied by the user should match the UID attribute.
- For profile A (see 9.5.1), the LDAP object used for RBAC should have an attribute *inetOrgPerson:userCertificate* holding the DER encoded X.509 Certificate of the user (see RFC2798).

To fetch the access token for a dedicated subject, System B uses the supplied user credentials. After successful retrieval of the access token from the LDAP repository, system B validates the access token.

8 General application of RBAC access token

8.1 General

This specification defines the format and content as well as transport options of access tokens to be used for RBAC. Three profiles are defined covering the application of ID certificates, attribute certificates, and software tokens. These access tokens can generally be used on different OSI layers. This specification focuses on their application for transport and application layer but does not limit their applicability to these. Thus, they may be utilized also in protocols on other OSI layers. Moreover, the credentials can be used on a per session basis or on a per message basis. Therefore, this clause provides information and potential boundary conditions regarding the session based and the message based approaches.

A session-based approach assumes that there exists an end-to-end communication dialog between two entities, which has been set up in an authenticated way. It is expected that the authentication is bound to the RBAC credential. During the setup phase, a session key is established to cryptographically protect the communication session and to ensure that there is a cryptographic binding of the communication security to the initial authentication and authorization.

A message-based approach assumes that the RBAC credential is cryptographically bound to the content of a single message.

The RBAC applying application or protocol has to integrate one of the two approaches.

8.2 Session based approach

Applying the RBAC credential on transport layer is a typical example for the realization of the session-based approach, when the transport connection is end-to-end. Particularly for the application of TLS, authentication and authorization can easily be achieved during the TLS handshake phase.

TLS (see RFC5246), which is used in different parts of IEC 62351, utilizes ID certificates during the key establishment phase for mutual authentication. As Profile A (see 9.5.1) uses an ID certificate with a RBAC extension, session-based authorization can easily be achieved. The Profile A credential can be validated an authenticated on transport layer, while the application can validate the role information.

Profile B instead applies attribute certificates, which are typically bound to an ID certificate. With the TLS extension for authorization (see RFC5878), the application of attribute certificates during the TLS handshake is defined allowing for direct application of Profile B (see 9.5.2).

Profile C defining a software token is not likely to be used in conjunction with TLS directly, as the appropriate message field allowing the transport of the software token is not available directly within TLS.

If a cryptographic session is to be bound to the transport connection, the application has to ensure the binding of the initial authentication of the transport connection including the access token to the remaining part of the communication exchange. TLS, as stated above, provides an example for this.

Binding of the access token to a transport connection shall only be done if there is a one-to-one mapping of the sender and the receiver applications possible. There may be scenarios in which this is not always provided:

– If there is more than one application utilizing the same transport connection (or more specifically the same TLS connection), the cryptographic session binding needs to be done on a higher communication layer to avoid ambiguities of the authorization information and to ensure an appropriate authorization level per application. This situation may occur for instance, if there are multiple MMS instances on a substation controller, which communicate via a single TLS connection to a field device.
– Another scenario is provided through the existence of multiple hops on the transport connection, while the application connection is intended to be end-to-end in a single hop fashion. This situation may occur in gateway scenarios, where the gateway is an intermediate device on the TLS level terminating both ends and forwarding for instance the MMS communication between a control center and a field device. The authentication on the single TLS connections is not visible end-to-end. Thus end-to-end authentication and authorization needs to be provided on higher communication layers.

Figure 6 shows a generic approach for establishing a secure session between two communication peers. Here, in the first phase digital signatures are used to protect the establishment of the session key. The key establishment is done using Diffie Hellman key agreement. Afterwards, the session key is applied to achieve integrity protection of the session.

