COMITATO
ELETTROTECNICO
ITALIANO

Estratto CEI 0-16

Extract from CEI 0-16

data di pubblicazione: 2024-12

Allegato T – Scambio informativo basato su standard 61850

Annex T - Information exchange based on IEC 61850

ESTRATTO IN INGLESE DELLA NORMA CEI 0-16

Sommario

Il presente documento è la traduzione in inglese dell'Allegato T della Norma CEI 0-16 2023-05 V2.
Si evidenzia che il CEI non ha pubblicato una versione in inglese della Norma CEI 0-16. Questa traduzione del solo Allegato T è stata predisposta dal CT 316 e dal CT 57 per essere utilizzata come documento di lavoro nell'ambito di gruppi di lavoro CENELEC o IEC.

Abstract

This document is an English translation of Annex T of CEI 0-16 2023-05 V2.
It should be noted that the CEI has not published an English version of CEI 0-16. This translation of Annex T only has been prepared by CT 316 and CT 57 for use as a working document within CENELEC or IEC working groups.

PREMESSA

Il presente documento è la traduzione in inglese dell'Allegato T della Norma CEI 0-16 2023-05 V2.

Si evidenzia che il CEI non ha pubblicato una versione in inglese della Norma CEI 0-16. Questa traduzione del solo Allegato T è stata predisposta dal CT 316 e dal CT 57 per essere utilizzata come documento di lavoro nell'ambito di gruppi di lavoro CENELEC o IEC.

Si riportano di seguito alcuni dei termini e delle definizioni della Norma CEI 0-16 utili per la corretta lettura di questo Allegato T.

FOREWORD

This document is an English translation of Annex T of CEI 0-16 2023-05 V2.

It should be noted that the CEI has not published an English version of CEI 0-16. This translation of Annex T only has been prepared by CT 316 and CT 57 for use as a working document within CENELEC or IEC working groups.

Below are some of the terms and definitions of the CEI 0-16 useful for the correct reading of this Annex T.

Terms and definitions

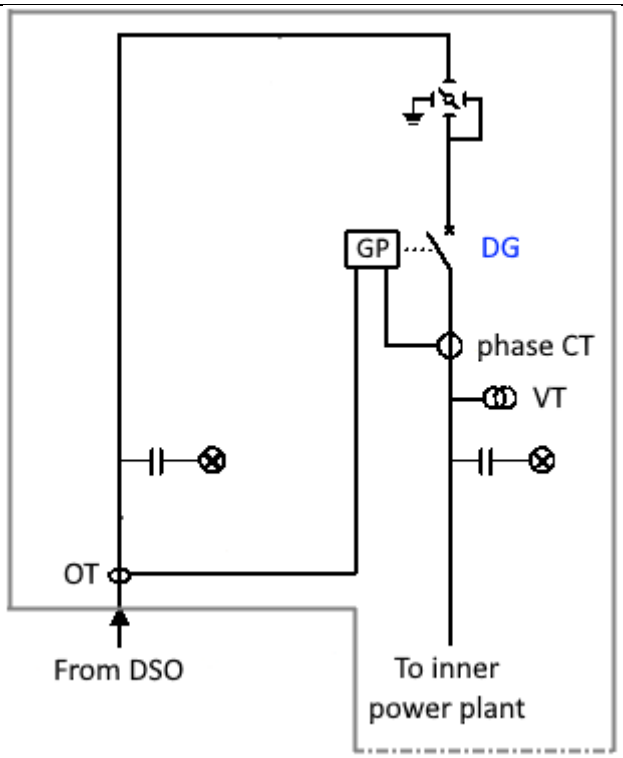
3.16

DER Plant Controller (CCI)
IED whose main functions are plant monitoring, data exchange between the plant and the DSO and any other enabled remote actors, as well as the operation and control of the plant itself.

3.25

Main power plant breaker (DG)

Protection, switching and disconnection equipment whose opening (controlled by the General Protection System) ensures the separation of the user's entire installation from the DSO's grid.



Main power plant breaker (DG) example

O.6

Control modes of operation (FR)
PF2-related operating mode of the CCI.

Interoperability
ability of two or more IEDs from the same vendor (or different vendors) to exchange information and use that information for correct co-operation.

O.6

Functional Performance (PF)
Set of functions aggregated according to the classification proposed in the Annex O, section O.6 of CEI 0-16: Mandatory (PF1 - Observability), Optional (PF2 – Control), Discretionary (PF3 – Participation in the MSD).

3.80

Point of connection (PdC)
Point of electrical connection of the DER plant to the DSO grid; hereafter used with the same meaning as PoC, PCC or ECP.

Single Generating Unit (SGG)
Generator whose Nominal Power exceeds the observability threshold defined in O.8.4.

Abbreviated terms

CCI	DER Plant Controller
CID	Configured IED Description
DG	Main power plant breaker
DO	Data Object
ECP	Same as PdC
GD	Distributed Generation
IED	Intelligent Electronic Device
LN	Logical Node
LD	Logical Device
MSD	Market for Dispatching Services
PD	Physical Device (e.g. an IED)
PdC	Point of electrical connection
POD	Point Of Delivery
PoC	Same as PdC
SCL	System Configuration Language (IEC 61850-6)

Allegato T
(normative)

Information exchange based on IEC 61850 [237)]

T.1 Introduction

In the perspective of evolution of distribution networks towards the smart grid paradigm, it is necessary to define a set of information exchanges aimed at governing the power grid when a significant amount of Distributed Generation (hereafter GD) at the point of connection with the distribution network.

The model taken into account for defining the DER Plant Controller (hereafter CCI) interface requires the GD to communicate with the Distribution System Operator (hereafter DSO), the Aggregator and the GD operator (or User) and does not define the communication to the elements of the plant.

Implementation and use of the IEC 61850 standard as required in this Annex is mandatory for communications with the DSO. This solution may also be adopted for communications to other enabled actors, respecting their respective roles, but this approach is not required by this Annex.

Concerning communication security, the requirements of this document refer to network interfaces for remote access to the device. Remote access is provided both for monitoring and control functions and for plant management needs.

Guidance will be provided to ensure an adequate level of security, applicable to protocols standardized by international bodies or organizations (IEC, ITU-T, IETF, etc.). When not otherwise specified, reference to a standard is intended to the latest published version.

The basic mechanisms for security of information exchanges based on IEC 61850 protocols, security requirements for support services, and processes related to the management of electronic certificates will then be presented.

How CCI is integrated into the system architecture is beyond the scope of this document, which specifies the IEC 61850 interface of CCI.

T.2 Structure of the Annex

The structure of the Annex includes a first section that defines the technical/functional requirements (in compliance with Annex O) and a second section that specifies the resulting technological solution for implementing the communication interfaces of the CCI device.

More specifically, the first section defines the functional requirements, the resulting information exchange and related technical requirements.

The second section defines the technological solution to be adopted in terms of Data Model, Communication Services, mapping o specific protocol, requirements, algorithms and cybersecurity processes, for the purpose of implementing the functionalities defined in the previous section.

T.3 Specifications associated with CCI – IEC 61580 interface

Based on the functional and technical requirements associated with both the management of the distribution network and the provision of network services by the GD, this specification has identified the information exchanges and the resulting IEC 61850-compliant interface that the GD shall expose to the expected power system actors.

237) For the volumes of the standard already transposed by CEI and in force, one can equivalently refer to the homologous CEI EN.

To be interoperable with the intended actors, the IEC 61850 interface of the GD has been detailed in terms of Data Model, ACSI Services, mapping to specific communication protocol and related cybersecurity specifications.

The CCI interface involves the implementation of an IEC 61850 server with a single logical access point concretely represented by an IP address made accessible to stakeholders.

In the following subclauses, the tables defining the information content to be exchanged through the IEC 61850 interface of the CCI contain a "Presence" field: it identifies the purpose of the data (Observability/Control) and the implementation constraint (Mandatory/Optional).

For the specific implementation of the CCI communication mode, please refer to the Technical Report “Example of SCL file for the IEC 61850 communication of CCI”.

T.3.1 Definition of the functional requirements associated with the CCI

The information exchanges associated with the CCI shall enable it to support the functionalities defined in Annex O of CEI 0-16, summarized below:

- deliver network services through appropriate modulation of active and reactive power as required;
- provide measurements of electrical variables as required in Article O.8;
- the status of the DG breaker and Individual Generation Unit as required in Article O.8.

Communication to plant elements is not covered.

Information is conceptually grouped into the following functional categories.

Table 79 – Functional organization of CCI-related information

Information related to plant design	Information related to the configuration, characteristics and rated capacities of the installation constituent elements. This information is derived from the plant and is not subject to modification by remote processes
Information regarding the operating status of the plant	Information regarding the operating status of the plant and physical equipment in the installation, such as the position of the DG switch and the operation of Single Generating Unit. The status may change as a result of events in the plant or as a result of remote controls
Information related to plant measurements	Analog values measured directly or determined by processing measured quantities such as voltages, currents, powers, etc.
Information related to operating parameter values	Reference values required for the operation of functions and algorithms. The parameters are set during initialization of the device and can later be changed remotely

The information concerning the power characteristics of the elements constituting the plant, provided in the "Messages concerning plant characteristics" are expressed by means of a unified vector containing the quantities in Table 80. All electrical quantities are at the terminals of the elements constituting the plant, except where otherwise specified.

Table 80– Definition of vector of characteristic powers

Information	Description	Unit of measurement
Maximum active power input	Maximum active power that the generating or storage unit can generate	kW
Maximum active power in absorption	Maximum active power that the consumer or storage unit can absorb	kW
Maximum apparent power of the system S_{max}	Maximum apparent power of the system S_{max} of the generating or storage units	kVA
Maximum inductive reactive power	Maximum inductive reactive power that the generic component can continuously exchange	kVAr
Maximum capacitive reactive power	Maximum capacitive reactive power that the generic component can continuously exchange	kVAr

Where required by Annex O, the origin of configuration and command actions towards the CCI will also be specified, as specified in the following Table.

Table 81 – Identity of authorized actors

Origin	Category	Identity
Distributor	automatic-station Remote control/command operation from station-level automatic function	DSO
Aggregator	remote-control Control/command operation from a remote operator outside the plant (e.g. a network control centre)	AGGREGATOR

T.3.1.1 Information on installation characteristics

The information on the characteristics of the plant elements is "static" information to be defined at the initial configuration stage on the CCI or in case of relevant changes to its components, and "dynamic" information because of operating conditions. In particular, the required information is shown in Table 82 as specified in the dedicated paragraphs of Articles O.9 and O.10. Should one or more sections not be present in the plant, the relevant characteristics shall not be filled in.

Table 82 – Information concerning the characteristics of the plant

Information	Description	Type of information / Unit of measurement	Presence
Static information (Configuration)			
Manufacturer of the Installation monitoring equipment	Descriptive text: plant manufacturer	Text string	Observability Mandatory
Plant Monitoring Device software version	Descriptive text: SW version of the Central Installation Controller	Text string Stringa di testo	Observability Mandatory
Point of delivery (POD)	Identifier of the installation's connection point to the electricity grid as defined by DSO	Text string	Observability Mandatory
Power at connection point	It defines the power vector referred to the grid connection point. It is represented by Table 80 The value of the maximum apparent power of the installation Smax constitutes the reference for all active and reactive power values expressed in percentages.	See vector of characteristic powers (Table 80)	Observability Optional
Dynamic information (Operation)			
Control functions available in the plant	Lists the control functions that the CCI can operate in relation to the technical capabilities of the plant: Active power limitation, Active power modulation, Voltage regulation with reactive power exchange, PF setpoint, Q(V) regulation, cosφ(P) regulation	Function status (list of possible values): Not available / Autonomous / Automatic The priority of the control functions available in the system is defined in the detail tables Autonomous/Automatic	Control Optional
	Lists the control functions that the CCI can implement in relation to the technical capabilities of the plant: Active power setpoint, Reactive power setpoint	Function status (list of possible values): Not available / Automatic	Participation in MSD Optional

T.3.1.2 Information on the status of the power plant

This type of information allows for the detection of the plant's mode of operation. In Table 83, it is specified according to 3 categories that refer to what is provided in section O.8.6.

Table 83– Information on the status of the power plant

Information	Description	Type of information / Unit of measurement	Presence
General information on the installation			
Availability to operate the current control functions	Availability for plant control Generation macrogroup Storage macrogroup	Availability: Not available / Available	Control Optional
Operating mode of plant	Indicates the operating mode of the plant Active power limitation, Active power modulation, Voltage regulation by reactive power, PF setpoint, Q(V) regulation, cosφ (P) regulation	Status (per individual function) Operating/Not-operating	Control Optional
	Indicates the operating mode the system is in: Active power setpoint, Reactive power setpoint Further operating modes may be defined in subsequent versions of this specification	Status (per individual function) Operatingl/Not-operating	Participation in MSD Optional
Availability for plant control	Availability of the system to operate the control function	Status: Available/Not Available	Observability Mandatory
General breaker status	Indicates the status of the system main breaker (DG)	Status: Open/Closed	Observability Mandatory
Macrogroup generation			
Availability for macrogroup control	Availability of the generation macrogroup to operate the control functions	Status: Available/Not Available	Observability Mandatory
Operating status of the single generating unit (SGG)	Indicates whether the single generating unit (SGG) is operating or not	Status: Operating/Not-Operating	Observability Mandatory
Single generating unit identifier (SGG)	Number Identifier of the single generating unit (SGG)	Numeric code	Observability Mandatory
Macrogroup storage systems			
Availability for macrogroup control	Availability of the storage system to operates the control functions	Status: Available/Not Available	Observability Mandatory
Operating status of the storage system	Indicates whether the storage system, is operating or out of service	Status: Operating/Not-operating	Observability Mandatory

T.3.1.3 Information on measurements of electrical quantities of the installation

CCI acquires measurements from field devices, if the data is available, or through its own sensors.

The measurements to be handled by the CCI are listed below in Table 84. Power measurement information is expressed by a unified vector containing the quantities listed in Table 80.

Table 84 – Measurements

Information	Description	Unit of measuremente Unità di misura	Presence
Point of delivery			
Active power	Value with sign of active power	kW	Observability Mandatory
Reactive power	Value with sign of reactive power	kVAr	Observability Mandatory
Voltages	Value of phase-to-phase voltages	kV	Observability Mandatory
Currents of phases	Value of phase-to-phase voltage	A	Observability Optional
Generation aggregates (Photovoltaic/Wind/Thermal/Hydroelectric)			
Active power	Signed value of active power Total value of the active power produced by generators with the same primary energy source (photovoltaic/wind/thermal/hydroelectric). A separate value shall be provided according to the primary source.	kW	Observability Mandatory
Storage systems (equivalent to generation aggregates)			
Active power	Value with sign of active power	kW	Observability Mandatory
Single generation group (Photovoltaic/Wind/Thermal/Hydroelectric)			
Active power	Value with sign of active power	kW	Observability Mandatory
Storage System (equivalent to Single Generation Group)			
Active power	Value with sign of active power	kW	Observability Mandatory

T.3.1.4 Information of plant operating parameters

This type of information allows the parameters associated with the system's operating modes to be set. The activation of an operating mode shall only take place if the operating conditions of the system allow the set operating parameters to be fulfilled. There can be more than one operating mode that can potentially be activated, if they are functionally compatible.

If an operating mode is already active, changing one of its parameters causes the setting to change to conform to the new setting.

T.3.1.4.1 Control function - Limitation of Active Power

Table 85 below specifies information on the configuration and status of the function that implements the limitation of the active power that can be injected into the grid.

Table 85 – Parameters of the "Active power limitation" function

Parameter	Units of measurement	Range	Reference	Default value	Presence
Operating status	-	1 = Operating/ 5 = Not-Operating	-	5	Control Optional
Active power limit in generation mode	%	0..100	Maximum apparent system power S_{max}	0	Control Optional
Activation command	–	5 = Inactive, 1 = Active	–	5	Control Optional
Status of Setpoint function from DSO	–	0= Not available / 1 = Autonomous/ 2 = Automatic(Priority) Automatic	–	1	Control Optional
Limit function status of P 110%	–	0=Not available / 1=Autonomous;	–	2	Control Optional

T.3.1.4.2 Control Function - Modulation of Active Power

Table 86 below specifies information on the configuration and status of the function that, on command from the DSO, implements modulation of the active power that can be exchanged with the network.

Table 86 – Parameters of the 'Active Power Modulation' function

Parameter	Units of measurement	Range	Reference	Default value	Presence
Operating status	–	1 = Operating/ 5 = Not-Operating	–	5	Control Optional
feed-in and feed-out active power setpoints	%	0..100 (+ = feed-in, - = feed-out)	Maximum apparent system power S_{max}	100 / 0	Control Optional
Activation command	–	5 = Inactive, 1 = Active	-	5	Control Optional
Function status	–	0= Not available / 2 = Automatic (Priority)	–	2	Control Optional
Feed-in active power means the power that the plant injects into the grid. Feed-out active power means the power that the plant absorbs from the grid.					

T.3.1.4.3 Control Function - Active Power Set-Point Function

The following Table 87 specifies the configuration and status information of the function which, based on market signals, implements the setpoint of the active power that can be exchanged with the grid.

Table 87 – Parameters of the 'Active Power Setpoint' function

Parameter	Units of measurement	Range	Reference	Valore di default	Presence
Operating status	–	1 = Operating/ 5 = Not-Operating	–	5	Participation in MSD Discretionary
feed-in and feed-out active power setpoints	%	0..100 (+ = feed-in, - = feed-out)	Maximum apparent system power Smax	100 / 0	Participation in MSD Discretionary
Activation command	–	5 = Inactive, 1 = Active	–	5	Participation in MSD Discretionary
Function status	–	0= Not available/ 2 = Automatic (Priority)	–	2	Participation in MSD Discretionary
Feed-in active power means the power that the plant injects into the grid. Feed-out active power means the power that the plant absorbs from the grid.					

T.3.1.4.4 Control function - Voltage control mode with Reactive Power supply

Table 88 below specifies information on the configuration and status of the function which, at the Distributor's command, implements voltage regulation with delivery of capacitive or inductive reactive power that can be exchanged with the grid.

Table 88 – Parameters of the "voltage control mode with reactive power supply" function

Parameter	Units of measurement	Range	Reference	Default value	Presence
Operating status	–	1 = Operating/ 5 = Not-Operating	–	5	Control Optional
Feed-in and feed-out of reactive power	%	0..100 (+ = Capacitive, - = Inductive)	Maximum apparent system power Smax	0 / 0	Control Optional
Activation command	-	5 = Inactive, 1 = Active	–	5	Control Optional
Function status	–	0= Not available / 2 = Automatic (Priority)	–	2	Control Optional
Feed-in reactive power means the power that the plant injects into the grid through the overexcited operation of the generators (capacitor system behavior). Feed-out reactive power means the power that the plant absorbs from the grid through the under-excited operation of the generators (system behavior as an inductor).					

T.3.1.4.5 Control Function - Reactive Power Set-point Function

Table 89 specifies the configuration and status information of the function which, based on market signals, implements the setpoint of capacitive and inductive reactive power that can be exchanged with the grid.