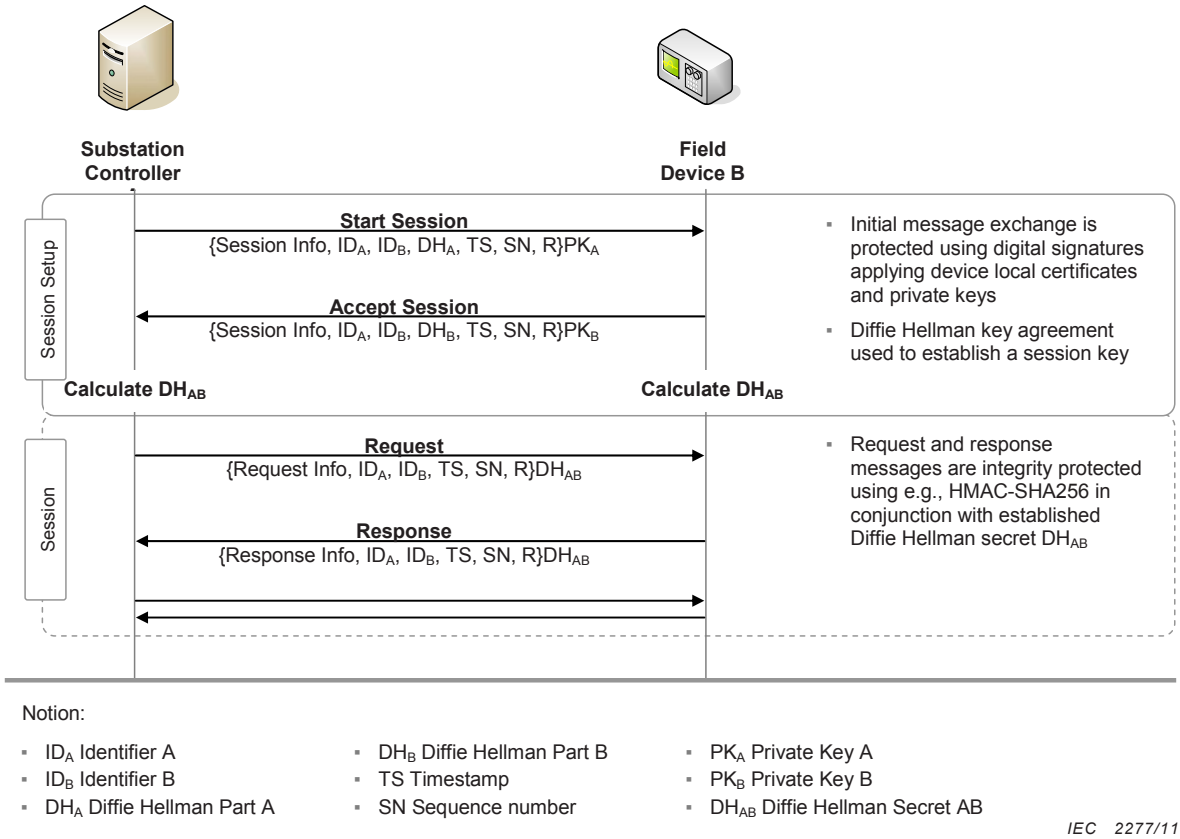


Figure 6 – Session based RBAC approach

The advantage of session based approaches (see Figure 6) is the cryptographic binding of a series of command exchanges to an initial authentication and authorization phase. Here, the authentication and authorization phase, which can be time-consuming, is executed just once. The disadvantage is that the mixing on commands connected with different roles requires separate sessions, either connected with a transport connection or a higher layer communication connection.

8.3 Message based approach

In contrast to the session-based approach, the message based approach applies the access token to every single message. Using profile A or B for instance will result in a digital signature applying the certificate connected with the RBAC information. Thus, each message can be handled independently. A situation where this is a desired behavior is given through a substation controller having multiple inbound connections, which are mapped to a single outbound connection to a field device. The substation controller in this scenario acts as data concentrator for commands from different source to be submitted to the field device.

The advantage of this approach allows for mixing messages from different originators on the same transport layer connection or on the same higher layer communication connection, while still being able to authenticate and authorize the single message. The disadvantage lies in the fact that time-consuming operations like verification or creation of digital signatures have to be carried out on a per message basis.

9 Definition of access tokens

9.1 General

Access tokens are used to transport roles.

9.2 Supported profiles

Three different formats of access tokens are supported:

– profile A: X.509 ID certificates with extensions;
– profile B: X.509 attribute certificates;
– profile C: Software tokens (not using asymmetric cryptography).

NOTE The combination of the profiles is not intended to avoid ambiguities.

9.3 Identification of access token

The identification of the access token is realized using an OID. The root for the IEC 62351 OID tree is 1.2.840.10070. For IEC/TS 62351-8 this results in 1.2.840.10070.8. To provide an option to use different OIDs within IEC/TS 62351-8, a further substructure is defined, which currently only uses the one number to identify the IEC/TS 62351-8 access token.

The OID for the definition of the IEC/TS 62351-8 access token is: 1.2.840.10070.8.1.

NOTE The OID is the same for all supported profiles. The profile itself can easily be identified through the used access token format. If the access token content changes over time, it is expected that a new OID will be given for any changed version of the access token.

9.4 General structure of the access tokens

9.4.1 Mandatory fields in the access tokens

An access token shall contain at least the following information:

– serial number of the access token;
– name of the subject and access token holder;
– role assigned to the subject and access token holder;
– issuer of the access token;
– time-stamp of the issuing moment;
– time-period during which the access token and thus the role assignment is valid; and
– revision number of the subject-to-role assignment.

9.4.2 Mandatory profile-specific fields

For profiles A and B only:

– signature algorithm; and
– signature value of the issuing instance.

For profile C only:

– Hash algorithm;
– key length; and
– Hash value.

9.4.3 Optional fields in the access tokens

For all profiles:

– area of responsibility (defines the area (geographic or organizational) where the role is applicable);

– role definition (refers to the definition of role resp. the underlying data model);

– description of attribute related operations in an `operation` field for use cases, where the access token is applied for user related administrative purposes at the IED; and

– dedicated sequence number field (`statusChangeSequenceNumber`) to provide means for replay protection in environments without time synchronization.

9.4.4 Definition of specific fields

9.4.4.1 RoleID

The role is defined using a mapping to an integer space, whereby the numbers:

– `<0 .. 32767>` are reserved for application within IEC 62351;

– `<-32768 .. -1>` are reserved for private usage, e.g., by other protocols, e.g., IEEE 1815.

All roles to be used in the context of IEC protocols shall be defined as part of IEC/TS 62351-8. The current definition of roles comprises IEC 61850 specific roles.

Format: `INTEGER (-32768..32767)`

A token may specify more than one role; if more than one role is specified, the subject is authorized to enact any combination of identified roles.

9.4.4.2 Role definition

To allow for uniqueness of roles in terms of a unique role-to-right mapping, a further parameter is used to provide information about the used data model. This parameter (`roleDefinition`) is optional and to be treated as “IEC62351-8” per default for positive role IDs. In case of the private usage numbers (negative numbers), it reflects the associated role definition standard. An own role definition may be provided by other standards (other than IEC/TS 62351-8), by a utility operator or other. The `roleDefinition` is valid in the context of the defined `UserRoleInfo` (access token). If multiple role definitions are used, multiple access tokens shall be used to ensure a unique role-to-right mapping.

If the `roleDefinition` field is present the relying party shall use the mapping defined by that field.

The relying party shall reject any role ID that has a `roleDefinition` associated value that it does not recognize.

Format: `UTF8String (0..23)`

9.4.4.3 Operation

The `operation` field supports environments that use the access token for administrative purposes in order to change user permissions (roles) on an IED rather than using the access token by the subject itself. It allows a receiving IED to modify locally stored user permissions (roles) in terms of add, delete, and change.

Format: `ENUMERATION { Add (1), Delete (2), Change (3) }`

9.4.4.4 Sequence number

The `statusChangeSequenceNumber` field supports environments, where time synchronization is not available. If time synchronization is not available, this field carries an always increasing sequence number and can be used for replay protection. In those environments, the receiver needs to store the subject specific sequence number to validate the next received access token. If a received token has a sequence number which is smaller than or equal to the stored sequence number, the access token shall be rejected. The actual use of this field is more explicitly defined by the protocols that require this field.

Format: `INTEGER (0..4294967295)`

9.4.4.5 Resolution of the timestamp

The time resolution shall be in seconds.

Format: GENERALIZEDTIME in UTC according to IEC/TS 62351-4.

9.4.4.6 Maximum lifetime of the access token

The maximum lifetime is 3 years.

Remark: The minimal lifetime is an implementation issue and given by local requirements (see NERC CIP 001-009.

9.4.4.7 Size of access tokens

The maximum supported size of the access tokens shall be 8192 octets.

9.4.4.8 Revision number

The revision number is a monotonically increasing integer number and represents the version of the subject-to-role mapping.

9.4.4.9 Area of responsibility

The area of responsibility (AoR) restricts the applicability of a subject's role to a set of objects. This standard defines the field and the format for the AoR as follows:

Field name	Coding, max length (byte)	Example
Area of responsibility	UTF8, 64	DE.BAVARIA

The AoR is an identifier and should define a hierarchical name space or a reference to the namespace. Note that these identifiers are typically alphanumeric.