Table 89 – Parameters of the "Setpoint Reactive Power" function

Parameter		Units of measurement	Range	Riferimento	Default value	Presence
Operating status		–	1 = Operating/ 5 = Not-Operating	–	5	Participation in MSD Discretionary
Feed-in and feed-out of reactive power		%	0..100 (+ = Capacitive, - = Inductive)	Maximum apparent system power S_{max}	0 / 0	Participation in MSD Discretionary
Activation command		–	5 = Inactive, 1 = Attiva	–	5	Participation in MSD Discretionary
Function status		–	0= Not available/ 2 = Automatic (Priority)	–	2	Participation in MSD Discretionary
Feed-in reactive power means the power that the plant injects into the grid through the overexcited operation of the generators (capacitor system behavior). Feed-out reactive power means the power that the plant absorbs from the grid through the under-excited operation of the generators (system behavior as an inductor).						

T.3.1.4.6 Control Function - Reactive Power Control at a fixed Power Factor

The following Table 90 specifies the configuration and status information of the function implementing the power factor setpoint.

Table 90 – "Setpoint Power Factor" Function Parameters

Parameter		Units of measurement	Range	Reference	Default value	Presence
Operating stataus		–	1 = Operating / 5 = Not-Operating	–	5	Control Optional
Cosϕ setpoint in case of active power generation		P.U.	-1.00..+1.00 (+ = Capacitive, - = Inductive)	–	-0.95	Control Optional
Cosϕ setpoint in case of active power absorption		P.U.	-1.00..1.00 (+ = Capacitive, - = Inductive)	–	0.95	Control Optional
Activation command		–	5 = Inactive, 1 = Attiva	–	5	Control Optional
Function status		–	0= Not available / 1 = Autonomus / 2 = Automatic (Priority)	-	1	Control Optional
The value of reactive power to be exchanged with the grid is to be determined by considering the absolute value of the imposed power factor. The sign associated with the power factor determines whether the reactive power is fed in through over-excitation operation of the generators (capacitor system behaviour) or absorbed by the grid through under-excitation operation of the generators (inductor system behaviour).						

T.3.1.4.7 Reactive Power control according to the curve Q=f(V)

Table 91 *[It is Table 92 in Italian version]* below specifies information on the configuration and status of the function implementing reactive power tuning with respect to the voltage value at the point of connection.

Table 91– Function parameters "Q(V)"

Parameter	Units of measure ment	Range	Reference	Default value	Presence
Operating status	–	1 = Operating / 5 = Not-Operating	–	5	Control Optional
Activation command	-	5 = Inactive, 1 = Active	–	5	Control Optional
Function status	–	0= Not available / 1 = Autonomus / 2 = Automatic (Priority)	–	1	Control Optional
K	–	-1.00..1.00	–	0	Control Optional
Active power lock-in	P.U.	0.00..max	Nominal Active Power	0.20	Control Optional
Active power lock-out	P.U.	0.00..max	Nominal Active Power	0.05	Control Optional
V higher than 1	P.U.	0.00..max	Nominal voltage at PdC	1.08	Control Optional
V less than 1	P.U.	0.00..max	Nominal voltage at PdC	0.92	Control Optional
V higher than 2	P.U.	0.00..max	Nominal voltage at PdC	1.10	Control Optional
V less than 2	P.U.	0.00..max	Nominal voltage at PdC	0.90	Control Optional

T.3.1.4.8 Reactive Power Control with Power Factor depending on the Active Power

Table 92 below specifies information on the configuration and status of the function that implements power factor tuning considering the active power value at the point of delivery.

Table 92 – Parameters of the "cosφ (P)" function

Parameter	Units of measure ment	Range	Reference	Default value	Presence
Operating stataus	–	1 = Operating/ 5 = Not-Operating	–	5	Control Optional
Activation command	–	5 = Inactive, 1 = Active	–	5	Control Optional
Function status	–	0= Not available/ 1 = Autonomus/ 2 = Automatic (Priority)	–	1	Control Optional
P-value (point A)	P.U	0.00..max	Nominal Active Power	0.20	Control Optional

Parameter	Units of measure ment	Range	Reference	Default value	Presence
Cosϕ-value (point A)	P.U.	-1.00..-0.1 +0.1..1.00 (+ = Capacitive, - = Inductive)	–	1.00	Control Optional
P-value (point B)	P.U	0.00..max	Nominal Active Power	0.50	Control Optional
cosϕ-value (point B)	P.U.	-1.00..-0.1 +0.1..1.00 (+ = Capacitive, - = Inductive)	–	1.00	Control Optional
P-value (point C)	P.U	0.00..max	Nominal Active Power	1.00	Control Optional
cosϕ-value (point C)	P.U.	-1.00..-0.1 +0.1..1.00 (+ = Capacitive, - = Inductive)	–	0.95	Control Optional
Voltage Lock-in	P.U.	1.00..1.10	Nominal voltage at PdC	1.05	Control Optional
Voltage Lock-out	P.U.	0.90..1.00	Nominal voltage at PdC	0.98	Control Optional

T.3.2 Definition of technical requirements associated with CCI interface

T.3.2.1 Communication modes

The complete set of information related to the functional requirements of CCI as set out in Annex O shall be made available to DSO.

The actor acting as Aggregator will only have access to the information functional to participation in MSD.

The exchange of information may take place on request, or on a periodic basis or by variation of the value of a parameter, possibly providing for a tolerance band. Information may be requested or sent individually or by homogeneous groups.

Where not otherwise specified, T.1 shall be considered.

For the evaluation of communication performance:

- within the substation by IEC 61850-5 "Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models" and
- between substations by IEC 61850-90-1 Ed.1.0 “Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations”,

consider that the information is essentially exchanged between a Client device (e.g. SCADA or central network evaluation system) and Server (CCI); for this type of information flow, the expected performance is “low speed messages” with transit times between end-points in the order of 500 ms when inside the substation. Outside the substation, on the other hand, these types of exchanges are not catalogued. Furthermore, as far as the measurements published periodically by the ICC are concerned, the communication is not merely IEC 61850, as the user (TSO), through DSO, uses different IEC standards. Table 95 prescribes the expected performance based on the type of information.

Table 93 – Communication mode

Information type	Mode of sending the message	Performance (where applicable according to IEC 61850-5)	Presence
Plant features	upon request	Type 3 - Low speed messages	Observability Mandatory
Plant operating status	upon request and variation	Type 3 - Low speed messages	Observability Mandatory
Measures of plant	periodic 4 s	Type 3 - Low speed messages	Observability Mandatory
Operating parameter values	upon request and variation	Type 3 - Low speed messages	Control Optional

The latencies associated with the power Setpoint are required as Performance Class Type 3.

Although the CCI is not expected to expose a GOOSE interface, this device shall be able to subscribe GOOSE messages regarding control functions (according to "CCI System Outline with Related Functional Interfaces" in Annex O); any developments in information exchanges with high-speed services are required as Performance Class Type 1.

T.3.2.2 Definition of access rules for IEC 61850 services of the CCI IED

To implement service access rules differentiated according to the role of the actor connecting to the IEC 61850 server, it is necessary to identify the relevant authorisation methods in accordance with IEC 62351 (see Subclause T.3.3.4.3).

T.3.3 Technology solution for implementing the interface according to IEC 61850 associated with the CCI

This Subclause defines the technological solution to be adopted in terms of Data Model, Services, mapping to a specific protocol and cybersecurity requirements, to implement the CCI device compliant with the requirements defined in the previous chapters.

T.3.3.1 IEC 61850 data model of information associated with the CCI

In the implementation of the IEC 61850 data model corresponding to the information identified in the previous section, an attempt was made to use as far as possible objects already defined in the standard, with reference to IEC 61850-7-4 "Communication networks and systems for power utility automation - Part 7-4: Basic communication structure -Compatible logical node classes and data object classes" or DER-specific volumes (e.g. IEC 61850-7-420 Ed.2.0 "Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes").

The parameters identifying the version of this namespace are:

- Namespace Version: 2022
- Namespace Revision: 1
- UML model file which reflects this namespace edition: N.A.
- Namespace release date:1-04-2022
- Namespace name: “(Tr) IEC 61850-CEI016:2022”.

Note that the 'M/O/C' (presence condition) attribute of the elements constituting a Common Data Class or a Logical Node has been extended by adding the attributes formalized in the following Table:

Table 94 – Presence of data in the model

Attribute	Description
M = Mandatory	Mandatory data prescribed by the standard
O = Optional	Optional data provided by the standard
C = Conditional	Data available according to conditions set by the standard
R = Required	Datum standardized as O/C by IEC 61850 but required to enable the functions in the Annex O
E = Extension	The information is an extension as Not available in the standard and is required to enable the functions in Annex O
F = Forbidden	The information is not applicable for the uses envisaged by the presence condition (normally specified in connection with statistical uses of the information)

The profile, for the sake of simplicity of the data model, is characterized by a single Logical Device:

Table 95 – CCI Logical Device

Logical Device	Description
LD_Plant	Contains all Logical Nodes related to the system (combination of generators and energy storage systems)

To differentiate between the various installation sections, a different prefix (hereafter prefix) will be used for each section. The prefix will be placed before the name of each logical node within the Data Object LNName, to indicate the installation section to which the node refers. It will be used:

Table 96 – LN prefix for specific installation sections

Prefix	Description
Global	Data models for the installation as a whole
St	Storage system data models
GenPV	Photovoltaic generator data models
GenWi	Wind turbine data models
GenTer	Thermal generator data models
GenIdr	Hydro generator data models

In the following, the information will be modelled through the "Logical Nodes (LN)"; therefore, some Tables will be taken directly from IEC 61850; they will be followed by a further detail Table to better define the relevant information (prescribed set of data) of the single Data Objects (DO), possibly specifying the main Data Attribute (DA), used in the information exchange of CCI.

Note that LN-specific DOs/DAs and those inherited from the Common Logical Node Class shall only be mentioned and detailed if explicitly used in the information exchange required to fulfil the requirements expressed in the previous Subclauses. Of course, data models considered mandatory by the standard shall be implemented in the model of the CCI.

The data modelled by LN/DO in the following Subclauses, where required by the IEC 61850 standard, shall also be transmitted including the associated DAs of “q” (quality) and “t” (time stamp).

There are three separate sections dedicated to data models relating to:

- Observability,

- Control (entirely Optional),

- Participation in the Dispatching Services Market (entirely Discretionary).

T.3.3.1.1 Observability Data Models

The data models specified in the Observability section, unless otherwise specified, are mandatory.

T.3.3.1.1.1 Logical node zero

The logical node LLN0 shall be present as stated in IEC 61850-7-4.

T.3.3.1.1.2 Physical device information

LPHD logical node (from IEC 61850-7-4) is used to identify CCI

LPHD class – type LPHD1				
Data object name	**CDC**	**Explanation**	**T**	**M/O/C**
…	…	…		…
PhyNam	DPL	Physical device name plate		M
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
PhyNam	vendor	CCI producer	123456
	swRev	CCI software version	V02.00
	location	Connection Point Identifier (POD)	IT000E123456789

T.3.3.1.1.3 Operating Characteristics at the Connection Point

The logical nodes DPCC (4 instances) and DGEN are used to define the operating data that characterize the overall system at PdC.

For the complete list of Data Objects, refer to IEC 61850-7-420.

Maximum active power input

DPCC class – type DPCC1 - prefix PdC_Wi				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
WRtg	ASG	(inherited from: PhysicalElectricalConnectionPointLN) Electrical active power rating at ECP		R/F
…	…	…		…

In addition to all LN mandatory DOs, those selected above (minimum set of nameplate data at the PdC) shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
WRtg	setMag	Connection point - Maximum active power feed	200 kW

Maximum active power in absorption

DPCC class – type DPCC1 - prefix PdC_Wa				
Data object name	CDC	Explanation	T	**PresCond nds/ds**
…	**…**	**…**		**…**
WRtg	ASG	(inherited from: PhysicalElectricalConnectionPointLN) Electrical active power rating at ECP		R/F
…	**…**	**…**		**…**

In addition to all LN mandatory DOs, those selected above (minimum set of nameplate data at the PdC) shall be implemented in the model capability of CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
WRtg	setMag	Connection point - Maximum active power feed	200 kW

Maximum inductive reactive power

DPCC class – type DPCC2 - prefix PdC_Qi				
Data object name	**CDC**	**Explanation**	**T**	PresCond nds/ds
…	…	…		…
VArRtg	ASG	(inherited from: PhysicalElectricalConnectionPointLN) Reactive power rating at ECP		R/F
…	…	…		…

In addition to all LN mandatory DOs, those selected above (minimum set of nameplate data at the PdC) shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
VArRtg	setMag	Connection point - Maximum inductive reactive power	50 kVAr

Maximum capacitive reactive power

DPCC class – type DPCC2 - prefix PdC_Qc				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
VArRtg	ASG	(inherited from: PhysicalElectricalConnectionPointLN) Reactive power rating at ECP		R/F
…	…	…		…

In addition to all LN mandatory DOs, those selected above (minimum set of nameplate data at the PdC) shall be implemented in the model capability of CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
VArRtg	setMag	Connection point - Maximum capacitive reactive power	50 kVAr

Maximum apparent system power Smax

DPCC class – type DPCC3 - prefix PdC_VA				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
VARtg	ASG	(inherited from: PhysicalElectricalConnectionPointLN) Apparent power rating at ECP		R/F
…	…	…		…

In addition to all LN mandatory DOs, those selected above (minimum set of nameplate data at the PdC) shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
VARtg	setMag	Connection point - Maximum apparent system power Smax	210 **kVA**

T.3.3.1.1.4 Power Plant Control Function

The logical node DECP is used to represent the availability of the system to operate the control functions.

For the complete list of Data Objects, refer to IEC 61850-7-420.

DECP class – type DECP1 - prefix DisFR				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
Beh	ENS	(inherited from: DomainLN) Read-only value, describing the behaviour of a domain logical node. [...]		M / M
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
Beh	stVal	Installation ready to operate the adjustment functions [1 = Available, 5 = Not available]	Available

T.3.3.1.1.5 Control of Generation Macrogroup

DGEN logical node is used to represent the readiness of the generation macrogroup to operate the control functions.

For the complete list of Data Objects refer to IEC 61850-7-420.

DGEN class – type DGEN1 - prefix DisFR				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
Beh	ENS	(inherited from: DomainLN) Read-only value, describing the behaviour of a domain logical node. [...]		M / M
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
Beh	stVal	Generation macrogroup ready to operate the adjustment functions [1 = Available, 5 = Not available]	Available

T.3.3.1.1.6 Control of storage macrogroup

The logical node DSTO is used to represent the availability of the storage macrogroup to operate the control functions.

For the complete list of Data Objects, refer to IEC 61850-90-9 (Ed.1.0).

DSTO class – type DSTO1 - prefix DisFR				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
...	...	...		...
Beh	ENS	inherited from: DomainLN		M / M
...	...	...		...

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
Beh	stVal	Storage macrogroup ready to operate the adjustment functions [1 = Available, 5 = Not available]	Available

T.3.3.1.1.7 Plant measurements

The MMXU (multi-installation) logical node is used to represent the measurements of the plant both at the PdC and, where present, of the individual generation and storage types.

In Annex O, measurements for the estimation of the power flows of the MV grid are provided every 4 sec:

- P, Q, V at connection point (phase currents I are optional);
- P per single generation source and storage where applicable.
- P for single generation unit.
- For the complete list of Data Objects, refer to IEC 61850-7-4.P, Q, V in the connection point (optional line currents I);

Measurements at every 4 seconds at the connection point

MMXU class – type MMXU1 - prefix PdC				
Data object name	**CDC**	**Explanation**	**T**	**M/O/C**
...	...	...		...
TotW	MV	Total active power (total P)		R
TotVAr	MV	Total reactive power (total Q)		R
PPV	DEL	Phase to phase voltages (VL1, VL2, ...)		R
...	...	...		...
A	WYE	Phase currents (IL1, IL2, IL3)		O
...	...	...		...

In addition to all the mandatory DOs of the LN, those selected above (minimum set of measurements required from the PdC) shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
TotW	mag	Connection point - total instantaneous active power (the information conveyed to the DSO may optionally be made available to the Aggregator)	198 kW
TotVAr	mag	Connection point - total instantaneous reactive power	-45 kvar
PPV	mag	Connection point - line voltages (VL1L2, VL2L3, ...)	20000V, 20002V, 19993V
A	mag	(Opt.) Connection point – phase currents (IL1, IL2, IL3)	100A, 101A, 99A

Aggregated measures for single source every 4 sec:

MMXU class – type MMXU2 - prefix GenXX (type of generator, as specified in 0)				
Data object name	**CDC**	**Explanation**	**T**	**M/O/C**
...	...	...		...
TotW	MV	Total active power (total P)		R
...	...	...		...

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
TotW	mag	Photovoltaic / Wind/ Thermal / Hydro – instantaneous active power	189 kW

Aggregated measures for Storage System every 4 sec:

MMXU class – type MMXU2 - prefix St				
Data object name	**CDC**	**Explanation**	**T**	**M/O/C**
...	...	...		...
TotW	MV	Total active power (total P)		R
...	...	...		...

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
TotW	mag	Storage System – instantaneous active power	189 kW

Measurements for Single Generation Group aevery 4 sec (multi-instances with N= 1..99)

MMXU class – type MMXU2 - prefix SGG				
Data object name	**CDC**	**Explanation**	**T**	**M/O/C**
...	...	...		...
TotW	MV	Total active power (total P)		R
...	...	...		...

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
TotW	mag	Single generating unit (n) – Istantaneous active power	189 kW

T.3.3.1.1.8 Operating state of the plant - position of the breakers

The XCBR logic node is used to represent the position of the breaker (Open/Closed) of the main power plant breaker for separating the overall electric system (plant) from the grid.

Please refer to IEC 61850-7-4 for the complete list of Data Objects.

Main Power Plant Breaker*Position*

XCBR class – type XCBR1 - prefix IDG				
Data object name	**CDC**	**Explanation**	**T**	**M/O/C**
…	…	…		…
Pos	DPC	Switch position		M
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
Pos	stVal	Main Power Plant breaker position [intermediate-state | off | on | bad-state]	Chiuso Closed

T.3.3.1.1.9 Operating status of the plant - single generating unit

The DGEN (multi-instances) logical node is used to represent the operating status of each generation unit (Operating/Not-Operating) and is multi-instantiated (with N= 1..99).

For the complete list of Data Objects, please refer to IEC 61850-7-420.

DGEN class – type DGEN2 - prefix SSGG				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
Health	ENS	(inherited from: DomainLN) Reflects the state of the logical node related hardware and software. [...]		R / O
…	…	…		…
GnGrId	INS	CEI 0-16 Specific		E / F
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
Health	stVal	Single Generating Unit (N) - Operating Status Multi-installable with N= 1..99 [1 = Operating, 3 = Not-Operating	Operating
GnGrId	stVal	Single Generating Unit Identification Number (N)(N) [1..99]	17

T.3.3.1.2 Control Data Models (Optional)

The Control section is optional and additional to the Observability model specified in T.3.3.1.1. If implemented, the presence of data (M/O/C/R/E) follows the rules specified in Table 94.

The operation of CCI control functions is characterized by the states specified in Table 97.