The relying party / IED shall validate the complete AoR and shall ignore any `UserRoleInfo` definition which includes an unrecognized AoR.

When UTF8String encoding is used, all character sequences should be normalized according to Unicode normalization form C (see Unicode Standard Annex #15).

9.5 Specific structure of the access tokens

9.5.1 Profile A: X.509 ID certificate

9.5.1.1 Format

X.509 (see RFC5280) defines a certificate in ASN.1 notation as follows

```
Certificate                    ::=  SEQUENCE  {
     tbsCertificate                     TBSCertificate,
     signatureAlgorithm                 AlgorithmIdentifier,
     signatureValue                     BIT STRING  }

TBSCertificate ::=  SEQUENCE  {
     version                   [0]    Version must be v3,
     serialNumber                     CertificateSerialNumber,
     signature                        AlgorithmIdentifier,
     issuer                           Name,
     validity                         Validity,
     subject                          Name,
     subjectPublicKeyInfo             SubjectPublicKeyInfo,
     issuerUniqueID            [1]    IMPLICIT UniqueIdentifier OPTIONAL,
                                      -- If present, version MUST be v2 or v3
     subjectUniqueID           [2]    IMPLICIT UniqueIdentifier OPTIONAL,
                                      -- If present, version MUST be v2 or v3
     extensions                [3]    EXPLICIT Extensions OPTIONAL
                                      -- If present, version MUST be v3
     }
```

To become an ID certificate, the subject must contain the name of the subject (= the access token holder).

The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with subjects (e.g. nationality of the subject) or public keys and for managing a certification hierarchy. The X.509 v3 certificate format also allows communities to define private extensions to carry information unique to those communities.

RFC5280 allows the definition of private extensions to carry information unique to communities. This possibility is used here to convey all subject role attributes in a dedicated structure to be used in the context of IEC/TS 62351-8. Moreover, the extension is defined to allow for multiple different role attributes to be contained. Thus, the subject of the certificate can be assigned multiple roles. It is a non critical standard X509v3 extension and defined in the following subclause. The access token is recognized through a dedicated OID. The OID value is 1.2.840.10070.8.1 reflecting the IEC/TS 62351-8 access token.

9.5.1.2 Certificate attributes

For the certificate format X.509v3 shall be used with the following role related attributes defined to be included in the extension. The OID identifying the extension is already given through 1.2.840.10070. The specific value for the access token is 1.2.840.10070.8.1.

The value for the extension is defined as following:

```
id-IEC62351 OBJECT_IDENTIFIER::= { 1 2 840 10070 }

id-IECuserRoles OBJECT_IDENTIFIER::= id-IEC62351 { 8 1 }

IECUserRoles::= SEQUENCE OF UserRoleInfo

UserRoleInfo::= SEQUENCE { -- contains the role information blob
   -- IEC62351 specific parameter
    userRole                    SEQUENCE SIZE (1..MAX) OF RoleID
    aor                         UTF8String (SIZE(1..64)),
    revision                    INTEGER (0..255),
    roleDefinition              UTF8String (0..23) OPTIONAL,
    -- optional fields to be used within IEEE 1815 and IEC60870-5
    operation                   Operation OPTIONAL,
    statusChangeSequenceNumber  INTEGER (0..4294967295) OPTIONAL,
    }

RoleId::= INTEGER (-32768..32767)

Operation::= ENUMERATED { Add (1), Delete (2), Change (3) }
```

As this extension describes a sequence, it allows to associate more than one role to a subject. Within any access token, there shall only be one `UserRoleInfo` record for any given combination of `aor` and `roleDefinition`.

NOTE When UTF8String encoding is used, all character sequences should be normalized according to Unicode normalization form C (see Unicode Standard Annex #15).

9.5.1.3 Algorithms and key length

For the used identity certificates the following Hash functions shall be supported:

– mandatory Hash-operation: SHA-1;

– mandatory Hash-operation: SHA-256.

NOTE 1 The mandatory support for SHA-1 is intended for backward compatibility and affects mainly the receiver side. SHA-256 must be supported and is the preferred hash algorithm to be used.