Table 97 – Operation of control functions

DO	FctOpSt (Status info to remote enabled actor)	Mod (Configuration by remote enabled actor)	Beh (Status info to remote enabled actor)	Operating Status	Notes
Value	Autonomous	Active	Operating	Operating = ACT	Function configured to operate according to local logics. This function is always Autonomous, irrespective of the connection with remote enabled actors
			Not Operating	Active = ON	
		Inactive	Not Operating	Rest (Inactive) = OFF	

DO	FctOpSt (Status info to remote enabled actor)	Mod (Configuration by remote enabled actor)	Beh (Status info to remote enabled actor)	Operating Status	Notes
	Automatic	Active	Operating	Operating = ACT	Function capable of operating according to a remote setpoint when a communication channel is available. When the CCI is connected at least with the DSO (high priority), the function is Automatic; in case of complete loss of communication, for functions that support it, it becomes autonomous.
			Not Operating	Active = ON	
		Inactive	Not Operating	Rest (Inactive) = OFF	
	Not available	N.A.	Not Operating	Rest (Inactive) = OFF	

T.3.3.1.2.1 Control Function - Limitation of Active Power

The DWMX logic node is used to perform configuration/setting and to represent the status of the P-limit control function.

Refer to IEC 61850-7-420 for the complete list of Data Objects.

DWMX class – type DWMX1 - prefix Wlim				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
Beh	ENS	(inherited from: DomainLN) Read-only value, describing the behavior of a domain logical node. […]		M / M
…	…	…		…
WMaxSptPct	APC	Setpoint reflecting the maximum limit of generated active power as a percentage of Maximum Active Power capability, WMax at the Referenced ECP. Its mxVal attribute reflects the value of the setpoint that is requested.		R / O
…	…	…		…
Mod	ENC	(inherited from: DomainLN) (controllable) Operating mode of the domain logical node that may be changed by operator. Processing of the quality status ('q') of the received data is the prerequisite for correct interpretation of the operating mode.		R / O
FctOpStAuto	ENS	CEI 0-16 specific		E / F
FctOpStEx	ENS	CEI 0-16 specific		E / F
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
Beh	stVal	Operating status of the active power limit function [1 = Operating, 5 = Not-Operating]	Operating
WMaxSptPct	ctlVal	Active power limit setpoint in generation (%, compared to maximum apparent system power S_{max}) - value[0..100]	20
	origin	Active power limit setpoint in generation (%, compared to maximum apparent system power S_{max}) – identity of the authorised actor orCat = [automatic-station, remote-control]; orIdent = [DSO, AGGREGATORE]	automatic-station DSO
Mod	ctlVal	Activation/deactivation of operating mode - active power limit - only on signal from DSO - value [5 = Inactive, 1 = Active]	Attiva
	origin	Activation/deactivation of operating mode - active power limit - only on signal from DSO – identity of the authorised actor orCat = [automatic-station, remote-control]; orIdent = [DSO, AGGREGATORE]	automatic-station DSO
FctOpStAuto	stVal	Active power limit function status (internal for V close to 110%) [Not available / Autonomous]	Autonomous
FctOpStEx	stVal	Active power limit function status (on external signal from DSO) [Not available/Autonomous/Automatic (priority mode)]	Autonomous

T.3.3.1.2.2 Control Function - Modulation of Active Power

The DAGC logic node is used to perform configuration/setting and to represent the status of the active power feeded-in/feeded-out at PoC when the command is sent by the DSO.

For the complete list of Data Objects refer to IEC 61850-7-420.

DAGC class – type DAGC1 - prefix WSd				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
Beh	ENS	(inherited from: DomainLN) Read-only value, describing the behavior of a domain logical node. […]		M / M
…	…	…		…
WSptPct	APC	(inherited from: ActivePowerLN) Active power setpoint setting as a percentage of Maximum Active Power capability, WMax at the Referenced ECP, and in the case of signed setpoint (typically for storage systems) as a percentage of Maximum Active Power charging (consuming) capability for values related to the charging phase. Its mxVal attribute reflects the value of the setpoint that is requested..		R / O
Mod	ENC	(inherited from: DomainLN) (controllable) Operating mode of the domain logical node that may be changed by the operator. Processing of the quality status ('q') of the received data is the prerequisite for correct interpretation of the operating mode.		R / O

DO name	DA name	Meaning	Example	
FctOpSt	ENS	CEI 0-16 specific		E / F
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
Beh	stVal	Operating status of the tuning function of the feed-in/feed-out active power at the PoC (on external command from the DSO) [1 = Operating, 5 = Not-Operating]	Operating
WSptPct	ctlVal	Setpoint tuning of active power feed-in/feed-out at the PoC (percentage, with sign, in relation to the Maximum apparent system power Smax) on external command from the DSO - value [-100..+100]	20
	origin	Setpoint tuning of active power feed-in/feed-out at the PoC (percentage, with sign, with respect to maximum apparent system power Smax) on external command from the DSO - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR].	automatic-station DSO
Mod	ctlVal	Activation/deactivation of operating mode - tuning of active power feed-in/feed-outat the PoC on external command from the DSO - value [5 = Inactive, 1 = Active].	Active
	origin	Activation/deactivation of operating mode - tuning of active power feed-in/feed-out to the PoC on external command from the DSO - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR].	automatic-station DSO
FctOpSt	stVal	Tuning function status of the active power feed-in/feed-outat the PoC (on external command from the DSO) [Not available/Automatic (priority mode)].	Automatic

T.3.3.1.2.3 Control function - Voltage control mode with Reactive Power

The logic node DVAR is used to perform configuration/tuning and to represent the status of the voltage tuning function with inductive/capacitive reactive power output on external command from DSO.

For the complete list of Data Objects refer to IEC 61850-7-420.

DVAR class – type DVAR1 - prefix VArSd				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
Beh	ENS	(inherited from: DomainLN) Read-only value, describing the behavior of a domain logical node. […]		M / M
…	…	…		…
VArTgtSptPct	APC	(inherited from: ReactivePowerLN) Target reactive power setpoint expressed as percent as indicated by VArSetRef. Its mxVal attribute reflects the value of the setpoint that is requested.		R / O
Mod	ENC	(inherited from: DomainLN) (controllable) Operating mode of the domain logical node that may be changed by operator. Processing of the quality status ('q') of the received data is the prerequisite for correct interpretation of the operating mode.		R / O
FctOpSt	ENS	CEI 0-16 specific		E / F
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	**DA name**	**Meaning**	**Example**
Beh	stVal	Operating status of the voltage tuning function with inductive/capacitive reactive power supply on external command from the DSO [1 = Operating, 5 = Not-Operating]	Operating
VArTgtSptPct	ctlVal	Setpoint of the voltage tuning function with inductive/capacitive reactive power output (percentage, with sign, compared to the Maximum apparent system power Smax) on external command from the DSO – value [-100..+100]	20
	origin	Setpoint of the voltage tuning function with inductive/capacitive reactive power supply (percentage, with sign, compared to the maximum apparent system power Smax) on external command from the DSO - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR].	automatic-station DSO
Mod	ctlVal	Activation/deactivation of operation mode - voltage tuning with inductive/capacitive reactive power supply on external command from DSO - value [5 = Inactive, 1 = Active]	Attiva
	origin	Activation/deactivation of operation mode - voltage tuning with inductive/capacitive reactive power supply on external command from the DSO - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR].	automatic-station DSO
FctOpSt	stVal	Inductive/Capacitive reactive power exchange set point status (V control operation with Q exchange) on external command from DSO [Not available/Automatic (priority mode)].	Automatic

T.3.3.1.2.4 Control Function - Reactive Power Control at a fixed Power Factor

The logical node DFPF is used to perform configuration/setting and to represent the status of the cosϕ set point control function.

For the complete list of Data Objects, please refer to IEC 61850-7-420.

DFPF class – type DFPF1 - prefix PFSP				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
Beh	ENS	(inherited from: DomainLN) Read-only value, describing the behavior of a domain logical node. […]		M / M
…	…	…		…
PFGnTgtSpt	APC	Target power factor setpoint when generating. [...]		M / O
…	…	…		…
PFLodTgtSpt	APC	Target power factor setpoint when acting as a load (consuming, charging). [...]		R / O
Mod	ENC	(inherited from: DomainLN) (controllable) Operating mode of the domain logical node that may be changed by operator. Processing of the quality status ('q') of the received data is the prerequisite for correct interpretation of the operating mode.		R / O
FctOpSt	ENS	CEI 0-16 specific		E / F
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	**DA name**	**Meaning**	**Example**
Beh	stVal	Operating state of the PF set point function (Operation in Q supply with constant cosϕ) [1 = Operating, 5 = Not-Operating].	Operating
PFGnTgtSpt	ctlVal	Cosϕ setpoint in case of active power generation – value [-1.00..0.00]	-0.95
	origin	cosϕ setpoint in the case of active power generation - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR]	automatic-station DSO
PFLodTgtSpt	ctlVa	Cosϕ setpoint in case of active power consumption –value [0.00..1.00]	0.95
	origin	Cosϕ setpoint in case of active power consumption - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR]	automatic-station DSO

DO name	DA name	Meaning	Example
Mod	ctlVal	Activation/deactivation of operating mode - PF set point (Q operation with constant cosϕ) - value [5 = Inactive, 1 = Active].	Attiva
	origin	Activation/deactivation of operating mode - cosϕ set point (Q operation with constant cosϕ) - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR].	automatic-station DSO
FctOpSt	stVal	PF set point function status (Operation in Q supply with constant cosϕ) [Not available / Autonomous / Automatic (priority mode)].	Autonomus

T.3.3.1.2.5 Control Function - Reactive Power control according to the curve Q=f(V)

The logical nodes DVVR, DPMC (2 instances) and DECP (2 instances) are used to perform configuration/setting and to represent the status of the Q(V) control function.

Refer to IEC 61850-7-420 for the complete list of Data Objects.

DVVR class – type DVVR1 - prefix VArV				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
Beh	ENS	(inherited from: DomainLN) Read-only value, describing the behaviour of a domain logical node. […]		M / M
Mod	ENC	(inherited from: DomainLN) (controllable) Operating mode of the domain logical node that may be changed by operator. Processing of the quality status ('q') of the received data is the prerequisite for correct interpretation of the operating mode.		R / O
FctOpSt	**ENS**	**CEI 0-16 specific**		**E/F**
K	**ASG**	**CEI 0-16 specific**		**E/F**
…	**…**	**…**		**…**

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
Beh	stVal	Operating state of the Q(V) function (Operation in automatic supply of Q according to the curve Q=f(V) [1 = Operating, 5 = Not-Operating].	Operating
Mod	ctlVal	Activation/deactivation of the Q(V) function (Operation in automatic supply of Q according to curve Q=f(V)) - value [5 = Inactive, 1 = Active].	Attiva
	origin	Activation/deactivation of the Q(V) function (Operation in automatic supply of Q according to the curve Q=f(V)) - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR].	automatic-station DSO
FctOpSt	stVal	Q(V) function status (Operation in automatic Q delivery according to curve Q=f(V)) [Not available /Autonomous /Automatic (priority mode)]	Autonomus
K	setMag	Q(V) Function K parameter [-1.00..1.00]	0.00 (for Photovoltaics and Storage)

DPMC class – type DPMC1 - prefix VArV – Instance 1				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
WSpt1	APC	Active power setpoint. Its mxVal attribute reflects the value of the setpoint that is requested.		R / O
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
WSpt1	ctlVal	Active Power Lock-in of function Q(V) - value [0.00..max] of the $P_{Nominal}$ (P.U.)	0.20
	origin	Active Power Lock-in of the Q(V) function - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR]	automatic-station DSO

DPMC class – type DPMC1 - prefix VArV – Instance 2				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
WSpt1	APC	Active power setpoint. Its mxVal attribute reflects the value of the setpoint that is requested.		R / O
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
WSpt1	ctlVal	Active Power Lock-outof function Q(V) – value [0.00..max] of the $P_{Nominal}$ (P.U.) [0.00..max] of $P_{Nominal}$ (P.U.)	0.05
	origin	Active Power Lock-outof the Q(V) function - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR]	automatic-station DSO

DECP class – type DECP2 - prefix VArV – Instance 1				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
VMax	ASG	(inherited from: PhysicalElectricalConnectionPointLN) Rated maximum voltage		R / F
VMin	ASG	(inherited from: PhysicalElectricalConnectionPointLN) Rated minimum voltage		R / F
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
VMax	setMag	Upper voltage 1 of function Q(V) [0.00..max] of $V_{Nominal}$ (P.U.)	1.08
VMin	setMag	Lower voltage 1 of function Q(V) [0.00..max] of $V_{Nominal}$ (P.U.)	0.92

DECP class – type DECP2 - prefix VArV – Instance 2				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
VMax	ASG	(inherited from: PhysicalElectricalConnectionPointLN) Rated maximum voltage		R / F
VMin	ASG	(inherited from: PhysicalElectricalConnectionPointLN) Rated minimum voltage		R / F
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following Meaning:

DO name	DA name	Meaning	Example
VMax	setMag	Q(V) function voltage upper threshold 2 [0.00..max] of (P.U.)	1.10
VMin	setMag	Q(V) function voltage lower threshdol 2[0.00..max] of $V_{Nominal}$ (P.U.)	0.90

T.3.3.1.2.6 Control function - Reactive Power Control with Power Factor depending on the Active Power

The DPFW logic node was specially created to perform configuration/setting and to represent the state of the cosϕ = f(P) control function (operation with cosϕ control as a function of P).

DPFW class – type DPFW1 - prefix PFW				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
Descriptions				
NamPlt	LPL	(inherited from: DomainLN) Name plate of the logical node.		MONamPlt / MONamPlt
Status Information				
Beh	ENS	(inherited from: DomainLN) Read-only value, describing the behaviour of a domain logical node. […]		M / M
FctOpSt	ENS	CEI 0-16 specific		M / F
Controls				
Mod	ENC	(inherited from: DomainLN) (controllable) Operating mode of the domain logical node that may be changed by operator. Processing of the quality status ('q') of the received data is the prerequisite for correct interpretation of the operating mode.		R / O
Settings				
WSetA	ASG	CEI 0-16 specific		M / F
PFSetA	ASG	CEI 0-16 specific		M / F
WSetB	ASG	CEI 0-16 specific		M / F
PFSetB	ASG	CEI 0-16 specific		M / F
WSetC	ASG	CEI 0-16 specific		M / F
PFSetC	ASG	CEI 0-16 specific		M / F
VLkIn	ASG	CEI 0-16 specific		M / F
VLkOut	ASG	CEI 0-16 specific		M / F

The following DOs shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
Beh	stVal	Operating state of the cosϕ function = f(P) (Operation with cosϕ control as a function of P) [1 = Operating, 5 = Not-Operating]	Operating
Mod	ctlVal	Activation/deactivation of the PF function = f(P) (Operation with PF regulation as a function of P) – value [5 = Inactive, 1 = Active]	Active
	origin	Activation/deactivation of the PF function = f(P) (operation with PF regulation as a function of P) - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR]	automatic-station DSO
FctOpSt	stVal	PF(P) function status (operation with cosϕ control as a function of P) [Not available /Autonomus / Automatic (priority mode)]	Automatic
WSetA	setMag	P value (point A) [0.00..max] of $P_{Nominal}$ (P.U.)	0.20
PFSetA	setMag	Cosϕ value (point A) [-1.00..1.00]	1.00
WSetB	setMag	P value (point B) [0.00..max] of $P_{Nominal}$ (P.U.)	0.50
PFSetB	setMag	Cosϕ value (point B) [-1.00..1.00]	1.00
WSetC	setMag	P value (point C) [0.00..max] of $P_{Nominal}$ (P.U.)	1.00
PFSetC	setMag	Cosϕ value (point C) [-1.00..1.00]	0.95
VLkIn	setMag	Voltage Lock-inof the cosϕ function = f(P) [1.00..1.10] of $V_{Nominal}$ (P.U.)	1.05
VLkOut	setMag	Voltage Lock-outof the cosϕ function = f(P) [0.90..1.00] of $V_{Nominal}$ (P.U.)	0.98

T.3.3.1.3 Data Models for Participation in the MSD (Discretionary)

The aggregator section is optional and additional to the observability model specified in T.3.3.1.1. If implemented, the presence of data (M/O/C/R/E) follows the rules specified in Figure 95.

T.3.3.1.3.1 Power Plant measurements

The logical node MMXU is used to represent the power plant measurements at the PoC. Annex O provides the active and reactive power reported every 4 sec. As this is the same information already modelled in the Observability paragraph, please refer to Section T.3.3.1.7 for the quantities "TotW" and "TotVAr" for its description.

T.3.3.1.3.2 Control function - Active Power Set-Point Function

The DAGC logic node is used to perform configuration/setting and to represent the status of the feed-out/feed-in active power set point control function for the purposes of the participation in the MSD.

Refer to IEC 61850-7-420 for the complete list of Data Objects.

DAGC class – type DAGC1 - prefix WSa				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
Beh	ENS	(inherited from: DomainLN) Read-only value, describing the behaviour of a domain logical node. […]		M / M
…	…	…		…
WSptPct	APC	(inherited from: ActivePowerLN) Active power setpoint setting as a percentage of Maximum Active Power capability, WMax at the Referenced ECP, and in the case of signed setpoint (typically for storage systems) as a percentage of Maximum Active Power charging (consuming) capability for values related to the charging phase. Its mxVal attribute reflects the value of the setpoint that is requested		R / O
Mod	ENC	(inherited from: DomainLN) (controllable) Operating mode of the domain logical node that may be changed by the operator. Processing of the quality status ('q') of the received data is the prerequisite for correct interpretation of the operating mode.		R / O
FctOpSt	ENS	CEI 0-16 specific		E / F
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shalm be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	**DA name**	**Meaning**	**Example**
Beh	stVal	Operating status of the active power feed-out/feed-in set point function (for Participation in the MSD) [1 = Operating, 5 = Not-Operating]	Operating
WsptPct	ctlVal	Active power feed-out/feed-in setpoint (percentage, with sign, in relation to the maximum apparent power of the system S_{max}) for participation in the MSD – value [-100 .. +100]	20
	origin	Active power feed-out/feed-in setpoint (percentage, with sign, with respect to maximum apparent system power Smax) for participation in the MSD - identity of the authorised actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR]	automatic-station DSO

DO name	DA name	Meaning	Example
Mod	ctlVal	Activation/deactivation of operating mode - active power feed-out/feed-in set point for the participation in the MSD - value [5 = Inactive, 1 = Active]	Active
	origin	Activation/deactivation of operating mode - active power feed-out/feed-in set point for the participation in the MSD - identity of authorised actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR]	automatic-station DSO
FctOpSt	stVal	Active power feed-out/feed-in set point status for the participation [Not available/ Automatic (priority mode)]	Automatic

T.3.3.1.3.3 Control Function - Reactive Power Set-point Function

The DVAR logic node is used to perform configuration/setting and to represent the status of the Inductive/Capacitive exchanged reactive power set point control function for the purposes of the participation in the MSD.

Refer to IEC 61850-7-420 for the complete list of Data Objects.

DVAR class – type DVAR1 - prefix VArSa				
Data object name	**CDC**	**Explanation**	**T**	**PresCond nds/ds**
…	…	…		…
Beh	ENS	(inherited from: DomainLN) Read-only value, describing the behavior of a domain logical node. […]		M / M
…	…	…		…
VArTgtSptPct	APC	(inherited from: ReactivePowerLN) Target reactive power setpoint expressed as percent as indicated by VArSetRef. Its mxVal attribute reflects the value of the setpoint that is requested.		R / O
Mod	ENC	(inherited from: DomainLN) (controllable) Operating mode of the domain logical node that may be changed by operator. Processing of the quality status ('q') of the received data is the prerequisite for correct interpretation of the operating mode.		R / O
FctOpSt	ENS	CEI 0-16 specific		E / F
…	…	…		…

In addition to all the mandatory DOs of the LN, those selected above shall be implemented in the model capability of the CCI; they shall be used for device communication and have the following meaning:

DO name	DA name	Meaning	Example
Beh	stVal	Operating status of the Inductive/Capacitive reactive power exchange set point function (for the participation in the MSD) [1 = Operating, 5 = Not-Operating]	Operating
VArTgtSptPct	ctlVal	Inductive/Capacitive exchanged reactive power setpoint (percentage, with sign, relative to Maximum apparent system power S_{max}) for the participation in the MSD – value Exchanged reactive power setpoint [-100 .. +100]	20
	origin	Inductive/Capacitive exchanged reactive power setpoint (percentage, with sign, with respect to Maximum apparent system power S_{max}) for the participation in the MSD - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR]	automatic-station DSO
Mod	ctlVal	Activation/deactivation of operating mode - reactive power exchange set point Inductive/Capacitive for the participation in the MSD [5 = Inactive, 1 = Active]	Active
	origin	Activation/deactivation of operating mode - inductive/capacitive reactive power exchange set point for the participation in the MSD - identity of the enabled actor [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATOR]	automatic-station ~~e~~ DSO
FctOpSt	stVal	Inductive/Capacitive reactive power exchange set point status (V-controlled operation with Q-delivery) for the participation in the MSD [Not available / Automatic (priority mode)]	Automatic

T.3.3.1.4 CCI data model and access privileges for security purposes

This paragraph specifies the access privileges to data managed by the CCI for the purposes of IED monitoring and control/configuration reserved to enabled DSO and Aggregator actors.

The device shall allow the use of access privileges only after the identification and authentication of the Actors according to the cryptographic logic described in paragraph T.3.3.4 and in compliance with the configurations described in paragraphs T.3.3.4.9.4 and T.3.3.4.9.9.1.

In particular, the device shall allow the use of the access privileges assigned to the DSO roles:

i) DSO_OPERATOR (see T.3.3.4.3.1)

ii) VIEWER

only after the identification and the authentication of the DSO, excluding the access for roles presented by the DSO other than those listed above.

Similarly, for the role of Aggregator, the device shall allow the use of access privileges assigned to the Aggregator roles:

i. AGGREGATOR_OPERATOR (see T.3.3.4.3.1, or equivalent role, see T.3.3.4.4.2)

ii. VIEWER (or equivalent role)

only after the identification and the authentication of the Aggregator, excluding access for roles presented by the Aggregator other than those listed above[238].

[238] The CCI accepts client/server communication sessions from multiple clients at the same time, e.g. several remote entities that need access with multiple simultaneous roles. Consistently the CCI shall offer the possibility to enable multiple instances of the same reports to connected clients

This classification supports the definition of roles and privileges as prescribed in T.3.3.4.3.1.

The authorized subjects (i.e. those identified and authenticated) not identified as DSOs or Aggregators shall get access privileges consistent with the role assigned to them.

Table 98 – Data reserved for the DSO

Access Privileges	IED	LD	LN Type	LN Prefix	LN Class	LN Inst.	DO (.SDO)	CDC	DataSet / Report
RO	(1)	LD_Installation	LPHD1		LPHD	1	PhyNam	DPL	(2)
RO	(1)	LD_Installation	DPCC1	PdC_Wi	DPCC	1	WRtg	ASG	(2)
RO	(1)	LD_Installation	DPCC1	PdC_Wa	DPCC	1	WRtg	ASG	(2)
RO	(1)	LD_Installation	DPCC2	PdC_Qi	DPCC	1	VArRtg	ASG	(2)
RO	(1)	LD_Installation	DPCC2	PdC_Qc	DPCC	1	VArRtg	ASG	(2)
RO	(1)	LD_Installation	DPCC3	PdC_VA	DPCC	1	VARtg	ASG	(2)
RO	(1)	LD_Installation	DECP1	DisFR	DECP	1	Beh	ENS	(3) Status, Alarms, Signals
RO	(1)	LD_Installation	DGEN1	DisFR	DGEN	1	Beh	ENS	(3) Status, Alarms, Signals
RO	(1)	LD_Installation	DSTO1	DisFR	DSTO	1	Beh	ENS	(3) Status, Alarms, Signals
RO	(1)	LD_Installation	DWMX1	Wlim	DWMX	1	Beh	ENS	(2)
RW	(1)	LD_Installation	DWMX1	Wlim	DWMX	1	WMaxSptPct	APC	(2)
RW	(1)	LD_Installation	DWMX1	Wlim	DWMX	1	Mod	ENC	(2)
RO	(1)	LD_Installation	DWMX1	Wlim	DWMX	1	FctOpStAuto	ENS	(2)
RO	(1)	LD_Installation	DWMX1	Wlim	DWMX	1	FctOpStEx	ENS	(2)
RO	(1)	LD_Installation	DAGC1	WSd	DAGC	1	Beh	ENS	(2)
RW	(1)	LD_Installation	DAGC1	WSd	DAGC	1	WSptPct	APC	(2)
RW	(1)	LD_Installation	DAGC1	WSd	DAGC	1	Mod	ENC	(2)
RO	(1)	LD_Installation	DAGC1	WSd	DAGC	1	FctOpSt	ENS	(2)
RO	(1)	LD_Installation	DVAR1	VArSd	DVAR	1	Beh	ENS	(2)
RW	(1)	LD_Installation	DVAR1	VArSd	DVAR	1	VArTgtSptPct	APC	(2)
RW	(1)	LD_Installation	DVAR1	VArSd	DVAR	1	Mod	ENC	(2)
RO	(1)	LD_Installation	DVAR1	VArSd	DVAR	1	FctOpSt	ENS	(2)
RO	(1)	LD_Installation	DFPF1	PFSP	DFPF	1	Beh	ENS	(2)
RW	(1)	LD_Installation	DFPF1	PFSP	DFPF	1	PFGnTgtSpt	APC	(2)
RW	(1)	LD_Installation	DFPF1	PFSP	DFPF	1	PFLodTgtSpt	APC	(2)
RW	(1)	LD_Installation	DFPF1	PFSP	DFPF	1	Mod	ENC	(2)
RO	(1)	LD_Installation	DFPF1	PFSP	DFPF	1	FctOpSt	ENS	(2)
RO	(1)	LD_Installation	DVVR1	VArV	DVVR	1	Beh	ENS	(2)
RW	(1)	LD_Installation	DVVR1	VArV	DVVR	1	Mod	ENC	(2)
RO	(1)	LD_Installation	DVVR1	VArV	DVVR	1	FctOpSt	ENS	(2)
RW	(1)	LD_Installation	DVVR1	VArV	DVVR	1	K	ASG	(2)
RW	(1)	LD_Installation	DPMC1	VArV	DPMC	1	WSpt1	APC	(2)
RW	(1)	LD_Installation	DPMC1	VArV	DPMC	2	WSpt1	APC	(2)
RW	(1)	LD_Installation	DECP2	VArV	DECP	1	VMax	ASG	(2)
RW	(1)	LD_Installation	DECP2	VArV	DECP	1	Vmin	ASG	(2)
RW	(1)	LD_Installation	DECP2	VArV	DECP	2	VMax	ASG	(2)

Access Privileges	IED	LD	LN Type	LN Prefix	LN Class	LN Inst.	DO (.SDO)	CDC	DataSet / Report
RW	(1)	LD_Installation	DECP2	VArV	DECP	2	Vmin	ASG	(2)
RO	(1)	LD_Installation	DPFW1	PFW	DPFW	1	Beh	ENS	(2)
RW	(1)	LD_Installation	DPFW1	PFW	DPFW	1	Mod	ENC	(2)
RO	(1)	LD_Installation	DPFW1	PFW	DPFW	1	FctOpSt	ENS	(2)
RW	(1)	LD_Installation	DPFW1	PFW	DPFW	1	WSetA	ASG	(2)
RW	(1)	LD_Installation	DPFW1	PFW	DPFW	1	PFSetA	ASG	(2)
RW	(1)	LD_Installation	DPFW1	PFW	DPFW	1	WSetB	ASG	(2)
RW	(1)	LD_Installation	DPFW1	PFW	DPFW	1	PFSetB	ASG	(2)
RW	(1)	LD_Installation	DPFW1	PFW	DPFW	1	WSetC	ASG	(2)
RW	(1)	LD_Installation	DPFW1	PFW	DPFW	1	PFSetC	ASG	(2)
RW	(1)	LD_Installation	DPFW1	PFW	DPFW	1	VLkIn	ASG	(2)
RW	(1)	LD_Installation	DPFW1	PFW	DPFW	1	VLkOut	ASG	(2)
RO	(1)	LD_Installation	MMXU1	PdC	MMXU	1	TotW	MV	(3) PdC measurements 4sec
RO	(1)	LD_Installation	MMXU1	PdC	MMXU	1	TotVAr	MV	(3) PdC measurements 4sec
RO	(1)	LD_Installation	MMXU1	PdC	MMXU	1	PPV.phs A/B/C	DEL	(3) PdC measurements 4sec
RO	(1)	LD_Installation	MMXU1	PdC	MMXU	1	A.phsA/B /C	WYE	(2)
RO	(1)	LD_Installation	MMXU2	GenPV	MMXU	1	TotW	MV	(3) Measurements per source Gen. 4sec
RO	(1)	LD_Installation	MMXU2	GenWi	MMXU	1	TotW	MV	(3) Measurements per source Gen. 4sec
RO	(1)	LD_Installation	MMXU2	GenTer	MMXU	1	TotW	MV	(3) Measurements per source Gen. 4sec
RO	(1)	LD_Installation	MMXU2	GenIdr	MMXU	1	TotW	MV	(3) Measurements per source Gen. 4sec
RO	(1)	LD_Installation	MMXU2	St	MMXU	1	TotW	MV	(3) Measurements Accumulation 4sec
RO	(1)	LD_Installation	MMXU2	SGG	MMXU	1..N	TotW	MV	(3) Measures Single Gen. 4sec
RO	(1)	LD_Installation	XCBR1	IDG	XCBR	1	Pos	DPC	(3) Status, Alarms, Signals
RO	(1)	LD_Installation	DGEN2	SSGG	DGEN	1..N	Health	ENS	(3) Status, Alarms, Signals
RO	(1)	LD_Installation	DGEN2	SSGG	DGEN	1..N	GnGrId	INS	(3) Measures Single Gen. 4sec
RW	(1)	LD_Installation	DataSet_DSO (n)						(2)
RW	(1)	LD_Installation	ReportControl Block_ DSO (n)						(2)

Notes:

(1) the name of IED depends on the specific project/installation.

(2) the inclusion of the data in a DataSet, the name of the DataSet and the name and parameters of the Report Control Block referring to the DataSet depend on the specific project/installation.

(3) For Observability purposes, the name of the DataSet and the name and parameters of the Report Control Block that refers to the DataSet depend on the specific project/installation.

RO = Read-only data.

RW = Read/Write data.

Table 99 – Data reserved for the Aggregator

Access Privileges	IED	LD	LN Type	LN Prefix	LN Class	LN Inst.	DO (.SDO)	CDC	DA	DataSet / Report
RO	(1)	LD_Installation	DAGC1	WSa	DAGC	1	Beh	ENS	stVal	(2)
RW	(1)	LD_Installation	DAGC1	WSa	DAGC	1	WSptPct	APC	ctlVal	(2)
RW	(1)	LD_Installation	DAGC1	WSa	DAGC	1	Mod	ENC	ctlVal	(2)
RO	(1)	LD_Installation	DAGC1	WSa	DAGC	1	FctOpSt	ENS	stVal	(2)
RO	(1)	LD_Installation	DVAR1	VArSa	DVAR	1	Beh	ENS	stVal	(2)
RW	(1)	LD_Installation	DVAR1	VArSa	DVAR	1	VArTgtSptPct	APC	ctlVal	(2)
RW	(1)	LD_Installation	DVAR1	VArSa	DVAR	1	Mod	ENC	ctlVal	(2)
RO	(1)	LD_Installation	DVAR1	VArSa	DVAR	1	FctOpSt	ENS	stVal	(2)
RO	(1)	LD_Installation	MMXU1	PdCi	MMXU	1	TotW	MV	mag	(2)
RO	(1)	LD_Installation	MMXU1	PdCi	MMXU	1	TotVAr	MV	mag	(2)
RW	(1)	LD_Installation	DataSet_Aggregatore (n)							(2)
RW	(1)	LD_Installation	ReportControl Block_Aggregatore (n)							(2)

Notes:

(1) the name of the IED depends on the specific project/installation.

(2) the inclusion of the data in a DataSet, the name of the DataSet and the name and parameters of the Report Control Block referring to the DataSet depend on the specific project/installation.

RO = Read-only data.

RW = Read/Write data.

T.3.3.2 ACSI services

Against the data model given in the previous section, the IEC 61850 server shall implement the following communication services (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)". - Table 1 - ACSI classes).

Table 100 –ACSI classes and services

ACSI class	CSI services	Privileges	DSO/Aggregator
Server	GetServerDirectory	Listobjects	Applicable
Association	Release	Listobjects	Applicable
	Abort		Applicable
	GetServerDirectory		Applicable
LogicalDevice	GetLogicalDeviceDirectory	Listobjects	Applicable
Logical Node	GetLogicalNodeDirectory	Listobjects, Readvalues	Applicable
	GetAllDataValues		Applicable
Data Object	GetDataValues,	Readvalues, Control/config, Listobjects	Applicable
	SetDataValues,		Applicable
	GetDataDirectory,		Applicable
	GetDataDefinition		Applicable

ACSI class	ACSI services	Privileges	DSO/Aggregator
DataSet	GetDataSetValues	Dataset Allows the subject/role to obtain the values and structure of datasets without allowing them to be modified	Applicable
	SetDataSetValues		Not Applicable
	CreateDataSet		Not Applicable
	DeleteDataSet		Not Applicable
	GetDataSetDirectory		Applicable
Buffered Report Control Block	Report	Reporting: Allows the subject/role to use both buffered and unbuffered reports without allowing them to be modified	Applicable
	GetBRCBValues		Applicable
	SetBRCBValues		Not Applicable
UnBuffered Report Control Block	Report	Reporting: Allows the subject/role to use both buffered and unbuffered reports without allowing them to be modified	Applicable
	GetURCBValues		Applicable
	SetURCBValues		Not Applicable

For further developments in high-speed information exchanges with protections (PG perspective), according to the “General scheme of the CCI system with related functional interfaces” in Annex O, the use of GOOSE-class ACSI services is envisaged.

T.3.3.3 Communication Protocol Mapping

To create a CCI that is interoperable with external systems (DSO and Enabled Remote Actors), it is necessary to specify the mapping of the abstract concepts listed in T.3.1 and T.3.1.1 to a specific communication protocol.

To identify this mapping, the following aspects have been considered.

- The information exchange associated with the CCI is compatible with the "Type 2/Type 3”[239] typologies described in 5.1 of IEC 61850-8-1 "Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3", which for this type of message proposes the mapping to the MMS protocol
- The need to define a correlation between roles (DSO, Enabled Remote Actors) and access to specific IEC 61850 services suggests a two-party application association model typical of the Client/Server model.

Based on these considerations, the IEC 61850-8-1 mapping on MMS protocol was selected (with the perspective considerations for GOOSE communications mentioned in T.3.2.1 and T.3.2.2).

To facilitate the realization of interoperable CCI devices, the relevant configuration file will be made available according to the IEC 61850 SCL formalism.

T.3.3.4 Cyber Security of CCI

Regarding communication security, the requirements in this document refer to the architecture of the CCI device specified in Annex O, which provides two network interfaces for remote access to the device, and one or more interfaces for local access. Remote access is provided both for monitoring and control functions, and for system management needs.

In this section, the security specification of the CCI monitoring and control functions refers to the mapping of communication functions to the MMS (Manufacturing Message Specification) protocol indicated in Subclause T.3.3 and specified by IEC 61850-8-1.

Some mechanisms for securing GOOSE communications for CCI subscriber functions are also specified.

[239] Performance class P4 for Type 2; Performance class P5 for Type 3; Referrer to IEC 61850-5 paragraph 11.2.2 and 11.2.3

The security of IEC 61850 communication profiles has been standardised in IEC 62351-6 “Power systems management and associated information exchange - Data and communication security - Part 6: Security for IEC 61850”.

The specification of the security functions in this section considers the developments in the parts of IEC 62351 of interest to the CCI [240] device. Regarding the conformity tests to IEC 62351, reference is made to Annex O, Subclause O.15.5. Subclauses are structured as follows:

- Subclauses T.3.3.4.1, T.3.3.4.3 and T.3.3.4.4 present the basic security mechanisms for information exchange based on IEC 61850 protocols;

- Subclauses T.3.3.4.5, T.3.3.4.6, T.3.3.4.7 and T.3.3.4.8 provide the security requirements for support services;

- Subclause T.3.3.4.9 presents the processes related to the management of electronic certificates used by both IEC 61850 communications and support services;

- Subclause T.3.3.4.10 specifies the traffic segregation requirements;

- Subclause T.3.3.4.11 covers the security of communications through local (non-network) interfaces.

T.3.3.4.1 IEC 61850/MMS Communication Security

IEC 62351-6 provides the cybersecurity specifications of the communication protocols defined by the standard. Regarding communications implementing the MMS protocol, IEC 62351-6 refers to the standard IEC 62351-4 “Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS and derivatives”.

According to IEC 62351-4, the security of MMS communications is achieved by defining measures at the transport profile, hereafter also referred to as the T-profile, which addresses levels 1-4 of the ISO/OSI stack, and at the application profile, which instead addresses levels 5-7 of the ISO/OSI model.

In the application profile, the authentication of the communicating parties and the integrity of the communications shall be guaranteed. Cryptographic support shall also be implemented to guarantee the confidentiality of communications, but this functionality shall be able to be activated or deactivated according to the specific security policies agreed between the communicating parties.

The public key algorithms to be used for the application profile are:

- RSA cryptography: object identifier { iso(1) member-body(2) us(840) ansi-x9-62(10045) keyType(2) 1}
- Elliptic curve cryptography:
  - secp256r1: object identifier { iso(1) member-body(2) us(840) ansi-x9-62(10045) curves(3) prime(1) 7 }
  - brainpoolP256r1: object identifier { iso(1) identified-organization(3) teletrust(36) algorithm(3) signature-algorithm(3) ecSign(2) 8 ellipticCurve(1) versionOne(1) 7 }

Keys with a length of 2048 bits shall be supported in the case of RSA cryptography, while, in the case of ECDSA cryptographic keys, a length of 256 bits shall be supported; these values shall be considered as minimums: it is strongly recommended to support also keys longer than these minimums (e.g. 3072 bits in the case of RSA keys and/or 384 bits in the case of ECDSA keys).