For the used identity certificates, the following signature functions shall be supported:

– mandatory Signature-operation: RSA with a key length of 1024 Bit;

– mandatory Signature-operation: RSA with a key length of 2048 Bit.

NOTE 2 The mandatory support for RSA with 1024 bit keys is intended for backward compatibility and affects mainly the receiver side. RSA with 2048 bit keys must be supported and is the preferred signature algorithm to be used.

Optional Signature-operation: ECC-based using elliptic curves defined over finite prime fields with signature algorithm ECDSA or ECGDSA (for ECGDSA, see ISO/IEC 15946-2). Recommended minimum key lengths:

- 192 Bit (in combination with SHA-1);
- 256 bit (in combination with SHA-256).

9.5.1.4 Field of applications

X.509 ID certificates with extensions are suitable in environments when one or more of the following are true.

– Lifetime of the right(s) encapsulated by a role is aligned with that of the public-key included in the certificate; thus, if the public key and the certificate is revoked, the role for the certificate holder is also revoked.
– The same physical entity is acting both as a certificate authority and as an attribute authority.
– Delegation is permitted, but for any one delegation, all rights in the certificate have the same delegation parameters and all extensions relevant to delegation apply equally to all rights in the certificate.

For further information, please refer to ISO 9594-8/ITU-T Recomendation X.509.

9.5.2 Profile B: X.509 attribute certificate

9.5.2.1 Format

An attribute certificate is typically bound to an ID certificate of the same subject. It can be seen as a temporary extension of the ID certificate.

According to X.509 v3 an attribute certificate is defined as follows (see also ISO 9594-8/ ITU-T Recommendation X.509):

```
AttributeCertificate::= SEQUENCE {
               Acinfo                  AttributeCertificateInfo,
               signatureAlgorithm      AlgorithmIdentifier,
               signatureValue          BIT STRING
            }

AttributeCertificateInfo::= SEQUENCE {
               version                 AttCertVersion -- version is v2,
               holder                  Holder,
               issuer                  AttCertIssuer,
               signature               AlgorithmIdentifier,
               serialNumber            CertificateSerialNumber,
               attrCertValidityPeriod  AttCertValidityPeriod,
               attributes              SEQUENCE OF Attribute,
               issuerUniqueID          UniqueIdentifier OPTIONAL,
               extensions              Extensions OPTIONAL
            }

Attribute::= SEQUENCE {
               Type                    AttributeType,
               values                  SET OF AttributeValue
                                       -- at least one value is required
                      }

AttributeType::= OBJECT IDENTIFIER
AttributeValue::= ANY DEFINED BY AttributeType
```

Remark: For a given AC, each AttributeType `OBJECT IDENTIFIER` in the sequence must be unique. That is, only one instance of each attribute can occur in a single AC, but each instance can be multi-valued.

AC users must be able to handle multiple values for all attribute types.

An AC shall contain at least one attribute. That is, the `SEQUENCE OF Attributes` shall not be of zero length.

9.5.2.2 Certificate attributes

For the certificate format X.509v3 shall be used with the following role related attributes defined to be included in the extension. The OID identifying the extension is already given through 1.2.840.10070. The specific value for the access token is 1.2.840.10070.8.1.

The value for the extension is defined as following:

```
id-IEC62351 OBJECT_IDENTIFIER::= { 1 2 840 10070 }

id-IECuserRoles OBJECT_IDENTIFIER::= id-IEC62351 { 8 1 }

IECUserRoles::= SEQUENCE OF UserRoleInfo

UserRoleInfo::= SEQUENCE { -- contains the role information blob
   -- IEC62351 specific parameter
    userRole                    SEQUENCE SIZE (1..MAX) OF RoleID
    aor                         UTF8String (SIZE(1..64)),
    revision                    INTEGER (0..255),
    roleDefinition              UTF8String (0..23) OPTIONAL,
    -- optional fields to be used within IEEE 1815 and IEC60870-5
    operation                   Operation OPTIONAL,
    statusChangeSequenceNumber  INTEGER (0..4294967295) OPTIONAL,
    }

RoleId::= INTEGER (-32768..32767)

Operation::= ENUMERATED { Add (1), Delete (2), Change (3) }
```

As this is extension describes a sequence, it allows the association of more than one role to a subject. Within any access token there shall only be one `UserRoleInfo` record for any given combination of `aor` and `roleDefinition`.