[240] For interoperability reasons, the CCI security requirements necessarily apply to remote devices hosting the corresponding IEC 61850 clients

The SHA256 hash algorithm shall be used both for digital signature purposes and for the calculation of Integrity Check Values (ICVs): object identifier is { joint-iso-itu-t(2) country(16) us(840) organisation(1) gov(101) csor(3) nistAlgorithm(4) hashalgs(2) 1 }

The following two algorithms, both based on SHA256, shall be supported for digital signatures:

- RSA-with-SHA256: object identifier { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11) }
- ECDSA-with-SHA256: object identifier { iso(1) member-body(2) us(840) ansi-x9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }

Moreover, to verify the integrity of a message, the following algorithm for calculating ICVs shall be supported:

- hmacWithSHA256: object identifier { iso(1) member-body(2) us(840) rsadsi(113549) digestAlgorithm(2) 9 }

The following symmetric encryption algorithms shall be supported:

- aes128-CBC: object identifier { joint-iso-itu-t(2) country(16) us(840)organisation(1) gov(101) csor(3) nistAlgorithm(4) aes(1) 2}
- aes256-CBC: object identifier { joint-iso-itu-t(2) country(16) us(840)organization(1) gov(101) csor(3) nistAlgorithm(4) aes(1) 42}

The following algorithms shall also be supported, which, in addition to information confidentiality, can also guarantee integrity and authentication:

- aes128-GCM: object identifier { joint-iso-itu-t(2) country(16) us(840)organisation(1) gov(101) csor(3) nistAlgorithm(4) aes(1) 6 }
- aes256-GCM: object identifier { joint-iso-itu-t(2) country(16) us(840)organization(1) gov(101) csor(3) nistAlgorithm(4) aes(1) 46 }

In particular aes128-GCM and aes256-GCM shall also be usable without the communication confidentiality functionality and may be combined in this case with aes128-CBC and aes256-CBC to provide this functionality.

The certificates presented when creating the application profile association shall not exceed 8192 octets.

Mechanisms or procedures shall be provided so that the internal clock used to obtain time references remains synchronised with UTC; a deviation of more than 10 minutes between the clocks of the two entities involved in the communication shall cause the communication to fail.

Within Diffie-Hellman (DH) keys exchange, DH group "14" (2048-bit) shall be supported when RSA algorithm is used; when ECDH algorithm is used, both DH group "23" (secp256r1) and DH group "28" (BrainpoolP256r1) shall be supported.

For the application profile, IEC 62351-4 is the reference standard regarding ACSE protocol requirements.

End-To-End (E2E) security shall be used for the application profile, following specifications in IEC 62351-4 regarding the association phase between the two communicating parties and the data transfer phase.

In the association phase, the SecPDUs shall contain the specified MMS protocol PDUs, to which the digital signature shall be applied to ensure the integrity of the communication.

In the data transfer phase, plain-text PDUs are optionally allowed with verification of the integrity of the communications, as well as encrypted PDUs to ensure the confidentiality of the communications.

Failures in the association phase and in the data transfer phase shall be handled by the appropriate SecPDUs both in the case where the origin comes from the MMS protocol and in the case where the origin derives from security-related anomalies. The diagnostic codes specified by the standard shall be used to indicate the causes of failure in the association or data transfer phase.

The T-profile provides authentication, integrity and confidentiality functions at the transport layer. Regerding MMS communications implementations that use the TCP protocol at the transport layer, the secure T-profile requires the use of TLS (Transport Layer Security) as specified by IEC 62351-3 'Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP'.

The TLS profile specified by IEC 62351-3 states the following:

- TCP port 3782 is defined as the default for T-profile communications with TLS;
- regarding TLS version, TLS version v1.2 [241]*[Nota 241 nella CEI 0-16 2023-5 V2]* shall be supported;
- regarding cipher suites, support of at least the following three cypher suites is required:
  1. TLS_RSA_WITH_AES_128_CBC_SHA256;
  2. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256;
  3. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256;
- in addition to the cypher suites indicated above, support for the TLS_RSA_WITH_NULL_SHA256 cypher suite is also required. Since it does not provide traffic encryption, this cypher suite may only be used when the administrative domain has determined that the data exchanged does not require confidentiality (e.g. to simplify traffic monitoring) and other solutions are in place to adequately protect data confidentiality (e.g. VPNs). To prevent unconscious use, this cypher suite shall be disabled by default and specific procedures shall be adopted to intentionally enable it when necessary;
- by default, the renegotiation of the TLS session should take place at time intervals aligned with the CRL (Certificate Revocation List) update period, and in particular at least half of this period; however, not to overload client and server communications, the renegotiation interval may not be less than 10 minutes;
- to renew session encryption keys, the TLS session resumption technique shall be supported. TLS session resumption also avoids the repetition of certain information exchanges (e.g. transmission of digital certificates) that take place in the case of reconnection and may therefore be efficient in restoring short interruptions in connectivity. The resumption of the TLS session shall take place at a configurable time interval and in any case at least every 2 hours; in any case in a shorter time than the resumption and aligned to CRL update period;
- support is required for at least five different root certificates related to different Certificate Authorities [242];
- the size of the public key certificates used should be a maximum of 8192 octets for interoperability reasons; any implementation shall manage certificates at least up to this size;
- the CRL should be updated at least every 24 hours. If OCSP (Online Certificate Status Protocol) is used, responses may be cached for a maximum of 24 hours. However, an active session should not be terminated just because these limits are exceeded.

241 Edition 2 of IEC 62351-3 provides for migration to TLS version v 1.3, in accordance with NIST standard SP 800-52 Rev. 2 'Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations', which requires TLS version 1.3 support by January 2024

242 Edition 2 of IEC 62351-3 specifies this minimum limit; it has been incorporated in this document with the aim of conforming devices to the growing need for operational flexibility.

To prevent both unauthorized access and unauthorized modification/interception of control information in different network architectures, it is considered mandatory for the CCI to support both the E2E application profile and the T-profile with TLS [243] cybersecurity.

In this subclause the specifications provided by IEC 62351-3, IEC 62351-4 and IEC 62351-6 standards, which shall be referenced for implementation details, have been summarized with regard to the security of IEC 61850/MMS communications; the following table summarizes the characterizing aspects of the profile defined in this document, derived from the reference standards.

Aspect of the IEC 62351 profile	IEC 62351 profile configuration
Application Profile	Support of the E2E safety specification as stated earlier in this document and in the reference standard IEC 62351-4 is required [244]
Transport profile	Support of the TLS security specification, as stated earlier in this document and in the reference standard IEC 62351-3 is required.
Public/private key length	It is required the use, and thus support, of RSA keys with a minimum length of 2048 bits. A minimum limit is also indicated for ECDSA cryptographic keys selected to guarantee a level of security at least comparable with that of RSA keys [245]
TLS protocol versions	Use, and thus support, of TLS protocol version v1.2 is required [246]
Cypher suite	Support of the TLS_DH_RSA_WITH_AES_128_GCM_SHA256 cypher suite is not required even if it is specified by current standards [247]
Root certificate	Support of at least five different *root certificates* is required [248]

T.3.3.4.2 Communication Security IEC 61850/GOOSE [Informative]

The confidentiality of GOOSE communications is not mandatory in IEC 62351-6 mainly to meet the performance requirements (especially latency) of these communications. To ensure maximum flexibility, the standard allows secure and non-secure communications to co-exist, to ease transitioning to higher levels of cybersecurity and business continuity.

Even if data encryption is not used, IEC 62351-6 still indicates security solutions to guarantee the integrity and authentication of communications; these are based on the extension of the format of the Protocol Data Units (PDUs) exchanged, the use of hash functions, message digests and public key cryptography.

PDUs may be extended by appropriately enhancing the specific Reserved1 and Reserved2 fields which will contain, respectively, the length in octets of the extension containing the security parameters and a checksum calculated on the contents of the extended PDU.

To guarantee the authenticity of the contents of the PDU, a Message Authentication Code (MAC) is adopted, and consists in the hash value returned by the HMAC-SHA256 or AES-GMAC algorithm calculated on the contents of the extended PDU. In particular, the octets from the

243 The choice of the safety profile(s) effectively configured on the CCI depends on the cybersecurity policies agreed between the parties.

244 This solution stems from reasons of stability over time and completeness of the safety functionality offered; it is expected that future editions of the IEC 62351-4 standard will mandate the E2E option while the current alternatives might be deprecated (see also IEC 62351-6:2020-5.2.1 and IEC 62351-4:2018-7.1)

245 There are no backward compatibility reasons that would motivate the support of smaller cryptographic keys, whose cybersecurity level is now considered insufficient.

246 No backward compatibility reasons are envisaged that would motivate the support of earlier TLS versions, whose cybersecurity level is now considered insufficient.

247 It is expected that future editions of the reference standards will not indicate this cypher suite.

248 The value indicated shall be intended as a minimum value: it is recommended that a higher number be considered in the interests of greater flexibility and future-proofness of the device.

Ethertype Identifier to the end of the PDU can be considered. The hash value may be truncated to 128 or 256 bits.

The Extended PDU also contains the time references which specify the validity of the current key and of the next key distributed via the Group Key Management Protocol; by knowing the validity interval of a key, receivers can obtain in advance the next key that will be made available for distribution knowing the time of its usability.

Upon receipt of an extended PDU containing a MAC, the receiver can verify the correctness of the MAC before further processing of the PDU contents.

The Stnum and Sqnum values of a received PDU may be considered to identify potential reply attacks; even if the arrival of a PDU with lower values than those received may be motivated by the use of multi-path communications, the PDU should be discarded as if it originated from a reply attack.

T.3.3.4.3 Role Management in IEC 61850/MMS Communication

The IEC 61850 server of the CCI is set up to communicate in a differentiated way with different appropriately identified actors, such as the DSO and any additional external operators authorized to the remote control, using the concepts of access privileges (Paragraph T.3.3.1.4) and roles.

For each enabled role, custom or standard, it shall be configured and verified who can take that role, defining which entities (DSOs and other Actors) are authorized to request it. If profiles A and B are used, for this purpose, individual certificates can be specified, or all those certificates issued by certain CAs.

The details of role implementation and management are specified in IEC 62351-8 “Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control”.

IEC 62351-8 defines a set of seven mandatory roles that shall be supported, and a predefined set of privileges associated with them.

The objects and operations to which the roles apply are defined by the data model used: for CCI, the objects map to the Data Objects and the operations to the IEC 61850 services specified in the previous sections.

T.3.3.4.3.1 Definition of roles and privileges

Access control is applied both to allow and to prohibit access to an ACSI server through an access point or, more specifically, to each instance of the logical-device, logical-node and data-object hierarchy. Assigning a role to a given subject will result in different responses to requested services based on the privileges that have been assigned to that role.

Specifically, considering the ACSI services that shall be implemented for communication with the CCI (Section T.3.2.2), the following standard-derived privileges are required:

- LISTOBJECTS: allows a subject/role to discover which objects are present within the Logical Device through the type and ID of these objects. LISTOBJECTS will include in the list only the objects for which the subject/role has the privilege READVALUES;
- READVALUES: allows a subject/role to obtain some or all of the values in addition to the type and ID of the objects pertaining to a Logical Device;
- CONTROL: allows a subject/role to perform control operations;
- CONFIG: allows the subject/role to configure locally or remotely all or some objects that are present in the IED;
- DATASET: allows the subject/role to have access to both persistent and non-persistent dataset services;

- REPORTING: allows the subject/role to use both buffered and unbuffered reporting related to the control block records of a logical node.

Table 101 shows the privileges for each ACSI service with reference to the service classes identified as significant for the implementation of CCI.

Table 101 – Mapping privileges on ACSI services

ACSI class	ACSI services	Privileges
Server	GetServerDirectory	Listobjects
Association	Release, Abort, GetServerDirectory	Listobjectts
LogicalDevice	GetLogicalDeviceDirectory	Listobjects
Logical Node	GetLogicalNodeDirectory, GetAllDataValues	Listobjects, Readvalues
Data Object	GetDataValues, SetDataValues, GetDataDirectory, GetDataDefinition	Readvalues Control/config Listobjects
DataSet	GetDataSetValues, GetDataSetDirectory	Dataset
Buffered Report Control Block	Report, GetBRCBValues	Reporting
UnBuffered Report Control Block	Report, GetURCBValues	Reporting

The IEC 62351-8 standard provides the possibility of defining customized roles to fit the required security model. In addition to the mandatory roles defined in the IEC 62351-8 standard, the CCI shall implement the two custom roles DSO_OPERATOR and AGGREGATOR_OPERATOR.

According to their definition, the DSO will have the privileges to:

- “LISTOBJECTS”,
- “READVALUES”,
- “DATASET” with read-only access,
- “REPORTING” with write access only for report enable,
- “CONTROL” and “CONFIG” on the Data Objects defined in Table 98 of Paragraph T.3.3.1.4.

Similarly, the Aggregator will have the following privileges (or equivalent, see T.3.3.4.4.2):

- “LISTOBJECTS”,
- “READVALUES”,
- “DATASET” with read-only access,
- “REPORTING” with write access only for report enable,
- “CONTROL” and “CONFIG” on the Data Objects defined in Table 99 of Paragraph T.3.3.1.4

Table 102 shows the mapping between the roles identified as relevant to the operation of the CCI and the privileges associated with each role.

Table 102 – CCI Roles/Privileges

Value	Right Role	LIST OBJECTS	READ VALUES	DATA SET	REPORTING	FILE READ	FILE WRITE	FILE MNGT	CONTROL	CONFIG	SETTINGGROUP	SECURITY		
-1	DSO_OPERATOR	X	X	C1	C2				C3	C3				
-2	AGGREGATOR_OPERATOR	X	X	C1	C2				C3	C3				

- C1= read-only access to the dataset
- C2= write-only access to report enable
- C3= conditional access only to specific Data Objects described in the tables in Section T.3.3.1.4

The information exchange required for assigning permissions to CCI roles shall be described using XACML (eXtensible Access Control Markup Language) as defined by the IEC 62351-8 standard. The object used to define a role in XACML format shall contain the following fields:

- RoleID: value for role identification
- unique-ID: random string to ensure uniqueness within the policy decision point (PDP) domain
- RoleName: contains the name of the role in readable form
- roleDefinition: contains a reference to the document containing the role definition. E.g. IEC 62351-8
- revision: revision number
- PermissionGroup: name of the group containing the permission set
- Permission: name of the defined permission.

In particular, the new roles are defined as follows:

- DSO_OPERATOR
  - Role-id: -1
  - Revision: 1.0
  - RoleDefinition: “IEC 62351-8-CEI016:2021”
- AGGREGATOR_OPERATOR
  - Role-id: -2
  - Revision: 1.0
  - RoleDefinition: “IEC 62351-8-CEI016:2021”

T.3.3.4.3.2 Roles transportation

For the transport of roles, access tokens are used, which may have different formats. For CCI, support is required for the access token format specified by either profile A or profile B in IEC 62351-8, and support is also optionally required for profiles C (JSON-based webtoken) and D (RADIUS token).

An access token shall contain at a minimum the information contained in Table 103.

Table 103 – Access Token Mandatory Fields [IEC 62351-8]

Token component	Comment
Token holder	Name of the subject and access token holder
RoleID	Role assigned to the subject and access token holder
Revision number	Revision number of role-to-permission assignment
RoleDefinition	Role definition refers to the standard or document defining the role resp. the underlying data model.
AoR	Area of responsibility (defines the area (geographic or organizational) where the role is applicable);
Issuer	Issuer of the access token
Validity from	Validity starting time
Validity to	Validity end time

In addition to the previous fields, the components in Table 104 shall also be supported for profiles A and B.

Table 104 – Specific fields for profiles A and B [IEC 62351-8]

Token component	Comment	A	B
Serial number	Serial number of the access token	X	X
Signature algorithm	Relates to signature algorithm used to create the access token from the instance issuing a certificate	X	X
Signature value	Relates to the calculated signature value using the specified signing algorithm	X	X

T.3.3.4.3.2.1 Profile A: ITU-T X.509 Public Key Identity Certificate Extension

Profile A requires that the role information of each actor authorised to communicate with the CCI be provided as an extension of the public key identity certificate (X.509 ID certificate with extension). Profile A can be used with both PUSH and PULL models. In particular, the IECUserRoles extension was specified specifically for power systems to properly manage role-based access control. Certificate management is detailed in IEC 62351-9, while the access token structure for profile A is detailed in IEC 62351-8.

The access token is identified through OID 1.0.62351.8.1

In detail, a certificate extension shall be in accordance with the following definition:

```
Extensions::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension::=  SEQUENCE  {
     extnID      OBJECT IDENTIFIER,
     critical    BOOLEAN DEFAULT FALSE,
     extnValue   OCTET STRING
                 -- contains the DER encoding of an ASN.1 value
                 -- corresponding to the extension type identified
                 -- by extnID
     }
```

OID value is defined as follows:

```
id-IEC62351 OBJECT_IDENTIFIER::= { 1 0 62351 }

id-IECUserRoles OBJECT_IDENTIFIER::= { id-IEC62351 8 1 }
```

The value for the extension is defined as follows:

```
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 (SIZE(0..23)),
    -- 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) }
```

T.3.3.4.3.2.2 Profile B: ITU-T X.509 attribute certificate

Profile B requires the use of X.509 attribute certificates (AC) for the transport of role information. The use of this profile allows for a shorter certificate validity period than the X.509 public key identity certificate. It can be used with either the PUSH or PULL model. IEC 62351-8 provides details on the structure and format of the attribute certificate to be used for this profile.

The access token is identified through OID 1.0.62351.8.1 and contains several fields. The mandatory fields are related to the access token serial number, the name of the token owner subject, the assigned role, information about the token issuance (issuing subject and its timestamp), token validity and revision number of the subject-to-role assignment. In addition, the access token shall indicate the signing algorithm and the signature of the instance that issued it. The extension allows more than one role to be assigned to the same subject.

The object identifier for the AttributeType is defined as the OID value given in profile A. The value of the AttributeValue field is defined as the extension for profile A.

T.3.3.4.3.3 Mapping with existing authorisation systems

Role management involves a close relationship with the authorisation system implemented by the organisation. In fact, the existing authentication mechanisms are used and extended. Profile A is part of the PKI (Public Key Infrastructure) while profile B is developed by means of a PMI (Privilege Management Infrastructure) interconnected with the PKI as established by ISO/IEC 9594-8 standard. PMI provides the complete set of processes required for the provision of an authorisation service.

The following Table shows the mapping between identity certificate (ID certificate) and attribute certificate.

Concept	PKI	PMI
Name of certificate	Public key 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

T.3.3.4.3.4 Algorithms and keys for role management

IEC 62351-8 also specifies minimum requirements in terms of algorithms and key lengths used for role management. The use of SHA-256 for hash operations is recommended. For signature functions, RSA with a 2048-bit key is recommended. Additionally, ECC-based algorithms with 256-bit keys (with SHA-256) can optionally be used. OID to be used for ecdsa-with-SHA256 is: iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2., aligned with the requirements of IEC 62351-3.

T.3.3.4.3.5 Access token

Access tokens may be used at different levels of the OSI stack. Generally, the focus is on the transport and application level, but other solutions are not excluded. For MMS communications over TCP, the use of access tokens may take place in two stages:

- at the transport level, during the establishment of a secure connection according to IEC 62351-3;

- at the application level, during the authorization process that includes the assignment of the access token containing the role.

Credentials may be used in a session-oriented or single-message approach.