NOTE When UTF8String encoding is used, all character sequences should be normalized according to Unicode normalization form C [Unicode Standard Annex #15].

9.5.2.3 Algorithms and key length

For the used identity certificates, the following Hash functions shall be supported:

– mandatory Hash-operation: SHA-1;
– mandatory Hash-operation: SHA-256.

NOTE 1 The mandatory support for SHA-1 is intended for backward compatibility and affects mainly the receiver side. SHA-256 must be supported and is the preferred hash algorithm to be used.

For the used identity certificates, the following signature functions shall be supported:

– mandatory Signature-operation: RSA with a key length of 1024 Bit;
– mandatory Signature-operation: RSA with a key length of 2048 Bit;

NOTE 2 The mandatory support for RSA with 1024 bit keys is intended for backward compatibility and affects mainly the receiver side. RSA with 2048 bit keys must be supported and is the preferred signature algorithm to be used.

– optional Signature-operation: ECC-based using elliptic curves defined over finite prime fields with signature algorithm ECDSA or ECGDSA. (For ECGDSA, see ISO/IEC 15946-2). Recommended minimum key lengths:
  - 192 bit (in combination with SHA-1);
  - 256 bit (in combination with SHA-256).

9.5.2.4 Field of applications (informative)

X.509 attribute certificates are suitable in environments when one or more of the following are true:

– lifetime of the subject-to-role assignment differs from that of the user's public-key certificate validity;
– the right is valid only during certain intervals of time which are asynchronous with that user's public-key validity or with validity of other rights;
– a different entity is responsible for assigning a particular role to a subject than for issuing public-key certificates to the same subject;
– there are a number of roles assigned to the subject from a variety of issuing authorities.

The attribute certificate may form its own certificate hierarchy and be completely independent of the ID certificates (used for a PKI).

Attribute certificates can also form a sub-tree in a PKI in that the certificate of the source-of-authority is signed by the root of the PKI.

For further information, please refer to ISO 9594-8/ITU-T Recommendation X.509.

9.5.2.5 Mapping between ID and attribute certificate (see Table 8)

Table 8 provides the mapping between ID and attribute certificate.

Table 8 – Mapping between ID and attribute certificate

Concept	PKI	PMI
Name of certificate	ID certificate	Attribute certificate
Certified contents	ID for the public key	ID for the attribute
Issuer of the certificate	Certificate authority (CA)	Attribute authority
Certified holder	Subject	Subject
Revocation	CRLs	ACRLs
Anchor of trust	Root-CA	Source of Authority

9.5.3 Profile C: Software token

9.5.3.1 General

The software token is an unsigned sequence defined as follows:

```
Token::=   UNSIGNED{
               HASHED{
                   SEQUENCE{
                         Access token type (OBJECT IDENTIFIER)
                         Serial number of the Access Token;
                         Revision number of role-to-right assignment;
                         Name of the subject;
                         RoleID assigned to the subject;
                         Area of Responsibility;
                         roleDefinition (OPTIONAL);
                         Issuer of the Access Token;
                         Time-stamp of the issuing moment;
                         Time-period during which the Access Token is valid;
                         Hash algorithm;
                         Key length;
                         Operation (OPTIONAL);
                         statusChangeSequenceNumber (OPTIONAL);
                         Extensions (OPTIONAL);
                   }
                   Hash Value of the SEQUENCE;
               }
           }
```

The OID identifying the access token is already given through 1.2.840.10070.8.1.

Using multiple access tokens for one subject allows the association of more than one role to this subject. There shall only be one access token for any given combination of `Area of Responsibility` and `roleDefinition`.

The extension field may be used to provide further role related information.

9.5.3.2 Hash function and key length

HMAC shall be computed according to FIPS 198. The HMAC value is not truncated.

– mandatory Hash-operation: SHA-1;

– mandatory Hash-operation: SHA-256.

NOTE 1 The mandatory support for SHA-1 is intended for backward compatibility and affects mainly the receiver side. SHA-256 must be supported and is the preferred hash algorithm to be used.

Mandatory key length: A fixed key length equal to the output length of the hash functions shall be supported (160) bits for SHA-1and 256 bits for SHA-256).

NOTE 2 This requires a shared secret (key for HMAC) between the involved parties, i.e., between the token repository and the receiving peer, allowing the receiving peer to validate the token.