A session-based approach assumes that there is an end-to-end communication between two entities initialised using authentication. Such authentication is expected to be linked to RBAC credentials. During the setup phase, a session key is established to cryptographically protect the communication session and guarantee authentication and authorization. An application may refer to the application-level security profiles described in IEC 62351-4.

The message-based approach, on the other hand, assumes that RBAC credentials are linked to the content of the individual message. In several cases, this approach is implemented by means of digital signature.

T.3.3.4.4 Security of communication services with enabled remote actors other than DSO

According to Annex O, CCI has an interface for the remote access by types of operators other than the DSO, such as the User and the Aggregator.

T.3.3.4.4.1 User

To enable monitoring, configuration and maintenance functions by the authorized users, the CCI allows remote connections to the interface for remote accesses. These communications shall use standard protocols equipped with security services, designed to guarantee confidentiality, authenticity and integrity of the session, such as SSH or HTTPS. The use of cryptographic credentials (e.g. digital certificates) is required and it is required to establish the mutual authentication of the communicating parties.

To simplify the device management and to allow plant owners to define a hierarchy of roles for the security management of the device, the CCI shall implement a user permission management system that allows to operate an appropriate segregation of duty aimed at limiting access to subsets of functions and parameters of the CCI, through the attribution of specific roles to individual users (see section T.3.3.4.9.4).

T.3.3.4.4.2 Aggregator

For the remote access to CCI, the Aggregator may use standard communication protocols equipped with:

- a documented semantic data model, able to guarantee interoperability of information exchanges between CCI and client devices of different Aggregators;

- end-to-end security functions, capable of guaranteeing authentication, integrity and confidentiality on the entire communication path, from the CCI node to the Aggregator node in any type of network architecture used by the organization for implementing communications on the geographic network;

- a role management system to restrict access to subsets of CCI's data, by assigning permissions defined with the same granularity as the access control system specified for the CCI's IEC 61850 data model (see section T.3.3.4.3).

T.3.3.4.5 Time synchronization

According to Annex O, Subclause O.13.1.5, the time synchronization function can be performed by a GPS receiver integrated in the CCI, or it can be provided via a communication network service. In the CCI, this function provides the reference for the time stamping of measurements and signals, for data logger events and for checking the temporal validity of electronic certificates.

The time stamp shall be measured with reference to the UTC (Coordinated Universal Time). The value of the time measurement in UTC coincides with the value expressed in Greenwich Mean Time (GMT), unless there are infinitesimal approximations. The uncertainty of the reference time shall not exceed +/- 100 ms.

To meet the accuracy requirements of the CCI time synchronization function, the use of the Network Time Protocol (NTP) is recommended in the case of synchronization via a communication network.

NTP is an application-layer client-server IETF standard protocol, listening on UDP port 123. The CCI acts as an NTP client through unicast communication with NTP servers providing the time reference.

To protect the CCI from cyber-attacks (e.g. spoofing attacks to the server IP), the CCI client shall use the NTS (Network Time Security) secure version of NTP specified by the standard IETF RFC 8915 with TLS-based authentication and integrity functions. For the implementation of the TLS profile refer to Subclause T.3.3.4.1.

In addition, to protect the CCI from attacks by fake tickers (i.e. servers that send incorrect time references), a redundant NTP [249] server architecture shall be used.

T.3.3.4.6 Log Management

As specified in Article O.14 "Data Loggers" of Annex O, CCI shall be equipped with event logging functions relevant to the verification and monitoring of its operating and security status.

This section provides guidance on the storage and transmission of logs by the CCI. In addition, for information purposes, the cybersecurity-relevant events introduced by IEC 62351-14 “Power systems management and associated information exchange - Data and communications security - Part 14: Cybersecurity event logging” are detailed.

T.3.3.4.6.1 Storage and transmission of CCI logs

The storage of events in CCI shall comply with the requirements specified by IEEE 1686 standard. CCI shall record safety events in a sequential circular buffer (first in, first out) in the order in which they occur. This circular buffer cannot be deleted or modified and shall store at least 2048 events (IEEE 1686:2013) before the circular buffer starts to overwrite the oldest event with the most recent event.

For the transmission of log events from the CCI to a remote server (possibly integrated in a system for security collection and monitoring), the use of the Syslog protocol is recommended in accordance with the IETF standards RFC 5424 and RFC 5425, which specify the protocol format and its encryption with TLS profile. For the implementation of the TLS profile, reference shall be made to Section T.3.3.4.1.

In the event that the IETF SNMP (Simple Network Management Protocol) [250], standard protocol is to be used for the transmission of messages in syslog RFC 5424 format, IETF RFC 5676 shall be used for mapping from Syslog to SNMP.

For SNMP communications, it is recommended to use the secure SNMPv3 version with a TSM (Transport Security Model, RFC 5591) profile based on TLS (RFC 6353). Refer to Subclause T.3.3.4.1 for the implementation of the TLS profile.

T.3.3.4.6.2 CCI security log [informative]

Each event is characterised by a mnemonic identifier, a level of severity and a descriptive text. Four distinct categories are used for the severity levels of a log event:

- alarm: unauthorised cybersecurity activity (see IEEE 1686 “IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities”);

- error: error condition;

- notice: authorised cybersecurity activity, which occurs, for example, during the routine use and maintenance of an entity (see IEEE 1686). This type of notification is classified as a cybersecurity event, but not a security breach, or an attack, or a deviation from the normal operating conditions of the CCI;

- warning: an abnormal event, i.e. a deviation from the normal operating conditions of an entity, but not necessarily a cyber attack. For example, if a TLS version vulnerable to cybersecurity problems is used for the TLS handshake, this event is classified as a 'warning'. The use of a weak version of TLS could be imposed by the local security policy of the target environment.

---

249 An architecture consisting of 4 NTP servers protects the NTP client from a single false ticker. Given n the number of false tickers to be tolerated, the architecture must be redundant with a number of servers equal to 2n + 1.

250 In this regard, it is noted that IEC 62351-7 “Power systems management and associated information exchange - Data and communications security - Part 7: Network and System Management (NSM) data object models” specifies a set of objects relevant to device and CCI communications security mapped onto the SNMP protocol.

In the following sections, security events are grouped according to the security functions of CCI described in the previous sections, namely

- events relating to the security of the CCI system

- TLS profile security events;

- events relating to the security of MMS communications;

- events relating to certificate management;

- events relating to role management.

T.3.3.4.6.2.1 System logs

The following are the security-relevant events of the CCI system.

Mnemonic name	Severity	Text
LOGIN_OK	notice	Succesful log-in
LOGIN_OK_PW_EXPIRED	notice	Password expired, successful log-in
LOGIN_FAIL_WRONG_CR	notice	Log-in failed - Wrong credentials
LOGIN_FAIL_PW_EXPIRED	alarm	Log-in failed – Password expired
LOGIN_FAIL_3_TIMES	alarm	Log-in failed 3 times
LOGIN_FAIL_SESSIONS_LIMIT	alarm	Log-in failed due to session limit reached
LOCK_USER_WRONG_CR	alarm	User blocked - wrong credentials
LOGOUT_USER	notice	User log-out
LOGOUT_TIMEOUT	notice	Log-out due to user inactivity (timeout)
VIEW_SEC_EV_LIST_OK	notice	Successful Log display of security events
FILE_HASH_CHECK_FAIL	alarm	File hash check failed
FILE_DS_CHECK_FAIL	alarm	Digital signature check failed
WRITE_CERTS_FAIL	notice	Saving and writing certificates to the component failed
SW_UPDATE_OK	notice	Software successfully updated
SW_UPDATE_FAIL	alarm	Software update failure
VIEW_SEC_EV_LIST_FAIL	notice	Failed displaying the list of security events
PW_RESET_FACTORY_DEF	alarm	Password reset to Default value
USER_ACCNT_CREATE_OK	notice	User account successfully created
USER_ACCNT_ENABLE_OK	notice	User account successfully enabled
USER_ACCNT_DISABLE_OK	notice	User account successfully disabled
USER_ACCNT_DEL_OK	notice	User account successfully deleted
USER_ACCNT_CREATE_FAIL	notice	User account creation failed
USER_ACCNT_ENABLE_FAIL	notice	User account abilitation failed
USER_ACCNT_DISABLE_FAIL	notice	User account disabilitation failed

Nome mnemonico	Severità	Testo
USER_ACCNT_DEL_FAIL	notice	Failed deletion of a user account
USER_NEW_ROLE_OK	notice	New role successfully assigned to the user
USER_PERMISSION_CHANGE_OK	notice	Permissions successfully modified
USER_PERMISSION_ADDED_OK	notice	Permissions successfully added
USER_ROLE_REMOVED_OK	notice	Successful removal of user role assignment
USER_PERMISSION_REMOVED_OK	notice	User permissions successfully removed
NEW_ROLE_CREATE_OK	notice	Successful creation of new role
ROLE_DELETE_OK	notice	Successful deletion of new role
USER_PW_CHANGE_OK	notice	Successful user password change
USER_PW_CHANGE_FAIL	notice	User password change failed
USER_NEW_ROLE_FAIL	notice	Failed assignement of new user role
USER_PERMISSION_CHANGE_FAIL	notice	User permission change failed
USER_PERMISSION_ADDED_FAIL	notice	Added permission failed
USER_PW_CHANGE_FAIL_SHORT	notice	Failed change of the user password – too short
USER_PW_CHANGE_FAIL_POLICY	notice	Failed change of the user password due to policy
USER_SESSION_ROLE_CHANGE_OK	notice	Successful modification of the user session role
USER_SESSION_ROLE_CHANGE_FAIL	notice	Change of the user session role failed
USER_ROLE_REMOVED_FAIL	notice	Removal of user role assignment failed
USER_PERMISSION_REMOVED_FAIL	notice	Failed removal of user permission
NEW_ROLE_CREATE_FAIL	notice	Failed creation of a new role
ROLE_DELETED_FAIL	notice	Failed role deletion
TCP_COMM_LOG_SUBS_FAIL	alarm	TCP communication with security log subscriber failed
LOG_DATA_HASH_FAIL	alarm	Failed log data hash (altered log data)
TCP_COMM_LOG_PUBL_FAIL	alarm	Failed TCP communication with log publisher of security log
TCP_COMM_LOG_SRV_FAIL	alarm	Failed TCP communication with log server (not sent event)
COMM_CS_NEGOTIATION_FAIL	alarm	Failure in the communication – – cipher suite negotiation failed
COMM_KEY_NEGOTIATION_FAIL	alarm	Failure in the communication - key negotiation failed
COMM_PEER_AUTHENTICATION_FAIL	alarm	Failure in the communication - peer authentication failed

Menomonic name	Severity	Text
COMM_PACKET_AUTHENTICATION_FAIL	alarm	Failure in the communication – failed packet authentication
TLS_CONN_OK	notice	Successful TLS Connection
TLS_CERT_ACCEPTED_OK	notice	TLS connection/certification accepted
TLS_CERT_CHECK_DIS_OK	notice	Successfully TLS certificate validation check disabled
TLS_CONN_FAIL_CERT	alarm	Failed TLS connection – validation of the certificate failed
TLS_CONN_FAIL_IKE	alarm	TLS connection failed – IKE failed
TIME_SYNC_SRC_OK	notice	Source for time synchronization OK
TIME_SYNC_SRC_FAIL	notice	Source for time synchronization KO
AV_VIRUS_FOUND	alarm	Identified malicious or corrupt code
NEW_CERT_GEN_OK	notice	New certificate correctly generated
PKI_CSR_OK	alarm	CSR approved and certificate issued correctly
PKI_CSR_FAIL	alarm	Certificate signature request failed
PKI_CERT_EXP_NEAR	alarm	Certificate about to expire
X509_CERT_OK	alarm	Certificate successfully validated
X509_CERT_FAIL	alarm	Certificate validation failed
X509_CERT_EXPIRED	alarm	Certificate validation failed - certificate expired
X509_CERT_REVOKED	alarm	Certificate validation failed - certificate revoked
X509_CERT_UNTRUSTED	alarm	Failed certificate validation - failed certificate signature check
CRL_TRANSFER_OK	notice	Successful CRL transfer into the component
CRL_TRANSFER_FAIL	alarm	Failure to transfer the CRL into the component
CRL_NOT_AVAILABLE	alarm	Certificate revocation status unknown - CRL Not available
CRL_EXPIRED	alarm	CRL expired
OCSP_COMMUNICATION_FAIL	alarm	Failure in OCSP communications
OCSP_UNKNOWN_STATUS	alarm	OCPS: certificate revocation status unknown
TRANSFER_CERTS_OK	notice	Certificate successfully transferred into the component
ADD_ENTITY_CERT_OK	alarm	Successful installation of the certificate in the component
REMOVE_ENTITY_CERT_OK	alarm	Certificate successfully removed from component
ADD_TRUST_ANCHOR_CERT_OK	alarm	Trust anchor certificate successfully installed

Mnemonic name	Severity	Text
REMOVE_TRUST_ANCHOR_CERT_OK	alarm	Trust anchor certificate successfully removed
TRANSFER_CERTS_FAIL	notice	Failure to transfer the certificate to the component
READ_CERTS_FAIL	notice	Certificate reading from component failed
TRANSFER_PW_FILE_OK	notice	Successful transfer and saving of the password file
READ_PW_FILE_OK	notice	Successful reading or export of the password file
TRANSFER_PW_FILE_FAIL	notice	Failure to transfer the password file to the component
READ_PW_FILE_FAIL	notice	Failure to read the password file in the component
UNKNOWN_SYSLOG_EV	notice	Unknown Syslog event

T.3.3.4.6.2.2 TLS Communication Logs

Significant log events relating to TLS profile security are listed below.

Mnemonic name	Severity	Text
TLS_WRONG_VERSION	alarm	Unsecure communication
TLS_WEAK_VERSION	warning	Unsecure TLS version
TLS_VERSION_CHANGE	alarm	TLS version change detected
TLS_NO_RENEG	alarm	Renegotiation period expired
TLS_NO_ROOT_MATCH	alarm	Unable to find the CA certificate
TLS_CERT_SIZE_MISMATCH	alarm	Certificate size not supported
TLS_NO_LOCAL_CERT	alarm	Certificate unavailable
TLS_NO_CA_MATCH	alarm	Certificate validation: CA certificate unavailable
TLS_NO_IND_TRUST_MATCH	alarm	Certificate validation: individual certificate unavailable
TLS_NO_CRL	warning	CRL inaccessible
TLS_NO_OCSP	warning	OCSP responder inaccessible
TLS_CRL_EXP	warning	Warning: CRL expired
TLS_OCSP_RES_EXP	warning	OCSP response expired
TLS_SIG_ALG_MISMATCH	alarm	Certificate Validation: the certificate signature cannot be validated
TLS_CERT_VAL_ERR	alarm	Certificate validation: algorithms not supported
TLS_SHORT_KEY	alarm	Insufficient key length

T.3.3.4.6.2.3 Logs of MMS communications with E2E Security Profile

Significant events relating to the application profile are listed below.

Menmonic name	Severity	Text
SIGNATURE_ALGO_NOT_SUP_ASS_REQ	error	A SecPDU of type HandshakeReq specified digital signature algorithms not supported by the server
SIGNATURE_ALGO_MISMATCH_REQ	alarm	A SecPDU of the HandshakeReq type had an incompatibility in the encryption algorithms whereby the protected algorithm is different from the unprotected one
INV_SIGNATURE_ASS_REQ	alarm	A SecPDU of type HandshakeReq had an invalid digital signature
PROTECTED_PROT_NOT_SUP_REQ	error	A SecPDU of type HandshakeReq specified an invalid protected protocol
PROTOCOL_ERR_ASS_REQ	error	A SecPDU of type HandshakeReq had a protocol error in the E2E security protocol control information
ADDR_MISMATCH_ASS_REQ	alarm	A SecPDU of type HandshakeReq had an address incompatibility
UNEXP_VERSION_ASS_REQ	error	A SecPDU of type HandshakeReq had specified an unexpected version
INV_TIME_ASS_REQ	error	A SecPDU of type HandshakeReq had an invalid time value
REPLAY_DETEC_ASS_REQ	alarm	A SecPDU of type HandshakeReq was a retransmission
UNSUP_DH_GROUP_ASS_REQ	error	A SecPDU of type HandshakeReq specified an unsupported DH group
HMAC_ALGO_NOT_SUP_ASS_REQ	error	A SecPDU of type HandshakeReq specified an unsupported HMAC algorithm
AEAD_NOT_SUP_ASS_REQ	error	A HandshakeReq had specified an authenticate encryption algorithm unsupported by the server.
AEAD_WHEN_NO_ENCR_ASS_REQ	error	A HandshakeReq had selected authenticate encryption when encryption is not required.
AE_ALGO_NOT_SUP_ASS_REQ	error	A HandshakeReq had specified an authenticate encryption algorithm unsupported by the server.
AE_IS_REQUIRED_ASS_REQ	error	A HandshakeReq had not selected authenticate encryption, but this is required by the server.
ENCR_NOT_REQ_ASS_REQ	error	A HandshakeReq had not selected authenticate encryption but did selected encryption, where the server does not want or support encryption.
ENCR_ALGO_NOT_SUP_ASS_REQ	error	A SecPDU of type HandshakeReq specified symmetric key algorithm(s) not supported by the server

Mnemonic name	Severity	Text
ICV_ALGO_NOT_SUP_ASS_REQ	error	A SecPDU of type HandshakeReq specified an ICV algorithm(s) not supported by the server
ENCR_NOT_REQUIRED_REQ	error	A SecPDU of type HandshakeReq with the confidentiality component of type Confidentiality requires encryption when the server does not accept it
ENCR_IS_REQUIRED_REQ	error	A SecPDU of type HandshakeReq with the confidentiality component of type Confidentiality does not propose encryption when the server requests it
PROTOCOL_ERR_ASS_ACC	error	A SecPDU of the HandshakeAcc type produced a protocol error in the E2E security protocol control information
SIGNATURE_ALGO_MISMATCH_ACC	alarm	A SecPDU of the HandshakeAcc type had an incompatibility in the digital signature algorithm where the protected algorithm is different from the unprotected one
SIGNATURE_ALGO_NOT_SUP_ASS_ACC	error	The algorithm(s) in a received HandshakeAcc SecPDU is not supported
INV_SIGNATURE_ASS_ACC	alarm	Invalid digital signature in a received SecPDU HandshakeAcc
ADDR_MISMATCH_ASS_ACC	alarm	A SecPDU of type HandshakeAcc had an address incompatibility
UNEXP_VERSION_ASS_ACC	error	A SecPDU of type HandshakeAcc had an unexpected specified version
INV_TIME_ASS_ACC	error	A SecPDU of type HandshakeAcc had an invalid time value
REPLAY_DETEC_ASS_ACC	alarm	A HandshakeAcc SecPDU was a retransmission
INV_DH_GROUP_ASS_ACC	error	A SecPDU of type HandshakeAcc had an invalid DH group value
INV_AE_ALGO_ASS_ACC	error	A SecPDU of type HandshakeAcc specified authenticated encryption with the specified data algorithm not among those specified in the corresponding SecPDU HandshakeReq
SINGLE_AE_ALGO_REQ_ASS_ACC	error	A SecPDU of type HandshakeAcc has specified multiple authenticated encryption algorithms or has specified none, when only one is required
AEAD_NOT_USED_ASS_ACC	error	A SecPDU of type HandshakeAcc selected the aea alternative of the enc-mode component, while the corresponding HandshakeReq SecPDU selected the non-aea alternative
INV_ENCR_ALGO_ASS_ACC	error	A SecPDU of type HandshakeAcc specified a symmetric key algorithm not listed in the corresponding SecPDU of type HandshakeReq
SINGLE_ENCR_ALGO_ASS_ACC	error	A SecPDU of type HandshakeAcc specified either an empty sequence or multiple symmetric key algorithms
INV_ICV_ALGO_ASS_ACC	error	A SecPDU of type HandshakeAcc specified an ICV algorithm not listed in the corresponding SecPDU of type HandshakeReq

Menmonic name	Severity	Text
SINGLE_AE_ALGO_ASS_ACC	error	A SecPDU of type HandshakeAcc specified either an empty sequence or multiple ICV algorithms
ENCR_NOT_REQUIRED_ACC	error	A SecPDU of type HandshakeAcc with the confidentiality component of type Confidentiality requires encryption when the corresponding SecPDU HandshakeReq does not propose it
ENCR_IS_REQUIRED_ACC	error	A SecPDU of type HandshakeAcc with the confidentiality component of type Confidentiality does not propose encryption when the corresponding SecPDU HandshakeReq requires it
ALARM_SEC_HANDSHAKE_REJECT_RCV	alarm	A HandshakeSecReject SecPDU was received without the diag component, indicating that the server did not accept the HandshakeReq SecPDU and generated an alarm
SIGNATURE_ALGO_NOT_SUP_REQ_REJ	error	A SecPDU of type HandshakeSecReject was received with the diagnostic code invalid-signatureAlgorithm
PROTECTED_PROT_NOT_SUP_REJ	error	A SecPDU of type HandshakeSecReject was received with the diagnostic code protected-protocol-not-supported
PROTOCOL_ERR_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with protocol-error diagnostic code
UNEXP_VERSION_ASS_REQ_REJ	error	A SecPDU of type HandshakeSecReject was received with diagnostic code unexpected-version
INV_TIME_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with diagnostic code invalid-time-value
UNSUP_DH_GROUP_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with diagnostic code dhGroup-not-supported
HMAC_ALGO_NOT_SUP_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with diagnostic code hmac-algorithm-not-supported
AEAD_NOT_SUP_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with diagnostic code encr-mode-aea-not-supported
AEAD_WHEN_NO_ENCR_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with diagnostic code aea-select-but-encrypt-not-supp
AE_ALGO_NOT_SUP_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with diagnostic code aea-algorithms-not-supported
AE_IS_REQUIRED_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with aea-is-required diagnostic code
ENCR_NOT_REQ_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with an encryption-not-required diagnostic code
ENCR_ALGO_NOT_SUP_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with diagnostic code encrypt-algorithms-not-supported.
ICV_ALGO_NOT_SUP_ASS_REJ	error	A SecPDU of type HandshakeSecReject was received with diagnostic code icv-algorithms-not-supported
ENCR_NOT_REQUIRED_REJ	error	A SecPDU of type HandshakeSecReject was received with an encryption-not-required diagnostic code

Mnemonic name	Severity	Text
ENCR_IS_REQUIRED_REJ	error	A SecPDU of type HandshakeSecReject was received with an encryption-is-required diagnostic code
ALARM_HANDSHAKE_SEC_ABORT	alarm	A SecPDU of type HandshakeSecAbort was received without the diag component indicating that the client did not accept the SecPDU HandshakeAcc and issued an alert
SIGNATURE_ALGO_NOT_SUP_ASS_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico invalid-signatureAlgorithm
PROTOCOL_ERR_ASS_REJ	error	A SecPDU of type HandshakeSecAbort was received with protocol-error diagnostic code
UNEXP_VERSION_ASS_ACC_ABT	error	A SecPDU of type HandshakeSecAbort was received with diagnostic code unexpected-version
INV_TIME_ASS_ABT	error	A SecPDU of type HandshakeSecAbort was received with a diagnostic code invalid-time-value
INV_DH_GROUP_ASS_ABT	error	A SecPDU of type HandshakeSecAbort was received with diagnostic code illegal-dhGroup-selected
INV_AE_ALGO_ASS_ABT	error	A SecPDU of type HandshakeSecAbort was received with diagnostic code invalid-ae-algorithm
SINGLE_AE_ALGO_REQ_ASS_ABT	error	A SecPDU of type HandshakeSecAbort was received with single-ae-algorithm-required diagnostic code
AEAD_NOT_USED_ASS_ABT	error	A SecPDU of type HandshakeSecAbort was received with diagnostic code ae-not-used.
INV_ENCR_ALGO_ASS_ABT	error	A SecPDU of type HandshakeSecAbort was received with a diagnostic code invalid-encryption-algorithm.
SINGLE_ENCR_ALGO_ASS_ABT	error	A SecPDU of type HandshakeSecAbort was received with a single-encrypt-algo-required diagnostic code
INV_ICV_ALGO_ASS_ABT	error	A SecPDU of type HandshakeSecAbort was received with diagnostic code invalid-icv-algorithm
SINGLE_AE_ALGO_ASS_ABT	error	A HandshakeSecAbort SecPDU was received with a single-icv-algo-required diagnostic code.
ENCR_NOT_REQUIRED_ABT	error	A SecPDU of type HandshakeSecAbort was received with an encryption-not-required diagnostic code
ENCR_IS_REQUIRED_ABT	error	A SecPDU of type HandshakeSecAbort was received with an encryption-not-required diagnostic code
ALARM_DATATRF_SEC_ABORT	alarm	A SecPDU of type DtSecAbort was received without a diagnostic code
DATA_PROT_ERROR_ABT	error	A SecPDU of type DtSecAbort was received with a protocol-error diagnostic code
ENCR_NOT_SEL_ABT	error	A SecPDU of type DtSecAbort was received with diagnostic code encryption-not-selected
ENCR_WAS_SEL_ABT	error	A SecPDU of type DtSecAbort was received with an encryption-required diagnostic code
DATA_INV_TIME_ABT	error	A SecPDU of type DtSecAbort was received with diagnostic code invalid-time-value

Mnemonic name	Severity	Text
INV_SEQ_NR_ABT	error	A SecPDU of type DtSecAbort was received with diagnostic invalid-sequence-number
UNEXP_RE_KEY_ABT	error	A SecPDU of type DtSecAbort was received with diagnostic code unexpected-rekey-req
UNEXP_CHG_KEYS_ABT	error	A SecPDU of type DtSecAbort was received with diagnostic code unexpected-changedKeys
CLEAR_DATA_PROT_ERROR_TRF	error	A ClearTransfer SecPDU had a protocol error
ENCR_WAS_SEL_TRF	error	A ClearTansfer SecPDU was received when encryption was requested during pairing
CLEAR_INV_ICV_ALG_TRF	alarm	A received ClearTransfer SecPDU used an ICV algorithm that was not agreed upon during the creation of the association
CLEAR_GMAC_NONCE_REQ	Error	A ClearTransfer SecPDU was received without GMAC nonce when nonce is required
CLEAR_BAD_ICV	alarm	A received ClearTransfer SecPDU had an ICV that did not verify
CLEAR_DATA_INV_TIME_TRF	error	A received ClearTransfer SecPDU had an invalid time stamp
CLEAR_DATA_REPLAY_DETECTED	alarm	A received ClearTransfer SecPDU appears to be a retransmission
CLEAR_INV_SEQ_NR_TRF	error	A received ClearTransfer SecPDU had an invalid time stamp
CLEAR_UNEXP_RE_KEY_REQ	error	A ClearTransfer SecPDU received from the server had an unexpected key change request
CLEAR_UNEXP_CHG_KEYS_IND	error	A ClearTransfer SecPDU received by the client had an unexpected key change indicated
ENCR_DATA_PROT_ERROR_TRF	error	A received ClearTransfer SecPDU had a protocol error
ENCR_NOT_SEL_TRF	error	An EncrTansfer SecPDU was received when encryption was not requested at the association stage
ENCR_INV_ICV_ALG_TRF	alarm	An EncrTansfer SecPDU was received with an ICV algorithm that was not agreed upon in the association phase
ENCR_GMAC_NONCE_REQ	Error	An EncrTansfer SecPDU was received without GMAC nonce when nonce is required
ENCR_BAD_ICV	alarm	A received EncrTansfer SecPDU had an ICV that did not verify
ENCR_DATA_INV_TIME_TRF	error	A received EncrTansfer SecPDU had an invalid time stamp
ENCR_DATA_REPLAY_DETECTED	alarm	A received EncrTansfer SecPDU appears to be a retransmission
ENCR_INV_SEQ_NR_TRF	error	A received EncrTansfer SecPDU had an invalid time stamp

Menmonic name	Severity	Text
AES_IV_REQ	error	A received EncrTansfer SecPDU does not include the AES initialisation vector
ENCR_UNEXP_RE_KEY_REQ	error	An EncrTansfer SecPDU received from the server had an unexpected key change indicated
ENCR_UNEXP_CHG_KEYS_IND	error	An EncrTansfer SecPDU received by the client had an indication of an unexpected key change
TRUST_ANCHOR_NOT SUPPORTED	error	An EncrTansfer SecPDU includes a certification path that originates from a trust anchor not recognised by the receiver
BAD_PKC_CHAINING	error	A SecPDU includes an incorrectly chained certification path
INVALID_SIGNATURE_ON_PKC	alarm	An EncrTansfer SecPDU includes a certification path where one or more public keys do not verify
PKC_WITH_NOT_VALID_BEFORE_ERROR	error	An EncrTansfer SecPDU includes a certification path where one or more digital certificates have a notBefore value in the future
EXPIRRED_PKC	error	An EncrTansfer SecPDU includes a certification path where one or more digital certificates has expired
PKC_RPESENT_MORE_THAN_ONCE	error	An EncrTansfer SecPDU includes a certification path where one or more certificates is repeated
OSI_ENV_PROT_ERR	error	OSI Operating Environment Protocol Error
OSI_INV_INDR_REF	error	Invalid indirect reference in the OSI operational environment
OSI_INV_PCI	error	Invalid PCI security

T.3.3.4.6.2.4 Log related certificates

IEC 62351-14 reports the following log events related to certificate management as significant.

Menmonic name	Severity	Text
CERT_PROFILE_MISMATCH	warning	Incompatibility of the certificate profile
CERT_ALG_MISMATCH	alarm	Algorithm incompatibility, result: verification failed
CERT_FORM_MISMATCH	warning	Format incompatibility, result: verification failed
CERT_PKCS12_MISMATCH	warning	Mandatory format incompatibility (PKCS #12)
CERT_PKCS8_MISMATCH	warning	Mandatory format incompatibility (PEM., PKCS#8)
CERT_OID_ERROR_AVL_EXT	warning	OID errors when using Certificate Authorisation List Extensions (avl62351Extention incompatibility)
CERT_OID_ERROR_AVL_ENTRY	warning	OID errors when using Certificate Authorisation List Entry Extensions (avl62351EntryExt incompatibility)

Menmonic name	Severity	Text
CERT_OID_ERROR_AVL_PROTID	warning	OID Errors in the Use of Certificate Authorisation List Protocol Identifiers
CERT_OID_ERROR_AVL_EXT	warning	OID errors when using Certificate Authorisation List Extensions (avl62351Extention incompatibility)
NO_LOCAL_CERT	notice (results in inability to communicate securely)	The communication parties shall have at least one public/private key pair
CERTREG_MISSING_CN	warning	Insufficient registration data. Absence of CN
CERTREG_MISSING_OTP	warning	Insufficient registration data. OTP not available
CERTREG_MISSING_PRE_CERT	warning	Insufficient registration data. Pre-existing credentials unavailable
CERTREG_MISSING_DN	warning	Insufficient registration data. Absence of DN for CSR generation
CERT_MISSING_RCERT	notice	Insufficient data. Absence of acceptable root CA certificates
CERT_NO_CA	warning	Lack of information about the CA's address for enrolment
CERT_NO_REG_INFO	warning	Absence of registration information on the entity to be enrolled
CERT_POP_ERROR	error	Error in proof of possession (Cannot validate CSR)
CERT_POI_ERROR	error	Error in proof of identity (OTP or device manufacturer's certificate error)
CERT_SCEP_PROT_ERROR	error	SCEP-related errors
CERT_EST_PROT_ERROR	error	EST-related errors
CERT_EST_TA-UPDATE_ERROR	error	EST-related errors when updating CA certificates (using the Root CA key update)
CERT_TAMP_ERROR	error	TAMP-related errors
CERT_VAL_EXPIRED	alarm	Certificate expired
CERT_VAL_SIG_ERROR	alarm	Failure in CA signature verification
CERT_VAL_REVOKED	alarm	Certificate revoked
CERT_VAL_NO_AVL_MATCH	warning	Certificate not contained in CertAVL
AVL_VAL_SIG_ERROR	alarm	Error when verifying CertAVL signature
AVL_VAL_COMP_ERROR	warning	Failures in CertAVL components
AVL_VAL_EMPTY_LST	notice	Provided an empty list

T.3.3.4.6.2.5 Role-related logs

The following role management logs are relevant for security aspects.

Menmonic name	Severity	Text
RBAC_USR_AUTH_AUTHZ_SUCCESS	Notice	User authentication and association on the server was successful
RBAC_PERM_ASSIGN_SUCCESS	Notice	The update of the permit assignment was successful
RBAC_NO_REPO_CONN_PKI_REV	warning	The revocation repository is unavailable
RBAC_NO_CRED	warning	RBAC credentials not provided (e.g. missing certificate extension)
RBAC_INVALID_TOKEN	alarm	The authentication of the subject was unsuccessful
RBAC_TOKEN_VALIDITY_ERROR	alarm	The validity of the access token cannot be verified
RBAC_TOKEN_VERIFICATION_FAILED	alarm	Authentication using the access token failed
RBAC_TOKEN_ROLEID_UNKNOWN	alarm	The value of RoleID is unknown
RBAC_TOKEN_ROLEDEF_UNKNOWN	warning	The definition of the role is unknown
RBAC_TOKEN_AOR_UNKNOWN	warning	AoR cannot be solved
RBAC_TOKEN_REV_MISMATCH	warning	Non-compatibility in token revision number
RBAC_TOKEN_ALG_MISMATCH	alarm	Non-compatibility of the cryptographic algorithm
RBAC_TOKEN_NO REVOCATION	warning	Withdrawal information is not available
RBAC_TOKEN_NO REVOCATION_EXP	warning	Expired revocation information
RBAC_ATTRIB_INVALID	alarm	The validity period of the RBAC token is outside the validity period of the credentials
RBAC_ATTRIB_NO_MATCH_BASE_CRED	warning	Missing credential match for RBAC token
RBAC_ATTRIB_NO_REV_INFO	warning	Revocation information is not available

T.3.3.4.7 Asset management and monitoring

As indicated in Subclause O.13.7.2 "Asset Inventory" of Annex O, the CCI shall be setup to interface with an asset inventory infrastructure.

For this purpose, the CCI shall be configured to make available an updated list of fields useful for its unique identification.

According to T.3.3.1.2, the CCI is identified by the LPHD logical node, and in particular by the PhyNam Data Object, which includes information on the manufacturer, software version and connection point identifier (*).

T.3.3.4.8 Secure Boot and Firmware Update

To prevent counterfeiting, ensure the integrity of the device, and minimise the risk of executing unauthorised code at boot time, a trusted secure boot sequence shall be performed, i.e. a phased boot sequence in which the validity of each phase is verified prior to the installation and subsequent initialisation of the firmware, which is generally stored in the reprogrammable flash memory of the CCI. As indicated in Annex O, for security reasons the upgrade of the CCI firmware is under the responsibility of the User owning the device and shall only take place after a procedure that includes:

i. Checking the credentials and authorisations of the User activating the update procedure;

ii. Verifiying the full integrity and authenticity of the new firmware through the digital signature against the public key present on the certificate of the equipment manufacturer;

iii. Deactivation of the functions of the CCI in a controlled manner;

iv. Recording of the firmware update activity in the system data logger. No step of the procedure shall delete the data in the aforementioned data logger.

T.3.3.4.9 Key and certificate management: Public Key Infrastructure (PKI)

The cryptographic functions that secure the operations of the CCI device require at least one pair of related asymmetric keys, known as Private Key and Public Key, stored on an appropriate storage medium (see Annex O.15.3 - Hardware Cybersecurity Testing).

Two scenarios are considered:

- CCI generates its own asymmetric cryptographic key pairs;
- CCI stores asymmetric cryptographic key pairs generated externally from a trusted source, distributed and installed securely in a protected location.

The latter approach shall be used if the device cannot support one of the critical key generation components, namely the random number generator (RNG) (see Annex B - IEC 62351-9).

CCI shall generate or receive new key pairs when one of the following conditions occurs:

- No key pair is present at start-up time;
- Change in controllership of the device (change of ownership, control authority and/or reconfiguration of the device);
- Command from an authorised entity (e.g. certificate renewal request, service certificate request);
- The device's private key has been compromised.

An infrastructure is needed to ensure the proper management of all cryptographic keys and metadata required to:

- identify and authenticate the device;

(*) To equip the asset management infrastructure with monitoring capabilities, the IEC 62351-7 “Power systems management and associated information exchange - Data and communications security - Part 7: Network and System Management (NSM) data object models” provides additional Data Objects on the operating and security status of a device and the mapping of these abstract Data Objects to the MIB structure of the SNMP protocol. The Technical Report IEC 62351-90-3 “Power systems management and associated information exchange - Data and communications security - Part 90-3: Guidelines for network and system management” provides useful information on the use of monitoring Data Objects.

- enable CCI's secure communication profiles (e.g. TLS sessions);
- enable secure device update processes (see T.3.3.4.8).

The infrastructure in charge of managing the life cycle of cryptographic keys and associated digital certificates is a public key infrastructure (PKI). Refer to IEC 62351-9 standard for precise indications regarding the characteristics and components of this infrastructure.

T.3.3.4.9.1 Privilege Management Infrastructure - (PMI)

To supplement the services performed by the PKI and to support profile B (see T.3.3.4.3.2.2), an extension to the public key infrastructure responsible for managing attribute certificates is detailed. This extension is called PMI or Privilege Management Infrastructure. Refer to the IEC 62351-9, IEC 62351-8 and ISO 9594-8/ITU-T Rec. X.509 for details on the characteristics and components of this extension.

Below are specified, in brief, the Attribute Certificate distribution methods that shall be supported by the device and by the privilege management infrastructure to enable correct access to device resources by an authorised user:

- **PUSH model**: attribute Certificates are sent from users to devices as part of the application protocol using attribute certificates for authorisation.
- **PULL model**: users' Attribute Certificates are stored in a repository and retrieved from devices when needed.

In general, the “PUSH” model requires changes in the application protocols, but is more efficient, since no additional request from the device is required to retrieve the attribute certificate from the repository.

To ensure the highest degree of interoperability, support for both authorisation token retrieval modes is required. Furthermore, to avoid potential replay attacks and in accordance with the IEC 62351-9 standard, it is recommended to use short-lived Attribute Certificates (e.g. under 24 hours).

T.3.3.4.9.2 PKI procedures

PKI supports the management of the entire lifecycle of keys, describing the security policies at the various stages: from creation to activation, from storage to transport and, finally, revocation.