9.6 Distribution of the access tokens

The distribution of the access tokens to the subject is an administrative task and is handled on an on-demand basis via an LDAP-enabled service.

Profile A (see 9.5.1): The subject authenticates towards the repository (with an ID certificate or username and password or similar) and receives the access token (ID certificate). Note that this distribution path only carries the certificate. To apply the certificate, the subject may need the associated private key. The distribution of the associated private key is typically part of a certificate enrollment process and out of the scope of this specification. An example for certificate enrollment is provided in PKCS#10.

Profile B (see 9.5.2): The subject authenticates towards the repository (with an ID certificate for instance) and receives the access token; the attribute certificate shall be tied to the ID certificate.

Profile C (see 9.5.3): The subject authenticates towards the repository (with an ID certificate for instance) and receives the SW token.

10 Transport profiles

10.1 Usage in TCP-based protocols

For TCP-based protocols, the role information encapsulated in the access token is sent in a two phase process.

Phase 1 – transport layer: Establish a secure connection according to IEC/TS 62351-3 where applicable. For authentication, the access token according to profile A (ID-certificate) or B (attribute certificate) are applied directly. For profile A, the ID certificate is directly applied in TLS (see IEC/TS 62351-3). For profile B, the attribute certificate is transmitted according the TLS authorization extension (RFC5878) while the corresponding ID certificate is applied as required in IEC/TS 62351-3.

Phase 2 – application layer: Authorization process which comprises the hand-over of the access token containing the role. As specified in 9.2, the access token can either be an ID certificate, an attribute certificate or a SW token.

NOTE It is also possible to apply the same access token in Phase 1 and Phase 2 allowing for optimization of the access token verification process.

10.2 Usage in non-Ethernet based protocols

Non-Ethernet based protocols subsume serial communications.

The access tokens are transmitted after establishing a secure, serial communication channel. Secure means in this context at least authenticated as specified in IEC/TS 62351-5.

This method is irrespective of the profile in use, i.e., Profile A, B, or C.

11 Verification of access tokens

11.1 Normative part

11.1.1 General

The following subclauses depict items of the access token which shall be verified:

11.1.2 Access token authenticity

Before the access token can be used, the subject shall be authenticated. Authentication in this context means that a sender proves his right to use the access token.

Depending on the profile and the used model (PULL or PUSH), this proof can be either

– a digital signature involving the private key corresponding to the subjects certificate associated with the access token, which can be verified by the receiver together with the verification of the subjects certificate suitable for profile A and B; or
– a challenge response mechanism involving an authentication credential bound to the access token suitable for all profiles requiring the use of either digital signatures or a shared key between the involved entities (subject and target peer).

NOTE If the access token of Profile A or B is applied on transport layer as described in 10.1, phase 1, the token verification is being done in the context of the TLS handshake, while the role application has to be done within the application.

Optimization option for Profile A and B over TCP-based protocols:

The verification of the ID certificate can be neglected, if the ID certificate in the application layer is the same (based on serial number and issuer) as used in the TLS protected transport layer.

11.1.3 Time period

Time-period of the access tokens shall be verified.

11.1.4 Access token integrity

For profile A and B: Signature verification of access token along the certificate chain to the CA root.

For profile C: Integrity checks using the pre-shared key.

11.2 Optional part

The following items of the access token may be verified:

– Revision number (see 9.4.4.8): Comparison of the revision number for role assignment in the access token with the revision number of the configuration (right assignment) in the object;
– AoR (see 9.4.4.9): For use of network segregation;
– Issuing instance of the access token;
– Revocation list (see 11.3);
– RoleDefinition (see 9.4.4.2);
– Operation (see 9.4.4.3);
– Sequence number (see 9.4.4.4).

11.3 Revocation methods

11.3.1 General

The verification step is based on the trust relationship between the identity provider and the service provider/object: Depending on that trust, a revocation list may be obsolete. E.g. a CRL may not be necessary when the lifetime of the access token is less than the refresh time of the CRL (i.e. less that one day according to IEC/TS 62351-3).

It is recommended to prefer a restricted life-time of the access token over the utilization of revocation lists as not all objects will have on-line access to a CRL. Revocation methods are thus optional and can be used after verification.

Profile A – ID certificate: The use of a CRL is recommended as machine/ID certificates usually have a long lifetime. The need for a CRL may be subsumed by administrative measures, i.e. with a restricted lifetime of the ID certificates.