The main procedures related to the management of keys and associated certificates are described by the IEC 62351-9 and can be summarised as follows:

- **Device registration**: configuration of identification information and credentials aimed at registering the device to the Registration Authority (RA) of the operational domain.
- **Device Configuration**: configuration of the parameters necessary to allow the device to interface correctly with the PKI of the operational domain.
- **Enrolment of the CCI in the PKI infrastructure**: using the credentials specified at the time of registration, enrolment of CCI to the PKI that issues the certificate enabling the cryptographic functions of the device.
- **Certificate Renewal**: at predetermined time intervals or upon the occurrence of certain conditions (e.g. request by the administrative user) the cryptographic keys are renewed and a new certificate is issued before the expiry of the old certificate. This is essential to ensure the continuity of the functioning of CCI.
- **Certificate revocation**: in the event that the CCI digital identity is deemed to be compromised, the certificate is revoked.
- **Checking the validity status of the certificate**: the devices, at predetermined time intervals, shall check whether the certificates proposed by the other communicating entities are actually valid by implementing these checks through the use of revocation lists (CRL- Certificate Revocation List) or the real-time protocol (OCSP- Online

Certificate Status Protocol). To guarantee the highest degree of interoperability, support of both control modes is required.

Depending on the protocols used, the procedures may include several steps to cryptographically authenticate the identity of the device. These steps differ according to the type of protocol used and are specified by the IEC 62351-9 standard.

T.3.3.4.9.3 Device registration

All devices shall be registered with at least one registration authority (RA), which may be co-located with the organisation's approved certificate authority (CA). This RA shall be able to verify the identity of devices related to a certificate signing request (CSR).

The data required to register the device shall be configured by the manufacturer and shall include a subject, i.e. the set of identification parameters of the certificate (see T.3.4.9), and at least one of the following:

- one-time unique activation code (or OTP), which enables the device to authenticate itself against the RA, e.g., when performing a signature request (CSR).
- public key certificate embedded in the device by the manufacturer signed by the manufacturer's PKI (Manufacturer's Trust Anchor).

The registration data shall be individually installed and configured in the CCI to ensure that the RA can authenticate the device performing a CSR.

The corresponding registration data shall be imported at the RA of the operational domain and shall include the subject identifier and, depending on the enrolment mode envisaged, either the one-time unique activation code (or OTP) configured on the device, or the public key certificate of the PKI issuing the Certificate of Enrolment (Trust Anchor of the Manufacturer).

T.3.3.4.9.4 Device configuration

In addition to the basic certificate parameters defined in ISO/IEC 9594-8: 201x|Rec. ITU-T 1122 X.509, the configuration data of CCI shall include the parameters reported by the following table:

Parameter Name	Description Parameter	Role Enabled to configure/modify the Parameter
Public Key/Certificate issued by the CA of the Administrative Domain	Certificate(s) issued by the CA of the administrative domain that the device attributes to the Owner (or his delegate) designed to allow cryptographic authentication, identification, use of access permissions and roles as described in paragraph T. 3.3.4.4.1 as well as the authentication of the entity (PKI) with which the device will communicate during key management procedures (enrollment, automatic updating of Trust Anchors, checking of validity status, download of revocation lists, etc.)	User profiles with administrative privileges (e.g.: Device owner)
DSO CA Public Key/Certificate	CA certificate that the device attributes exclusively to the DSO capable of allowing cryptographic authentication, identification and use of the dedicated access permissions described in paragraph T.3.3.1.4 and of the dedicated role described in paragraph T.3.3.4.3.1	User Profiles to which administrative and/or operational privileges are recognized (i.e. Device Owner/Authorized Technician)
IP address or a domain name (e.g. IEC 62351. LocalCA)	Address relating to the PKI endpoint of the Administrative Domain	User Profiles to which administrative and/or operational privileges are recognized (i.e. Device Owner/Authorized Technician)

CSR timeout parameters established by the CA	Polling rate, number of attempts, etc.	User Profiles to whom administrative and/or operational privileges are recognized (i.e. Device Owner/Authorized Technician)
Subject of the device certificate	The set of fields that allow the device to be uniquely identified and which will be specified by the CSR (Certificate Signing Request) during enrollment	User Profiles to which administrative and/or operational privileges are recognized (i.e. Device Owner/Authorized Technician)
dnsName	Name of the DNS that the device will refer to. A device can receive more than one DNSName. IP addresses can also be used in environments without DNS services	User Profiles to which administrative and/or operational privileges are recognized (i.e. Device Owner/Authorized Technician)
Device Manufacturer's Public Key/CA Certificate	CA certificate that the device attributes to the entity that will issue the device's firmware updates to allow authentication and integrity verification as described in paragraph T.3.3.4.8.	User Profiles to which administrative and/or operational privileges are recognized (i.e. Device Owner/Authorized Technician) N.B. Although modifiable by the authorized administrative and/or technical user, this parameter shall be pre-configured by the manufacturer of the device.

The CCI guarantees the authenticity and integrity of the configuration data present in the table, by means of dedicated cryptographic techniques.

T.3.3.4.9.5 Enrollment

Once the configuration procedure has been completed, the device shall be able to complete the enrolment procedure by means of the enrolment protocol that will allow a Certificate Signing Request (CSR) to be submitted to the PKI.

Only registered devices shall be enrolled by the RA/CA.

Devices generate the CSR using the PKCS #10 format and send the CSR to the RA specified during configuration. The RA verifies the validity of the request by checking the following:

- proof of possession of the corresponding private key by verifying the CSR signature;
- proof of identity (using the activation code (OTP) or an already available certificate and the corresponding private key together with the registration data on the RA).

If the request is valid, the RA shall send a request to the respective CA. The CA generates a public key certificate and sends it to the RA, which sends it to the requesting entity.

If the request is not valid, the RA will not send any request to the CA.

This procedure is carried out automatically by means of specific protocols that, after verifying the identity of the CCI at the RA, enable the issuance of a CA-validated certificate associated with a client, with its own corresponding identifier and public key.

The IEC 62351-9 specification indicates several protocols that enable the above procedure. Among these, two protocols in particular are indicated for application in the electrical systems domain, namely **SCEP** and **EST**:

- **SCEP (Simple Certificate Enrollment Protocol)**, an enrollment protocol specified by the IETF RFC 8894 that uses Cryptographic Message Syntax (CMS) and PKCS #10 as its message

format, conveyed through an HTTP communication channel. It is recommended not to use versions of SCEP that are considered legacy (pre-2015).

- **EST (Enrollment over Secure Transport)** enrollment protocol specified by the IETF RFC 7030 that uses Cryptographic Message Syntax (CMS) as the message format, conveyed over a secure communication channel (TLS 1.2 or future versions).

In accordance with IEC 62351-9 (Annex A) standard and in order to guarantee the highest degree of interoperability, public key infrastructures are required to support both protocols.

Support of at least one of the indicated enrolment protocols (SCEP or EST) is required for the CCI device.

T.3.3.4.9.6 Certificate renewal

Devices shall generate or request a new key pair and perform a CSR upon the occurrence of one of the following conditions:

- after the expiry dates of their public key certificates reach a certain percentage of the maximum allowed duration, as specified by the organisation's certificate policies;

- direct request by an authorised administrative user.

Devices shall renew their public key certificates before they expire, and shall create a log of certificate renewal actions (such as successful or failed events).

Devices shall allow configuration of the public key certificate renewal policy, e.g:

- Support or not support of automatic renewal through implemented protocols;

- Time period before expiry for certificate renewal.

Particular attention shall be paid to the time alignment between the CCI and the RA as this allows proper synchronisation on certificate expiry using a dedicated protocol (e.g. NTP). Time synchronisation shall be implemented using IETF's NTS (see T.3.3.4.5).

T.3.3.4.9.7 Certificate revocation

In case of suspected compromise of the certificate (e.g. device tampering, theft, etc.) or in case of transfer of ownership or control to another remote management system, CCI's authenticated access to the former infrastructure shall be revoked.

Adequate time synchronisation accuracy between CCI and the system creating and distributing the CRLs shall be ensured so that the time information in the CRLs is accurate and that entities have accurate information on revoked certificates.

Certificates shall be revoked on the following grounds and using the reason codes defined in Section 9.5.3.1 of ISO/IEC 9594-8: 201x | Rec. ITU-T X.509:

- The private key is suspected to be compromised;

- The CA private key associated with the CA certificate is suspected to be compromised;

- The entity's affiliation has changed (assignment, handover to other control, etc);

- The certificate relating to the public key has been replaced;

- CCI ceases to function;

- The privilege relating to the role expressed by the certificate has been withdrawn;

- The Attribute Authority (SME) private key is suspected to be compromised.

T.3.3.4.9.8 Checking the Validity Status of the Certificate

The device shall be configured to support checking the validity status of certificates by means of the following methods

- Certificate Revocation Lists (CRL) request;

- Online Certificate Status Protocol (OCSP).

The OCSP, defined by RFC 6960, is an alternative to retrieving the validity status of certificates via CRLs, which is useful to prevent the phenomenon of "bloating" of CRLs that could cause, over time, the exhaustion of the device's memory resources.

The protocol provides for an OCSP revocation status verification request to be sent to the OCSP server (or CA) responsible for the entity's certificate. This OCSP request contains:

- the protocol version;

- the service request;

- the entity's certificate identifier and extensions.

To avoid replay attacks, a 'nonce' is mandatory to distinguish this status request from any previous status request. The OCSP responder then validates the certificate and returns 'good', 'revoked' or 'unknown', using its own digital signature to authenticate the response.

In general, persistent connectivity between the requesting entity and the responder is required. However, such persistent connectivity may be difficult to adopt for some field configurations. Furthermore, the computational effort to process the OCSP response and the communication delay may not be adequate for some scenarios. Since OCSP servers do not issue spontaneous status updates following certificate revocation events, but control is left to the requesting devices, OCSP responses shall have a short validity time.

Therefore, depending on the system configuration and device capabilities, a hybrid combination of CRL and OCSP may be used where an entity that normally has connectivity acts as a proxy OCSP responder. This proxy entity retrieves a CRL list at a specific time period, e.g. every hour or within 24 hours. The proxy entity (e.g. Station Controller) then serves as an OCSP responder for other entities that do not normally have connections to OCSP. This approach is detailed in the IEC 62351-9 standard to which reference is made for further details.

T.3.3.4.9.9 CCI Public Key Certificates

A public key certificate is a digital document that binds the identity of the entity to a cryptographic key pair (private key/public key). This association is verified by a digital signature of the issuing CA. In addition to the public key and the identity of the certificate owner, public key certificates contain verified information on the validity period and the identity of the issuer.

This document imposes neither a minimum nor a maximum duration of the public key certificate. A certificate expiry date shall be chosen according to the type of certificate and the security policies of the actors involved.

A public key certificate may include extensions that provide additional information. An extension is identified by an object identifier assigned by the organisation defining the extension. A public key certificate may be issued for a CA and is thus called a CA certificate, or for an end entity and is thus called the end entity's public key certificate.

Public key Certificates and Attribute Certificates are defined by a basic set plus extensions to the basic set. The extensions are identified by an international register of object identifiers (OID).

Public key certificates shall include a private key usage extension, which specifies the period during which the corresponding private key may be used by its owner. This period is normally set to be shorter than the validity period of the certificate, ensuring that certificates remain valid

for a minimum period after use by their owner. Details on the use of the private key extension may be found in Subclause 9.2.2.5 of ISO/IEC 9594-8 | Rec. ITU-T X.509.

Following enrolment procedures, CCI device shall possess at least one X.509 certificate identifier having the function of:

- allow authentication by the other entities involved while performing its function;
- guarantee the integrity and authenticity of the device's communications;
- enable the CCI device to request additional Service Certificates from PKI (see T.3.3.4.9.3).

T.3.3.4.9.9.1 Trust Anchor

When a device passes through a supply chain that includes Manufacturer, Buyer, Installer, etc. it is advisable to equip the device with the Trust Anchor certificates of the CAs whose reliability is implicit and shall not be derived from the device through verification of the Chain of Trust

It is considered necessary to equip CCI with at least the following elements:

- Public Key/Certificate of the DSO's CA, which the DSO intends to use as a Trust Anchor;
- Public Key/Certificate of the CA of the Administrative Domain, which the User intends to use as a Trust Anchor;
- Manufacturer CA Public Key/Certificate, which the Manufacturer intends to use as a Trust Anchor.

With the addition of the following optional elements:

- Public Key/Certificate (Trust Anchor) of the CA whose certificates will be used in the process of digitally signing device updates, in the event that the CCI manufacturer is not directly responsible for the updates;
- Public Key/Certificate (Trust Anchor) of the Aggregator's CA, if the Aggregator is present;
- Public Key/Certificate (Trust Anchor) of the CA that issues the certificate used to access PKI services, in the case of using protocols where it is necessary to establish an SSL session (e.g. EST - RFC7030).

Example of Certificate X.509

IEC 62351 Certificate Profiles User Group			Cluster: Name: Typ:	DEFAULT Root/Sub/Leaf	Power System Operator (PSO) PSO Root CA Root	PSO Sub-CA 1 Sub	Entity Cert Leaf
tbsCertificate	Version			2 (X.509v3)	2 (X.509v3)	2 (X.509v3)	2 (X.509v3)
	SerialNumber			Integer	Integer	Integer	Integer
	Signature			rsa-with-SHA256, ecdsa-with-SHA256	rsa-with-SHA256, ecdsa-with-SHA256	rsa-with-SHA256, ecdsa-with-SHA256	rsa-with-SHA256, ecdsa-with-SHA256
Issuer	Country			(x)	(x)	(x)	(x)
	Organization			x	x	x	x
	Organization Unit			(x)	(x)	(x)	(x)
	Common Name			x	x	x	x
	Domain Component			(x)	(x)	(x)	(x)
Validity					[PSO policy]	[PSO policy]	[PSO policy]
Subject	Country			(x)	(x)	(x)	-
	Organization			x	x	x	x
	Organization Unit			(x)	(x)	(x)	(x)
	Common Name			x	x	x	x
	Domain Component			(x)	(x)	(x)	(x)
SubjectPublic KeyInfo	Public Key			x	x	x	x
	Cryptographic Algorithm			id-rsaPublicKey, id-ecPublicKey	id-rsaPublicKey, id-ecPublicKey	id-rsaPublicKey, id-ecPublicKey	id-rsaPublicKey, id-ecPublicKey
	Parameters			ECParameters (namedCurve secp256r1)	ECParameters (namedCurve secp256r1)	ECParameters (namedCurve secp256r1)	ECParameters (namedCurve secp256r1)
Extensions	AuthorityKeyIdentifier			(x) / nc	(x) / nc	(x) / nc	(x) / nc
	SubjectKeyIdentifier			(x) / nc	(x) / nc	(x) / nc	(x) / nc
	KeyUsage			c	c	c	c
		digitalSignature		0/1	0/1	0/1	1
		nonRepudiation (contentCommitment)		0/1	0/1	0/1	1
		keyEncipherment		0/1	0/1	0/1	1
		dataEncipherment		0	0	0	0
		keyAgreement		0/1	0/1	0/1	1
		keyCertSign		1	1	1	0
		cRLSign		1	1	1	0
		encipherOnly		0	0	0	0
		decipherOnly		0	0	0	0
	ExtendedKeyUsage			-	-	-	-
	CertificatePolicies			-	(x) / nc	-	-
	BasicConstraints			c	c	c	c
		CA		TRUE	TRUE	TRUE	FALSE
		PathLength		-	-	1	-
		subjectAltName		(x) / nc	(x) / nc	(x) / nc	(x) / nc
	CRLDistributionPoints			(x) / nc	(x) / nc	(x) / nc	(x) / nc
	Authority Information Access (OCSP)			(x) / nc id-ad-ocsp / location of the OCSP responder	(x) / nc id-ad-ocsp / location of the OCSP responder	(x) / nc id-ad-ocsp / location of the OCSP responder	(x) / nc id-ad-ocsp / location of the OCSP responder
	Custom Extensions						
		RBAC (IEC 6251-8)		-	-	-	1.2.840.10070.8.Profile A/B/C
		CertAVL Distribution Point (IEC 62351-9)		(x)	-	-	(x)
		CertAVL Verification (IEC 62351-9)		c	-	-	(c)
		CertAVL Siging (IEC 62351-9)		0/1	0/1	0/1	-
		CertAVL Siging (IEC 62351-9)		0/1	0/1	0/1	-
Signature Value	Cryptographic Algorithm Signature Value			rsa-with-SHA256, ecdsa-with-SHA256 Octet-String	rsa-with-SHA256, ecdsa-with-SHA256 Octet-String	rsa-with-SHA256, ecdsa-with-SHA256 Octet-String	rsa-with-SHA256, ecdsa-with-SHA256 Octet-String

T.3.3.4.9.9.2 Pre-enrolment Certificate (EST Protocol)

The Pre-Enrolment Certificate is an ITU-T X.509v3 type certificate used to establish a mutually authenticated TLS connection between CCI and PKI to enable the enrolment process via EST protocol. The Manufacturer shall provide the CCI of the Pre-Enrolment Certificate signed by a CA federated by the PKI of the operational domain.

T.3.3.4.9.9.3 Service Certificates

Service Certificates are public-key certificates, distinguished by a dedicated public/private key pair, of type ITU-T X.509v3 or other formats provided by the infrastructure (e.g. OpenSSH) signed by the CA of the operational domain and aimed at:

- enabling authentication of MMS Application Profile communications as described in T.3.3.4.1 and specified by IEC 62351-4 standard;
- enabling authentication of T (Transport Layer Security) profile communications as described in T.3.3.4.1 and specified by IEC 62351-3 standard;
- enabling authentication of HTTPS protocol communications as per RFC 2818 (HTTP Over TLS);
- enabling authentication of SNMPv3 protocol communications TSM profile;
- enabling authentication of NTS protocol communications;
- enabling SSH protocol communications authentication;
- enabling syslog protocol communications over TLS secure transport.

T.3.3.4.10 Segregation of the CCI traffic

The segregation of the remote accesses to CCI, which are used for the plant monitoring, control, protection and operation functions, shall be carried out by router devices capable of separating the plant internal networks from the external networks and of segregating the traffic of the protocols used by the network interfaces. The router device shall be equipped with NAT, VLAN, firewalling and VPN functionality with channel encryption. The possible use of connectivity services on the public network shall provide for the configuration of a secure VPN and exclude the use of the connectivity service for purposes other than those required by the communications for the control and operation of the plant.

T.3.3.4.11 Local Communication Security

All the communications for the commissioning and configuration of the CCI via the local interface shall be protected by a user authentication system subject to specific security policies.

La presente Norma è stata compilata dal **Comitato Elettrotecnico Italiano** e beneficia del riconoscimento di cui alla legge 1° Marzo 1968, n. 186.

Editore CEI, Comitato Elettrotecnico Italiano, Milano

Comitato Tecnico Elaboratore

CT 57 - Scambio informativo associato alla gestione dei sistemi elettrici di potenza
CT 316 - Connessioni alle reti elettriche Alta, Media e Bassa Tensione

Via Saccardo, 9
20134 Milano
Tel. 02.21006.1
www.ceinorme.it
info@ceinorme.it

CEI-Comitato Elettrotecnico Italiano
@CEInorme
CEI-Comitato Elettrotecnico Italiano