Profile B – Attribute certificate: The need for an ACRL can be subsumed by administrative measures, i.e. with a restricted lifetime of the attribute certificates. The revocation of the underlying machine/ID certificates are out of the scope of this standard.

Profile C – Token: The need for a revocation list can be subsumed by administrative measures, i.e. with a restricted lifetime of the tokens.

In case of revocation requests to the identity provider, the service provider / object shall have a secured connection (by TLS/SSL) with mutual authentication to the identity provider.

11.3.2 Supported methods

Profile A: A CRL; according to IEC/TS 62351-3, the revocation of an ID certificate shall be checked.

Profile B: An Attribute CRL (ACRL).

Profile C: A revocation list based on access token serial number and issuer.

NOTE The definition of CRL handling will be addressed in IEC/TS 62351-9[2].

12 Interoperability

12.1 General

Interoperability means proper operability between different objects from different manufacturers.

The interoperability is not dependent on the set of roles and associated rights definition, but on their exchange.

12.2 Supported access tokens

Supported access tokens are:

– X.509 ID certificates as defined in 9.5.1;
– X.509 attribute certificates as defined in 9.5.2;
– software token as defined in 9.5.3.

12.3 How to ensure backward compatibility

RBAC to legacy protection equipment is not possible. Retrofit of those systems is a local implementation issue; a unified architecture is generally missing and a one-fit-all solution difficult to realize.

Administrative measures must be installed, i.e., the network administrator shall segregate the network into areas where RBAC is operational and areas where it is not.

The extension field in the access tokens shall be used to specify the area/network segment where the RBAC in use is valid, i.e. the AoR attribute.

---

2 Under consideration.

12.4 How to extend the list of roles and rights

The list of roles and rights shall be extendable. The maximum length of the list is a local implementation issue.

12.5 How to map this specification to specific authorization mechanisms

Profile A is part of a PKI.

Profile B is a PMI interconnected with a PKI: For information on the combination of PKI and PMI, see ISO 9594-8/ITU-T Recommendation X.509.

Profile C: Similar to Kerberos. A PKI can be realized underneath the software token system and may protect the access to the central repository.

Bibliography

ISO/IEC 15946-2, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures* (withdrawn)

IEC 61784 (all parts), *Industrial communication networks – Profiles*

IEC 61968 (all parts), *Application integration at electric utilities – System interfaces for distribution management*

IEC 61970, *Energy management system application program interface (EMS-API)*

IEC/TS 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*[3]

IEC/PAS 62400, *Structuring principles for technical products and technical product documentation – Letter codes – Main classes and subclasses of objects according to their purpose and task*

IEC/ISO 9798-2, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms*

ANSI X.9.69-2006, *Framework for Key Management Extensions*

ANSI X.9.73-2002, *Cryptographic Message Syntax*

IEEE 802.1X-2004, *IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control*

IEEE 1518:2010, *Distributed Network Protocol (DNP3)*

IEEE P1689, *Trial Use Standard for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access*

NIST: SP 800-82, *Guide to Industrial Control Systems (ICS) Security, Second Public Draft.*

XCAML, *Extensible Access Control Markup Language (XCAML) v2.0, February, 2005*

PKCS#12, *Personal Information Exchange Syntax Standard*

RFC2798, *Definition of the inetOrgPerson LDAP Object Class*

RFC2904, *AAA Architecture*

RFC2905, *AAA Authorisation Application Examples*

RFC4524, *COSINE LDAP/X.500 Schema*

RFC5246, *The Transport Layer Security (TLS) Protocol Version 1.2*

RFC5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

---

3 Under consideration.

RFC5878, *Transport Layer Security (TLS) Authorization Extensions*

NERC CIP-001 – CIP-009, *North American Electric Reliability Corporation: Critical Infrastructure Protection, NERC CIP-001 – CIP-009*

ANSI INCITS 359-2004, Role Based Access Control

Kerberos, Distributed Authentication in Kerberos using Public Key:
http://www.mit.edu/kerberos/

FIPS198a, The Keyed-Hash Message Authentication Code:
http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

Unicode Standard Annex #15 Unicode Normalization Forms", October 2006, Davis, M. and M. Duerst, http://www.unicode.org/reports/tr15/

PKCS#10, Certificate Request Syntax Standard

———————

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™